ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
«ИНСТИТУТ СОЦИАЛЬНО-ПОЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ
ФЕДЕРАЛЬНОГО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО СОЦИОЛОГИЧЕСКОГО
ЦЕНТРА РОССИЙСКОЙ АКАДЕМИИ НАУК»

На правах рукописи

ВИЛОВАТЫХ Анна Вячеславовна

ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО В ПОЛИТИЧЕСКОМ ПРОЦЕССЕ: ТРЕНДЫ ЦИФРОВОЙ РЕАЛЬНОСТИ

23.00.02 – Политические институты, процессы и технологии

Диссертация
на соискание ученой степени
доктора политических наук

Научный консультант: доктор
экономических наук, профессор
Рогачев Сергей Владимирович

Москва – 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....3
Глава 1. ПОЛИТИЧЕСКАЯ СУЩНОСТЬ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В КОНТЕКСТЕ СИСТЕМНОГО ПОДХОДА.....19
1.1. Теоретико-методологические основы анализа информационного противоборства.....19
1.2. Информационное противоборство в истории политических отношений.....39
1.3. Исследование информационного противоборства с позиций постнеклассической рациональности.....58
Глава 2. ЦИФРОВИЗАЦИЯ КАК ФАКТОР ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА И ЕЕ ВЛИЯНИЕ НА РАЗВИТИЕ ПОЛИТИЧЕСКИХ ПРОЦЕССОВ.....80
2.1. Ориентация ведущих государств мира на лидерство в области цифровых технологий.....80
2.2. Тренды информационного противоборства в свете форсированных процессов цифровизации 109
2.3. Информационное противоборство в цифровой сфере и перспективы трансформации миропорядка.....136
Глава 3. ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В УСЛОВИЯХ СТАНОВЛЕНИЯ ЦИФРОВОЙ РЕАЛЬНОСТИ.....163
3.1. Современные разработки в области манипулирования социальными массами.....163
3.2. Политологический анализ социального поведения в сети Интернет.....182
3.3. Потенциал меметики в информационно-психологическом воздействии на массовое сознание.....199
Глава 4. УПРЕЖДЕНИЕ ПОЛИТИЧЕСКИХ РИСКОВ СОВЕРШЕНСТВОВАНИЯ ПРАКТИК ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В ЦИФРОВУЮ ЭПОХУ.....224
4.1. Вероятностные социально-политические последствия применения цифровых технологий в информационном противоборстве.....224
4.2. Трансформация облика военных конфликтов будущего.....248
4.3. Возможные меры России по купированию вызовов и угроз в области информационной безопасности.....278
ЗАКЛЮЧЕНИЕ.....308
СПИСОК ЛИТЕРАТУРЫ.....318

ВВЕДЕНИЕ

Актуальность диссертационного исследования

Цифровые технологии являются важным фактором развития современных политических процессов. В свете стремительной цифровизации беспрецедентная доступность информации сочетается со столь же беспрецедентным ее переизбытком. Это стимулирует развитие информационно-коммуникационной сферы, инновационные решения которой активно используются политическими акторами для анализа экономической, социальной, политической обстановки в отдельных странах и регионах, а также для подготовки общественного мнения к принятию важных политических решений. В интернете (прежде всего социальных сетях и блогосфере) регулярно апробируются новые, все более совершенные практики информационного воздействия на массовое сознание. Это обусловливает качественно новую декомпозицию отношений между властью и обществом, что существенно повышает уровень социально-политических рисков развития государства, прежде всего в сфере информационной безопасности.

Одновременно происходит более активное, чем в прежние годы включение в процессы информационного противоборства новых, нередко нелегитимных участников политических отношений, список которых постоянно расширяется. Сегодня таковыми являются не только государства, но также «акторы вне суверенитета»: военно-политические блоки, террористические и экстремистские группировки, спонтанно организованные социальные движения, отдельные личности («лидеры мнений», «хакеры», «хактивисты» и пр.). В процессе информационного противоборства они активно пользуются преимуществами утверждающейся цифровой реальности, которая предоставляет большой потенциал воздействия на массовое сознание населения. В данном контексте показательна дестабилизация социально-политической обстановки в регионе Ближнего Востока и Северной Африки и на пространстве Содружества Независимых Государств, которая привела к важным военно-политическим

последствиям и государственным переворотам, окончившихся сменой властных элит.

Целесообразность комплексного исследования научной мысли и политической практики в области информационного противоборства также во многом связана с форсированными процессами трансформации системы международных отношений, когда конкуренция между ослабевающими и возвышающимися центрами силы все более усиливается. Данные явления сопровождаются соперничеством крупных политических акторов за завоевание технологического лидерства, в том числе в деле создания и апробирования на практике инновационных средств и методов информационной борьбы. Недостаточная изученность рассматриваемого феномена в условиях состоявшейся цифровизации социальной и политической жизни, безусловно, может повлечь дополнительные риски развитию нашей страны.

В условиях цифровой революции меняется сущность протекания военно-политических конфликтов. Все больше государств на мировой арене считают одним из действенных способов достижения превосходства над противником «размывание» границ военного конфликта, то есть перевод его в «серую зону». В связи с этим возникает настоятельная необходимость системного исследования указанной среды противостояния, поскольку протекающие в «серой зоне» процессы практически не попадают под нормы и принципы действующего международного права, а новые постулаты в этой сфере вырабатываются с существенным отставанием. К наиболее важным инструментам такого противостояния относится информационное противоборство: информационно-психологическое воздействие на сознание населения и политической элиты противоборствующей стороны, а также информационно-техническое воздействие на кибернетические системы.

В свете указанных тенденций все более рельефно проступает нелинейность развития политических процессов, выражающаяся в их растущей турбулентности и непропорциональности причинно-следственных взаимосвязей. С точки зрения обеспечения безопасности государства основная проблема, порождаемая такой

нелинейностью, состоит в снижении возможностей качественного прогноза событий в области международной политики и, соответственно, эффективности принятия политических решений. Складывающаяся ситуация во многом обусловлена форсированным развитием цифровых технологий, применение которых в практике информационного противоборства вне пространственных и временных границ вносит существенную долю дисбаланса в шаблонные схемы социальной и политической динамики.

В свете цифровизации социальной и политической реальности важным фактором является скорость реагирования на сигналы из глобального информационно-коммуникационного пространства, однако – не в ущерб возможности доходчивого разъяснения официальной позиции страны для ее населения и международной общественности. Такой подход крайне важен в условиях нестабильной политической и социально-экономической обстановки в государстве, поскольку способствует достаточно убедительному опровержению ложных политически мотивированных новостей. При этом превентивное создание информационного фона в виртуальном пространстве, отвечающего национальным интересам страны, может существенно минимизировать негативные последствия деятельности внешних сил, стремящихся обычно использовать все инструменты достижения политических и военных целей, в том числе и преимущества цифровой среды.

Соответственно, явно проступает необходимость выработки проактивной политики в рассматриваемой сфере, призванной упредить вероятные социально-политические риски форсированных процессов цифровизации. Представляется весьма важным политологическое осмысление проблем соответствия проводимой РФ политики по нейтрализации деструктивного информационного воздействия на российское население и формированию негативного по отношению к нашей стране общественного мнения в международном масштабе.

Актуальность анализа процессов информационного противоборства в условиях цифровой среды также определяется относительно невысоким уровнем исследования данной проблемы в современной научной литературе. Многие

политологические аспекты исследования процессов информационного противоборства разработаны отечественной наукой фрагментарно, особенно в свете технологических достижений последнего десятилетия. И это несмотря на то, что потребность в указанных трудах сегодня значительно выросла. В зарубежных источниках процессы информационного противоборства нередко рассматриваются с точки зрения ангажированных политических предпочтений, а потому данный пласт работ лишен научного обоснования.

Анализ степени научной разработанности проблемы свидетельствует, что в отечественной научной мысли довольно качественно проработаны вопросы, связанные с информационным противоборством (информационной войной) в целом. Присутствуют труды, связанные с отдельными аспектами объектно-предметной области диссертационного исследования. В основном они нашли свое отражение в политологической, социологической и психологической отраслях социально-гуманитарного знания. Они исследуются в политологических научных трудах и аналитических разработках западных ученых. Эволюцию работ по рассматриваемой проблематике можно проследить в российских и зарубежных нормативно-правовых актах, а также в законодательной базе военно-политических блоков и региональных организаций, в частности НАТО.

Вместе с тем в политологических исследованиях, посвященных процессам информационного противоборства, практически отсутствует блок, посвященный рассматриваемому феномену с учетом изменений, обусловленных процессами цифровизации. Незначителен объем научных и аналитических материалов зарубежных авторов, где всеобъемлющее исследование данного явления в условиях цифровизации оуществляестя объективно, без политической ангажированности. Серьезно устарел соответствующий понятийно-категориальный аппарат в политологической литературе.

В целом совокупность источников, относящихся к предмету диссертационного исследования, представляется возможным разделить на несколько блоков.

Первая группа – работы, которые выступают общетеоретической базой исследований информационного противоборства. В настоящих трудах освещены вопросы сущности и содержания деятельности по оказанию воздействия на массовое сознание. К этой группе можно отнести работы зарубежных и отечественных классиков – например, Сунь-Цзы, Н. Макиавелли, А.В. Суворова, К. ф. Клаузевица, Г. Лассуэлла, П. Лайнбарджера, Р. Грина, Е.Э. Месснера и других авторов[1].

Вторая группа – исследования современных ученых, раскрывающие сущность и содержание процессов в области информационного противоборства с учетом происходящей технологической революции в контексте различных аспектов социально-гуманитарного знания. К таковым относятся работы Н. И. Турко, И. Н. Панарина, С.А. Модестова, М.А. Кочубей, Г.Ф. Сидненко, А.Г. Караяни, А.В. Брега, А.А. Бартоша, С.В. Рязанцева, А.Д. Шутова и других исследователей[2].

---

[1] См.: *Аристотель.* Этика / Аристотель. М.: Астрель, 2012. 492 с.; *Конрад Н.И.* Сунь-Цзы. Трактат о военном искусстве. М., 1950. 404 с.; *Макиавелли Н.* Государь / Н. Макиавелли; Пер.с итал. К.А.Тананушко. Минск: ООО «Харвест», 2004. 703 с.; *Суворов А.В.* Наука побеждать. М.: Изд. Центр «Анкил-Воин», 1996. С. 13; *Клаузевиц К.* О войне. М.: Эксмо, 2007. 861 с.; *Лассуэлл Г. Д.* Психопатология и политика: Монография. М.: Издательство РАГС, 2005. 352 с.; *Лайнбарджер П.* Психологическая война. Теория и практика обработки массового сознания. М.: Центрполиграф, 2013. 445 с.; *Грин Р.* 48 законов власти и обольщения / Пер. с англ. Е. Я. Мигуновой. М.: РИПОЛ классик, 2005. 736 с.; *Booth K., Wheeler N.* The Security Dilemma: Fear, Cooperation and Trust in World Politics. N.Y.: Palgrave McMillan, 2008. pp. 1–18.

[2] См.: *Модестов С.А.* Формирование геополитического пространства России: теоретические основы и методология исследования: Дисс. докт. ... полит.наук: 22.00.05; 23.00.04. Москва, 1998. 390 с.; *Панарин И.Н.* Информационная война и власть. М.: Мир безопасности, 2001. 223 с.; *Марченков В.И., Цибиков В.А.* О реализации возможностей сети интернет и программных средств в информационно-пропагандистской работе с военнослужащими / В.И. Марченков, В.А. Цибиков // Мир образования — образование в мире. 2015. № 3 (59). С. 197–204.; *Сидненко Г.Ф.* Информационное противодействие терроризму: политологический аспект. М.: Изд-во Триумф, Лучшие книги, 2019. 220 с.; *Караяни А.Г.* Информационно-психологическое противоборство в современной войне: учебное пособие. М.: Военный университет, 1997. 64 с.; *Брега А. В.* Политический риск в обеспечении военной безопасности: теория и основы управления: диссертация ... доктора политических наук: 23.00.02 / Брега Александр Васильевич. Москва, 2007. 337 с.; *Бартош А.А.* Конфликты XXI века. Гибридная война и цветная революция: монография / А. А. Бартош. Москва: Горячая линия-Телеком, 2018. 282 с.; Мегатренды. Основные траектории эволюции мирового порядка в двадцать XXI веке. Учебник / [А.А.Байков и др.]; под. Ред. Т.А. Шаклеиной, А.А. Байкова. М.: Аспект-пресс, 2014. 448 с.; *Шутов А.Д.* Исторические прозрения. М.: ЮНИТИ-ДАНА, 2017. 463 с.

Третья группа – труды исследователей, посвященные становлению новой информационно-коммуникативной среды и возможными социально-политическими последствиями этого процесса. В данном блоке научных публикаций особый интерес представляют работы С.В. Рогачева, Г.В. Осипова, В.К. Левашова, Л.Н.Тимофеевой, О. Ф. Шаброва, Л.Е. Ильичевой, И.Ф.Кефели, А.В. Манойло и других ученых[3].

Четвертая группа работ – это научные исследования, где даны вероятные прогнозы развития мирового политического процесса в контексте усиления фактора невоенного противоборства в развитии военно-политических конфликтов. В данном контексте представляется важным отметить работы Н. Рубини, А-М. Слотер, Г. Киссинджера, Дж. Фридмана, Э. Грема, Дж. Ная, Дж. Миршаймера, А. Ачария и других авторов[4].

---

[3] См.: *Рогачев С.В.* Российская социальная реальность: интересы по критериям риска. Аналитический доклад. М.: ФГБУН ИСПИ РАН, 2017. 104 с.; *Тимофеева Л.Н.* Управление через сотрудничество государства и общества: проблемы обоюдной ответственности / Л.Н. Тимофеева // Государство и граждане в электронной среде. Выпуск 1 (Труды XX Международной объединенной конференции «Интернет и современное общество». СПб: Университет ИТМО.2017. С. 188-203; *Ильичева Л.Е., Кондрашов А.О.* Фейковые новости и информационная война // Государственная служба. 2018. № 6. С. 77–82.; *Хрусталев М.А.* Международные аспекты социально-политической стабильности // Международные процессы. М., 2008. Т.6. №2. С. 48–59; *Николайчук И.А.* Политическая медиаметрия. Зарубежные СМИ и безопасность России: Монография/ И.А. Николайчук; Рос. Ин-т стратег. Исслед. М.: РИСИ, 2015. 230 с.; *Шабров О.Ф.* Глобальные факторы современной политики // Ежегодная Московская Конференция МРП СМП РАПН «Политические тенденции и явления: что определяет политику сегодня?». 2019. 6 апреля. URL: https://istina.msu.ru/conferences/188482207/ (дата обращения: 20.09.2019).

[4] См.: *Roubini Nouriel.* Our G-Zero World // Project Syndicate. 2011. February 11. URL: https://www.project-syndicate.org/commentary/our-g-zero-world?barrier=accesspaylog (дата обращения: 23.09.2019); *Xuetong Yan.* The Age of Uneasy Peace. Chinese Power in a Divided World // Foreign Affairs. 2019. January/February. URL: https://www.foreignaffairs.com/articles/china/2018-12-11/age-uneasy-peace (дата обращения: 01.10.2019); *Allison Graham*. China and Russia: A Strategic Alliance in the Making // The National Interest. 2018. December 14. URL: https://nationalinterest.org/feature/china-and-russia-strategic-alliance-making-38727 (дата обращения: 02.09.2019); *Acharya Amitav.* After Liberal Hegemony: The Advent of a Multiplex World Order // Ethics & International Affairs. https://www.ethicsandinternationalaffairs.org/2017/multiplex-world-order/ (дата обращения: 29.09.2019); *Nye Joseph.* Will the Liberal Order Survive? The History of an Idea//Foreign Affairs. Vol. 96, no.1; *Slaughter Anne-Marie.* The real new world order // Foreign Affairs. 1997. September. URL: http://www.columbia.edu/itc/sipa/S6800/courseworks/real_new_slaughter.pdf (дата обращения: 23.09.2019); *Mearsheimer John J.* Bound to Fail. The Rise and Fall of the Liberal International Order// International Security, Vol. 43, No. 4 (Spring 2019), pp. 7–50.

Анализ научных исследований в области информационного противоборства свидетельствует о том, что в свете стремительной цифровизации социально-политической реальности в политологической литературе указанные вопросы затрагиваются фрагментарно. Эти обстоятельства обусловили выбор данной проблематики в качестве темы диссертационной работы.

Объект исследования – информационное противоборство в политическом процессе.

Предмет исследования – информационное противоборство в политическом процессе в условиях становления цифровой реальности.

Цель диссертационной работы – опираясь на комплексный анализ научных работ и современных политических практик исследовать информационное противоборство в политическом процессе с учетом современных трендов цифровизации и выработать на этой основе рекомендации по упреждению вызовов и угроз безопасности России в информационной сфере.

Для достижения указанной цели в ходе исследования были решены следующие **задачи**:

– проанализирована динамически изменяющаяся политическая сущность и содержание информационного противоборства сквозь призму системного подхода;

– изучен потенциал постнеклассической рациональности к исследованию информационного противоборства в политическом процессе на современном этапе развития;

– описаны теоретические и практические аспекты деятельности в сфере информационного противоборства в истории политических отношений;

– выявлен объектно-субъектный состав процессов информационного противоборства на современном этапе развития;

– раскрыты тренды информационного противоборства в контексте стремительной цифровизации социально-политической реальности;

– исследован фактор информационного противоборства в политическом процессе в свете прорывного развития цифровых технологий;

– обобщены исследования отечественных и зарубежных ученых в области управления социальными массами в цифровую эпоху;

– раскрыты передовые информационно-аналитические разработки в области социального манипулирования в условиях цифровой среды;

– изучен потенциал применения меметических технологий и искусственного интеллекта в информационном противоборстве;

– спрогнозированы вероятностные социально-политические риски применения практик информационного противоборства в контексте современных тенденций цифровизации;

– осуществлен анализ роли информационного противоборства в трансформации облика военных конфликтов и обозначены перспективы их развития сквозь призму цифровой реальности;

– сформулированы и обоснованы текущие и вероятные вызовы и угрозы безопасности России в сфере информационной безопасности и предложен возможный комплекс мер по их купированию.

Научная новизна диссертационного исследования состоит в том, что на основе системного подхода, обобщения опыта зарубежных и отечественных трудов, посвященных информационному противоборству в истории политических отношений и на современном этапе, выявлены и раскрыты современные тренды в рассматриваемой сфере и теретически обоснованы их вероятные политические последствия в контексте динамики социально-политических и военно-политических процессов, а также сформулированы практические рекомендации по совершенствованию национальной системы информационного противоборства в условиях нарастания политических рисков.

Результаты, полученные автором и обладающие научной новизной, содержатся в следующих основных положениях и выводах:

Первое. Исследовано влияние фактора цифровых технологий на трансформацию содержания, динамики и объектно-субъектного состава процессов информационного противоборства, в результате чего теоретически обоснована потребность изучения современных политических процессов сквозь

призму постнеклассической рациональности с раскрытием потенциала цифровых технологий в контексте приращения методологии политологии.

Второе. Комплексно исследован потенциал междисциплинарных концепций, формирующих теоретический базис деятельности в сфере информационного противоборства в условиях цифровой реальности (концепция социальной физики А. Пентланда, теория подталкивания Р. Талера и К. Санстейна, Пятифакторная модель Г. Оллпорта и Р. Кэттела, военно-прикладной потенциал мететики), в результате чего обоснована взаимосвязанная сетка технологий информационного воздействия, используемых на просторах глоабльной сети Интернет.

Третье. Представлены и раскрыты основные факторы, обусловливающие усиление роли информационного противоборства в политическом процессе в условиях цифровой реальности: а) применение в политической практике мимикрирующих информационно-коммуникационных технологий, б) включение в процессы информационного противоборства новых, нередко нелегитимных политических акторов, в) усиление соперничества между ослабевающими и возвышающимися державами, в том числе за создание новых инструментов информационной борьбы.

Четвертое. Выявлены и обоснованы наиболее значимые тренды информационного противоборства в контексте стремительной цифровизации социально-политической реальности: а) повышение роли технологий искусственного интеллекта и машинного обучения, б) усиление соперничества в кибернетическом пространстве, в) расширение применения меметических технологий, г) обострение политической борьбы за контроль социальных сервисов интернета.

Пятое. Сформулированы перспективные направления совершенствования практик информационного противоборства в условиях цифровой реальности на основе комплексного анализа зарубежных исследований и разработок: а) технологии сбора, хранения, обработки и анализа больших объемов данных, б) технологии визуализации данных, в) современные гуманитарные технологии, г)

социокультурная разведка, д) анализ на основе открытых источников, е) работа в социальных сетях, ж) структурированные методы анализа информации.

Шестое. Определены и раскрыты политические риски усиления роли информационного противоборства с учетом форсированной цифровизации: а) возникновение интернет-зависимости у отдельных социально-демографических групп с вероятными социально-экономическими и политическими последствиями такой зависимости, б) усиление в политическом процессе роли протестных социальных движений, самоорганизующихся благодаря цифровым технологиям, в) размывание механизма государственного контроля функционирования средств массовой информации и коммуникации, г) усиление межгосударственной конкуренции за обладание передовыми цифровыми технологиями с последующим возможным подрывом системы стратегической стабильности.

Седьмое. Представлены перспективы развития военных конфликтов в «серой зоне» противостояния на основе проведенного военно-политического анализа процессов трансформации облика этого явления политики в свете современных трендов цифровизации. Выявлен повышенный риск неконтролируемого совершенствования практик информационного противоборства при усилении соперничества между легитимными и нелегитимными политическими акторами в информационной сфере.

Восьмое. Выявлены и обоснованы вероятные вызовы и угрозы безопасности России в области информационной безопасности в свете пониженной прогнозируемости политических процессов и их ускорении под влиянием качественно новых факторов, а также сформулирован комплекс возможных мер по совершенствованию национальной системы информационного противоборства в условиях стремительной цифровизации.

Положения, выносимые на защиту.

1. Политические процессы, развивающиеся в условиях синергетического эффекта взаимодействия устоявшихся и относительно новых факторов информационного противоборства, оказываются в фокусе цифровой революции. Исследование политической сущности информационного противоборства требует

учета пониженной прогнозируемости и нелинейности развития политических процессов, обусловленных мимикрией становления цифровой среды. Все это диктует целесообразность концептуального осмысления применения альтернативных научных подходов к их изучению.

2. На современном этапе развития информационное противоборство интегрирует совокупность информационных операций, реализующихся в двух основных формах: информационно-психологического воздействия на массовое и индивидуальное сознание, а также информационно-технического воздействия, нацеленного на кибернетическую сферу. По канонам политических установок большинства государств в условиях становления цифровой реальности информационное противоборство реализуется в обеих формах и на постоянной основе, как в мирное время, так и в период вооруженного конфликта.

3. Форсированное развитие цифровых технологий, применяемых многочисленными политическими акторами (легитимными и нелегитимными) в целях информационного противоборства, способствует формированию на просторах глоабльной сети Интернет малоконтролируемой государственными структурами трансграничной коммуникативной среды, где ложная информация тесно переплетается с правдивой. В условиях становления такой среды информационное противоборство реализуется с учетом феноменов коммуникации (эффектов «пузыря фильтров», «эхо-камеры», «информационных каскадов» и пр.), присущих социальному взаимодействию в условиях цифровой реальности.

4. В свете приближения перспектив трансформации однополярного мироустройства повышается вероятность интенсификации информационного противоборства между ведущими акторами мировой политики. В силу растущего использования цифровых ресурсов для управления общественным мнением политические процессы, скорее всего, приобретут еще более нелинейный и малопрогнозируемый характер, вплоть до разбалансировки всей системы стратегической стабильности.

5. В условиях набирающей силу цифровой революции возрастают риски гибридизации военных конфликтов. Наиболее эффективно гибридное

противоборство ведется на предвоенной стадии конфликта без задействования инструментов, которые применяются на этапах средней и высокой интенсивности вооруженного противостояния, что призвано заставить противника воздерживаться от эскалации напряженности до уровня, требующего международной реакции. Это свидетельствует о повышенной вероятности усиления фактора информационного противоборства как формы протекания военных конфликтов в будущем.

6. Нарастание рисков использования преимуществ цифровизации многочисленными акторами мировой политики обусловливает целесообразность проведения государственной политики в информационной сфере в дихотомии «риск-возможность»: более активного применения цифровых технологий в информационном обеспечении государственной политики, равно как и упреждения социально-политических и военно-политических рисков, формируемых в результате цифровизации социально-политической деятельности.

7. Масштабирование вызовов и угроз безопасности России в информационной сфере в условиях прорывного развития цифровых технологий свидетельствует о растущей целесообразности выработки на государственном уровне комплексного подхода к проблеме обеспечения информационной безопасности, нацеленного прежде всего на создание условий для развития нашей страны в будущем.

Научная гипотеза. В ходе проведенного исследования подтвердилось, что форсированное развитие практик информационного противоборства в цифровую эпоху, применяющихся легитимными и нелегитимными участниками мировой политки вне пространственных преград, обусловливает повышенную вероятность усиления социально-политических и военно-политических рисков с возможным утверждением «обществ риска». При таком развитии событий процессы трансформации мирового порядка могут приобрести существенно более скоротечный характер вплоть до перетекания в «динамический хаос», несмотря на применение участниками мировой политики преимущественно невоенных методов противоборства.

Теоретическая значимость диссертации. В диссертации представлен развернутый анализ информационного противоборства в политическом процессе в свете современных трендов цифровизации. Приведенные в диссертационном исследовании положения и выводы позволяют ознакомиться с современным научным знанием и обобщениями российских и зарубежных политологов по исследуемой проблеме. Материалы диссертации обогащают понятийно-категориальный аппарат отечественной политологической науки в условиях прорывного развития цифровых технологий, могут служить основой для будущих исследований в области информационного противоборства.

Практическая значимость диссертационной работы. Материал исследования может быть полезен органам государственной власти Российской Федерации и в том числе органам военного управления для углубленного прикладного анализа современных процессов информационного противоборства, развивающихся в условиях жесткого межгосударственного соперничества, а также для выявления перспективных направлений совершенствования технологий информационной борьбы с учетом форсированных процессов цифровизации всех сфер жизнедеятельности государства.

Изложенные в диссертации положения и выводы могут найти применение в образовательном процессе в ходе преподавания курсов политологии, социологии, теории безопасности и специальных дисциплин в высших и высших военных учебных заведениях. Исследование может быть полезно экспертам и ученым, в сферу интересов которых входят вопросы информационного противоборства, при дальнейшей разработке теоретических и практических аспектов обеспечения безопасности государства в условиях цифрового прорыва.

Теоретическая база диссертации представлена идеями и положениями, категориями и законами политологической науки, а также других отраслей социально-гуманитарного знания. Методологической основой исследования явился системный подход, который, ориентируя на комплексный анализ информационного противоборства как феномена науки и современной политической практики, способствовал выявлению причинно-следственных

связей развития данных процесов, определению приоритетных социально-политических и военно-политических рисков, обусловленных деятельностью политических акторов в цифровую эру.

При изучении особенностей информационного противоборства в истории политических отношений автор опирался на исторический метод (гл. 1.2). Исторический метод позволил проанализировать эволюцию совершенствования деятельности зарубежных государств в области информационного противоборства, а также выявить, что в условиях цифровизации все более активную роль в этом процессе начинают играть негосударственные акторы мировой политики.

Для определения приоритетов политики в области информационной безопасности различных политических акторов (НАТО, США, КНР, Евросоюза) в условиях цифровизации проведен контент-анализ документов. В целях формулирования мер по противодействию вызовам и угрозам, связанным с переносом информационного противоборства в нерегулируемую правом плоскость, в исследовании осуществлен сравнительный анализ документов (гл. 2.1 и 2.2).

Исследование социального поведения в условиях становления цифровой реальности обусловило обращение диссертанта к инструментарию экономической науки (теория подталкивания Р. Талера и К. Санстейна) и социальной психологии (Пятифакторная модель Г. Оллпорта и Р. Кэттела), а также концепции социальной физики А. Пентланда (гл. 3.1 и 3.2).

Проблема исследования потребовала и применения военно-политического анализа (гл. 4.2), который позволил спрогнозировать этапы управленческого процесса в области формирования внешнеполитической стратегии зарубежных государств в части, касающейся обеспечения военной безопасности государства, и дать сценарии развития военно-политической обстановки на среднесрочную перспективу.

Изучение формирования антироссийского общественного мнения обусловило обращение к социологическому методу (гл. 4.3).

Кроме того, анализ фактора информационного противоборства в условиях форсированного становления цифровой среды потребовал сбора независимых экспертных оценок (в основном крупных зарубежных политологов, правоведов, военных теоретиков), которые в диссертации обобщены, систематизированы, на основании этого даны сценарии развития политического процесса на краткосрочную перспективу.

В исследовании также широко используются общенаучные методы: анализ, синтез, дедуктивный и индуктивный методы.

Эмпирическую основу исследования составили нормативно-правовые акты в области обеспечения безопасности зарубежных стран. Широко применялись статистические данные профильных государственных структур, а также информационно-аналитические разработки зарубежных экспертных и научных центров, в частности, «Корпорации РЭНД» (*RAND Corporation*), Совета по международным отношениям (*Council on Foreign Relations*), Атлантического совета (*Atlantic Council*) и пр. Полезными явились материалы исследований международных и национальных социологических служб.

Апробация и внедрение основных результатов исследования. Авторские аргументы, полученные в ходе научного поиска, явились предметом исследовательских дискуссий на заседаниях Центра национальной безопасности и упреждения рисков ФГБУН «Институт социально-политических исследований Федерального научно-исследовательского социологического центра Российской академии наук» и на заседаниях Ученого совета учреждения. Диссертация была обсуждена в Центре национальной безопасности и упреждения рисков ФГБУН «Институт социально-политических исследований Федерального научно-исследовательского социологического центра Российской академии наук» и была рекомендована руководством Института к защите.

Изложенные в диссертации положения и выводы были апробированы в ходе выступлений на разнообразных конференциях и круглых столах в период 2011–2020 гг.; нашли отражение в процессе преподавания диссертанта в ФГКВОУ ВПО «Военный университет» в период 2011–2015 гг.; с 2020 г. применяются

профильными подразделениями Антитеррористического центра государств-участников Содружества Независимых Государств и Национального центра управления обороной Российской Федерации.

Научная специальность. Диссертация выполнена в соответствии с паспортом научной специальности ВАК 23.00.02 – Политические институты, процессы и технологии: п. 6. «Особенности и механизмы формирования общественного мнения в политике. Возрастание роли средств массовой информации в условиях утверждения информационного общества. Интернет и политика. СМИ и проблема информационной безопасности. СМИ и проблемы политического манипулирования»; п. 8 «Место политического процесса в системе общественных процессов. Субъекты и объекты политического процесса. Институированные и неинституированные политические процессы. Теневые субъекты в политике»; п. 10 «Основные концепции политических изменений современности. Бихевиористские и когнитивистские подходы к объяснению политического процесса. Концептуальные трактовки мировых политических процессов: современные школы и представления. Геополитические школы и подходы»; п. 11 «Факторы риска. Главные акторы политического управления. Публичная политика. Структура и технология политического управления».

Публикация результатов исследования. В период 2011–2020 гг. по теме диссертации автором были опубликованы более 50 научных работ общим объемом около 30 а.л., в том числе 25 статей в рецензируемых научных журналах объемом 16,7 а.л., две коллективные монографии. Под редакцией автора вышли два сборника материалов научных конференций.

Структура диссертации состоит из введения, четырех глав, двенадцати параграфов, заключения, библиографии. Список литературы содержит 418 источников.

Глава 1. ПОЛИТИЧЕСКАЯ СУЩНОСТЬ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В КОНТЕКСТЕ СИСТЕМНОГО ПОДХОДА

1.1. Теоретико-методологические основы анализа информационного противоборства

Совокупность процессов, происходящих в обществе, можно свести к нескольким десяткам видов социальных процессов. Серия социальных явлений может быть понята как процесс, если она сохраняет идентичность во времени, позволяющую выделить ее из других серий, если предшествующие явления обуславливают следующие за ними явления (хотя бы частично) и вызывают относительную однородность положения вещей.

Среди социальных процессов, складывающихся на основе разнообразных видов человеческой деятельности, политический процесс занимает особое место. С одной стороны, изменения жизнедеятельности отдельных индивидов, социальных групп и слоев, отражающиеся на ходе политической динамики, могут быть вызваны каким-либо политическим событием (или их цепью), запланированным или чрезвычайно произошедшим. Вместе с тем любые локальные изменения порядка жизни людей способны вызвать трансформации политической системы. По своей природе они могут быть обратимыми и необратимыми, направленными и ненаправленными, организованными, самоорганизующимися или спонтанными[5]. Как отметил в этой связи российский политолог А.И. Соловьев, «Политическая система под воздействием качественных изменений в социальной среде постоянно находится в движении и развитии. Фактически не существует двух идентичных друг другу состояний одной и той же политической системы»[6].

Указанная диалектика порождает определенное противоречие в подходах исследователей даже к самому определению политического процесса. Широка трактовка этого явления политики, введенная отечественным ученым

---

[5] См.: Новая философская энциклопедия. Т. 2. С. 87.

[6] *Соловьев А.И.* Политология: Политическая теория, политические технологии. М., 2003. С. 303.

А.Ю. Мельвилем: «Политический процесс – это последовательная и продолжительная по времени смена состояний политической системы и ее подсистем либо изменение в них отдельных элементов, которые совершаются под влиянием внутренних и внешних условий жизни общества. Он характеризуется, как правило, конкретным порядком взаимодействия его компонентов и разными темпами на каждой из своих стадий»[7].

Другие ученые, российские и зарубежные, нередко намеренно сужают сущность политического процесса. Так, политолог Е.Ю. Мелешкина определяет политический процесс как «упорядоченную последовательность единичных действий и взаимодействий политических акторов, как правило, создающих и воссоздающих политические институты»[8].

Подобная многозначность трактовок одного из ведущих терминов политологической науки выглядит симптоматичной, но она опеределяется самой вероятностной сущностью политологии как отрасли социально-гуманитарного знания и, соответственно, характера развертывания политического процесса и его отдельных фрагментов, в частности. Нередко это целый комплекс политических трансформаций, относящихся к функционированию политических институтов, и информация о таких упорядоченных политических изменениях в определенной мере поддается структурированию.

Вместе с тем у ученых налицо отсутствие знаний о детерминировнаности протекания различных политических процессов в каждом конкретном случае. Это обусловлено комплексностью и разноликостью данного феномена социального развития, что порождает ограниченность прогностического потенциала исследователя.

Соответственно, хотя мы и определяем политический процесс как целостное явление, поддающееся научному анализу, следует констатировать, что оно не может быть детализировано в высшей мере лапидарно, а ход развития

---

[7] Политология / А.Ю. Мельвиль и др. М.: МГИМО, 2008. С. 82.

[8] *Мелешкина Е.Ю.* Формирование партийных предпочтений избирателей в посткоммунистических странах Восточной Европы // Выборы в посткоммунистических обществах: Пробл.-тем. сб. / Отв. ред. Е.Ю. Мелешкина. М.: ИНИОН РАН, 2000. С. 51.

политического процесса – абсолютно точно предрешен. Как верно отмечает в этом контексте исследователь-методолог А.И. Ветренко, «в политике пока не обнаружены закономерности, которые действуют так же универсально и неумолимо, как законы физические. Здесь всегда есть выбор». Ученый убежден, что «политология имеет хорошие возможности быть наукой о накопляемом политическом опыте, меньшие – о политике настоящей и ограниченные – о политике будущего» [9].

При анализе сущности полититического процесса следует учитывать и то, что в современном взаимосвязанном и разветвленном мире насчитывается масса типологий политических процессов. Характер таких типологий зависит от того, что берется за основание дробления на группы. Так, политические процессы могут быть базовыми и периферийными, протекать явно или латентно, они могут развертываться на международном (глобальном), региональном, субрегиональном, национально-государственном или региональном внутригосударственном уровне и пр. Поэтому в стремлении дать собственное научное определение такой масштабной категории, как политический процесс, нередко ученые отталкиваются от предмета анализа, ставя во главу угла прежде всего решение собственных исследовательских задач. В связи с этим к настоящему времени в отечественной политологии даны определения политического процесса, где он смешивается с другими видами явлений подчиненного порядка, например, с демократическим процессом или с процессом государственного управления. Как нам представляется, такой подход не способствует выявлению сути и содержания непосредственно политического процесса, вносит определенный дисбаланс в понятийно-категориальный аппарат политологической науки.

Свойства стохастичности, нелинейности, накопления синергетического потенциала политических процессов проявляются особеннно в периоды качественной трансформации общественных отношений, когда решающее

[9] *Ветренко И.А*. Методологические особенности изучения политических процессов // Социум и власть. 2009. С. 45–48.

влияние на развитие политической системы начинают оказывать отдельные экономические, политические, социальные события, кардинально меняющие расстановку и соотношение политических сил. Наиболее ярко данные качества политических процессов проявились в период пандемии коронавируса нового типа (COVID-19), которая в 2020 г. стала испытанием для большинства государств мирового политического сообщества (более подробно этот феномен и его последствия проанализированы в следующих главах исследования). Вместе с тем именно в кризисных обстоятельствах гораздо сильнее, чем в условиях равновесного политического развития, проявляется адаптивный характер политических акторов, формирующих непосредственно институциональный контекст протекания политического процесса, определяющих его упорядоченный и осмысленный характер как целенаправленной политической деятельности.

С учетом изложенного нам представляется справедливым взгляд на проблему определения политического процесса отечественного исследователя А.Ю. Шутова, который выделил своеобразные «проекции» развития данного политического явления. С ученым можно согласиться в том, что «политический процесс способен приобретать различные очертания в зависимости от того, на каком уровне политики он протекает и рассматривается». Как отмечает А.Ю. Шутов: «на микроуровне политический процесс – это непосредственно наблюдаемая деятельность, а иногда даже единичные действия индивидов, тогда как на макроуровне он охватывает функционирование различных общественных институтов»[10].

Таким образом, политический процесс во многом обусловлен конвенциональными и неконвенциональными изменениями самой политической системы. И с этой точки зрения ясно, почему отдельные политические процессы могут совпадать по времени и масштабу со всем политическим пространством, другие – охватывать лишь их часть.

---

[10] *Шутов А.Ю.* Политический процесс. М.: Изд-во Московского университета, 1994. 80 с.

В диссертационном исследовании мы будем опираться на трактовку политического процесса, выработанную крупным российским политологом М.В. Ильиным, который определил политический процесс как «комплекс всех динамических изменений в поведении и отношениях субъектов, в исполнении ими ролей и функционировании институтов или же как совокупную деятельность всех субъектов политических отношений, связанную с формированием, изменением, преобразованием и функционированием политической системы, опосредствующей публичную власть»[11].

Если говорить об анализе содержательной стороны политических процессов, то ситуация выглядит еще сложнее, чем с научной категоризацией данной дефиниции. Эти трудности определяются спецификой политических процессов, нередко имеющих ненормативный и недостаточно структурированный в научном плане характер. Кроме того, как отмечалось выше, в политической реальности отсутствуют строгие закономерности, которые действуют столь же универсально, как физические принципы. Как отмечал западный социолог и политолог К. Поппер, «вообще не может существовать общественная теория, на основании которой можно было бы предвидеть историческое развитие, а значит и политическое»[12].

Таким образом, знание законов общественного развития, в частности политического развития, может быть получено большей частью в виде вероятностных аналитических прогнозов. В этом плане можно согласиться с исследователем И.А. Ветренко, по мнению которого «политология имеет хорошие возможности быть наукой о накопляемом политическом опыте, меньшие – о политике настоящей и ограниченные – о политике будущего»[13].

---

[11] *Ильин М.В.* Ритмы и масштабы перемен: О понятиях «процесс», «изменение» и «развитие» в политологии // Полис, 1993. №2. С. 75–77.

[12] *Поппер К.* Логика научного исследования // Поппер К. Логика и рост научного знания. М., 1983. С. 83.

[13] *Ветренко И.А*. Методологические особенности изучения политических процессов // Социум и власть. 2009. С. 45–48.

В целом в зависимости от предмета исследования в отечественной и зарубежной политологии выделяются следующие основные подходы к анализу политических процессов:

– системный;

– институциональный;

– бихевиористский;

– метод рационального выбора.

Последовательно рассмотрим каждый из обозначенных подходов.

Институциональный подход к исследованию политических процессов является одним из основополагающих методологических подходов в политологической науке. Институциональный подход концентрирует внимание на ведущей силе развития политических процессов – институтах, призванных выполнять общественные потребности, – с одной стороны, регулировать протекание процесса – с другой.

Бихевиористский подход заключается в исследовании поведения акторов политических процессов – отдельных личностей, социальных групп, социальных институтов и пр. Данный подход был разработан американскими социологами Г. Лассуэлом и П. Лазарфельдом. С позиций бихевиористского подхода, изучению собственно политических процессов должен предшествовать анализ установок политических лидеров, их личных качеств, имеющиеся и возможные ресурсы, способность лидеров разрабатывать и реализовать политику с учетом «групп интересов» и «давления», а также запроса общества. Исследователи считали важным выявление закономерностей поведения отдельных политиков (в основном их окружение, конкретные политические действия и публичные высказывания) и связанных с ними переменных. Примечательно, что с позиций бихевиористского подхода политическая деятельность не ограничивается сферой официальной политики, а осуществляется и в неформальной среде.

Важно отметить тот факт, что основоположники бихевиористского подхода рассматривают политический процесс как результирующий вектор поведения участвующих в нем субъектов, а его итог – как доминацию волевых устремлений

наиболее сильных участников процесса. Так, в своих исследованиях ученый Г. Лассуэл обращал особое внимание на аспекты милитаризации общества, на размывание границ между военными и гражданскими институтами власти, что, по их мнению, вызвано совершенствованием сил и средств политической борьбы. Поэтому «специалисты по насилию», располагающие новейшими техническими средствами осуществления политического давления, в том числе освоившие современные средства и приемы социального манипулирования, достаточно часто принимают на себя ведущую роль в политическом процессе и становятся его центром. С позиции бихевиористского подхода сущность политических процессов завлючается в «мобилизации ненависти к противнику, сохранение дружбы союзников, обеспечение сотрудничества нейтральных сил и деморализация конкурентов»[14].

Использование метода рационального выбора к анализу политических процессов предполагает концентрацию внимания исследователя на мотивах и интересах их акторов. Этот метод, предложенный американским экономистом Э. Даунсом, предполагает, что вектор развития политических процессов варьируется в зависимости политической выгоды, пользы, личном благе многочисленных акторов политического процесса. Таким образом, участие индивида или их групп в политике происходит в случае, если возможные доходы от такой деятельности будут превышать издержки («максимизация выгоды»). Основываясь на данном постулате, Э. Даунс выработал формулу рационального политического участия. Но в перспективе исследователи-политологи пришли к выводу, что оценка политического процесса только в контексте прагматичных действий и взаимодействий его участников не учитывает элементы иррациональности и субъективизма политики [15].

Наконец, при анализе политических процессов в политологии широко используется методологическая база общей теории систем, впервые идею о

---

[14] См.: Политическая мысль Новейшего времени. Персоналии, идеи, концепции: Краткий справочник. Чебоксары: ЧКИ РУК, 2010. С. 18.

[15] См.: *Downs A.* An economic theory of democracy. New York: Harper and Row. 1957. 320 p.

которой предложил австрийский биолог Л. Фон Берталанфи в 1937 г. на философском семинаре в Чикагском университете. Как отмечал ученый, отправной точкой системного подхода к изучению любого объекта, который предположительно рассматривается исследователем как система, является признание того факта, что система – это не только совокупность отдельных структурных звеньев, это прежде всего система отношений, взаимосвязей и взаимозависимостей между ними, формирующая в целостном виде систему. Позже отечественные ученые определили систему как «объективное единство элементов, взаимно связанных с помощью определенных связей, представляющее, в свою очередь, элемент системы более высокого порядка, тогда как ее элементы сами являются системами более низкого уровня»[16].

Зародившийся на базе общей теории систем системный подход перенимает методологическую основу теории социального действия, одним из разработчиков которой явился представитель американской социологической теории Т. Парсонс. В дальнейшем английский социолог Э. Гидденс, став основоположником структурно-функционального подхода, сфокусировал внимание на перманентном взаимодействии всех общественных подсистем, включая политическую. В ходе порождаемых в такой среде социальных процессов осуществляется их самоструктурирование посредством взаимодействия идей, ценностей, каналов взаимовлияния, социальных статусов и иерархий[17].

В 1960-х гг. как результат развития общей теории систем и системного подхода выделился системный анализ. Исследователь В.Н. Садовский определяет системный анализ как «совокупность методов и средств, используемых при исследовании и конструировании сложных и сверхсложных объектов, прежде всего методов выработки, принятия, и обоснования решений при проектировании, созданиии и управлении социальными, экономическими, человеко-машинными и

---

[16] *Пирумов В.С., Леин Е.Б., Евтеева Л.В.* Системный подход в современных исследовнаиях. Введение в теорию систем. Л.: Изд-во Военно-морской академии, 1973. С. 14.

[17] См.: Современная социальная теория: Бурдье, Гидденс, Хабермас. Новосибирск: Изд-во Новосиб. ун-та, 1995. С. 40–80.

техническими системами»[18]. Согласно принципам системного анализа, возникающая перед обществом та или иная сложная проблема, должна быть рассмотрена как система взаимодейсвия всех ее элементов, как нечто комплексное в единой целостности. Таким образом, системный анализ главным образом нацелен на решение проблем планирования.

Критики отмечают, что с позиций системного подхода политическая деятельность акторов процесса рассматривается как производная от их функционального статуса, недооценивается иррациональный фактор, а также самостоятельность и активность «внесистемных» (нелегитимных) политических субъектов, а также влияние социальных факторов. Ряд исследователей связывают это именно с тем, что «по своим познавательным установкам системный подход имеет много общего со структурализмом и структурно-функциональным анализом, с которыми его связывает не только оперирование понятиями системы, структуры и функции, но и акцент на изучение разнотипных связей объекта»[19].

Вместе с тем потенциал системного подхода в исследовании политических процессов существенно шире и гибче, чем возможности структурно-функционального анализа, поскольку в ходе своей эфолюции он не подвергся жесткой научной абсолютизации и концептуализации. С одной стороны, это обусловливает определенные трудности применения системного подхода к исследованию комплексных политических процессов, относящихся к сфере национальной безопасности, в том числе процесса информационного противоборства, но одновременно дает исследовательский простор. Как отмечают крупные отечественные методологи, специалисты по данной проблеме Блауберг И.В., Юдин Э.Г., Садовский В.Н. «системный поход не существует в виде строгой теоретической или методологической концепции: он выполняет свои эвристические функции, оставаясь совокупностью познавательных принципов,

---

[18] Цит. по.: *Кокошин А.А.*О системном и ментальном подходах к мирополитическим исследованиям. Краткий очерк. 2-е изд. М.: УРСС, 2008. С.17.

[19] *Блауберг И.В., Юдин Э.Г., Садовский В.Н.* Системный подход // Новая философская энциклопедия: В 4-х т.М.: Мысль, 2001. Т.3. С. 560.

основной смысл который состоит в соответствующей ориентации конкретных исследований»[20].

В целом, с нашей точки зрения, изучение условий функционирования сложной системы с позиции связей ее элементов и отношений между ними, равно как и внесистемных факторов, влияющих на развитие политического процесса, является вневременной и важнейшей задачей политологических исследований. В этом плане представляется возможным согласиться с академиком РАН А.А. Кокошиным, который отмечает, что «эффективное прогнозирование в политической, политико-военной и военно-технической сфере требует нахождения оптимального сочетания между "системным подходом" и частными методами и методиками прогнозирования»[21].

Соответственно, несмотря на определенную долю критики, основным методологическим инструментом исследования политических процессов является системный подход. Он предоставляет возможность проанализировать объект изучения в его единстве и целостности, способствует нахождению корреляций между взаимодействующими в рамках системы элементами, помогая выявить основы такого взаимодействия, с тем чтобы определить закономерности функционирования и причинно-следственные связи развертывания политических процессов.

Одновременно системный подход, изучая в качестве субъектов процесса совокупность многообразных политических акторов, уделяет важное внимание внутренним структурно-функциональным характеристикам среды, где протекает процесс. Это позволяет учитывать наиболее значимые функционально–ролевые структуры и выстраивать соответствующие модели их взаимодействий. В условиях, когда внешние внесистемные факторы чаще всего придают процессу деструктивное начало, приводят политическую систему и ее отдельные элементы в неравновесное состояние, внутренние условия протекания процессов являются

---

[20] *Блауберг И.В., Юдин Э.Г., Садовский В.Н.* Системный подход // Новая философская энциклопедия: В 4-х т.М.: Мысль, 2001. Т.3. С. 560.

[21] *Кокошин А.А.* Методологические проблемы прогнозирования в интересах национальной безопасости России. М.: ИВ РАН, 2014. С.33.

необходимыми компонентами их движения, поэтому столь важны с исследовательской точки зрения.

Наконец, принципиально важным с нашей точки зрения является то, что системный подход предполагает осмысление политического процесса с нейтральной идеологической позиции, что является важной особенностью качественного научного исследования. В этом контексте еще в 1969 г. отечественный ученый-методолог И.Т. Фролов одной из своих работ отметил следующее: «системно-структурный подход вообще не может рассматриваться как некий мировоззренческий и тем более идеологический феномен»[22].

Указанные обстоятельства обусловливают исследование процессов информационного противоборства с позиций методологической базы системного подхода, способствующего всестороннему анализу пространственно-временных изменений в протекании такого комплексного политического процесса, как информационное противоборство, что поспособствует выявлению особенностей взаимодействия его субъектов, роли институциональных и внеинституциональных факторов, причинно-следственных взаимосвязей и пр.

Переходя к анализу политической сущности информационного противоборства первоначально важно заметить, что в отечественной политической науке понятие «информационное противоборство» нередко пеесекается с понятием «информационная война». Это связано с многозначностью оригинального англоязычного термина information warfare, что породило множество разночтений при его переводах на русский язык («информационная война», «информационное противоборство», «информационно-психологическая война» и пр.).

Термин «информационное противоборство» введен в российский политологический дискурс в конце 1990-х гг. отечественным ученым И.Н. Панариным. По его мнению, «информационное противоборство – форма борьбы сторон, заключающуюся в воздействии на информационную среду

[22] *Фролов И.Т.* Системно-структурный метод и диалектика // Вопросы философии. 1969. № 12. С. 153.

противостоящей стороны, и защите собственной от негативных информационных воздействий». Причем, по экспертной оценке И.Н. Панарина, основное различие понятий «информационная война» и «информационное противоборство» состоит лишь в том, что «информационная война производится более активно с использованием диверсионных и террористических методов»[23].

Подобной позиции придерживается российский политолог А.В. Манойло. Ученый указывает, что «информационная война» и «информационное противоборство», по существу, являются смежными понятиями. Специалист также обращает внимание, что категория «информационно-психологическая война» привнесена в отечественную науку из терминологии военных кругов США (information and psychological warfare). Соответственно, она может переводиться как «информационное противоборство» или «информационная психологическая война» в зависимости от контекста[24].

Обоснование ученых И.Н. Панарина и А.В. Манойло применительно к категориям «информационное противоборство» и «информационная война», с нашей точки зрения, выглядит правомерным. В диссертационном исследовании мы будем обращаться к используемому российскими государственными органами термину «информационное противоборство».

Информационное противоборство является предметом исследования разнообразных отраслей социально-гуманитарного знания. Междисциплинарный характер данной научной категории определяется прежде всего тем, что процесс информационнного противоборства даже сквозь призму политологической науки имеет массу сущностей.

Социально-коммуникативный аспект информационнного противоборства подчеркивает украинский политолог Г.Г. Почепцов. С его точки зрения, господствующее влияние в новой интерактивной реальности имеет прежде всего информация, которая и влияет на формирование когнитивных ориентаций

---

[23] *Панарин И. Н.* СМИ, пропаганда и информационные войны // Либрус. URL: http://lib.rus.ec/b/358612/read#t32 (дата обращения: 20.08.2019).

[24] *Манойло А. В*. К вопросу о содержании понятия «Информационная война» // АШПИ. URL: http://ashpi.asu.ru/ic/?p=1552 (дата обращения: 23.08.2019).

личности. Таким образом, информационная война как наиболее динамичная фаза информационного противоборства является, как отмечает Г.Г. Почепцов, прежде всего коммуникативной технологией по воздействию на массовое сознание[25].

В свою очередь, отечественные исследователи Д. А. Волкогонов и Н. И. Живейнов выдвигают на первый план психологический контекст рассматриваемого феномена. Эти ученые оценивают информационное противоборство в качестве «системы подрывных идеологических воздействий империализма, направленных на сознание людей преимущественно через сферу общественной психологии»[26].

Информационное противоборство как инструментарий решения межгосударственных проблем анализируют отечественные политологи А.А. Стрельцов и Г.В. Емельянов. Эти ученые концентрируются на динамике протекания информационного противоборства, указывая на то, что оно является «особым видом отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств»[27].

Подобное определение дефиниции «информационное противоборство» дано в Соглашении между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности, принятом в июне 2009 г. В данном документе информационное противоборство трактуется как «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации

---

[25] *Почепцов Г. Г.* Информационные войны. М.: Рефл–бук, Киев: Ваклер, 2000. 573 с.

[26] *Волкогонов Д. А.* Психологическая война. М., 1986. 86 с.; *Живейнов Н. И.* Операция «PW»: «психологическая война» американских империалистов. М., 1996. 282 с.

[27] *Стрельцов А. А.* Информационная безопасность России. Основные понятия и определения: Учеб. пособие / Под общ. ред. проф. А. Прохожева. М.: РАГС, 1999. Ч. 1. С.34.

общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»[28].

Нам видится важным то обстоятельство, что в приведенных выше трактовках рассматриваемого термина не учитывается включение в информационное противоборство негосударственных акторов мировой политики, в последние десятилетия все чаще влияющих на развитие политических процессов и нередко даже определяющих ход их развития.

Целесообразно обратить внимание и на тот факт, что некоторые политологи рассматривают информационное противоборство исключительно как часть военно-политической деятельности. В частности, представитель отечественной военной науки С.Л. Комов трактует это явление как «комплекс мероприятий информационного обеспечения, информационного противодействия и информационной защиты, проводимых по единому замыслу и плану в целях захвата и удержания информационного превосходства над противником при подготовке и в ходе военных (боевых) действий»[29].

В целом контент-анализ используемых российскими учеными дефиниций понятия «информационное противоборство» свидетельствует о том, что этот феномен можно исследовать в зависимости от контекста, как минимум, в следующих плоскостях:

- как проекцию военного конфликта;
- как коммуникативную технологию;
- как способ психологического воздействия;
- как часть геополитических отношений.

[28] Соглашение между правительствами государств - членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. // Бюллетень международных договоров. 2012. №1. С. 13–21; Конвенция об обеспечении международной информационной безопасности (концепция) // Совет Безопасности РФ. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 14.03.2019).

[29] *Комов С. Л.* Информационная борьба в современной войне: вопросы теории // Военная мысль. 1996. № 3. С.73.

С нашей точки зрения, противоборство в информационной сфере охватывает каждую их указанных выше областей, особенно на современном этапе мирового развития.

В диссертационном исследовании мы сконцентрируемся непосредственно на политической сущности процесса информационного противоборства, раскрывающего политический процесс как результат политических действий конкретных политических акторов, объединенных единой целью; состоящего из цепи событий, характеризующих взаимодействие общественнных сил по поводу значимых для общества вопросов; включающего многообразные способы взаимодействия политических и социальных сил; способного изменять и воспроизводить институциональную матрицу доминирующей и оппонирующей политических систем.

Аналитико-прогностическое исследование информационного противоборства в политическом процессе с позиций системного подхода обусловлено самой сущностью данного процесса ввиду его комплексности и скрытого характера протекания. Суть информационного противоборства состоит в том, что политические акторы стремятся использовать в собственных интересах имеющуюся в их распоряжении информацию с тем, чтобы достичь политических целей.

Исходя из интересов политических акторов, формулируются цели информационного противоборства. Как свидетельствует политический опыт, к ним чаще всего относятся: нарушение устойчивого функционирования господствующей политической системы/системы государственного управления; дестабилизация социальной и/или экономической систем; подрыв системы военного управления.

Феномен информационного противоборства в политическом процессе отличает ряд характеристик:

– информационное противоборство в политическом процессе протекает преимущественно латентно, поскольку представляет собой совокупность относительно самостоятельной скрытной деятельности политических субъектов

(в том числе социальных институтов) с целью подавления воли оппонирующей стороны в собственных интересах, которая в итоге способна вызвать как локальные, так и масштабные трансформации социально-политической системы;

– информационное противоборство как своеобразная форма протекания политических изменений на пересечении самых разнообразных сфер жизни общества (экономической, политической, социальной и духовной) обладает не только собственной ритмикой (повторяемостью), но и достаточно высокой степенью динамизма, отличающей его среди других политических процессов;

– в информационном противоборстве участвует большое количество самых разнообразных политических акторов (причем как легитимных, так и нелегитимных), обладающих собственными ресурсами трансформации политической системы, сочетание которых лишает процесс информационного противоборства строгой устойчивости в отличие от некоторых других политических процессов (например, избирательного процесса);

– процесс информационного противоборства реализуется как результирующая сумма политических воль, но в основном посредством соответствующих нормативно определенных технологий и процедур действий. Развитие процесса информационнного противоборства можно спрогнозировать, но при наличии своевременной и достоверной информации о намерениях и планах участвующих в нем конкретных субъектов, применяющих привычные и чаще всего регламентированные способы и приемы деятельности.

Концептуально данные вопросы рассмотрены в исследовании американского экспертного центра «Корпорация РЭНД» (*RAND Corporation*), более полувека участвующей в информационно-аналитическом обеспечении органов власти США. В научном докладе под названием «Операции против лидеров противника»[30], опубликованном еще в 2001 г., указывается, что успех в области информационного противоборства способен запустить деградацию всей системы стратегического управления государства-противника, а успешно проведенная информационная операция по устранению государственных лидеров

[30] *Hosmer S.* Operations Against Enemy Leaders. Santa Monica: RAND, 2001. P.180.

с политической арены – резко негативно отразиться на морально-психологическом состоянии населения страны-оппонента.

В указанном докладе отмечается, что целями политического руководства при проведении информационных операций могут являться:

– принуждение государства-оппонента к отказу от собственной внешней или военной политики, которая не соотносится с американскими стратегическими установками;

– сдерживание государства-оппонента от возможных действий, противоречащих американским интересам в конкретном регионе мира;

– смещение потенциально враждебных Соединенным Штатам Америки политических режимов;

– лишение государства-оппонента возможности вести полномасштабные боевые действия или организовывать сопротивление[31].

Примечательно, что авторы доклада «Операции против лидеров противника» рассматривают «метод материального поощрения», применяемый политическим и военным руокводством США в отношении политических сил оппонирующей стороны, как намного более выгодный, чем политические, экономические, материально-технические и пр. издержки, обычно сопутствующие проведению полномасштабной военной операции. На этот факт указывают и другие американские специалисты в области информационного противоборства[32].

По основанию объектного поля воздействия и защиты информационное противоборство включает в себя две основные составляющие: информационно-психологическую и информационно-техническую. Информационно-психологическое воздействие интегрирует совокупность информационных операций, связанных с воздействием на психику человека и общественное

---

[31] См. подр.: Информационное оружие супердержавы: кибервойна и «управляемые кризисы» // Центр стратегических оценок и прогнозов. 2012. Май. URL: http://csef.ru/ru/articles/print/3105 (дата обращения: 23.07.2019).

[32] См. напр.: *Rid T., Hecker M.* War 2.0: Irregular Warfare in the Information Age. Westport (Calif.): Praeger, 2007.

сознание. Информационно-техническое воздействие предполагает оказание влияния на разнородные информационно-технические системы: системы передачи данных, системы защиты информации, радиоэлектронную борьбу. По канонам политических установок большинства государств на современном этапе мирового развития информационное противоборство ведется в форме информационно-психологического воздействия в тесном взаимодействии с методами информационно-технического воздействия, особенно в период вооруженного конфликта.

В настоящее время среди разнообразных участников мировой политики деятельность по осуществлению информационных операций в рамках информационного противоборства наиболее полно регламентирована в нормативно-правовых актах Североатлантического альянса, а также в национальном законодательстве входящих в него развитых стран Запада. Современный подход натовских государств к ведению информационного противоборства предполагает осуществление комплекса массированных, объединенных единой целью мер (операций) информационно-психологического и информационно-технического воздействия на систему принятия политических и экономических решений противостоящей стороны; психику ее политической элиты; систему формирования общественного мнения; систему формирования массового сознания в тесном сочетании с информационно-технической составляющей имплементации такой стратегии.

Например, в доктрине психологических операций Североатлантического союза от 2016 г. цели информационно-пропагандистского сопровождения деятельности альянса описываются еще более полно, чем в предшествующих аналогичных документах. Заметное внимание в документах НАТО уделяется и такой части информационного противоборства, как общественная дипломатия. При этом, согласно доктрине, все операции, реализуемые в рамках информационного противоборства, ведутся «в едином информационном пространстве и на общей территории, согласуются по стратегическим целям и решаемым задачам, оперируют однородной информацией, направлены на общие

или взаимосвязанные целевые аудитории, но при этом различаются по частным задачам, привлекаемым силам и средствам, а также по применяемым формам и методам действий»[33].

Как видно, государства трансатлантического сообщества подходят целенаправленно и планомерно к выстраиванию механизма информационного воздействия государственной политики. Каждая конкретная информационная операция определяется исходя из масштаба последствий принятых (или непринятых) под специально организованным воздействием решений, а также степенью влияния этого факта на политическую реальность: деятельность, процессы или даже политическую систему, в соответствующих случаях – на международное сообщество или его часть. Этот успех определяется исходя из учета субъектом информационного воздействия массы политических, социальных, культурных, экономических и пр. особенностей, присущих объекту такого воздействия. Иными словами, в какой мере субъект информационного воздействия способен настроиться и подстроиться под нарратив объекта.

В этом контексте представляется целесообразным обратиться к концепции «политического языка», предложенной автором теории политической пропаганды Г. Лассуэлом[34]. В организации информационного воздействия ученый выделял три уровня «политического языка»: миф, доктрину и формулу. Миф он рассматривал в качестве базисной перспективы рассмотрения политической действительности, с помощью которого устанавливаются рамки допустимого для данного общества политического диалога, в нем содержатся ключевые знаки и символы этого диалога. Благодаря мифу получают обоснование возможные формы информационного воздействия и реализации власти в целом.

На уровне доктрины, отмечал Г. Лассуэлл, формулируются основные ожидания и требования общества, которые не может не учитывать субъект информационного воздействия. К функциям доктрины относится удержание

---

[33] *Олевский В.* Доктрина психологических операций НАТО // Зарубежное военное обозрение. 2016. №5. С. 12–20.

[34] *Лассуэлл Г. Д.* Язык власти // Политическая лингвистика. Екатеринбург, 2006. С. 264–279.

некоторой области политической жизни в подчинении определенной группы должностных лиц и в обосновании действий этой группы.

Формула как язык политики выполняет дескриптивную и предписывающую функции в отношении деталей социальной структуры. Политическая формула представляет собой специфическое воплощение политической доктрины. Каждый из данных «языков политики» – миф, доктрина и формула – используется субъектом информационного воздействия на соответствующем уровне для достижения различных политических целей и обоснования перед населением или политическим сообществом определенных действий. Соперничающие политические мифы, доктрины и формулы могут стать конкурирующими точами зрения на господствующую политическую реальность.

Цели информационного противоборства определяют его содержание. В наиболее общем смысле оно заключается в установлении господства над информационным пространством (или его астью) конкретной страны (региона) для обеспечения необходимого уровня собственной безопасности. Вместе с тем содержание информационного противоборства подвержено влиянию ряда относительно постоянных факторов экономического, политического, социального порядка.

В данной связи следует отметить, что в последние десятилетия в мировой политике появились относительно новые факторы, которые вносят дисбаланс в развитие политических процессов, в том числе процессов информационного противоборства, и все еще недостаточно учтены отечественной политологической наукой.

Тренды технологического развития современных развитых государств и динамика самой системы мировой политики, набравшая обороты в последние годы, свидетельствует, что к таким факторам, как минимум, относятся:

– появление новых, более совершенных систем вооружений, с одной стороны, усиливающих конкуренцию по достижению более выгодных позиций государств в системе мировой политики, но одновременно форсирующих разработки в сфере информационного противоборства, что обусловлено

отсутствием непосредственно военного столкновения противоборствующих субъектов и нелетальным характером поражения, присущих информационному оружию;

– включение в состав информационного противоборства большего числа политических акторов, как легитимных, так и нелегитимных, причем композиция их участия в таком противоборстве постоянно меняется;

– наращивание геополитической конкуренции между крупными государствами, динамика ослабления и, напротив, усиления которых в системе мировой политики в последние годы имеет форсированные темпы;

– создание и внедрение в политическую практику цифровых достижений технологической революции, формирующих принципиально новую социальную, экономическую и политическую реальность.

В последние десятилетия информационное противоборство выделилось в самостоятельный и принципиально новый вид межгосударственного соперничества, призванный решать задачи в разнообразных сферах социальной жизнедеятельности непорседственно без применения вооруженной силы. Все чаще особую роль невоенных методов невоенного противоборства в достижении военных и политических целей на мировой арене отмечают представители глобального игрока соверменной мировой политики – Соединенных Штатов Америки. Однако выработке данного подхода к ведению информационного противоборства такого мощного центра политической силы, как США, предшествовал колоссальный политический опыт, накопленный за много веков до появления многих современных государств.

1.2. Информационное противоборство в истории политических отношений

Исторически причиной выделения информационного противоборства в самостоятельный политический процесс явилось перманентное стремление людей снизить собственные потери в конфликтах, сократить время на ослабление возможностей и воли соперника. Как указывает политолог И.Н. Панарин, «самая

ранняя из известных форм воздействия на противника не боевыми средствами – устрашение его своей (иногда мнимой) боевой мощью, – возникла очень рано. Ее следы мы видим в вооруженных столкновениях племен в эпоху разложения первобытно-общинного строя...»[35].

С появлением государства как субъекта организации социально-политической и хозяйственной деятельности человека информационное противоборство постепенно утверждалось в качестве самостоятельной и неотъемлемой части межгосударственных отношений, причем не только в военное, но и в мирное время. Оно являлось особым аспектом взаимодействия государственной власти с врагом и внутренними общественными силами, оппонирущими властным элитам[36].

По мере накопления опыта в области невоенного подавления соперника возникла потребность в его теоретическом осмыслении. Из документально зафиксированных источников первыми считаются труды исследователей, изданные в Китае. В этой стране научные обоснования важности невоенных форм воздействия на противника связываются с именами Конфуция и Сунь-Цзы.

Так, в произведении «Трактат о военном искусстве» китайский мыслитель Сунь-Цзы ставил несиловые меры подавления противника выше силовых: «Во всякой войне, как правило, наилучшая политика сводится к захвату государства целостным; разрушить его значительно легче. Взять в плен армию противника лучше, чем ее уничтожить... Одержать сотню побед в сражениях – это не предел искусства. Покорить противника без сражения – вот венец искусства»[37].

Большое значение идеологической подготовке общества в целях сохранения его устойчивости придавал древнегреческий философ, ученик Платона Аристотель. По его мнению, «комплекс философско-мифологических воззрений, который должен быть внушен населению, является по существу

---

[35] *Панарин И.Н.* Информационная война и Россия. М.: Мир безопасности, 2000. 159 с.

[36] См. подр.: *Виловатых А.В.* Информационная война: история и современность // Наука. Культура Общество. 2011. № 4. С. 73–83.

[37] Цит. по: *Головин Н..И.* Информационная война. М.: Мир безопасности. 1998. № 8–9 (60). С. 79.

общеобязательной государственной религией, нацеленной на достижение единомыслия граждан и упрочение социально-политического строя и законопорядка в обществе»[38].

Формированию концепции достижения превосходства в политической борьбе невоенными методами была подчинена деятельность крупного итальянского мыслителя эпохи Возрождения Н. Макиавелли. В своих военно-теоретических трудах «Государь» и «Рассуждения» он не претендовал на авторство системной теории информационного противоборства. Однако на основе исторических исследований и практических наблюдений Н. Макиавелли описал вневременные истины общественного и политического поведения политического деятеля, трансформировав их в набор афоризмов и предписаний, способных помочь государю обеспечить достижение превосходства невоенными методами в «предательском и ненадежном мире». По его словам, «расстояние между тем, как люди живут и как должны бы жить, столь велико, что тот, кто отвергает действительное ради должного, действует скорее во вред себе, нежели на благо...»[39]. В этом контексте представляется возможным согласиться с американским политологом, представителем теории неореализма К. Уолтцем, который отмечал, что применение любых средств достижения превосходства в политической борьбе допустимо при наличии главной цели – умения отступать от добра и пользоваться этим умением «смотря по надобности»[40].

Важный вклад в развитие теории и практики информационного противоборства внесли великие российские полководцы. Так, основоположник русской военной теории А.В. Суворов в своем труде «Наука побеждать» писал: «Развитие духа – первая необходимость для войска: кому не известно, что при робости духа парализуется ум и слабеет тело, и наоборот»[41].

---

[38] *Аристотель.* Соч.: В 4 т./ Пер. С древнегреч. М.: Мысль, 1983. Т. 4. 830 с.

[39] Machiavelli: Still Shocking after Five Centuries // National Interest. 2014. November. URL: https://nationalinterest.org/commentary/machiavelli-still-shocking-after-five-centuries-9126 (дата обращения: 12.09.2017).

[40] *Тененбаум Б.* Великий Макиавелли: Тёмный гений власти: «Цель оправдывает средства?». М.: Яуза, Эксмо, 2012. 480 с.

[41] *Суворов А.В.* Наука побеждать. М.: Изд. Центр «Анкил-Воин», 1996. С. 13.

Большое внимание вопросам информационного противоборства уделял выдающийся прусский военачальник и военный теоретик К. ф. Клаузевиц. В своем трактате «О войне» он писал: «Мы наталкиваемся еще на одно своеобразное средство: воздействие на вероятность успеха, не сокрушая вооруженных сил противника. Это – предприятия, непосредственно предназначенные для оказания давления на политические отношения...»[42].

Следует отметить, что описанные К.ф. Клаузевицем в трактате «О войне» методы информационного противоборства взяли за основу современные американские экономисты Э. Райс и Дж. Траут, положившие начало маркетинговым концепциям «позиционирования» и «маркетинговой войны». В своей книге «Маркетинговые войны» они проводят аналогию между борьбой корпораций за лидерство и военными действиями, где ослабление воли конкурента к сопротивлению обеспечивается за счет внезапности действий[43].

На рубеже XIX – XX веков деятельность военно-политического руководства многих стран по информационному воздействию на население и властные элиты оппонирующих государств приобрела принципиально новый размах и организационное оформление. Это было обусловлено не только накопленным теоретическим потенциалом в области информационного противоборства, но и постепенным приближением международного политического сообщества к Первой мировой войне.

К знаковым теоретическим трудам указанного периода относится, в частности, исследование упомянутого нами выше известного теоретика информационных войн американца Г. Лассуэла под названием «Техника пропаганды в мировой войне», которая была опубликована в 1927 г. Данная работа является одной из первых завершенных научных теорий в западной политической науке в сфере информационного противоборства. В ее основе лежат исследования в области психологии и контент-анализ официальных документов. Ученый, объединив черты бихевиоризма и фрейдизма, выделил информационно-

[42] *Клаузевиц К.* О войне. М.: Эксмо, 2007. 861 с.
[43] *Траут Дж., Райс Э.* Маркетинговые войны. М.: Питер, 2018. 288 с.

психологическую сферу противоборства в самостоятельную и рассмотрел пропаганду («менеджмент коллективных мнений с помощью манипуляций значимыми символами»[44]) как особый вид оружия, воздействующий на когнитивное состояние неприятеля.

В своем исследовании в качестве основных стратегических целей информационно-психологического воздействия Г. Лассуэл назвал: «возбуждение в собственном населении, а также в населении стран-союзников и нейтральных стран ненависти к неприятелю; поддержание дружественных отношений с союзниками; сохранение добрых отношений с нейтральными странами и получение их поддержки; деморализация противника»[45]. Ученый пришел к выводу, что управление пропагандой должна взять на себя так называемая научная технократия, которая будет осуществлять отбор информации и тем самым противостоять опасностям, угрожающим политической системе.

Несмотря на значительные достижения в накоплении теоретического материала и практики ведения информационного противоборства в годы Первой мировой войны, о прорыве в данной области политологической науки и военно-политической реальности можно говорить с наступлением периода Второй мировой войны. Эффективность совершенствования технологий информационного противоборства в политическом процессе на данном этапе мирового развиития во многом связывается с деятельностью германского руководства. Как известно, в тот исторический период гитлеровской Германии, по существу, удалось без единого выстрела захватить Австрию, Чехословакию, Норвегию, Данию, а также длительное время манипулировать общественным мнением в государствах-противниках.

Следует отметить и то, что во время Второй мировой войны высокая эффективность ведения информационного противоборства приписывается и странам англосферы, прежде всего Великобритании и США. В указанных государствах была налажена соответсвующая организационная система, а также

---

[44] *Лассуэл Г.* Техника пропаганды в мировой войне. М., 1929. С. 139–181.
[45] Там же.

осуществлялась тесная координация в военной сфере и между представителями специальных служб.

В качестве успешного примера функционирования созданных в странах англосферы подразделений в сфере информационного противоборства следует назвать то, что в 1942 г. перед сотрудниками исследовательского отдела Управления стратегических служб США была поставлена задача по изучению истории, культуры, языка населения стран – противников США во Второй мировой войне. Тогда социокультурному анализу была подвергнута японская культура – Токио был для Вашингтона самым трудным для понимания соперником из числа тех, с кем США приходилось когда-либо вести войну. Так, в 40-гг. прошлого века американский антрополог Р. Бенедикт писала: «Ни в какой другой войне с крупным противником мы не оказывались перед необходимостью принимать в расчет совершенно отличные от наших обыкновения в мышлении и поведении. Принятые западными народами как факты человеческой природы условные правила ведения войны не признавались японцами. Главной проблемой стала природа врага. Чтобы справиться с ними, нужно было понять поведение японцев»[46].

Соответственно, в то время одной из ведущих задач для американских специалистов стало выяснение реакций отдельных социальных групп на различные социально-экономические стимулы (в частности, долгосрочные). В результате проведенных экспериментов ученые из США пришли к выводу, что большинство людей не способны осознавать информационные и психоэмоциональные воздействия, даже если им об этом сообщают прямо. Именно в тот период истории эксперты, специализирующиеся на социологических, психологических, исторических знаниях, сформулировали

[46] *Benedict R.* The Chrysanthemum and the Sword. Patterns of Japanese Culture. Boston, 1946. p. 324.

прикладную междисциплинарную концепцию «психоистории» – обобщенной технологии управления историческим развитием больших социальных групп[47].

В целом, как нам представляется, комплексно деятельность англосаксонских стран в области информационного противоборства рассмотрена в научном труде под названием «Психологическая война» американского исследователя П. Лайнбарджера. В указанном исследовании особенно привлекает внимание разработанная П. Лайнберджером система знаний, необходимых специалистам в сфере информационного противоборства. К таковым ученый причислил: «знание современной политики и военного искусства; знание обычаев, языка, традиций населения региона страны психологического воздействия; профессиональное знание СМИ; понимание психологии, социологии, антропологии, истории»[48].

Активная деятельность созданных в период Второй мировой войны подразделений в Соединенных Штатах Америки привела к тому, что научные и аналитические исследования в области информационного противоборства стали развиваться в этой стране форсированными темпами. Но прежде всего этому способствовало появление у США стратегического противника – СССР. С началом холодной войны между этими двумя державами, ознаменованной разработкой оружия массового уничтожения (ОМУ), наметилась смена парадигмы достижения превосходства в военных конфликтах. Для удержания завоеванной позиции глобального гегемона американцы взяли курс на разработку различного рода невоенных концепций ведения боевых действий, с тем тобы, по Сунь-Цзы, «достигать превосходства в войне без непосредственного сражения с противником».

Соответственно, после Второй мировой войны расширилась проблематика исследований в области информационного противоборства, инструментами для которого теперь стали выступать и новые отрасли знания. Так, в целях решения определенных задач, расширяющих теоретический потенциал в сфере

---

[47] См. подр.: *Виловатых А.В.* Использование информационно-коммуникационных технологий в военно-политических целях: социально-психологический аспект // Проблемы национальной стратегии. 2018. № 2 (47). С.197–211.

[48] *Лайнбарджер П.* Психологическая война. М.: Воениздат, 1962. С. 122–132.

информационного противоборства, западные государственные деятели активно задействовали потенциал «буржуазных наук», в том числе прикладной социологии. Именно во второй половине прошлого века Соединенные Штаты создали национальную систему социологического мониторинга оперативной и стратегической информации, получаемой с помощью проведения соответствующих исследований. Основы этого заложил американский ученый, автор оригинальной концепции общественного мнения У. Липпман[49].

У.Липпман обосновал, что аккумулированные за многие годы результаты социологических исследований могут дать обширный эмпирический материал, значимый с точки зрения выстраивания государственной политики, причем как на внутриполитическом, так и на внешнеполитическом направлениях. Социологические опросы, утверждал ученый, являются важным источником для изучения долговременных и краткосрочных тенденций в национальном и мировом общественном мнении. Кроме того, отмечал У. Липпман, тщательное изучение общественного мнения имеет неоценимую важность в случаях выстраивания политики целенаправленного информационно-психологического воздействия на умонастроение людей.

В 1950-х гг. в Соединённых Штатах Америки был создан Центр русских исследований Гарвардского университета (в настоящее время – Центр российских и евразийских исследований им. Дэвиса), специалистами которого было инициировано интервьюирование советских граждан в целях получения дополнительной социально-политической информации о Советском Союзе. Исследование получило название «Гарвардский проект». Работа проводилась под эгидой группы политического планирования Государственного департамента США во главе с известным экономистом Дж. Кеннаном. В опросах приняли участие более двух тысяч респондентов (граждане Советского Союза, которые к окончанию Второй мировой войны находились в американской зоне оккупации). В результате были собраны сведения по основным социальным проблемам в

[49] *Липпман У.* Общественное мнение / Пер. с англ. Т. В. Барчунова, под ред. К. А. Левинсон, К. В. Петренко. М.: Институт Фонда «Общественное мнение», 2004. 384 с.

СССР и дополнительный материал, касающийся семейных, экономических, властных отношений в стране[50].

Данный проект поспособствовал не только описанию социокультурного базиса конкретного государства, но и эмпирически изучению качественных установок различных социальных групп. При этом выявление основных «болевых точкек» советского общества имело под собой вполне конкретное обоснование. Как отмечалось в официальном описании исследования, задачей Военно-воздушных сил США, финансировавших проект, была оценка:

а) психологической уязвимости гражданского населения при массированных бомбардировках;

б) непрямого эффекта таких действий.

Вместе с тем инициатор Гарвардского проекта Дж. П. Дэвис прямо указывал, что полученный материал необходим для планирования политики США по отношению к СССР в условиях начинавшейся тогда холодной войны. В целом сказанное свидетельствует о стремлении США разрушить идейный «стержень», длительное определявший внутреннюю и внешнюю политику СССР, а также увеличить социальный разрыв между советским народом и руководством страны.

Со второй половины XX в. наметился тренд на расширение количества участников информационного противоборства. Одним из первых ученых, комплексно проанализировавших данную проблему стал выдающийся отечественный социолог и военный теоретик Е.Э. Месснер. В 1960 г. он опубликовал книгу «Мятеж — имя третьей всемирной», став автором концепции о мятежевойне как новой форме протекания военного конфликта в условиях интеграции информационного противоборства в мировой политический процесс в принципе. С точки зрения ученого, суть войн будущего определит именно невоенный компонент противоборства[51].

---

[50] The Harvard Project on the Soviet Social System Online // Harvard Library. 2018. June 14. URL: https://library.harvard.edu/collections/hpsss/index.html (дата обращения: 03.04.2020).

[51] Мысли Е. Месснера о сути современной мятежевойны // Milresource. 2006. URL: http://www.milresource.ru/Quotations-Messner.html (дата обращения: 19.09.2019).

Е.М. Месснер уделял большое внимание анализу процесса организации стихийных социальных движений. Ученый придерживался позиции, что к началу XX в. военачальникам придется отказаться от установившихся понятий о войне, и в этом контексте он рекомендовал избегать разделения времени на «мирное» и «военное». В своих исследованиях ученый пришел к выводу, что в будущем внесистемному противнику станет «легче разложить государство, чем его покорить оружием»[52].

Примечательно, что именно в этот период, придавший мировой политике существенную долю турбулентности, Соединенные Штаты Америки включились в информационное противоборство глобального масштаба с целью доведения до мировой общественности сущности и содержания привлекательного во всех отношениях американского образа жизни. Видимо, конечная цель такой стандартизации заключалась в трансформации «культурных ядер» суверенных государств для формирования у людей восприятия себя «гражданами мира». Созданные специалистами из США идеи, образцы, социальные стереотипы в большинстве своем были направлены на ослабление культурно-исторических опор других стран, часто имеющих богатое культурное наследие. Данной цели и сегодня подчинены массовая популярная культура США, транслируемые Вашингтоном за рубеж американский кинематограф, искусство, литература и пр. При этом основной упор сделан на продвижении привлекательных американских ценностей и деформированных представлений о мироустройстве (так называемые индивидуальная свобода, права человека, демократические механизмы, рыночная экономика, правовое государство и пр.).

Во второй половине XX в. в американском политическом истеблишменте было принято решение создать многочисленные точечно ориентируемые структуры, которые занимались бы конкретными аспектами ведения информационного противоборства, причем преимущественно в мирное время. В этом контексте наиболее эффективно функционировало Информационное

[52] Мысли Е. Месснера о сути современной мятежевойны // Milresource. 2006. URL: http://www.milresource.ru/Quotations-Messner.html (дата обращения: 19.09.2019).

агентство США, учрежденное в 1953 г. при Государственном департаменте. Оно было вовлечено в пропагандистскую деятельность за рубежом до 1999 г., когда было интегрировано в систему указанного ведомства. Широко использовался и потенциал различных неправительственных организаций, культурных и гуманитарных миссий. Тогда были созданы первые экспертно-аналитические организации, ведущие исследовательскую и консультационную деятельность по государственным и корпоративным контрактам, в области политики, экономики, обороны и оценки возможных последствий политических решений для национальной безопасности. Со временем, помимо собственно профильных функций, они стали мощным рупором американской пропаганды.

Инструментарий информационного противоборства еще более расширился, когда со второй половины XX в. представители западной политологии и социологии начали активно изучать эффекты группового поведения, проявляющиеся под специально организованным воздействием. Они экспериментально апробировали наработки в области информационно-психологического воздействия на большие и малые социальные группы, большинство из которых вызвали широкий резонанс в мировой общественности. Важное значение в этом плане приобрели эксперименты зарубежных исследователей С. Аша, С. Милгрэма, Ф. Зимбардо и пр.[53]

Например, Стэнфордский тюремный эксперимент американского социального психолога Ф. Зимбардо, по официальной версии, заказанный в 1971 г. Военно-морским флотом США для объяснения социальных конфликтов в исправительных учреждениях ведомства и в морской пехоте, по этическим соображениям был прекращен досрочно (на шестой день вместо запланированных двух недель). Эксперимент представлял собой психологическое исследование реакции личности на ограничение свободы и влияние новой социальной роли человека на поведение в больших социальных группах. Для участия в нем 24 испытуемых (физически здоровые и психологически устойчивые мужчины) их

[53] *Грин Р.* 48 законов власти и обольщения / Пер. с англ. Е. Я. Мигуновой. М.: РИПОЛ классик, 2005. 736 с.

распределили случайным образом на группы «заключенных» и «надзирателей», которые были помещены в условную тюрьму. Участники исследования настолько быстро вжились в свои роли, что «надзиратели» стали слишком активно выражать садистские эмоции и намерения, а «заключённые» были морально травмированы, впали в глубокую депрессию[54].

Результаты исследования Ф. Зимбардо свидетельствуют о доминировании ситуативных социальных факторов в поведении человека над его личностными характеристиками. Они продемонстрировали восприимчивость и покорность людей, когда присутствует оправдывающая их поступки идеология и оказание давления со стороны общественности и государственных структур.

В целом подобные эксперименты явились подтверждением конформного поведения личности в социальных группах и впоследствии широко использовались для развития технологий информационно-психологического воздействия в политике.

Следует отметить и тот факт, что на сущность и содержание деятельности в области информационного противоборства повлияла набравшая силу со второй половины XX в. межгосударственная конкуренция по обеспечению превосходства в создании и апробировании в политической практике инновационных технологических решений. Под влиянием напряженной международной обстановки, обусловленной ломкой утвердившегося после распада СССР постбиполярного миропорядка, постепенно становилось ясно, что для достижения доминирующего положения государства в системе международных отношений военный потенциал малоприменимым ввиду его разрушительной силы. Соответственно, ученые и практики, вовлеченные в процессы обеспечения информационной безопасности государств, стали активно исследовать возможности технологических прорывов человечества как инструментов ведения информационного противоборства. В этой связи представляется важным обратить

---

[54] См. подр.: *Виловатых А.В.* Использование информационно-коммуникационных технологий в военно-политических целях: социально-психологический аспект // Проблемы национальной стратегии. 2018. № 2 (47). С. 197–211.

внимание на развитие технологий искусственного интеллекта как фактора, коренным образом изменившего практику информационного воздействия.

Прежде всего следует отметить, что в условиях дефицита знаний человека о мозге и когнитивном аппарате живых организмов понятие «искусственный интеллект»[55] толкуется исследователями многовариантно. Автор этого термина, американский информатик и член Национальной академии наук Дж. Маккарти, определяет искусственный интеллект как науку и технологию создания интеллектуальных машин, особенно интеллектуальных компьютерных программ[56].

В Международном терминологическом словаре по искусственному интеллекту дефиниция выглядит более пространно: искусственный интеллект характеризуется как область знаний, рассматривающая разработку таких технологий, чтобы действия вычислительных систем напоминали разумное поведение, в том числе поведение человека[57].

---

[55] Наряду с ИИ в различных контекстах употребляются следующие термины: *слабый*, или *специализированный, ИИ* представлен всеми без исключения существующими решениями и предполагает способность автоматизации реализации одной конкретной задачи, при этом отсутствует возможность самостоятельного обучения другим задачам без перепрограммирования человеком; *автономный ИИ* (Autonomous AI) предусматривает возможность системы функционировать долгое время без участия оператора; *адаптивный ИИ* (Adaptive AI) подразумевает способность системы адаптироваться к новым условиям, приобретая знания, не закладываемые при создании; *общий ИИ* (Artificial General Intelligence, AGI) характеризуется настолько высокой адаптивностью, что обладающая им система может быть использована в самых различных видах деятельности при соответствующем обучении, которое может быть как самостоятельным, так и направленным (с помощью инструктора); *сильный ИИ* (Strong AI), *ИИ человеческого уровня* (Human-Level AI) имеют уровень адаптивности, сравнимый с человеческим, т.е. система способна осваивать те же самые навыки, что и человек, в сопоставимые сроки обучения; *ИИ сверхчеловеческого уровня* (Super-human AI) предполагает ещё более высокую адаптивность и скорость обучения. Таким образом, система может обучиться тем знаниям и способностям, которые человеку в принципе не под силу. См. подробнее: *Колонин А.* Искусственный интеллект – благо или угроза для человечества? // Рос. совет по междунар. делам. 2018. 3 октября. URL: http://russiancouncil.ru/analytics-and-comments/analytics/iskusstvennyy-intellekt-blago-ili-ugroza-dlya-chelovechestva/ (дата обращения: 03.12.2018).

[56] *McCarthy J.* What is Artificial Intelligence? // Computer Science Department. 2007. November 12. URL: http://www-formal.stanford.edu/jmc/whatisai/whatisai.html (дата обращения: 03.12.2018).

[57] *Raynor W.* Jr International Dictionary of Artificial Intelligence / 2nd ed. L.: Global Professional Publishing, 2008.

Отечественные ученые под данным понятием, как правило, понимают компьютерную программу (алгоритм), способную решать задачи, с которыми в состоянии справиться мозг взрослого человека. Таким образом, исследования в области искусственного интеллекта нацелены на алгоритмическое решение проблем, требующих когнитивного напряжения.

Одними из первых вопрос о применении технологии искусственного интеллекта в политике подняли в середине 1950-х гг. военные США и СССР. Практически одновременно искусственный интеллект вошёл в сферу интересов экономистов. Уже в 1960-е гг. Управление перспективных исследований МО США начало изучать вопрос использования искусственного интеллекта в военных целях[58].

Однако вскоре наступила «зима искусственного интеллекта» (ее сроки варьируются с середины 1970-х гг. по окончание 1980-х гг.). В этот период во многих странах проявилось налицо разочарование, связанное с прежде всего завышенными ожиданиями экспертов и государственных деятелей от «математизации» исследований в сфере мировой политики, в частности эффективности применения инновационных технологий в исследовании и прогнозировании политических процессов[59].

Как отмечает в связи с этим академик РАН А.А. Кокошин, несмотря на организацию ряда трудоемких и дорогостоящих исследований в указаннном направлении (большая часть из них проведена аналитическими подразделениями Министерства обороны США), практика показала, что «высокоматематизированные исследования по мирополитической проблематике в основном не оправдали надежд энтузиастов и в целом не привели к сколько-

[58] *Цыгичко В.Н.* Модели в системе принятия военно-стратегических решений в СССР. М.: Империум Пресс, 2005. 94 с.

[59] *Виловатых А.В.* Искусственный интеллект как фактор военной политики будущего // Проблемы национальной стратегии. 2019. № 1 (52). С. 177–192.

нибудь значительному прямому приращению соответсвующих политологических и социологических знаний»[60].

Однако после «зимы искусственного интеллекта» зарубежные и отечественные ученые столкнулись с противоположным явлением – результатами «кибернетической революции», повлекшей массовое внедрение различных информационных систем во все сферы жизнедеятельности государства и общества. С этого времени финансирование государственных технологических инициатив в большинстве государств мира вновь было резко увеличено.

Описывая этот этап мирового развития, ученые сходятся во мнении о том, что он является совершенно новой вехой в истории человечества. Так, одной из первых зарубежных исследователей вопросы применения цифровых технологий в практике информационного противоворства проанализировала американский политолог А-М. Слотер. Еще в конце 1990-х гг. ученый отмечала, что под воздействием глобализации государства хотя и останутся наиболее важными акторами мировой политики, но существующие в них институты, вступая во взаимодействие с аналогичными институтами других стран, постепенно выйдут из-под государственного контроля и обретут относительную или полную самостоятельность. Она прогнозировала, что в будущем такие функциональные правительственные сети, связанные на информационно-коммуникационном уровне, станут ключевой чертой международной политики, поскольку они многообразны и гибки по своему происхождению, структуре, функциям, масштабам, характеру, числу участников и пр.[61]

Двадцатилетие спустя прогноз американского исследователя стал реальностью – установление «сетевой» реальности состоялось, и человечество

---

[60] *Кокошин А.А.* Методологические проблемы прогнозирования в интересах национальной безопасости России. М.: ИВ РАН, 2014. С.37.

[61] См.: *Slaughter Anne-Marie.* The real new world order // Foreign Affairs. 1997. September. URL: http://www.columbia.edu/itc/sipa/S6800/courseworks/real_new_slaughter.pdf (дата обращения: 23.09.2019).

вступило в новую технологическую революцию, ознаменованную в том числе прорывными разработками в информационно-коммуникационной сфере[62].

В целом к концу XX в. вектор исследовательской деятельности в сфере информационного противоборства на Западе сместился в сторону перспектив разработки особого вида информационного оружия, нацеленного на трансформацию стереотипов социального поведения и идентичности. Эти изменения привели к расширению научного инструментария и эмпирической базы, применимых в соответствующей деятельности в мирное и военное время, а также к введению необходимых категорий в законодательство многих государств и их коалиций.

Впервые в научно-исследовательском смысле понятие «информационная война» употребил крупный аналитик из США Томас Рон. В своих наработках в период середины 1970-80-х гг. эксперт отмечал, что с течением времени информационная инфраструктура станет ключевым компонентом американской экономики и политики, и одновременно превратилась в цель внешних сил не только в военное, но и в мирное время, причем довольно уязвимую[63].

В официальных американских документах термин «информационная война» закрепился не сразу. К числу первых нормативно-правовых актов, освещающих основы ведения информационного противоборства, относится директива Министерства обороны США Т3600.1 от 21 декабря 1992 г. под названием «Информационная война», выпущенная после проведения операции «Буря в пустыне» в Персидском заливе. В указанном документе впервые официально использовался рассматриваемый термин[64]. В 1993 г. в директиве Комитета начальников штабов № 30 уже были изложены основные принципы ведения информационной войны. Наконец, в 1996 г. Пентагон утвердил доктрину

---

[62] *Slaughter Anne-Marie.* Connections, not armies, make countries powerful // Financial Times. 2016. April. URL: https://www.ft.com/content/21973144-0544-11e6-9b51-0fb5e65703ce (дата обращения: 23.07.2019).

[63] *Thomas R.* Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976. p. 3–13.

[64] Information Warfare. Directive TS 3600.1. Washington D.C.: U.S. Department of Defense, 21 Dec. 1992.

под названием «Доктрина войны с системами боевого управления», где информационная война определялась как: «действия, предпринятые для достижения информационного превосходства в интересах национальной стратегии и осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации и своих информационных систем»[65].

Осуществление информационных операций как части военно-политической деятельности государства впервые было закреплено в американской нормативно-правовой базе. В 1998 г. в США была разработана «Объединенная доктрина информационных операций», где основной являлась категория «стратегическое информационное противоборство». Согласно документу, целями воздействия в стратегическом информационном противоборстве являются объекты противника, выбираемые по принципу так называемых пяти колец: политическое и военное руководство страны; системы жизнеобеспечения; инфраструктура; население; вооруженные силы[66].

Примечательно, что взгляды военно-политического руководства Соединенных Штатов Америки на вопросы регламентации информационного противоборства в политическом процессе нашли свое отражение в выработке основополагающих концептуальных и директивных документов Североатлантического союза. Первым из таковых стала доктрина психологических операций, выпущенная в 2003 г. под эгидой Комитета начальников штабов ВС США[67]. Ее содеражние, по оценкам российских ученых, базировалось на заимствованных у Вашингтона идеях и терминологии[68].

---

[65] Command and Control Warfare. Joint Publication 3-13.1. Washington D.C.: Joint Chiefs of Staff, Feb. 1996.

[66] Joint Doctrine for Information Operations. Joint Publication 3-13. Washington D.C.: Joint Chiefs of Staff, Dec. 1998.

[67] Joint Publication 3-53 // Doctrine for Joint Psychological Operation. 2003. September 5. URL: https://www.hsdl.org/?abstract&did=472329. (дата обращения 21.01.2018).

[68] См. подр.: *Виловатых А.В., Михеев Е.А.* Стратегические установки США и НАТО по организации и проведению операций информационно-психологического воздействия // Наука. Культура Общество. 2018. № 2–3. С. 131–143.

Более того, в 2007 г. наработки американских экспертов практически дословно были зафиксированы в новой доктрине психологических операций НАТО. Специалисты указывают, что в этом документе использовался «богатый опыт американских коллег мастерски камуфлировать истинные мотивы своих действий на идеологическом фронте»[69]. В доктрине выделялись три вида информационных операций, призванных воздействовать на массовое сознание населения противоборствующей стороны: стратегические психологические операции, психологические операции в рамках операций в кризисных ситуациях, боевые психологические операции[70].

В Доктрине психологических операций Североатлантического союза от 2014 г. уже учитывался комплекс достижений в области цифровых технологий, который, по оценкам автором документа, стал ключом к открытию возможностей по управлению социальными массами на принципиально новом уровне. В документе отмечалась важность исследования интернета как пространства мобилизации общественных масс и их идеологической индоктринации (п. 0109 – «раздел повышения эффективности планирования операций с учётом специфики целевой аудитории»). Для этих целей использовался термин «анализ целевой аудитории» – систематическое изучение социума с целью определения доступности, уязвимости и восприимчивости к поведенческому и установочному воздействию извне[71].

В указанном документе предложена классификация информации, получаемой при исследовании целевой аудитории (*Target Audience Analysis, TAA*) в зависимости от её характеристик. К анализу первого уровня *(Tier 1 TAA*) авторы доктрины отнесли материалы, «содержащие научно обоснованную информацию из множества источников, собранную диагностическими методами в конкретном

---

[69] *Олевский В.* Доктрина психологических операций НАТО // Зарубежное военное обозрение. 2016. №5. С. 24.

[70] Allied Joint Doctrine for Psychological Operations.AJP-3.10.1(A). 2007. October. URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf. (дата обращения 21.01.2018).

[71] Allied Joint Doctrine for Psychological Operations. AJP-3.10.1 // Ministry of Defence. 2014. September. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (дата обращения: 22.01.2018).

государстве на местном языке». Такая информация должна быть проверена на соответствие научным гипотезам, а ее практической реализацией является пребывание в определённой стране «с исследовательскими целями» не менее шести месяцев.

Анализ второго уровня (*Tier 2 TAA*), в соответствии с рассматриваемым документом, представляет собой эмпирические эксперименты, которые проводятся с аудиторией, не владеющей научно обоснованными дедуктивными методами. Исследование может быть проведено непосредственно в интересующей субъекта стране или удалённо (допускается «оценочность» суждений). В качестве аналитического продукта рассматривается информация, зафиксированная в ходе взаимодействия с целевой аудиторией. Примером информации, собранной в рамках второй категории, может служить социологический опрос.

Анализом третьего уровня (*Tier 3 TAA*), согласно доктрине психологических операций НАТО от 2014 г., являются «малоподробные исследования, основанные на вторичной информации, а их результатом выступает предположение». Пример подобных наработок – «интернет-аналитика специфических объектов»[72].

Таким образом, концептуальный подход крупнейшего военно-политического альянса в истории человечества к ведению информационного противоборства формировалось под сильным влиянием стран англосферы, в частности США. Причем в стратегических натовских документах, регламентирующих процессы информационного противоборства, налицо комплексный подход стран – членов альянса к ведению такой деятельности. Взгляды государств, входящих в Организацию Североатлантического договора, на ведение информационного противоборства можно охарактеризовать следующей целевой установкой: «массированное использование информационных ресурсов позволяет управлять общественным мнением вплоть до изменения системы ценностей широких масс населения, а манипуляции

[72] Allied Joint Doctrine for Psychological Operations.AJP-3.10.1 // GOV.UK. 2014. September. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (дата обращения 22.01.2018).

информацией могут кардинально менять восприятие и поведение избранных (целевых) аудиторий»[73].

В целом, как показывает история политических отношений, наработанные в периоды межгосударственной конфронтации формы и методы информационного противоборства позволили применяющим их субъектам более быстро достигать поставленных политических целей мирное время, а некоторым – занять привилегированное положение в системе глобальной политики.

В целом, проведенный анализ свидетельствует, что если в прежние времена теория и практика информационного противоборства опирались в основном на предшествующий политический опыт невоенного противостояния, накопленный в ходе исторического развития, основываясь прежде всего на традиционных методах убеждения социума и его отдельных групп, политических элит, то в условиях повсеместной цифровизации социально-экономической и политической реальности при формировании стратегий невоенного противоборства учитываются многочисленные аспекты социологии и психологии управления, которые могут быть использованы в манипулятивных политических целях на просторах трансграничной информационно-коммуникационной сети интернет[74].

1.3. Исследование информационного противоборства с позиций постнеклассической рациональности

Эволюция информационного противоборства в политическом процессе поспособствовала тому, что методы информационнного воздействия стали существенно эффективнее, чем в прежние времена. Соответственно, в настоящее время они чаще и масштабнее используются различными государствами, их блоками и коалициями, неправительственными организациями и прочими субъектами мировой политики для достижения поставленных политических целей.

---

[73] *Олевский В.* Доктрина психологических операций НАТО // Зарубежное военное обозрение. 2016. №5. С. 12–20.

[74] См. подр.: *Booth K., Wheeler N.* The Security Dilemma: Fear, Cooperation and Trust in World Politics. N.Y.: Palgrave McMillan, 2008. p. 1–18.

Еще несколько десятилетий назад важнейшим фактором достижения преимущества в информационном противоборстве являлось максимально разнообразное использование сильных сторон разнообразных средств массовой информации как инструментов информационного противоборства. Но в настоящее время, характеризующееся быстрой динамикой научно-технического прогресса, налицо всеобъемлющее распространение новых высокотехнологичных средств коммуникации. С совершенствованием инструментария, формированием массивов информации посредством социологических исследований, использованием преимуществ современных средств массовой коммуникации, наконец, форсированным развитием цифровых технологий современное общество сталкивается с принципиально новой социально-политической реальностью, последствия которой пока мало прогнозируемы. В данных условиях перед властями многих государств мира актуализировалась проблема пересмотра подходов и доктрин по защите национальных интересов в информационной сфере.

Прорывы в сфере развития инновационных технологий фактически ежедневно раскрывают новые возможности информационного воздействия на умонастроения масс. В особенности большой потенциал оказания информационного воздействия на противоборствующую сторону заключает в себе глобальная информационно-коммуникационная сеть интернет, где, как в огромном поведенческом архиве, накапливаются колоссальные массивы больших и сверхбольших объёмов данных. В этом контексте бывший директор по технологиям Центрального разведывательного управления США А. Г. Хант высказался следующим образом: «С точки зрения национальной безопасности США, большие данные – это все данные. Они должны быть у нас. И нас не устраивает, что они будут в базах данных – нам нужно, чтобы они были в оперативной памяти»[75].

[75] Society’s Nervous System: Building Effective Government, Energy, and Public Health Systems. A. Pentland in Computer, Vol. 45, No. 1. January 2012. p. 31–38.

Все усиленнее развиваются современные технологии формирования общественного мнения и манипулирования массовым сознанием, реализуемые посредством многочисленных интернет-сервисов (социальных сетей, форумов, интернет-порталов и пр.). Они выступают в качестве пространства и одновременно инструментов информационного воздействия, ломая шаблонные схемы, присущие прежде политической динамике. Специалисты также указывают на широкие перспективы применения в целях информационного воздействия технологий искусственного интеллекта, в частности машинного обучения. По некоторым оценкам, в скором времени это может даже ознаменовать собой новое качество протекания военных конфликтов будущего.

На современном этапе в большинстве стран мира использование цифровых технологий как инструмента информационного противоборства, ведущегося для достижения политических или военных целей, расценивается в качестве угроз безопасности, а международно-правовые рамки в этой сфере формируются с заметным отставанием. На данный факт указывается в Стратегии национальной безопасности Российской Федерации, где, в частности, отмечается: «Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории»[76].

Таким образом, возможности цифровой среды, еще только формирующей социально-политическую деятельность на современном этапе мирового развития, постепенно разрушают привычные шаблоны восприятия проблем безопасности, прежде всего в информационной сфере.

Кроме того, многие отечественные и зарубежные исследователи проблематики информационного противоборства указывают на то, что в

[76] Стратегия национальной безопасности Российской Федерации (Указ Президента РФ от 31.12.2015 № 683).

настоящее время на развертывание политических процессов самого разного профиля и масштаба влияют относительно новые акторы мировой политики. Так, российский политолог С.В. Куньщиков полагает, что сегодня «только деятельное меньшинство обладает значительной силой и играет важную роль в политическом процессе…». Это, по мнению ученого, позволяет говорить о «серьезной роли субъективных факторов в политическом процессе: характере лидеров и элит, их идеологических пристрастиях и ценностных приоритетах. Иными словами, отмечает автор, «политический процесс в его целостности не может быть рассмотрен вне контекста динамики общественного сознания вообще и идеологического сознания в частности»[77].

Соответственно, при политологическом анализе информационного противоборства в политическом процессе необходимо учитывать вес, значение и степень влияния на его развертывание различных политических субъектов. Это обсловлено тем обстоятельством, что на современном этапе развития участниками политических процессов являются не только государства, но и «акторы вне суверенитета»: военно-политические блоки, спонтанно организованные социальные движения, террористические и экстремистские группировки, хакеры и пр. В связи с этим нам представляется принципиально важным проанализировать включение в процесс информационного противоборства новых (нередко нелегитимных) политических акторов.

В целом со второй половины прошлого века и к настоящему времения окончательно выделились следующие относительно новые субъекты информационного противоборства.

Во-первых, расширяются масштабы деятельности в рамках информационного противоборства такого **крупного военно-политического блока, как Североатлантический союз.** Сегодня политическая воля и наличие объединенных ресурсов США и НАТО позволяют в рамках стратегии, направленной на глобальное доминирование, последовательно осуществлять

[77] *Куньщиков С.В.* Идеология в структуре политического процесса: сущность и динамика функционирования. Дис. канд. полит. наук. Екатеринбург, 2006. 149 с

комплексные подрывные операции информационного порядка. При этом за так называемой стратегией сдерживания, выстраиваемой государствами трансатлантического сообщества восточном фланге, просматривается стремление к проведению политики «активной обороны», имеющей выраженное наступательное измерение, в том числе за счет использования гибридных методов противоборства.

Необходимо отметить, что большие усилия НАТО в рамках деятельности по информационному противоборству направлены против Российской Федерации. В марте 2018 г. тогдашний глава Европейского командования вооруженных сил США и одновременно главнокомандующий Объединенными вооруженными силами НАТО в Европе Кёртис Скапаротти выступил в Комитете по вооруженными силам Сената США, заявив о необходимости существенного ужесточения политики сдерживания России с опорой на выстраивание комплексной системы информационного противоборства[78]. С точки зрения проведения активных информационных операций против РФ политик указал на потенциал Российской информационной группы *(Russian Information Group).* Решение о создании этой группы было принято еще в марте 2017 г., ее сопредседателями являются Европейское командование ВС США и Государственный департамент США, однако особенности деятельности структуры до недавних пор почти не афишировались.

В последние годы в информационное противоборство все активнее включаются **террористические и экстремистские группировки**. Как отмечается в Доктрине информационной безопасности РФ, они используют возможности современных информационно-коммуникационных технологий «для ведения пропагандистской и вербовочной деятельности, для информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания

[78] См.: Russia Will Challenge US Military Superiority in Europe by 2025: US General // Defense One. 2018. URL: https://www.defenseone.com/threats/2018/03/russia-will-challenge-us-military-superiority-europe-2025-us-general/146523/ (дата обращения: 20.08.2019).

этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников»[79].

В этом отношении особенно выделяется запрещенная в России международная террористическая организация «Исламское государство» (ИГИЛ), которая в том числе ведет широкую деятельность по информационно-психологическому воздействию в интернете. Как отмечают отечественные эксперты, в структуре данной организации функционирует самостоятельный медиахолдинг, который производит практически все элементы мультимедийной продукции (видеофильмов, агитационных роликов, аудиозаписей проповедей, журналов, буклетов, постеров и т. п.)[80].

Мощный потенциал участия в процессах информационного противоборства имеют также многочисленные н**еправительственные организации** (НПО): правозащитные организации, фонды политической направленности, экспертные учреждения и др. Чаще всего указанные структуры выступают как рупор пропаганды в конкретной сфере жизнедеятельности государства и социума. В этом плане показательна деятельность экспертно-аналитических центров Запада. К таковым политологи правомерно относят «Корпорацию РЭНД» *(RAND Corporation),* Совет по международным отношениям *(Council on Foreign Relations),* Атлантический совет *(Atlantic Council),* Альянс защиты демократии Германского Фонда Маршалла (*German Marshall Fund's Alliance for Securing Democracy*) и пр.[81]

Примечательно, что в последние годы западные экспертные центры все чаще выступают с прогнозами развития внешней и внутренней политики России, которые содержат идеологически окрашенные оценки социально-экономического

---

[79] Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 №646).

[80] См.: *Сундиев И.Ю., Смирнов А.А., Костин В.Н.* Информационно-пропагандистская деятельность террористической организации «Исламское государство Ирака и Леванта» // Библиотека криминалиста. 2015. №1. С. 208–218.

[81] *Смирнов А.А.* Негосударственные акторы в современных информационных войнах // Международная жизнь. 2018. № 5. URL: https://interaffairs.ru/jauthor/material/2020 (дата обращения: 04.10.2019).

положения в нашей стране и дают прогнозы ее противостояния с международным сообществом. Конечная цель авторов таких работ, скорее всего, сводится к тому, чтобы убедить мировую общественность в деструктивном характере политики РФ. Сотрудники западных НПО стремятся проанализировать потенциал протестных настроений российского населения с точки зрения социально-демографического состава (пол, возраст, уровень образования, место жительства и пр.), политических взглядов участников шествий, их персональной активности в социальных сетях, отношения к социально-экономическим проблемам и т.д.[82]

Например, в последние годы фокусе пристального внимания зарубежных неправительственных структур оказываются выступления российской оппозиции. К таковым относятся и митинги, состоявшиеся в Москве летом 2019 г. По мнению привлеченной к такой аналитической работе специалистов, курс российского руководства на внешней арене якобы призван компенсировать его «просчеты на внутриполитическом направлении». Эксперты констатировали, что в непростых социально-экономиеских условиях российские власти, вероятно, возьмут курс на «национальную мобилизацию в условиях стагнации качества жизни», а в среднесрочной перспективе в РФ будет ужесточен контроль правоохранительных органов над всеми структурами гражданского общества. В целом, по оценкам западных аналитиков, «Россия может качнуться в сторону принципиально новых мер в целях реидеологизации, причем в основу этого процесса будут положены принципы традиционализма и ортодоксальные традиционные ценности»[83].

Примечательно, что ведущие зарубежные эксперы исходят из безальтернативности продолжения конфронтации Запада и России в ближайшей перспективе. Вину за это они стремятся возложить на российское руководство, особенно на фоне трудностей, обусловленных пандемией нового коронавируса,

---

[82] См. напр.: *Petrov N.* Understanding Methods of Elite Repression in Russia // Chatham House. 2019. 4 June. URL: https://www.chathamhouse.org/expert/comment/understanding-methods-elite-repression-russia (дата обращения: 19.09.2019).

[83] См.напр.: Putin and Russia in 2018–24: What Next? // Chatham House. 2018. March 15. URL: https://www.chathamhouse.org/research/publications/putin-and-russia-2018-24-what-next (дата обращения 27.03.2017); Putin’s New Term—From Brezhnev to Stalin // Cato Institute.2018. March 21. URL: https://www.cato.org/blog/putins-new-term-brezhnev-stalin (дата обращения 28.03.2017).

хотя и признают возрастающую сложность данной задачи. Об этом свидетельствуют предлагаемые экспертами решения, в частности использование проверенного в годы холодной войны инструментария (выдвижение против РФ обвинений в нарушении прав человека и договоров по контролю над вооружениями) наряду с новыми средствами информационного (кампании типа «Рашагейт» или «дела Скриплей») и экономического давления (обновление санкционного законодательства)[84].

Важным представляется отметить также составление различными международными организациями, СМИ, коммерческими и некоммерческими структурами тематических рейтингов и индексов. Например, Всемирная туристская организация (*UWNTO*) публикует так называемый рейтинг свободы передвижения, где оценивается вклад отдельных стран в реализацию возможности путешествий без виз[85]; Движение по противодействию коррупции «Транспэрэнси Интернэшнл» (*Transparency International*) выпускает в свет индекс восприятия коррупции, в котором чаще всего бывают представлены большинство стран мира[86]; американское новостное агентство «Блумберг» *(Bloomberg)* ежегодно публикует рейтинг эффективности мировых систем здравоохранения[87]; американская неправительственная организация «ИРЕКС» (*IREX*), деятельность которой нацелена на «развитие демократического общества по всему миру», регулярно составляет отчеты о деятельности мировых СМИ, где дается оценка медиаландшафтов и анализируется свобода медиа в странах; британские исследователи составляют рейтинг стран, предоставляющих

---

[84] См.: One more term for Putin: Dark ambition, dim hopes // Brookings. 2018. March 20. URL: https://www.brookings.edu/blog/up-front/2018/03/20/one-more-term-for-putin-dark-ambition-dim-hopes/ (дата обращения 28.03.2017).

[85] International tourist arrivals up 4% reach a record 1.2 billion in 2015 // UNWTO. 2016. URL: https://media.unwto.org/Press-release/2016-01-18/international-tourist-arrivals-4-reach-record-12-billion-2015 (дата обращения: 14.07.2019).

[86] Corruption Perceptions Index 2018 // Transparency International. 2018. URL: https://www.transparency.org/cpi2018 (дата обращения: 14.07.2019).

[87] These Are the World's Healthiest Nations // Bloomberg. 2019. URL: https://www.bloomberg.com/news/articles/2019-02-24/spain-tops-italy-as-world-s-healthiest-nation-while-u-s-slips (дата обращения: 15.08.2019).

качественное и недорогое образование[88]; американское информационное агентство «Новости США и мир» (*U.S. News&World*) публикует ежегодный рейтинг стран мира, где созданы самые благоприятные для жизни условия[89]; американские агентства регулярно выпускают индексы экономического развития отдельных стран и отраслей, которые имеют большое значение для принятия решений в финансовой отрасли и пр.

Как нам представляется, реальной и основной целью таких оценок экспертов, являющихся фактически рупором пропаганды СМИ определенного толка, является поиск обоснования усиливающихся в последнее время кризисных тенденций в политике стран западного сообщества.

Участниками политических процессов современности, в том числе ведущих деятельность в области в сфере информационного противоборства, сегодня стали **научно-исследовательские и образовательные структуры**, то есть, по сути, политизируется социальный институт образования. Прежде всего это относится к некоторым организациям, функционирующим в сфере политологических и социологических исследований, призванным выступать контуром всей системы управления общественным мнением.

Мониторинг и формирование общественного мнения населения традиционно находится в фокусе внимания политических элит разлиных государств мира. Представляется целесообразным выделить некоторые приемы, характеризующие манеру проведения в ведущих странах Запада исследований, социальных экспериментов фокус-групп, массовых и экспертных опросов на современном этапе.

Формирование общественного мнения предполагает знание настроений широких народных масс. В частности, внешнеполитическое ведомство Британии регулярно заказывает исследования целевых групп и опросы общественного

---

[88] Norway, Russia and Luxembourg take the lead for being the cheapest countries in the world to be a student // The Independent. 2015. URL: http://www.independent.co.uk/student/news/norway-russia-and-luxembourg-take-the-lead-for-being-the-cheapest-countries-in-the-world-to-be-a-a6799211.html (дата обращения: 16.07.2019).

[89] Overall Best Countries Ranking Rankings // U.S. News & World Report. 2019. URL: https://www.usnews.com/news/best-countries/overall-rankings (дата обращения: 14.07.2019).

мнения с установкой на поддержку его работы в сфере стратегической коммуникации. Например, согласно отчетам Фонда предотвращения конфликтов, содействия стабильности и безопасности Великобритании, в 2017 г. на анализ целевой группы русскоязычного меньшинства в Прибалтике фонд выделил 1,3 млн евро, а в период особого осложнения российско-британских отношений в 2017 г. английские исследователи отличились включением России в многочисленные «индексы риска»[90].

Одновременно в настоящее время социологические исследования используются и как инструмент формирования общественного мнения. В данном случае настроения отдельных социальных групп изучаются с целью последующей коррекции общественного мнения по конкретной проблеме с привлечением средств массовой информации. Например, при проведении опросов натовскими структурами в государствах, формально придерживающихся политики военного неприсоединения (Швеции и Финляндии), в опросные листы аналитики традиционно включают «фактор России». Нередко даже напрямую ставится вопрос о том, является ли РФ угрозой национальной безопасности для данных стран. В частности, об этом свидетельствует тот факт, что под угрозой такого вымышленного феномена, как «российское вмешательство» в Швеции в 2016 г. была проведена серия опросов населения о целесообразности возрождения в стране воинской повинности[91]. Таким образом отношение финнов и шведов к вступлению в Североатлантический альянс автоматически увязывалось с их восприятием политики Москвы, чему способствовала сама формулировка инструментария подобного рода исследований, временной период их проведения, специфика анонсирования результатов и пр.

Соответственно, хотя в тактических целях институт социологических опросов был создан для поиска путей совершенствования системы социального

---

[90] См. подр.: *Виловатых А.В.* Военная политика Великобритании: фактор Brexit // Проблемы национальной стратегии. 2017. № 6 (45). С.127–144.

[91] См.подр.: Военно-политическая ситуация в Северной Европе и угрозы безопасности России // Тищенко Г.Г., Абаев Л.Ч., Николайчук И.А., Виловатых А.В., Бекман Й. Проблемы национальной стратегии. 2016. № 6 (39). С.11–38.

контроля: такие исследования были призваны выявить проблемные сферы и масштабы общественного недовольства, на современном этапе, в условиях повсеместного распространения цифровых технологий они являются и одним из способов воздействия на массовое сознание. Этому служат все виды опросов, в том числе закрытые, результаты которых известны только заказчикам. В такую деятельность вовлечены государственные структуры различных стран.

Безусловно, подаваемая в подобных опросах, рейтингах и индексах информация трактуется как «объективная» и способна оказать большое влияние на умонастроения масс. Соответственно, указанные инструменты можно рассматривать как способ производства и последующего закрепления определенного общественного мнения. В перспективе эффект подобных исследований сводится к утверждению в массовом сознании относительно однородного восприятия (позитивного или негативного) какой-либо конкретной проблемы и соответствующего отношения к проводимой властями на данном направлении политике.

При массированности усилий исследовательских структур с учетом выделяемой им поддержки тех или иных политических сил эффект от деятельности по оказанию информационного воздействия на систему формирования общественного мнения может иметь решающее значение при принятии конкретных политических решений.

Все большее влияние на развитие политических процессов современности, особенно ввиду утверждения цифровой реальности, в последние годы приобретают **хакерские и хактивистские группы, блогеры**. Как подчеркивается в обзоре одной из ведущих международных компаний по предотвращению и расследованию киберпреступлений «Груп Ай-Би» (*Group IB*) за 2017 г., в последние годы геополитические разногласия между странами сопровождает повышенная активность в кибернетическом пространстве, ведущаяся как государственными, так и негосударственными акторами диверсионными методами.

Современные хакерские группы чаще всего нацелены на осуществление несанкционированного доступа к информационным системам с целью хищения конфиденциальной и иной чувствительной информации и на совершение компьютерных атак на правительственные информационные ресурсы и критически важные объекты информационной инфраструктуры с целью нарушения их работы[92].

В свою очередь, хактивистские группировки ориентированы на достижение политических целей. Формами их деятельности преимущественно выступают публичное опубликование массивов перехваченной конфиденциальной информации и проведение пропагандистских информационных акций. В этом контексте необходимо упомянуть проект «Викиликс» (*WikiLeaks*), который с момента своего образования в 2006 г. опубликовал свыше 10 млн официальных документов самых разных государств[93].

В качестве самостоятельных субъектов информационного противоборства в последние годы выступают блогеры, причем в условиях форсированного развития социальных сетевых ресурсов их роль в формировании общественного мнения постепенно возрастает. Особенно заметно это проявилось в период пандемии коронавируса, когда в связи с деятельностью блогеров правительства многих стран мира столкнулись с так называемой «вирусной инфодемией». Чиновники Евросоюза назвали данным термином волну информации, связанную с распространением нового типа коронавируса, включая разнородные мистификации, теории заговора и дезинформацию, распространяющуюся в основном блогерами-одиночками на просторах сети интернет[94].

---

[92] См.: Putin’s landslide election makes it seem like Russia is stable. Don’t be fooled // CSIS. 2018. March 19. URL: https://www.csis.org/search?search_api_views_fulltext=russia%20elections&sort_by=field_publication_date&page= (дата обращения 27.03.2018).

[93] What is WikiLeaks // WikiLeaks. 2015. November. URL: https://wikileaks.org/What-is-Wikileaks.html (дата обращения: 10.12.2018).

[94] The EU's response to the coronavirus 'infodemic' // European Parliament. 2020. June 12. URL: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2020)651963 (дата обращения: 14.06.2020).

Наконец, все активнее в политические процессы, связанные с информационным противоборством, включаются **коммерческие организации**. Нередко к ним принадлежат частные военные компании, организации по мониторингу информационного пространства, защите информации и информационных систем (включая критически важные объекты информационной инфраструктуры), выполняя на основе аутсорсинга отдельные функции в рассматриваемой сфере.

В качестве примера таких организаций можно назвать одного из мировых флагманов в области аналитики больших данных – американскую компанию «Палантир» (*Palantir Technologies*), которая тесно сотрудничает с американскими специальными службами и выполняет важные проекты государственного масштаба. Например, эта компания участвует в программе «Тотальная/контртеррористическая осведомленность» (*Total/Terrorism Information Awareness)*[95], реализуемой совместно с Управлением перспективных исследований Минобороны США (*DARPA*). Ее дочерние проекты (*Gothem, Metropolis*) также приспособлены для решения задач, поставленных государственными ведомствами Соединенных Штатов Америки.

Учитывая тенденцию последних десятилетий по передаче военно-силовых функций государства коммерческим структурам («приватизация безопасности»), наиболее ярко проявившую себя в форме развития частных военных корпораций, специалисты полагают возможным и «появление в рассматриваемой нами сфере частных компаний, специализирующихся на проведении наступательных информационных операций («информационная война как услуга»)[96].

Средства массовой информации и сообщества журналистов-расследователей продолжают оставаться влиятельными источниками информирования общества, а потому неизбежно вовлекаются в механизм

---

[95] См.: Palantir Technologies, 2019. URL: http://www.palantir.com/ (дата обращения: 21.04.2019).

[96] *Смирнов А.А.* Негосударственные акторы в современных информационных войнах // Международная жизнь. 2018. № 5. URL: https://interaffairs.ru/jauthor/material/2020 (дата обращения: 04.10.2019).

информационного противостояния. Их основная функция в данном механизме состоит в трансляции определенных идей и ценностей, формировании нужной информационной повестки и соответствующем освещении событий в конкретной стране и даже в целом мире. В этом контексте в Великобритании выделяется деятельность Британского совета (*British Council),* способствующего популярности крупнейшей национальной телерадиовещательной корпорации «Би-би-си» (*British Broadcasting Company*). В свою очередь, США через правительственное агентство Совет управляющих по вопросам вещания (*Broadcasting Board of Governors*) напрямую осуществляется финансирование и координация известных СМИ.

В таблице 1.1 условно представлены легитимные или нелегитимные участники процессов информационного противоборства на современном этапе мирового развития.

Таблица 1.1 – Современные субъекты информационного противоборства

Легитимные	*Нелегитимные*
Государства	Террористические и экстремистские группировки
Международные и региональные организации	Нелегальные вооруженные формирования
Неправительственные организации	Хакерские и хактивистские сообщества
Средства массовой информации	Стихийные социальные движения
Отдельные личности	Отдельные личности

Источник: Составлено автором.

Проведенный анализ деятельности негосударственных участников информационного противоборства правомерно ставит на повестку дня политологов и правоведов вопрос об их субъектности в мировой политике. Как нам представляется, деятельность легитиных и нелегитимных акторов указанной сферы является частным аспектом более широкого вопроса о функциональной роли современных государств в условиях меняющегося мира. Так, еще в 1976 г. специальный парламентский комитет по изучению деятельности специальных служб США, установил, что Центральное разведывательное управление профинансировало почти половину грантов, выданных американским

неправительственным организациям в сфере международной деятельности. При этом отмечалось, что такие известные фонды как Форда, Рокфеллера и Карнеги являются «оптимальным и наиболее приемлемым инструментом финансового прикрытия, обеспечивающим деятельность американских спецслужб»[97].

Вместе с тем сказанное не отменяет того факта, что указанные участники мировой политики выступают и как самостоятельные субъекты, преследующие собственные цели. С учетом имеющихся ресурсов некоторые негосударственные участники мировой политики нередко становятся провокаторами проблем международного масштаба, и, как показывает практика, способны применять в том числе военные средства в достижении политических целей. Об этом, в частности, свидетельствует деятельность крупных террористических группировок с геополитическими амбициями, существенно затруднивших в последние годы процессы мирного урегулирования в регионе Ближнего и Среднего Востока[98].

Можно констатировать, что в условиях утверждения цифровой реальности интенсивность вовлечения негосударственных субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, в политические процессы достигла критичного уровня. Они продуцируют еще более скрытный, трансграничный и вневременной характер взаимодействий в ходе развертывания информационного противоборства. По всей видимости, их участие в политических процессах (в том числе в деятельности в сфере информационного противоборства) будет еще более нарастать[99].

В последнее десятилетие указанные обстоятельтсва привели к резкому понижению степени управляемости процессов информационного противоборства со стороны государственных структур. Об это весьма подробно высказался автор

---

[97] *Сондерс Ф.С.* ЦРУ и мир искусств: культурный фронт холодной войны. М.: Институт внешнеполитических исследований и инициатив, Кучково поле, 2013. С. 117.

[98] См.: *Кочубей М.А.* Современные практики деструктивного воздействия на сознание как политическая технология // Российская ассоциация международных исследований. URL: http://www.risa.ru/ru/sections/359-1-3 (дата обращения: 07.10.2019).

[99] См.подр.: *Виловатых А.В.* Информационно-психологическое воздействие на массовое сознание в условиях новой политической реальности // Свободная мысль. 2019. № 6. С. 165–177.

концепции «парадокса участия», британский политолог-международник М. Николсон. Согласно его концепции, рост открытости международной системы, увеличение числа и многообразия ее участников, выражающихся в том числе в свободе передвижений, обменов и взаимодействий частных лиц различных государств, являются причиной усиления нестабильности международной системы, провоцируя в конечном итоге ее дисбаланс. Вывод М. Николсона заключается в том, что «впечатляющие изменения, которые вносит сегодня в характер и состояние международных отношений все более широкое участие в них различного рода временных объединений и неорганизованных частных лиц, связаны прежде всего с тем, что такое участие становится источником абсолютной случайности в этой сфере»[100].

В целом на современном этапе мирового развития процессы информационного противоборства интенсифицируются, что обусловлено влиянием качественно новых факторов. К таковым возможно отнести в том числе мощный технологический рывок в сфере информационно-коммуникационных технологий, развивающихся форсированными темпами, подверженных взаимовлиянию и мимикрии. Он ведет человечество на тропу утверждения принципиально иной политической реальности, которая характеризуется полиакторными взаимодействиями вне пространственных и временных границ, а также отсутствием барьеров, традиционно присущих политико-дипломатической практике, – беспрецедентная доступность информации сочетается со столь же беспрецедентным ее переизбытком. Одновременно своеобразная цифровизация геополитики сопровождается усилением межгосударственной конкуренции между ослабленными и возвышающимися центрами силы, в том числе в сфере разработки цифровых технологий.

В этом контексте, с нашей точки зрения, важно обратить внимание на признаки кризисных явлений развития политологической науки, причем как в

---

[100] *Николсон М.* Влияние индивида на международную систему. Размышления о структурах / Жирар М. (рук. авт. колл.) // Индивиды в международной политике. М., 1996. С. 133–136.

России, так и на Западе. Налицо серьезное запаздывание развития академических знаний от современной политической реальности, неспособность научного сообщества признать достоинства междисциплинарности исследований, увидеть новые возможности методологического потенциала политологии, связанные с процессами цифровизации и пр. Основным и существенным недостатком классической теории политического процесса является гипертрофированное стремление ученых акцентировать исключительно объективные его стороны, придать им свойство имманентной универсальности развития. В целом на крупные проблемы современной отечественной науки, причем не только политологии, но и других отраслей социально-гуманитарного знания, указывают лишь некоторые наиболее смелые исследователи[101].

Складывающаяся ситуация указывает на потребность критического переосмысления базовых подходов к изучению политологических проблем, а также своеобразной инвентаризации методологического потенциала науки, «сухой остаток» которой заложил бы основы современных научных изысканий. Политические реалии, формирующиеся в результате синергетического эффекта взаимодействия устоявшихся и относительно новых факторов развертывания политических процессов, диктуют целесообразность концептуального осмысления применения альтернативных научных подходов к их изучению. Доминирующая во многих исследованиях косность исследовательского мышления способствует отставанию политологической науки от политической практики, что серьезно тормозит научный прогресс в нашей стране. Во многом это обусловлено тем, что накопленные знания в социальных и политических науках лежат в русле аналитики и экспертных мнений, не поддаваясь научной квалификации.

С учетом сказанного, с нашей точки зрения, весьма условно знания современных социально-гуманитарных наук можно разделить на «накопленные

---

[101] См.напр.: *Гаман-Голутвина О.* Современная сравнительная политология перед вызовами развития // Интернет-портал «Перспективы». 2020. 13 мая. URL: http://www.perspektivy.info/misl/cenn/sovremennaja_sravnitelnaja_politologija_pered_vyzovami_razvitija_2020-05-13.htm (дата обращения 20.05.2020).

внутри отдельных исследовательских сообществ, но непризнанные вовне» утерянные знания вследствие игнорирования научным сообществом прошлых результатов как вследствие утраты интереса, так и «устаревания» научных направлений; непризнанные знания, полученные на стыках научных дисциплин, а также интегрированные знания, под которым понимаются результаты, полученные в различных областях и имеющие при этом сущностное сходство, но которые не воспринимаются и непризнаются научным сообществом как таковые вследствие инерционности исследовательских парадигм.

Можно предположить, что потенциал развития альтернативных политологических подходов заключается в основах постнеклассической рациональности к исследованию социально-политической динамики. Термин «поснеклассическая наука» введен отечественным академиком В.С. Степиным для обозначения смены «эволюционной парадигмы» ввиду усиления сверхсложности, самоорганизации и самовозникновении «человекоразмерных систем, включающих человека и его деятельность в качестве составного компонента» [102].

Указанная парадигма могла бы поспособствовать приращению потенциала политологии как науки, расширению ее понятийно-катеригориального аппарата. Целесообразность курса на открытость к новым подходам и парадигмам обусловлена тем, что традиционные методы научных исследований, основанные на детерминизме событий, которые привычно применяются в политологических школах разнообразных направлений, оказываются несоответствующими нынешней политической турбулентности и масштабу технологической составляющей, влияющих на развертывание политических процессов. Современные социально-политические и экономические системы, характеризующиеся структурной неустойчивостью, динамикой их функционирования, важно рассматривать в комплексе как саморегулирующиеся и саморазвивающиеся, открытые для внешних воздействий и нелинейные в своем

[102] *Стёпин В.С.* Научное познание в ценности техногенной цивилизации // Вопросы философии. № 10, 1989. С.16.

развитии, при изучении которых на первый план выходит амбивалентность и нелинейность политических процессов, что требует прежде всего глубокой междисциплинарной интеграции.

На общем фоне современных научных работ, посвященных комплексному исследованию взаимосвязи прорывного технологического развития, социальной динамики и мирополитических трансформаций, выделяется научный труд крупного российского философа И.Ф. Кефели «Асфатроника: на пути к теории глобальной безопасности», где ученый предлагает принципиально новую парадигму экономических, политических, социальных процессов, а также технологического развития сквозь призму глобальных рисков. По мнению И.Ф. Кефели, постнеклассическая наука «позволила человеку не только проникнуть в микромир (это стало достоянием уже неклассической науки), но и выйти на рубежи создания нано-, био-, инфо- и когнитивных технологий»[103].

Указанный методологический ракурс вскрывает сущность современных политических процессов, связанных с трансформацией мироустройства, сопровождающихся острыми витками информационных войн с применением всевозможных сил и средств между крупными мировыми центрами силы и другими акторами мировой политики. Так, рассуждая об опасностях для социума в свете ожидаемого наращивания использования достижений цифровизации в процессах информационного противоборства, когда «затихает голос этика», зарубежные исследователи К. О'Нил и Г. Леонгард указывают на то, что «сегодня настало время разобраться в природе грядущих изменений: от искусственного интеллекта до редактирования генома, и признать важность утверждения морально-нравственной доминанты как ключевой составляющей опасностей, связанных с интернетом вещей и цифровым ожирением»[104].

Помимо отмеченных аспектов, с нашей точки зрения, при развертывании современных политических процессов целесообразно также учитывать и высокую

---

[103] *Кефели И. Ф.* Асфатроника: на пути к теории глобальной безопасности: монография. СПб.: ИПЦ СЗИУ РАНХиГС, 2020. С. 10.

[104] *Леонгард Г.* Технологии против человека. М.: АСТ, 2018 С. 21–28.

долю неопределенности, которая обусловливает то, что в совокупности новации Четвертой промышленной революции могут создать тот синергетический эффект, который будет способен перезапустить социальную и политическую динамику в принципе. Именно в связи с этим обстоятельством, как нам видится, многие ученые с мировыми именами намеренно «придерживают» развитие и, тем более, апробацию подрывных технологий в политической и социально-экономической практике, причем нередко действуя даже наперекор властным элитам. И крупные эксперты абсолютно правомерно указывают на то, что в ближайшем будущем на государственном уровне жизненно требуется признание «реальной опасности неконтролируемого развития и неэтичного использования технологий, и возможность преодоления этой опасности в фундаментальной трансформации социального мышления»[105].

Если говорить о научном изучении фактора информационного противоборства в политическом процессее, то здесь ситуация еще сложнее. На наш взгляд, трудности определяются особенностями информационного противоборства как комплексного политического явления, его скрытным и аморальным характером в принципе. С точки зрения политологического анализа среди основополагающих составляющих, необходимых для интерпретации политического процесса, к информационному противоборству относятся такие компоненты, как: среда; политические субъекты и их взаимодействия; нормы, регулирующие отношения; масштаб и период его развертывания. Кроме того, на современном этапе выделяется и субъективная составляющая политики, связанная с активизацией ведения информационного противоборства нелегитимными акторами политики.

В научном смысле важным является то, что ранее отсутствие должного внимания к указанным аспектам не привносило крупных искажений в исследовательский процесс. Однако в свете происходящей технологической революции, повлекшей внедрение цифровых инноваций во все сферы

[105] *Кефели И. Ф.* Асфатроника: на пути к теории глобальной безопасности: монография. СПб.: ИПЦ СЗИУ РАНХиГС, 2020. С. 20.

жизнедеятельности государства, формирования новой композиции взаимодействия участвующих в информационном противоборстве политических акторов, расширения пространств ведения информационного противоборства в кибернетической среде, появления новых инструментов воздействия на массовое сознание, мимикрирующий характер и нелинейность информационного противоборства выступают на ведущий план.

С позиций политической практики следует отметить прежде всего то обстоятельство, что в современных условиях государство как социальный институт, имеющий по Т. Гоббсу, «мандат на насилие», не способно в полной мере контролировать различные проекции ведения информационного противоборства – ни в концептуальном, ни в содержательном, ни в правовом ракурсе. Как отмечалось нами выше, это обусловлено не только крупными прорывами в военном деле, но и форсированным развитием цифровых технологий, преимуществами которых пользуются как легитимные, так и нелегитимные акторы политики. Фактически подорвался сам механизм работы госорганов с национальными средствами массовой информации и коммуникации, обеспечивающими совместно с силами информационно-психологических операций задействование соответствующих государственных структур не только в военное, но и непосредственно в мирное время. В условиях разрастания числа акторов информационного противоборства, использующих разнообразные преимущества социальных интернет-сервисов, налицо потеря управляемости процесса подачи информации до населения собственного государства, равно как и контролируемого режима ее распространения до противоборствующей стороны.

Можно достаточно уверенно предположить, что малоконтролируемое властными элитами технологическое развитие (в отдельных странах и на международном уровне в целом) способно запустить процессы, которые в итоге приведут к кардинальному переформитированию миросистемы. Именно поэтому во главу угла процессов цифровизации, оставляющих последствия в любой сфере жизни государства и социума в современных условиях, целесообразно ставить этические аспекты процессов современной технологической революции. На

государственном и международно-правовом уровнях указанный подход предполагает осознание властными элитами всех без исключения стран мира необходимости «включать главные ценности в наши алгоритмы, создавать такие модели больших данных, которые будут следовать за нашим этическим развитием»[106].

Таким образом, исследование процессов информационного противоборства сквозь призму постнеклассической научной картины мира обусловлено объективной необходимостью, связанной с нынешним переходом мировой политики в ее качественно новое состояние. Основной чертой современности становится усиление конкурентных начал, что знаменует собой возрастающую нелинейность развития мирополитических процессов, выражающуюся в их растущей турбулентности и ускорении. При наращивании нелинейности развития процессов информационного противоборства можно ожидать существенного усиления социально-политических рисков с последующим утверждением своеобразных «обществ риска», когда процессы трансформации мирового порядка могут приобрести существенно более скоротечный характер, а цена таких изменений может оказаться крайне высокой (вплоть до перетекания в «динамический хаос»), несмотря на использование участниками мировой политики прежде всего невоенных сил и средств противоборства.

[106] *О'Нил К.* Убийственные большие данные. Как математика превратилась в оружие массового поражения. М.: АСТ, 2018 С. 266–267.

Глава 2. ЦИФРОВИЗАЦИЯ КАК ФАКТОР ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА И ЕЕ ВЛИЯНИЕ НА РАЗВИТИЕ ПОЛИТИЧЕСКИХ ПРОЦЕССОВ

2.1. Ориентация ведущих государств мира на лидерство в области цифровых технологий

В условиях, когда для достижения доминирующего положения на мировой арене военный потенциал малоприменим ввиду его разрушительных возможностей, набирает силу международная конкуренция по созданию и апробированию в политической практике невоенных средств и методов противоборства. Этот процесс стимулируется происходящей в настоящее время технологической революцией, в частности процессами цифровизации.

С точки зрения основателя и президента Всемирного экономического форума К. Шваба, Четвертая технологическая революция характеризуется размыванием различий между физической, цифровой и биологической сферами. По мнению К. Шваба, уже в скором будущем стремительные технологические прорывы в таких областях, как квантовые вычисления, биотехнологии, искусственный интеллект, робототехника и нанотехнологии, и их синергетический эффект изменят практически все формы человеческой деятельности. Кроме того, отличием новой революции являются экспоненциальная скорость, с которой она разворачивается, и, соответственно, то, как она трансформирует государственную систему, бизнес-структуры и человеческое общество в их нынешнем виде[107].

Таким образом, еще несколько десятилетий назад цифровые технологии считались периферийным инструментом, оказывающим (даже опосредованно) несущественное влияние на развитие политических процессов, то сегодня использование возможностей цифровой среды определяет принципиально новый подход как к созданию, так и к решению проблем международного масштаба. Он базируется на пока еще промежуточных результатах повсеместного внедрения

[107] *Schwab K.* The Fourth Industrial Revolution // World Economic Forum. 2018. URL: https://www.weforum.org/pages/the-fourth-industrial-revolution-by-klaus-schwab (дата обращения: 02.12. 2018).

различных информационных систем во многие сферы хозяйственной деятельности человека. В частности, форсированное развитие и активное внедрение в политическую практику технологий предоставляет субъектам мировой политики дополнительные возможности по оказанию информационно-психологического воздействия на умонастроение населения различных стран мира. Бурно развивающиеся инновации цифровой среды способствуют формированию качественно новой декомпозиции форм и методов межгосударственного взаимодействия, в том числе в ходе информационного противоборства.

В последнее десятилетие ведущие государства мира активизировали усилия по разработке цифровых технологий. Ключевыми направлениями цифрового развития являются системы на базе искусственного интеллекта, связь нового поколения 5G (в будущем – 6G), а также квантовые компьютеры. Эксперты признают, что указанные технологии могут быть использованы для достижения гражданских (прежде всего экономических) и военных целей. Прогнозируется, что в более отдаленной перспективе они будут иметь определяющее значение для укрепления национальной мощи государства. Вместе с тем опасность повсеместного внедрения цифровых технологий в различные сферы жизнедеятельности общества чрезвычайно велика. **Возможно, инновации изменят человеческое восприятие пространства и времени, поскольку способны привнести революционную динамику в скорость обращения информации.**

По мнению американских ученых, к 2040 г. непосредственно «динамика жизни», обусловленная перманентным внедрением едва появляющихся технологий в социальную реальность, может стать серьезной угрозой безопасности человеческой популяции. Однако в свете набравшей силу апробации передовых достижений в различных сферах жизнедеятельности государства, связанной в основном с ожидаемым положительным экономическим эффектом от их применения, специалисты в различных странах мира не успевают оценить и глубоко проанализировать последствия подобных нововведений. Этому

способствует и то, что передовые технологии тесно взаимосвязаны между собой, а результаты их использования во многом имеют синергетический эффект. Данные обстоятельства частично объясняют, почему ученые пока не пришли к консенсусу, насколько серьезными могут быть долгосрочные последствия изменений, обусловленных форсированной цифровизацией, и способно ли общество адаптироваться к таким трансформациям в принципе[108].

Одним из важнейших факторов, который, по прогнозам зарубежных ученых, в среднесрочной перспективе сформирует новую динамику развития информационно-коммуникационного пространства станет внедрение квантовых компьютерных систем, в геометрической прогрессии увеличивающих имеющиеся сегодня вычислительные мощности. В настоящее время квантовые вычисления и квантовые компьютеры являются объектом научных исследований во всем мире. По оценкам специалистов американской «Корпорации РЭНД» (*RAND Corporation*), потребуется еще несколько лет для того, чтобы их потенциал был относительно полностью раскрыт[109].

Квантовые вычисления, хотя и находятся на ранней стадии развития, рассматриваются в числе наиболее перспективных исследований с точки зрения обеспечения национальной безопасности государства в цифровую эпоху. Современные НИОКР на указанном направлении предусматривают разработку квантового компаса, который, как считается, может успешно применяться в военном деле. Успехи в квантовых вычислениях также могут способствовать созданию высокозащищенных каналов шифрованной связи и взлому большинства традиционных шифров. Кроме того, по мнению некоторых ведущих отечественных и зарубежных специалистов в области информационной безопасности и квантовой физики, текущие технологические тренды (например, попытки конструирования межконтинентальных квантовых сетей с помощью

---

[108] What the Speed of Life Means for Security and Society // RAND Corporation. 2019. March 6. URL: https://www.rand.org/blog/rand-review/2019/03/what-the-speed-of-life-means-for-security-and-society.html (дата обращения: 19.05.2020).

[109] Securing Communications in the Quantum Computing Age. Managing the Risks to Encryption // RAND Corporation. 2020. April. URL: https://www.rand.org/pubs/research_reports/RR3102.html (дата обращения: 19.04.2020).

спутника) свидетельствуют в пользу того, что в будущем интернет станет квантовым[110].

Следует отметить и то, что на современном этапе многие развитые государства работают над созданием «безопасных и устойчивых» систем связи 5G, которые они стремятся навязать к использованию другим странам. Считается, что такие системы могут выступить в качестве связующей основы формирования качественно новой цифровой среды[111]. Не меньшее значение в этом контексте имеют технологии виртуальной[112] и дополненной реальности[113], которые, по оценкам специалистов, являются ключом к принципиально новому уровню взаимодействия человека с цифровым миром. В настоящее время данные технологии получили наиболее серьезное развитие на рынках развлечений и маркетинга, но, как отмечают эксперты, это только первая ступень их апробации. Как предполагается, уже в краткосрочной перспективе их внедрение поспособствует существенному повышению производительности и эффективности на промышленных предприятиях в рамках Индустрии 4.0, формированию новых подходов к процессу обучения и повышению уровня образования, качественному повышению уровня здравоохранения и доступности медицинской помощи за счет удаленного присутствия врача. Вместе с этим

---

[110] *Segal Adam.* When China Rules the Web // Foreign Affairs. 2018. September/October. URL: https://www.foreignaffairs.com/issues/2018/97/5 (дата обращения: 01.02.2020).

[111] White House Releases National Strategy for 5G Security // NextGov. 2020. March 25. URL: https://www.nextgov.com/emerging-tech/2020/03/white-house-releases-national-strategy-5g-security/164109/ (дата обращения: 19.05.2020).

[112] Технология виртуальной реальности (Virtual Reality) – это комплексная технология, позволяющая погрузить человека в иммерсивный виртуальный мир при использовании специализированных устройств. Виртуальная реальность обеспечивает полное погружение в компьютерную среду, окружающую пользователя и реагирующую на его действия естественным образом. Фактически виртуальная реальность конструирует новый искусственный мир, передаваемый человеку посредством ощущений: зрения, слуха, осязания и др. В итоге человек может не только взаимодействовать с трехмерной компьютеризированной средой, но и управлять объектами в этой среде.

[113] Технология дополненной реальности (Augmented Reality) – технология, позволяющая интегрировать информацию с объектами реального мира в форме текста, компьютерной графики, аудио и иных представлений в режиме реального времени. Информация предоставляется пользователю с использованием специального индикатора, очков, шлемов дополненной реальности или иной формы проецирования графики для человека (например, смартфон или проекционный видеомэппинг). Технология дополненной реальности позволяет принципиально расширить пользовательское взаимодействие с окружающей средой.

указанные технологии создают новейшие способы коммуникаций и потребительских сервисов, формируют массовые медиа для современного поколения[114].

Большие возможности с точки зрения совершенствования системы государственного управления в различных секторах несет развитие искусственного интеллекта – совокупности технологий, объединяющих базы данных, алгоритмы и вычислительные мощности. К настоящему времени потенциал искусственного интеллекта до конца не изучен, но его уже сейчас называют «новым электричеством». Ожидается, что искусственный интеллект позволит укрепить военную безопасность государства, нарастить эффективность многих секторов экономики, повысить уровень благосостояния населения. Поэтому в последние годы ведущие мировые державы концентрируют внимание на высокоинтеллектуальных разработках, провоцируя развитие новой межгосударственной гонки, в том числе в сфере таких перспективных технологий, как искусственный интеллект и машинное обучение[115].

Одними из первых ставку на лидерство в сфере цифровых технологий сделали Соединенные Штаты Америки. Согласно реализуемой с 2015 г. Третьей инициативой оборонных инноваций (*Defense Innovation Initiative*), разработка инструментария для ведения противоборства «нового типа» стала для Вашингтона основной задачей в условиях стремительной цифровизации. По замыслу разработчиков указанной концепции все высокие технологии в социальной, когнитивной и организационной сферах получили двойное назначение. Одновременно была поставлена задача максимально эффективно использовать преимущества Америки в таких областях знаний, как большие данные, робототехника, синтетическая биология, исследования человеческого

[114] Дорожная карта развития «сквозной» цифровой технологии «Технология виртуальной и дополненной реальности» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. 2019. URL: https://digital.gov.ru/uploaded/files/07102019vrar.pdf (дата обращения: 18.06.2020).

[115] См. подр.: *Селянин Я.В.* Технологическое лидерство, роль государства и неоднозначность цифр в высокотехнологичных областях на примере военно-промышленной политики США в области высокопроизводительных вычислений // Проблемы национальной стратегии. 2019. № 5. С. 137–167.

мозга, управление социальными массами и пр. Конечная цель доктрины сформулирована просто: к 2030 г. в Соединенных Штатах должна быть создана такая система уникальных технологий, которую ни одна страна в мире не сможет скопировать и, тем более, применить[116].

Западные специалисты отмечают, что курс США на достижение технологического превосходства обусловлен прежде всего их нацеленностью на удержание доминирующего положения на мировой арене. Так, гегемония в глобальной сети Интернет считается в Соединенных Штатах Америки не менее приоритетной задачей, чем контроль над космическим, водным, воздушным и космическим пространством. При этом Америка считает своей геополитической миссией сохранение за собой статуса мирового интернет-лидера, обеспечивающего доступ в киберпространство всем жителям Земли.

Безусловно, подобное целеполагание объясняется не столько гуманистическими соображениями, сколько стремлением вовлечь как можно большее количество людей в поле информационного влияния США. Исключительная популярность американских интернет-сервисов косвенно способствует улучшению внешнего имиджа страны, а, следовательно, и росту ее политического влияния на мировой арене. В Америке ясно сознают, что современные достижения в соответствующей области открывают качественно новые возможности управления социальными массами практически любой размерности. Возможности цифровой реальности могут быть использованы для зондажа и даже моделирования политической, экономической, социальной обстановки в отдельных странах и регионах мира.

Например, перспективным инструментом анализа социально-политической динамики американские специалисты называют Глобальную базу данных событий, языка и настроения (*The Global Database of Events, Language, and Tone*). Она создана ученым К. Литару при поддержке Джорджтаунского университета (*Georgetown University*) и Управления перспективных исследований МО США.

[116] Experimental evidence of massive-scale emotional contagion through social networks // PNAS. URL: http://www.pnas.org/content/111/24/8788.full (дата обращения: 19.02.2020).

Этот проект представляет собой базу данных о мировых политических событиях (более 200 млн событий, восходящих к 1979 году). Путем анализа открытых источников информации в интернете с использованием компьютерного автоматизированного метода определения отношения индивида к мировым новостям (3 млн узлов, интегрированных с 42 млн информационных ссылок) создан каталог социального поведения и убеждений населения по всему миру.

С использованием Глобальной базы данных событий, языка и настроения появилась возможность отследить уровень социально-политической напряженности в заданном регионе мира в текущий момент и с прогнозом на будущее. С этой целью ее разработчики провели анализ вооруженных конфликтов последних 50 лет. На основе собранной информации они предложили классификацию основных социальных групп: «малочисленная элита» (не более 1–3 %), «социально-политически пассивное население» (75–85 %), «социально-политически активное население» (10–20 %). Показателями, свидетельствующими о вероятности кризиса, специалисты назвали острое недовольство «социально-политически активной части населения» действующей политической элитой и резкое снижение уровня жизни населения после его длительного повышения. Следует также отметить, что указанная система использовалась для анализа и прогнозирования гражданских выступлений, государственных переворотов и вооруженных конфликтов в период 2014–2016 гг. Эффективность прогнозов составила около 85 %, что для событий социального порядка является большим достижением[117].

С учетом масштабов прогнозируемых возможностей и рисков американские государственные ведомства регулярно переформулируют национальные приоритеты страны в области отдельных аспектов цифрового развития страны. Так, в ноябре 2018 г. Национальный научный фонд США заявил о досрочном обновлении в 2019 г. Стратегического плана исследований и

---

[117] См. подр.: *Виловатых А.В., Хряпин А.Л.* Современные разработки в области социального управления: опыт Соединенных Штатов Америки // Информационные войны. 2019. № 4 (52). С. 45–49.

разработок в области кибербезопасности от 2016 г., который был рассчитан на десятилетнюю перспективу. Этот документ призван служить основой для координации проектов в указанной области, обеспеченных госфинансированием, в том числе касающихся образовательных программ и улучшения положения на рынке труда[118].

В качестве другого примера можно привести то, что в июле 2018 г. Белый дом выпустил меморандум для глав государственных агентств и ведомств о бюджетных приоритетах США в сфере НИОКР на 2019–2020 гг. В данном документе первым из трех высших национальных технологических приоритетов был назван искусственный интеллект[119].

В настоящее время настоящее время Соединённые Штаты Америки считаются лидером в области развития технологий искусственного интеллекта. В качестве рубежного события, предопределившего форсированное развитие искусственного интеллекта в США, специалисты считают письмо бывшего главы Пентагона Дж. Мэттиса, которое он адресовал Д. Трампу. В этом обращении военачальник призвал американского президента «вдохновить усилия всей страны на то, чтобы США стали мировым лидером в вопросах не только обороны, но и глубокой трансформации всех аспектов жизни человека на Земле»[120].

В принятых со времени опубликования указанного письма доктринальных документах США последовательно подчеркивается, что искусственный интеллект является важной составляющей сохранения глобального доминирования страны. Перед американским политическим и военным сообществом поставлена задача

---

[118] National Science Foundation requests input on updating cyber research and development plan // Inside Cybersecurity. 2018. November 12. URL: https://insidecybersecurity.com/daily-briefs/national-science-foundation-requests-input-updating-cyber-research-and-development-plan (дата обращения: 20.02.2020)

[119] Например, расходы на исследования автономии дронов, командного взаимодействия человек–дрон и роя в 2019 г. Составили примерно 865,9 млн долл. в сравнении с 833,8 млн долл. в 2018 и 549 млн долл. в 2017 г. Бюджет для программы флота "Беспилотные и автономные системы" увеличился с 48,4 млн до 60,1 млн долл. Финансирование ключевой для Пентагона программы Maven увеличилось практически вдвое – с 60 млн долл. в 2018 г. до 109 млн долл. в 2019 г.

[120] Artificial Intelligence and International Security // Center for a New American Security. 2018. July. URL: https://www.cnas.org/publications/reports/artificial-intelli gence-and-international-security (дата обращения: 20.04.2020).

обеспечить непревзойденное технологическое превосходство страны в сфере разработок на базе ИИ, и оно жестко следует этой линии. В 2018 г. в США был учрежден Объединённый центр искусственного интеллекта (*Joint Artificial Intelligence Center),* основной целью которого явилась выработка национального подхода к развитию искусственного интеллекта[121]. Уже в начале 2019 г. американский президент подписал Национальную инициативу по развитию искусственного интеллекта, важными направлениями реализации которой стали:

– проведение фундаментальных прикладных исследований;

– формирование ресурсной базы в области ИИ;

– установление стандартов использования искусственного интеллекта;

– подготовка специалистов, владеющих компетенциями в сфере ИИ;

– выпуск высокоинтеллектуальной продукции с целью обеспечить неприкосновенность преимуществ США на внешних рынках.

Примечательно, что, согласно приведенному документу, компетентные государственные органы Соединенных Штатов были вынуждены вдвое ускорить реализацию всех уже запущенных проектов в области развития технологий искусственного интеллекта. Зарубежные аналитики связали этот шаг с форсированным развитием высокоинтеллектуальных разработок в Китае[122].

К реконфигурации системы распределения приоритетов в области технологического развития, призванной поспособствовать удержанию доминирующего положения страны на мировой арене, привлечены влиятельные экспертные структуры США. Являясь крупным звеном американской внешнеполитической пропаганды, их представители в большинстве случаев связывают такую необходимость с усиливающимся международным влиянием новых и укрепляющихся центров силы. Например, в конце 2018 г. американский Центр стратегических и международных исследований (*Center for Strategic and*

[121] China in "full-speed" push for "intelligentized" weapons to defeat U.S. // Geostrategy-Direct. 2018. May 15. URL: http://geostrategy-direct-subscribers.com/china-infull-speed-push-for-intelligentized-weapons-to-defeat-u-s/ (дата обращения: 20.04.2020).

[122] Artificial Intelligence and National Security // Congressional Research Service. 2019. URL: https://fas.org/sgp/crs/natsec/R45178.pdf (дата обращения: 20.04.2020).

International Studies), осуществляющий научно-аналитическую деятельность в том числе по заказу Конгресса и Государственного департамента США, опубликовал доклад под названием «Когнитивный эффект и конфликт государств в киберпространстве».

В указанном документе его автор, вице-президент Центра Дж. Льюис отмечает, что «желание конкурентов Вашингтона разрушить ориентированную на США систему международных отношений и достичь регионального доминирования привели к разработке стратегий, тактик и технологий, которые уже в скором будущем могут подорвать американское лидерство на мировой арене»[123]. По словам аналитика, такие меры якобы «подтачивают основы демократического управления на Западе». При это, по словам Дж. Льюиса, центральный элемент российской военной доктрины отражает сущность взглядов руководства РФ на войны нового поколения. Его основу составляют операции по формированию у международной общественности определенного когнитивного эффекта, навязыванию чуждого образа мышления оппонентам Соединенных Штатов и странам, придерживающимся так называемой политики военного нейтралитета[124].

В последние годы США все активнее используют возможности внедрения передовых технологий в практику ведомств, обеспечивающих национальную безопасность. В Вашингтоне связывают это с тем, что в условиях нарастания нелинейных методов противоборства Соединённые Штаты должны выйти на принципиально новые способы достижения технологического превосходства над вероятным противником. Особое внимание в этом контексте было уделено потенциалу применения машинного обучения в военном деле и в целом

[123] *Lewis James.* Cognitive Effect and State Conflict in Cyberspace // Center for Strategic and International Studies. 2018. September 26. URL: https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace (дата обращения: 20.08.2019).

[124] Ibid.

внедрению возможностей искусственного интеллекта в повседневную практику Минобороны[125].

Следует отметить и то обстоятельство, что в последние годы власти Соединенных Штатов активизировали практику навязывания национальным технологическим гигантам (*Apple, Google, Amazon, IBM*) ограничений на торговлю с зарубежными конкурентами. В частности, предпринимаемые США попытки создания административных завалов на перспективных технологических направлениях демонстрируют давление на крупных китайских производителей. Об этом, в частности, свидетельствует развернутая Вашингтоном информационная компания на китайскую компанию «Хуавей» (*Huawei*), планирующую добиться лидерства во внедрении связи 5G, соответствующего оборудования и программного обеспечения, получив тем самым долгосрочные преимущества на мировом рынке технологий.

В свою очередь, в Китае сфера цифровых технологий воспринимается как область, форсированное развитие которой может бросить вызов глобальной гегемонии Соединенных Штатов Америки, не создавая при этом военной конфронтации между странами. Современная цифровая стратегия КНР базируется на нескольких концептуально связанных документах: Национальной стратегии информатизации, рассчитанной на 2016–2020 гг., Международной стратегии сотрудничества в киберпространстве от 2017 г., «Сделано в Китае 2025», «Интернет +» и пр.[126]. Они охватывают практически все сферы китайской экономики, военной сферы и социального сектора, и взаимно не противоречат друг другу, в отличие от многих документов США[127].

---

[125] *Sherman J.* Griffin looking beyond guns, bombs to ensure future U.S. military superiority // Inside Defense. 2018. October 31. URL: https://insidedefense.com/inside-pentagon/griffin-looking-beyond-guns-bombs-ensure-future-us-military-superiority (дата обращения: 21.02.2020).

[126] См. напр.: International Strategy of Cooperation on Cyberspace // Ministry of Foreign Affairs of the People's Republic of China. 2017. March 1. URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (дата обращения: 24.04.2020).

[127] *Harding Brian.* China's Digital Silk Road and Southeast Asia // Center for Strategic and International Studies. 2019. February 15. URL: https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia. (дата обращения: 24.04.2020).

Зарубежные эксперты отмечают, что успех Китая в цифровизации может иметь решающий вес в способности Поднебесной продвигать собственный, альтернативный американскому проект мирового порядка. Соответственно, особенное внимание в Китайской Народной Республике уделяется цифровому измерению инициативы «Пояс и путь» (*Digital Silk Road*)[128].

Еще в 2016 г. немецкий синолог С. Хайльман, возглавляющий германский Институт изучения политики Китая им. Герхарда Меркатора (*MERICS*), ввел термин «цифровой ленинизм». Политолог ввел его для описания методов использования Китаем достижений цифровой эпохи для контроля над внутриполитической обстановкой и технического усовершенствования традиционной («авторитарной») модели государственного управления. При этом было сделано предположение о том, что крупные прорывы на данном направлении позволили бы КНР создать предпосылки для проекции своего влияния вовне в условиях происходящей технологической революции. Эксперт отмечал, что «цифровой ленинизм» — это авторитаризм, основанный на больших данных и опирающийся на информационно-коммуникационные технологии. По его мнению, именно цифровой ленинизм якобы может поспособствовать становлению в КНР и вокруг нее совершенно новой модели «тоталитарного» будущего[129].

В псоледние годы большое внимание в экспертных публикациях западных политологов уделяется определению потенциала усиления репрессий внутри Китая в качестве побочного эффекта применения руководством КПК цифровых технологий для обеспечения безопасности. Немецкий исследователь С. Хайльман рассматривал такой тип репрессий внутри КНР как предпосылку попыток Пекина

---

[128] Vision and Actions on Jointly Building Silk Road Economic Belt and 21stCentury Maritime Silk Road // Reconasia-production. 2015. March. URL: https://reconasia-production.s3.amazonaws.com/media/filer_public/e0/22/e0228017-7463-46fc-9094-0465a6f1ca23/vision_and_actions_on_jointly_building_silk_road_economic_belt_and_21st-century_maritime_silk_road.pdf (дата обращения: 20.02.2020).

[129] *Heilmann Sebastian.* Leninism Upgraded: Xi Jinping's Authoritarian Innovations // Mercator Institute for China Studies. 2016. URL: https://www.merics.org/sites/default/files/2018-03/Heilmann_Leninism_Upgraded_China_Economic_Quarterly_Dec.2016.pdf (дата обращения: 01.02.2020).

экспортировать «нечестное» использование достижений цифровизации для трансформации международного порядка в интересах Поднебесной. Платформой для такой политики он признал цифровое измерение Шелкового пути.

Примечательной работой, посвященной развитию цифровых технологий в КНР, является опубликованная в конце 2018 г. статья американского исследователя Х. Шэня из Университета Карнеги — Меллона *(Carnegie Mellon University).* В этой концептуальной научной публикации представлен анализ целей китайского руководства при форсированном продвижении Цифрового шелкового пути, а также обозначена роль цифровых технологий в стратегическом планировании Китая.

Аналитические наработки исследователя Х. Шэня представляют несомненный интерес с точки зрения осмысления приоритетов китайцев в современной турбулентной международной среде, где понимание мотивов партнеров и соперников имеет важное значение для выработки политических ответных мер. Данная статья приоткрывает суть замысла Поднебесной, которая в стремлении к успешной реализации цифрового компонента нового Шелкового пути придает все большее значение достижению технологических прорывов и развитию цифровой инфраструктуры в условиях трансформации миропорядка.

Многие американские экспертно-аналитические структуры обращают внимание на такой аспект цифровизации в КНР, как создание сотовых сетей нового поколения (5G). В частности, по мнению аналитиков Центра стратегических и международных исследований *(Center for Strategic and International Studies),* эти сети и широкий спектр приложений для них окажутся центральным объектом новой конкуренции между мировыми державами на новом этапе развития. Они указывают, что в информационную эпоху лидерство в инновациях станет «источником экономической мощи и военной безопасности».

Кроме того, инфраструктура сетей 5G может рассматриваться в качестве краеугольного камня процессов цифровизации[130].

Геополитические последствия внедрения сетей связи 5G, продвигаемых КНР, находятся в фокусе внимания аналитиков международной консалтинговой компании «Группа Евразия» (*Eurasia Group).* В Белой книге, опубликованной данной влиятельной групой аналитиков в конце 2018 г., представлено состояние и тренды конкуренции между различными телекоммуникационными корпорациями с целями установления стандартов и получения патентов, которые обеспечат основу для распространения 5G.

Авторы указанного документа констатируют, что в случае ужесточения соперничества между Соединенными Штатами и Китаем в мире могут возникнуть две отдельные экосистемы 5G, одна из которых будет формироваться под эгидой Вашингтона, а другая — Пекина. По оценкам политологов, вероятная бифуркация процесса развития сетей 5G увеличит риск того, что глобальная технологическая экосистема прекратит существование и уступит место двум политически разделенным и потенциально не стыкующимся техносферам[131].

Примечательно, что в более поздних работах американских экспертов на эту тему приводятся убедительные факты, свидетельствующие, что риски возникновения в технологической области подобного «железного занавеса» становятся все более реальными[132].

Исследуя проблематику цифрвоизации в КНР, специалисты американского Тихоокеанского форума *(Pacific Forum)* обращают внимание на такой момент, как разное видение Вашингтоном и Пекином модели миропорядка, утвердившегося

---

[130] *Lewis James.* How Will 5G Shape Innovation and Security: A Primer // Center for Strategic and International Studies. 2018. December 6. URL: https://www.csis.org/analysis/how-5g-will-shape-innovation-and-security (дата обращения: 01.02.2020).

[131] *Triolo Paul, Allison Kevin, Brown Clarise.* Eurasia Group White Paper: The Geopolitics of 5G // Eurasia Group. 2018. November 15. URL: https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public%281%29.pdf (дата обращения: 03.02.2020).

[132] *Prasso Sheridan.* China's Digital Silk Road is Looking More Like an Iron Curtain // Bloomberg. 2019. January 10. URL: https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-likean-iron-curtain (дата обращения: 03.02.2020).

после Второй мировой войны. Но именно этот аспект, по их оценкам, и побуждает КНР делать ставку на Цифровой шелковый путь как «основу будущего могущества». Реализуя проекты в области цифровых технологий, Китай якобы стремится достичь стратегических целей и добиться способности проецировать нетрадиционный до недавнего времени компонент национальной мощи (цифровые технологии) за рубеж[133].

Структурная перестройка Поднебесной из «фабрики мира» в высокотехнологичную державу вплотную охватывает такие сферы, как нанотехнологии, квантовые вычисления, работу с большими данными, облачные хранилища, робототехнику и пр. Пекин придерживается стратегии «приоткрытой двери», стремясь заполучить новейшие технологии у передовых государств и их лучших специалистов. Одновременно он создает препятствия для закрепления иностранных компаний на внутреннем рынке КНР и в сферах собственного влияния за рубежом. Но в случае «зеленого света» обязательным условием выхода стороннего бизнеса на китайский рынок является передача ими технологий. Следует отметить и то, что китайские власти стремятся обеспечить распределение международных рынков между компаниями из Поднебесной таким образом, чтобы они не конкурировали между собой. В целом проповедуется своеобразный технонационализм, предполагающий агрессивную защиту интересов Китая в сферах торговли и услуг на внутреннем и внешнем рынках[134].

В настоящее время Китай является мировым лидером в сфере фундаментальных и прикладных квантовых исследований. В 2016 г. Пекин вывел на орбиту первый в мире спутник квантовой связи «Мо-Цзы» (*QUESS)*, который дополняет созданную в Китае систему квантовой коммуникации между Пекином и Шанхаем. В 2017 г. ученые из Китайского научно-технологического

---

[133] *Cheney Clayton.* China’s Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism // Pacific Forum. 2019. July. URL: https://www.pacforum.org/sites/default/files/issuesinsights_Vol19%20WP8FINAL.pdf (дата обращения: 03.02.2020).

[134] *Smith-Goodson Paul.* Quantum USA Vs. Quantum China: The World's Most Important Technology Race // Forbes. 2019. October 10. URL: https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#6c1f5f6472de (дата обращения: 22.04.2020).

университета в Шанхае разработали новый прототип квантовой вычислительной машины. В том же году в стране начато строительство Национальной лаборатории квантовой информатики. В 2018 г. китайский квантовый спутник впервые передал реальные данные по каналу, защищенному квантовым шифрованием, связав города, расстояние между которыми составляет 7,6 тыс. километров. В настоящее время в КНР идут разработки квантового компьютера, который должен превзойти помощности существующие ЭВМ. Цель страны — иметь развитую инфраструктуру квантовой связи к 2030 г.

В целом эксперты сходятся во мнении о том, что Пекин существенно опередил конкурентов в области квантовых вычислений. Вашингтон сосредоточен на прикладных квантовых исследованиях (*Qubitekk, Quantum Xchange*, лаборатория в Университете *Stony Brook*). В Европе работа ведется в основном над квантовым шифрованием, но менее активно, чем в Китае или в США. В обозримом будущем КНР, видимо, сохранит лидерство в области квантовых вычислений[135].

Несомненно, важнейшей точкой притяжения внимания китайских государственных деятелей и специалистов являются и разработки в сфере искусственного интеллекта. Опубликованный КНР в 2018 г. план развития искусственного интеллекта свидетельствует о том, что Китай рассчитывает утвердиться в качестве «научно-технической сверхдержавы», глобального центра инноваций с развитой коммерческой индустрией во всех цифровых секторах, пионера в создании промышленных роботов[136]. К окончанию 2020 г. предполагается привести разработки и применение в стране технологий искусственного интеллекта в соответствие с современными ведущими мировыми тенденциями, заложив основы национальной индустрии искусственного

---

[135] *Smith-Goodson Paul.* Quantum USA vs. Quantum China: The World's Most Important Technology Race // Forbes. 2019. October 10. URL: https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#6c1f5f6472de (дата обращения: 01.02.2020).

[136] *Bremmer Ian, Thompson Nicholas.* The AI Cold War That Threatens Us All // Wired Magazine. 2018. October 23. URL: https://www.wired.com/story/ai-cold-war-china-could-doom-us-all/ (дата обращения: 20.04.2020).

интеллекта с объемом производства свыше 20 млрд долларов. Уже к 2025 г. в Пекине намерены превратить искусственный интеллект в главную движущую силу индустриальной модернизации и экономических преобразований, укрепления государственной обороноспособности, внешней и внутренней безопасности, образования, медицины. Планируется, что к 2030 г. Китай основным мировым центром инноваций в сфере искусственного интеллекта, что позволит кардинально повысить возможности страны в использовании «мягкой силы» для эффективного продвижения национальных интересов на пространстве Азиатско-Тихоокеанского региона и на международном уровне в целом[137].

Наращивание усилий руководства КНР по формированию инфраструктуры и нормативно-правовой базы развития технологий искусственного интеллекта указывает на то, что искусственный интеллект рассматривается китайским руководством как основа для реализации долгосрочной экономической и военной стратегии. С целью более быстрого превращения в мирового лидера в сфере цифровых технологий, в стране создаются специальные рабочие группы, некоторые из которых получают статус центральных комиссий и напрямую подчиняются председателю КПК. Такой подход обосновывается необходимостью быстрее и эффективнее реализовывать решения, принятые высшим руководством страны, относящиеся к динамичной сфере цифровизации. Кроме того, согласно принятому Госсоветом КНР в сентябре 2019 г. плану, в стране учреждаются «экспериментальные зоны инновационного развития искусственного интеллекта нового поколения», которые призваны стать фундаментом развития этой отрасли. Работа данных зон организована по принципу открытых инновационных платформ. Предполагается, что такие экспериментальные кластеры поспособствуют поиску и отработке оптимальных моделей взаимодействия всех звеньев цепи развития цифровых технологий – от фундаментальных и

[137] *Cheney Clayton.* China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism // Pacific Forum. 2019. July. URL: https://www.pacforum.org/sites/default/files/issuesinsights_Vol19%20WP8FINAL.pdf (дата обращения: 25.02.2020).

прикладных НИОКР до их промышленного освоения – с учетом текущих и перспективных потребностей страны[138].

В КНР сознают, что стремительное развитие и внедрение в практику производства технологий искусственного интеллекта вносит неоценимый вклад в наращивание геополитической мощи государства. Как отмечатеся, в среднесрочной перспективе применение искусственного интеллекта в интересах национальных вооруженных сил станет определяющим фактором достижения военного превосходства над противником. В частности, китайские спеицалисты указывают на то, что развитие технологий искусственного интеллекта имеет обширный и еще не до конца исследованный потенциал с точки зрения обеспечения кибернетической безопасности. Это целесообразно рассматривать в контексте того, что киберпространство уже рассматривается США и их союзниками в качестве новой операционной среды[139].

Важно отметить и то, что в последние годы китайские государственные предприятия и крупные частные технологические корпорации начали претендовать на доминирующие позиции в поставке на мировой рынок подводных и наземных оптоволоконных кабелей, которые способны передавать большие объемы информации посредством интернета. Согласно оценкам германского Института изучения политики Китая им. Герхарда Меркатора (*MERICS*), участие КНР в проектах прокладки подводных оптоволоконных кабелей возросло с 6 % в 2012—2015 гг. до 20 % в 2016—2019 гг.[140] В частности, в Юго-Восточной Азии китайские корпорации уже завершили более десятка таких проектов, и еще около 20 находятся в процессе реализации[141].

---

[138] *Wright Nicholas.* How Artificial Intelligence Will Reshape the Global Order // Foreign Affairs. 2019. URL: https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order?cid=nlc-fa_twofa-20180802 (дата обращения: 22.04.2020).

[139] *Segal Adam.* When China Rules the Web // Foreign Affairs. 2018. September/October. URL: https://www.foreignaffairs.com/issues/2018/97/5 (дата обращения: 03.02.2020).

[140] China's Digital Rise. Challenges for Europe// MERICS. 2019. May. URL: https://www.merics.org/en/events/chinas-digital-rise-challenges-europe (дата обращения: 02.02.2020).

[141] *Harding Brian.* China's Digital Silk Road and Southeast Asia // Center for Strategic and International Studies. 2019. February 15. URL: https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia. (дата обращения: 02.02.2020).

Китай постепенно расширяет масштабы своей оптоволоконной кабельной сети, завоевывая доминирующее положение в Азиатско-Тихоокеанском регионе. Хотя в настоящее время самый большой объем китайских инвестиций в этом производственном секторе приходится на АТР, корпорации из КНР не намерены останавливаться на достигнутом и ориентируются на рынки далеко за пределами этого региона. Китайские компании (*Huawei, ZTE*) подписали соглашения о монтаже оптоволоконных сетей по всему миру, включая Белиз, Эквадор, Гвинею, Соломоновы острова и пр. Попытки заключения новых соглашений продолжаются, и Китай явно стремится занять лидирующие позиции как поставщик оптоволоконных кабелей в Африку и на Ближний Восток[142].

По оценкам американских экспертов, создание и обслуживание китайцами оптоволоконных кабельных сетей имеет геополитическую подоплеку и создает ряд рисков для международной информационной безопасности. Они, в частности, отмечают, что Китай может контролировать и перенаправлять трафик данных, а также прерывать интернет-соединение для некоторых из них. В Вашингтоне превалирует мнение о том, что в перспективе Китай однозначно будет использовать возможности оптоволоконных кабельных сетей в собственных национальных интересах. Между тем в самом Китае отмечают, что контроль над этими сетями является естественным средством защиты государственных коммуникаций от иностранных разведывательных служб, что имеет решающее значение для обеспечения информационной безопасности страны[143].

Важной составляющей строительства развития цифровой инфраструктуры в Китае является создание центров обработки данных. Китайские инвестиции в этой области пока в основном идут на оборудование таких центров внутри страны, но они развертываются и за рубежом. Считается, что финансирование

---

[142] *Patrick Stewart, Feng Ashley.* Belt and Router: China Aims for Tighter Internet Controls With Digital Silk Road // Council on Foreign Relations. 2018. July 2. URL: https://www.cfr.org/blog/belt-and-router-china-aimstighter-internet-controls-digital-silk-road (дата обращения: 04.02.2020).

[143] *Siddiqui Sabena.* BRI, BeiDou and the Digital Silk Road // Asia Times. 2019. April 9. URL: https://www.asiatimes.com/2019/04/opinion/bri-beidou-and-the-digital-silk-road/ (дата обращения: 02.02.2020).

центров обработки данных играет важную роль в содействии глобальной экспансии технологических компаний из Поднебесной.

Как отмечает основатель китайской фирмы «Алибаба» (*Alibaba*) Дж. Ма, когда государственные предприятия и бизнес-сообщество КНР расширяют финансирование центров обработки данных за рубежом, они преследуют цель «проложить дорогу и построить мост» (*paving the road and building the bridge*) для других китайских компаний и их зарубежных операций, особенно для фирм, профилирующихся на программном обеспечении. Продолжая свою мысль, Джек Ма подчеркивает, что вскоре «мир будет восхищаться Китаем не только ввиду роста его ВВП, но и благодаря тому, что и в каких объемах Китай делает для других стран»[144].

В этом контексте зарубежные аналитики указывают, что политика Поднебесной, требующая от иностранных корпораций сохранения пользовательских данных в Китае, нацелена прежде всего на увеличение объема информации, доступной для китайских властей (так называемая политика локализации данных). В последнее время такая политика вызывает все большие опасения у европейских бизнес-партнеров КНР в связи с отсутствием гарантии соблюдения принципа конфиденциальности, и это беспокойство активно «подогревается» политическим сообществом в конкурирующих с КНР странах.

В целом анализ китайской политики в сфере цифровизации последних лет свидетельствует, что в отличие от США при определении приоритетов технологического развития Пекин обращает основное внимание на экономическую трансформацию всех сфер жизнедеятельности государства, а не на военные разработки. По нашему мнению, в пользу данного факта свидетельствует то, что Китай активно занимается созданием цифровой инфраструктуры – причем как на территории страны, так и за ее пределами. В фокусе внимания китайских бизнесменов, поддерживаемых государством,

---

[144] *Hong Shen.* Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative // International Journal of Communication. № 12. 2018. URL: https://ijoc.org/index.php/ijoc/article/view/8405/2386 (дата обращения: 04.02.2020).

находятся сотовые сети нового поколения, оптоволоконные кабели и центры обработки данных. Кроме того, признавая важность международной экономической взаимозависимости, как значимого фактора социально-политической стабильности в самой Поднебесной, Китай делает акцент на электронной торговле посредством создания цифровых зон свободной торговли. Примечательно, по мнению специалистов, что сегодня КНР уже в состоянии задавать новые мировые тенденции в указанных областях[145].

Технологический рывок Китая в области цифровизации предполагает опору руководства КПК на действующую в стране плановую систему управления и тесное взаимодействие китайского государственного и частного секторов. Для этого в 2019 г. в КНР создана «национальная команда» по разработкам в сфере искусственного интеллекта, куда вошли известные китайские технологические гиганты. В результате такого замысла дать точную оценку масштабам и глубине связей между крупными технологическими предприятиями, инновационными стартапами, венчурными фондами, местными властями и военными ведомствами КНР весьма непросто. Причем, как отмечают американские эксперты, США существенно недостает подобной кооперации[146].

Считается, что именно благодаря выстроенной бизнес-модели КНР она сумела достичь успехов не только в исследованиях современных передовых технологий, в частности искусственного интеллекта, но и внедрении высокоинтеллектуальных решений в производственные процессы, выстроить лучшие в мире системы электронной торговли и электронной медицины, запустить выпуск беспилотных автомобилей и пр. В настоящее время 9 из 20

---

[145] См. подр.: *Комиссина И. Н.* Современное состояние и перспективы развития робототехники в Китае // Проблемы национальной стратегии. 2020. № 1. С. 123–146.

[146] *Cheney Clayton.* China’s Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism // Pacific Forum. 2019. July. URL: https://www.pacforum.org/sites/default/files/issuesinsights_Vol19%20WP8FINAL.pdf (дата обращения: 22.04.2020).

крупнейших цифровых компаний уже принадлежат китайскому бизнесу, тогда как оставшиеся 11 – американцам[147].

Подтверждением знаковой роли цифровых технологий в долгосрочной стратегии развития Поднебесной является также резкий рост числа фундаментальных и прикладных исследований китайских ученых по данной проблематике. В обозримом будущем КНР, видимо, продолжит форсировать научно-технологическое развитие, способствовать региональной экономической взаимозависимости, инвестировать в цифровую инфраструктуру. **Не исключено, что комплексный подход действующего руководства Китая к развитию цифровых технологий с учетом соблюдения Пекином международно-правовых норм и принципов, позволит ему в более отдаленной перспективе потеснить США с позиций технологического лидера.**

Курс Китая на форсированное технологическое развитие вызывает большую тревогу в Соединенных Штатах Америки. Американское экспертное сообщество с беспокойством указывает, что за все время президентского срока Д. Трампа его администрация так не выработала комплексную стратегию противодействия КНР в цифровой сфере. Например, данному вопросу посвящен доклад продемократического Центра за новую американскую безопасность, опубликованный в конце января 2020 г.[148]

Как отмечается в научном докладе, реакция Белого дома касается лишь отдельных, наиболее заметных эпизодов глобального «китайского цифрового наступления» (например, активности Пекина в создании систем связи нового поколения 5G). Во избежание размывания глобальной мощи США, во многом базирующейся на технологическом фундаменте, специалисты рекомендуют вашингтонской элите в ближайшее время разработать и приступить к реализации комплексной долгосрочной стратегии, нацеленной на противодействие

---

[147] *Aum Dan, Silverberg Elliot*. Opportunity for the U.S. to Show Global Leadership // National Bureau of Asian Research. 2020. March 18. URL: https://www.nbr.org/publication/opportunity-for-the-u-s-to-show-global-leadership/ (дата обращения: 21.04.2020).

[148] Rising to the China Challenge // Center for New American Security. 2020. January 28. URL: https://www.cnas.org/publications/reports/rising-to-the-china-challenge (дата обращения: 24.05.2020).

наращиванию технологического могущества КНР. Она должна включать в себя, как минимум, три компонента.

Во-первых, по мнению экспертов, следует усилить роль США в развитии цифровой инфраструктуры в отдельных регионах мира, в частности АТР. В целях реализации крупных инфраструктурных проектов с союзниками и партнерами страны предлагается учредить так называемый фонд цифрового развития. Кроме того, для увеличения конкурентных преимуществ американских компаний, присутствующих на азиатских рынках, отмечается необходимость обращения к ресурсам созданной в августе 2019 г. Финансовой корпорации международного развития США (*U.S. International Development Finance Corporation*), а также Экспортно-импортного банка США (*U.S. Export-Import Bank*).

Во-вторых, рекомендуется создать дополнительные стимулы для укрепления позиций частного сектора в тех сферах цифровизации, где угроза для Соединенных Штатов отстать от Китая особенно велика. Американские аналитики считают важным использовать широкий набор мер (субсидирование НИОКР, налоговые льготы, государственные закупки и пр.) для создания экосистемы, поощряющей конкуренцию и инновационные проекты. Одновременно давление на китайские компании, не соответствующие американским представлениям о «честной конкуренции», должно сохраняться и расширяться.

Наконец, как отмечают специалисты Центра за новую американскую безопасность, США целесообразно более активно противодействовать продвижению набирающей популярность в развивающихся государствах, и, более того, также странах Европы российско-китайской концепции «суверенного интернета». Большой акцент американские аналитики делают также на поощрении развития технологий, способных преодолевать вводимые иностранными государствами ограничения доступа пользователей к сайтам, социальным сетям, базам данным и другим источникам информации. Одновременно, по мнению экспертов, США следовало бы обратить пристальное внимание на «развитие демократии и гражданского общества, продвижение

свободы СМИ и защиту прав человека», в частности в союзных им государствах по другую сторону Атлантики. Кроме того, специалисты утверждают, что для сохранения имеющихся преимуществ Америке крайне важно поддерживать научные и коммерческие обмены с европейскими, канадскими и израильскими специалистами[149].

Как указывают представители американского Управления перспективных исследований в сфере разведки (*IARPA*), цифровая мошь Китая нарастает стремительнее, чем могли ожидать в Пентагоне. При этом они прогнозируют, что развитие индустрии искусственного интеллекта в КНР встретит меньше барьеров, чем в Соединенных Штатах Америки, особенно с точки зрения возможности сопряжения потенциала военного и коммерческого секторов. Это обстоятельство во многом определяет объем работы для американских военных разработчиков на обозримую перспективу, поскольку риски конфронтации между конкурентами в будущем, вероятно, повысятся[150].

В США высказываются опасения, что успех Пекина в сфере развития цифровых технологий и их экспорта за рубеж может подорвать способность Вашингтона создавать долговременные альянсы, причем даже в странах трансатлантического сообщества. Первым свидетельством этого якобы уже является всплеск недемократических настроений во многих европейских государствах. Причем Китай не только продвигает концепцию цифрового суверенитета (по определению западных политологов – «цифрового авторитаризма») вовне, но и создает законодательный базис для его утверждения.

Можно предположить, что в случае приближения сценария достижения КНР превосходства в области развития и внедрения в практику человеческой жизнедеятельности инновационных цифровых технологий под угрозой окажется не только складывающийся международный режим управления цифровыми

---

[149] Rising to the China Challenge // Center for New American Security. 2020. January 28. URL: https://www.cnas.org/publications/reports/rising-to-the-china-challenge (дата обращения: 24.05.2020).

[150] *Bertuca T.* Intel research chief wants to maintain "healthy" U.S. lead over China in AI race // Inside Defense. 2018. 14 March. URL: https://insidedefense.com/daily-news/intel-research-chief-wants-maintain-healthy-us-lead-over-china-ai-race (дата обращения: 21.02.2020).

ресурсами, но даже роль Америки как мирового лидера. По мнению крупных зарубежных специалистов, это может стать предпосылкой для утверждения в мире отдельных, не взаимодействующих технологических экосистем, жестко разделенных по политическим линиям. Надежда на предотвращение этого обусловлена взаимовыгодным характером существующих глобальных технологических цепочек и высокой степенью экономической взаимозависимости Вашингтона и Пекина.

В свете американо-китайского противоборства, резко набравшего обороты в последние годы, внимание к возможностям ведения самостоятельных фундаментальных и прикладных исследований в цифровой сфере проявляют страны, входящие в Евросоюз.

Цифровая политика ЕС, ослабленного многочисленными кризисами последнего времени, движима прежде всего ожидаемым экономическим приростом от внедрения цифровых технологий в различные сферы жизнедеятельности государства. Одновременно европейцы стремятся прорабатывать вопросы заполнения нормативно-правовых лакун в указанной области, ставя во главу угла процессов цифровизации прежде всего социально-ориентированный подход. На глобальном уровне ЕС реализует проект *EU Cyber Direct*, учредителями которого являются брюссельский Институт ЕС по изучению вопросов безопасности (*EU Institute for Security Studies*) в сотрудничестве с Германским фондом Маршалла в Вашингтоне (*German Marshall Fund of the US*) и фондом «Новая ответственность» (*Stiftung Neue Verantwortung*) в Берлине. Инициатива финансируется Еврокомиссией по линии партнерства ЕС в рамках международного цифрового сотрудничества по обеспечению доверия и безопасности в киберпространстве.

В целом ЕС традиционно придерживается сходной с США линии по кибертематике. Так, еще в сентябре 2017 г. на саммите по цифровым технологиям президент Литвы Даля Грибаускайте выступила с инициативой создания в рамках ЕС «кибернетического Шенгена» – сил быстрого реагирования на кибернетические атаки. Данная структура призвана дополнять НАТО в борьбе с

гибридными угрозами, терроризмом и в помощи третьим странам. Уже в декабре 2017 г. участники европейской программы Постоянного структурированного сотрудничества в области обороны и безопасности (*PESCO*) одобрили оказание взаимопомощи для обеспечения кибербезопасности и создание кибергрупп быстрого реагирования.

В настоящее время Брюссель и Вашингтон в рамках программы двустороннего диалога координируют усилия по продвижению и выполнению на региональных уровнях собственных кибернетических стратегий. Для Евросоюза это программный документ «Устойчивость, сдерживание и оборона: построение сильной системы кибербезопасности для ЕС» (*Resilence, Deterrence, and Defence: Building Strong Cybersecurity for the EU*). Американские и европейские элиты сходятся во мнении о том, что для декриминализации киберпространства достаточно реализации норм принятой еще в 2001 г. Будапештской конвенции о преступности в сфере компьютерной информации, открытой для подписания всеми государствами мира. Брюссель при поддержке Вашингтона выступает против подписания другого документа в этой области под эгидой международных или региональных организаций, членом которых он является.

Кроме того, европейские чиновники делают ставку на расширение сотрудничества по вопросам кибербезопасности в двустороннем и региональном форматах, отмечая важность такого направления политики как кибердипломатия. Во многих европейских странах введена должность кибератташе. В отношениях с соседними государствами по периметру ЕС использует механизмы евроинтеграции, которые обязывают страны, являющиеся кандидатами на вступление в Евросоюз или вступившие в ассоциацию с ним, идти в русле общеевропейского подхода в организации работы по линии кибернетической безопасности.

Одновременно ЕС и США усиливают собственные рычаги давления на третьи страны и так называемые злонамеренные действия в киберпространстве (*malicious cyber activities*). Именно американцы подтолкнули ЕС к принятию в 2019 г. сходного с вашингтонским механизма введения санкций против

иностранных физических и юридических лиц в ответ на якобы состоявшиеся кибератаки и/или попытки проведения таковых. Причем данный механизм, по задумке Белого дома, должен применяться вне зависимости от того, исходила ли киберугроза от правительственного учреждения или от негосударственного субъекта. Более того, трансатлантические партнеры намерены применять указанный механизм санкций к кибератакам, которые имели место в прошлом. Это обосновывается тем, что медленная реакция на киберинциденты или ее отсутствие в принципе может привести к резкому всплеску преступности в кибернетическом пространстве. Причем недостаточность и достоверность доказательной базы причастности того или иного субъекта мировой политики к кибернападению, по мнению брюссельской элиты, не должна являться препятствием для ответных мер, поскольку для этого якобы вполне достаточно отрытых данных, размещенных в интернете.

Вместе с тем следует отметить, что в последние несколько лет европейские бюрократы осознали важность независимости ведения собственных высокоинтеллектуальных разработок, в том числе в информационно-коммуникационной сфере. Поводом к этому послужил именно конфликт между Вашингтоном и Пекином относительно развертывания систем связи 5G, заложником которого в итоге оказался ЕС. В Брюсселе созрело понимание того, что любые новые угрозы, связанные с форсированным технологическим рывком человечества (кибератаки, кража персональных данных, дезинформация, манипуляции общественным мнением и пр.), многократно усиливаются для Евросоюза в связи с тотальным доминированием в европейском цифровом пространстве китайских и американских технологических гигантов.

Соответственно, несмотря на широкий потенциал взаимодействия союзников и партнеров по обеим сторонам Атлантики в области цифровых технологий, в ЕС питают все меньше иллюзий к возможности развития полноценного и взаимовыгодного сотрудничества в области цифровых технологий с США. Это обусловлено прежде всего несовпадающими в своей основе подходами сторон к развитию и внедрению в жизнь социума инноваций

будущего. Так, в прямое противоречие вступают американские и европейские регламенты по работе с персональными данными, нацеленные на защиту «цифрового суверенитета» государств. По мнению экспертов, в перспективе это может послужить большими убытками как для Соединенных Штатов Америки, так и для Европейского союза[151].

На фоне возрастающих перспектив возникновения критической зависимости Брюсселя от Вашингтона или Пекина летом 2019 г. канцлер ФРГ А. Меркель отметила, что европейским государствам предстоит совместный поиск путей преодоления технологического отставания от лидеров «цифровой гонки». Данный курс приобрел еще более ясные очертания после смены состава Еврокомиссии осенью 2019 г. В ЕС пришли к выводу о необходимости формирования на пространстве объединения «новой высокоинтеллектуальной экономической и кибернетической среды», которая функционировала бы на основе уже существующих норм и принципов международного права.

Со сменой состава Еврокомиссии, состоявшейся осенью 2019 г., в Брюсселе заявили о необходимости формирования на пространстве объединения «новой высокоинтеллектуальной экономической среды». ЕС связал это с высокой степенью нестабильности миросистемы, а также с необходимостью избежать навязывания европейским государствам чуждых правил технологического развития. В 2020 г. Евросоюз активизировал проведение прикладных научно-аналитических работ, нацеленных на оценку влияния, которое может оказать внедрение цифровых технологий на конкурентоспособность объединения[152].

В феврале 2020 г. Еврокомиссия опубликовала рабочий документ под названием «Экономический потенциал», который содержит оценки возможного воздействия цифровых технологий на экономику и общество отдельных стран ЕС и Евросоюза в целом. Документ был подготовлен компанией «МакКинси» по

---

[151] The US-EU Rivalry for Data Protection: Energy Sector Implications // IFRI. 2019. February. URL: https://www.ifri.org/en/publications/editoriaux-de-lifri/edito-energie/us-rivalry-data-protection-energy-sector-implications (дата обращения: 20.05.2020).

[152] A new Industrial Strategy for a globally competitive, green and digital Europe // European Commission. 2020. March 10. URL: https://ec.europa.eu/commission/presscorner/detail/en/fs_20_425 (дата обращения: 25.05.2020).

поручению Генерального директората ЕК по вопросам развития систем связи, информационного обеспечения и технологий. Центральное место в нем заняло симуляционное макроэкономическое моделирование воздействия подрывных технологий, таких как ИИ и робототехника, на экономику Европы. На его основе произведена суммарная оценка как позитивного, так и негативного воздействия этих технологий. Верификация модели базового сценария, разработанного европейскими экспертами, свидетельствует о том, что суммарный позитивный экономический эффект, полученный от роста и сдвигов в структуре занятых, освоения и распространения нововведений, превышает связанные с этим издержки, включая потери от роста безработицы в ЕС[153].

Сказанное свидетельствует, что цифровизация находится в фокусе внимания Европейского союза и входящих в него стран. Там активно развиваются крупные программы прикладного и фундаментального исследования потенциала цифровых технологий. На современном этапе развития основная проблема для Евросоюза заключается в том, что внедрение высокоинтеллектуальных достижений в производственные процессы в странах – участницах европроекта пока находится на несравнимо низком уровне по сравнению экономическими нововведениями США и тем более КНР[154].

Можно предположить, что с учетом имеющегося потенциала и целевых установок политических элит в европейских столицах в обозримой перспективе ЕС проявит волю к тому, чтобы задавать международно-правовые принципы и нормы в области кибербезопасности. Но, скорее всего, формулироваться они будут, как и прежде, в Вашингтоне.

В целом проведенный анализ свидетельствует о том, что сегодня мир сталкивается со становлением принципиально новой социально-политической реальности, в условиях которой крупные мировые центры силы стремятся

---

[153] Shaping the digital transformation in Europe. Working paper: Economic potential // European Commission. 2020. February. URL: https://ec.europa.eu/digital-single-market/en/news/shaping-digital-transformation-europeworking-paper-economic-potentialIbidem (дата обращения: 25.05.2020).

[154] Digitalreport 2020. Berlin: European Center for Digital Competitiveness by ESCP Business School. Januar 2020. P. 15.

реализовать свои интересы и возможности в цифрровой сфере. Эти развитые государства делают ставку на достижение технологического прорыва как на предпосылку закрепления собственных позиций на международной арене. Данные процессы сопровождаются ускоренным внедрением перспективных технологий в политическую практику, причем как во внутренней сфере, так и вовне, особенно в отраслях, которые определяют национальную мощь и влияние.

2.2. Тренды информационного противоборства в свете форсированных процессов цифровизации

По мере расширения сфер ведения информационного противоборства современный мир становится более взаимосвязанным, чем прежде, что открывает новые возможности для осуществления информационных операций. Однако такая ситуация, обусловленная форсированными процессами цифровизации, влечет и появление новых рисков, достоверный масштаб которых в условиях набравшей силу динамики процессов информационного противоборства прогнозировать весьма непросто. Тем не менее, явно прослеживаются тенденции развития данных практик и связанные с ними политические риски, которые могут иметь важное значение для обеспечения национальной безопасности России, а также международной информационной безопасности в целом.

В обозримом будущем можно ожидать повышения роли цифровых технологий во всех сферах общественной жизни. Соответственно, **процессы информационного противоборства будут, видимо, все более усложняться, развиваясь по нелинейной траектории, в силу растущего использования ведущими акторами мировой политики (прежде всего США и КНР) ресурсов глобальной сети Интернет для управления общественным мнением в отдельных странах или даже регионах мира.**

К настоящему моменту дезинформационные кампании в интернете стали, по существу, отличительной особенностью политической жизни любого государства. В данных обстоятельствах такой мировой центр силы, как США, последовательно придерживается позиции о необходимости совершенствования

национальной системы информационного противоборства, якобы уязвимой перед иностранной пропагандой. По оценкам американских экспертов, налицо разработки «объективного комплекса мер», который должен широко вовлечь в процесс противодействия такой политике правительственные структуры и гражданское общество в целях проведения мероприятий, скоординированных на федеральном уровне[155].

Так, в Стратегии национальной безопасности США, принятой в декабре 2017 г., в качестве угрозы безопасности государства отмечается воздействие американских оппонентов на средства массовой информации, политические процессы, финансовые сети и использование персональных данных с целью подрыва легитимности правительств демократических государств[156]. На этом фоне авторы документа признали усилия Соединенных Штатов по противодействию противнику в сфере информационных операций «слабыми и фрагментарными», в том числе из-за недостатка специалистов. Для исправления ситуации американское руководство указало на целесообразность:

– проанализировать действия оппонентов по использованию информации и психологических приёмов в политических интересах, а также усилить работу в сфере публичной дипломатии;

– проводить информационные кампании, «основанные на американских ценностях, выявляющие вражескую пропаганду и дезинформацию», для распространения американского влияния в мире, а также противостояния политическим идеологиям конкурентных держав и радикальных исламистских группировок;

– использовать в своих интересах «местные голоса» как наиболее убедительные и эффективные в идеологическом соперничестве, в частности, как

---

[155] См.: Russia Is Our Adversary // The Atlantic. 2018. February 9. URL: https://www.theatlantic.com/politics/archive/2018/02/russia-is-our-adversary/552962/ (дата обращения 16.05.2018).

[156] National Security Strategy of the United States of America, 2017 P. 12-13, 31–32. // The White House. 2017. December 18. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 02.10.2019).

отмечается, «американский частный сектор должен внести свою лепту в продвижение американоцентричных ценностей в СМИ и интернете»;

– развивать сотрудничество с государствами-партнерами в информационной сфере;

– провести ревизию имеющихся платформ распространения информации по всему миру, оценить наиболее эффективные с точки зрения затрат и эффективности методы распространения контента, отражающего интересы национальной безопасности Америки[157].

Помимо сказанного, в последние годы на совершенствование системы информационного противоборства США выделялись весьма крупные финансовые средства по сравнению с другими странами. В сентябре 2018 г. по линии Госдепартамента было анонсировано предоставление ассигнований на «противодействие иностранной дезинформации и пропаганде» в объеме около 40 млн долларов. При этом отмечалось, что половина этой суммы должна быть перечислена на баланс Центра глобального взаимодействия (*Global Engagement Center*), входящего в систему Госдепартамента. Остальные средства планировалось израсходовать на внедрение технологий раннего распознавания дезинформации и анализ политических предпочтений зарубежной аудитории. Также отмечалась необходимость налаживание эффективного взаимодействия с влиятельными игроками на рынке региональных социальных медиа, неправительственным организациями и журналистами[158].

Следует заметить и то, что в конце 2018 г. политическое руководство США приняло решение учредить в составе Совета национальной безопасности специализированный орган информационной борьбы – Управление стратегических нарративов. Указанное ведомство подчинено заместителю помощника президента по национальной безопасности по вопросам

---

[157] См.: National Security Strategy of the United States of America, 2017 P. 12-13, 31–32. // The White House. 2017. December 18. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 02.10.2019).

[158] См.: New players join race for offensive cyber abilities // Oxford Analytica. 2018. 20 August. URL: https://dailybrief.oxan.com/Analysis/DB236921/New-players-join-race-for-offensive-cyber-abilities- (дата обращения: 20.09.2019).

стратегических коммуникаций, что позволяет Управлению самостоятельно выходить на главу государства с предложениями по решению задач в области информационного противоборства[159].

В настоящее время Управление стратегических нарративов вовлечено в разработку эффективных методов информационного противодействия международным соперникам США. Этот орган взаимодействует с аналогичными структурами стран НАТО в разработке комплексного механизма противодействия борьбы с пропагандой вероятных противников Вашингтона. В целом, по прогнозам американских военных экспертов, в обозримом будущем указанная структура позволит существенно нароастить информационную безопасность Соединенных Штатов. Предполагается, что по своей эффективности она должна превзойти Информационное агентство США, существовавшее в 1953–1999 гг.

К реконфигурации системы информационного противоборства США, призванной поспособствовать удержанию доминирующего положения страны на мировой арене, привлечены влиятельные экспертные центры Соединенных Штатов. В частности, выделяется деятельность в рамках информационного противоборства таких американских структур, как Совет по международным отношениям (*Council on Foreign Relations*), Атлантический совет (*Atlantic Council),* Альянс защиты демократии Германского Фонда Маршалла (*German Marshall Fund's Alliance for Securing Democracy*), «Корпорация РЭНД» и пр.[160]

Являясь крупным звеном американской внешнеполитической пропаганды, представители указанных аналитических центров в большинстве случаев связывают свою деятельность с растущим международным влиянием новых и укрепляющихся политических субъектов. Например, в конце 2019 г. специалисты американского аналитического центра «Корпорация РЭНД» выпустили доклад, посвященый ведению так называемой политической войны. В нем эксперты

---

[159] См.: How to Stop Losing the Information War // Defense One. 2018. July 26. URL: https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/ (дата обращения: 20.08.2019).

[160] См. напр.: Monitoring Social Media. Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations // RAND. 2017. URL: https://www.rand.org/pubs/research_reports/RR1742.html (дата обращения 13.05.2018).

указывали, что проводимые конкурентами США на международной арене активные мероприятия в области информационного противоборства составляют базу политической войны против государств демократического Запада. В частности, якобы ведущаяся в настоящее время «политическая война РФ нацелена на дискредитацию образа жизни, ценностей, лидеров западных стран». Авторы документа убеждены, что именно это является «сутью подхода России к противоборству с превосходящим ей по силам соперником»[161].

В данных условиях Вашингтон рассматривает всеобъемлющие меры в сфере информационного противоборства на вероятного противника в качестве полноценного инструмента защиты американских национальных интересов наряду с дипломатическими, военными, экономическими, финансовыми, правоохранительными инструментами, и работает над отработкой их согласованного использования государственными ведомствами США. Обеспечение национальной безопасности непосредственно в информационной сфере предполагает повышение эффективности использования Вашингтоном потенциала цифровых технологий, а также его дискредитации оппонентов в глазах мирового общественного мнения[162].

В обозримой перспективе можно ожидать повышения значимости проблемы кибербезопасности, что будет сопровождаться не только информационными операциями политического влияния на просторах социальных сервисов интернета, но и кибератаками, реализующимися в интересах различных политических элит.

Сегодня проблема обеспечения кибернетической безопасности волнует совершенно все слои общества, так как затрагивает их самые разнообразные интересы. Налицо возрастание роли защиты электронных массивов для обеспечения безопасности государственных структур, а также данных о частной

---

[161] The Growing Need to Focus on Modern Political Warfare // RAND. 2019 URL: https://www.rand.org/pubs/research_briefs/RB10071.html (дата обращения: 12.09.2019).

[162] National Security Strategy of the United States of America, 2017 P. 12-13, 31–32. // The White House. 2017. December 18. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 02.10.2019).

жизни граждан, гарантий их прав и демократических свобод, в том числе неприкосновенности и безопасности. Одним из важных факторов риска является повышенная уязвимость государственных структур перед хакерскими атаками ввиду того, что большинство объектов критической инфраструктуры взаимодействуют в режиме реального времени. Одновременно учащаются случаи утечки размещенных в интернете персональных данных.

В последние годы в американском военном ведомстве активно разрабатывали процедуры по интеграции стратегических информационных операций и информационных операций с использованием киберпространства. Властные элиты США планировали обеспечить, чтобы эти совместно процедуры представляли собой комплексную общую военную стратегию, планирование и составление бюджета в области обороны в отношении проведения таких операций Департаментом, включая мероприятия по противодействию и сдерживанию таких операций со стороны недобросовестных субъектов. В рамках этой работы каждое боевое командование ВС США в координации с Госдепартаментом и при содействии Центра глобального взаимодействия разрабатывало региональную информационную стратегию и межведомственный план её имплементации[163].

Важно отметить, что в связи с «масштабом прогнозируемых вызовов» американские государственные ведомства регулярно переформулируют национальные приоритеты страны в области информационного противоборства. В открытой части американской Стратегии национальной обороны, опубликованной в январе 2018 г., отмечается, что в перспективе США будут уделять приоритетное внимание инвестициям, нацеленным на совершенствование национального киберпотенциала с тем, чтобы за счет эффективности сопряжения связки операций информационно-психологического воздействия и кибератак быть способными осуществлять весь спектр военных операций.

---

[163] S.2943 – National Defense Authorization Act for Fiscal Year 2017. SEC. 1287 // Congress.gov. URL: https://www.congress.gov/bill/114th-congress/senate-bill/2943 (дата обращения: 05.04.2018).

Кроме того, в ноябре 2018 г. Национальный научный фонд США заявил о досрочном обновлении в 2019 г. Стратегического плана исследований и разработок в области кибербезопасности от 2016 г., который был рассчитан на десятилетнюю перспективу. Этот документ призван служить основой для координации проектов в указанной области, обеспеченных госфинансированием, в том числе касающихся образовательных программ и улучшения положения на рынке труда[164].

Практически одновременно с этим Соединенные Штаты взяли курс на ведение наступательных операций в киберпространстве на постоянной основе. Первые признаки этого появились в опубликованной Киберкомандованием США в апреле 2018 г. «дорожной карте» наращивания национального военного потенциала под названием «Достижение и удержание кибернетического превосходства Соединенных Штатов Америки»[165].

В указанном документе приведены императивы деятельности военного ведомства США в киберпространстве, где в качестве одного из них названо использование передовых информационно-коммуникационных технологий в военно-политических целях. Авторы инициативы исходят из целесообразности внедрения в практику деятельности национального военного ведомства новейших кибернетических разработок темпами, значительно опережающими усилия вероятных противников Вашингтона в сфере кибербезопасности. Обеспечить технологический отрыв США от вероятных противников предполагается с опорой на исследования таких американских структур, как Управление перспективных исследований в сфере разведки, Управление перспективных исследований МО, Центр прикладного интеллекта и когнитивных наук и пр. Ключевая роль в разработке кибервооружения возлагается на компанию «Нортон Груман Корпорэйшн» (*Northon Gruman Corporation*), с которой Пентагон заключил

---

[164] См.: National Science Foundation requests input on updating cyber research and development plan // Inside Cybersecurity. 2018. 12 November. URL: https://insidecybersecurity.com/daily-briefs/national-science-foundation-requests-input-updating-cyber-research-and-development-plan (дата обращения: 20.09.2019).

[165] Department of Defense Cyber Strategy 2018 // US DOD. 2018. September. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_ (дата обращения: 01.10.2019).

крупные финансовые контракты, нацеленные на разработку, внедрение и обслуживание единой платформы для ведения наступательных, оборонительных и разведывательных операций в киберпространстве[166].

Примечательно и то обстоятельство, что в августе 2018 г. Д. Трамп отменил принятую в 2013 г. его предшественником на посту главы государства директиву, которая регламентировала порядок проведения операций в киберпространстве. По заявлению экс-помощника по национальной безопасности президента США Дж. Болтона, ответственного за реализацию указанной инициативы, с этого времени кибератаки рассматриваются в качестве «уникального и нетрадиционного» инструмента достижения военно-политических целей Вашингтона. Таким образом, если ранее на проведение кибератак были наложены серьезные ограничения, то с отменой таковых политика Соединенных Штатов в этой области будет активизирована с прицелом на «поддержку национальных военных операций, а также отражение попыток вмешательства в выборные процессы и хищение интеллектуальной собственности» [167].

Концептуально данные меры отражены в национальной стратегии кибербезопасности Соединенных Штатов, опубликованной в сентябре 2018 г., где содержится установка на сдерживание противников Вашингтона с опорой на наступательный киберпотенциал, а не усовершенствованные защитные технологии. В этом документе прямо указывается, что в противостоянии с вероятными противниками (согласно стратегии национальной безопасности США, к таковым причисляются прежде всего Россия и Китай) американцы планируют придерживаться «проактивных оборонительных действий» (так называемой концепции передовой обороны) даже в ситуациях, не требующих

---

[166] Achieve and Maintain Cyberspace Superiority // U.S. Cyber Command. 2018. March 23. URL: https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf (дата обращения: 27.08.2019).

[167] Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive // The Wall Street Journal. 2018. August 15. URL: https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721 (дата обращения: 23.09.2019).

вмешательства третьей стороны, исходя из норм и принципов международного права[168].

Согласно стратегии, для предотвращения и сдерживания «злонамеренной деятельности» против США, их союзников и партнеров, а также для реагирования на нее американские власти могут использовать все доступные средства, в том числе дипломатические, информационные, военные (как кинетические, так и кибернетические), финансовые, юридические, разведывательные механизмы, а также прибегать к публичной атрибуции кибератак. Кроме того, в соответствии с документом к «злонамеренной деятельности» в информационном пространстве Соединенные Штаты теперь причисляют не только кибератаки, но также пропагандистские и дезинформационные кампании[169].

Как отмечал П. Накасоне, глава Кибернетического командования ВС США и Агентства национальной безопасности в президентство Д. Трампа, на современном этапе развития наибольшие технические заделы в области кибербезопасности имеет Россия. В то же время генерал называл КНР «стратегическим соперником, практически равным Соединённым Штатам», а ее возможности – крайне опасными для американских правительственных и коммерческих сетей. Уровень угрозы со стороны Северной Кореи американский военачальник считал «средним», так же как и со стороны Ирана[170].

Выступая на слушаниях в американском Конгрессе весной 2018 г., П. Накасоне подтвердил своё согласие с выводами рабочей группы Научного совета МО США по вопросам сдерживания в киберпространстве. В 2017 г. указанная группа пришла к заключению о необходимости: проведения адаптированных кампаний по обеспечению сдерживания условных противников в

---

[168] National Cyber Strategy of the United States of America // The White House. 2018. September. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 23.09.2019).

[169] National Cyber Strategy of the United States of America // The White House. 2018. September. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 23.09.2019).

[170] См.: *Bendett Samuel.* Here's How the Russian Military Is Organizing to Develop AI // Defense One. 2018. July 20. URL: https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/ (дата обращения: 23.09.2019).

данной среде; повышения устойчивости американских сил и средств к киберугрозам; развития возможностей по осуществлению атрибуции атак в киберсреде.

В последние годы в качестве наиболее серьезной киберугрозы национальной безопасности США американские специалисты считают уязвимость частного сектора, особенно военно-промышленной базы, которая наряду с критической инфраструктурой является богатым источником информации для противника и имеет неоценимую важность для обороны страны. Концепция действий США в киберпространстве, известная как «постоянный контакт» (*constant contact*) или «непрерывное столкновение» (*persistent engagement*) обеспечивает широкие возможности, особенно если не ведет к пересечению «порога» вооружённого конфликта. Концепция предполагает перехват инициативы в киберпространстве посредством непрерывного оспаривания (*continuously contesting*) действий и позиций противника. При этом важно учитывать, что в настоящее время Киберкомандование проводит операции в отношении оппонентов США в киберпространстве, которые не требуют сокрытия того факта, что они осуществляются силами и средствами ВС США.

Можно констатировать, что ведущаяся в настоящее время отдельными развитыми государствами мира (прежде всего США) системная работа по обеспечению кибербезопасности во многом угрожает дестабилизировать всю систему стратегической стабильности. Учитывая суть концепции «постоянного контакта», данная деятельность, по всей видимости, будет носить перманентный и наступательный характер в отношении конкурирующих с США державами, однако он не превзойдет (по возможности) «порога» военного конфликта.

С учетом сказанного, в обозримом будущем Соединенные Штаты планируют выстроить стратегические партнерские отношения со странами, заинтересованными в содействии, что поможет усилить влияние на их оппонентов в киберпространстве. Стержневым элементом сотрудничества на этом направлении должна стать так называемая инициатива в сфере киберсдерживания, которая предусматривает согласование позиций государств-

единомышленников относительно активности оппонентов в киберпространстве, в том числе посредством взаимопомощи в атрибуции анонимных действий, совместных публичных заявлений о поддержке и других коллективных акций. Готовность подключиться к отмеченной инициативе уже выразило правительство Великобритании[171].

В целом Пентагон рассматривает развитие стратегического диалога с Соединенным Королевством, а также Израилем в качестве одного из приоритетов политики ведомства в указанной области. По модели, принятой в данных странах, Вашингтон намерен апробировать сопряжение усилий частного и государственного секторов в обеспечении собственной информационной безопасности. Взаимодействие с союзными государствами Белый дом планирует осуществлять в рамках Управления информационного обеспечения МО и АНБ.

Помимо тесно сотрудничающих с США союзников, способность к ведению наступательных боевых действий в киберпространстве наращивают и другие страны мира. Так, Бразилия добилась объединения усилий различных силовых ведомств страны и создала собственное киберкомандование в 2016 г. Индия и Вьетнам предприняли шаги в этом направлении в начале 2018 г. ЮАР приступила к работе по созданию подобного подразделения под эгидой своего МО, но была вынуждена отложить принятие запланированных мер до весны 2019 г. в связи с бюджетными трудностями[172].

Таким образом, в настоящее всемы все больше государств мира склоняются к позиции, что кибератаки якобы уже стали неотъемлемой частью современных военных конфликтов и легли в основу документов, определяющих военную стратегию Вашингтона и других столиц. Между тем приоритетность

---

[171] См.: *Horowitz Michael.* Strategic Competition in an Era of Artificial Intelligence // Center for a New American Security. 2018. July. URL: http://files.cnas.org.s3.amazonaws.com/documents/CNAS-Strategic-Competition-in-an-Era-of-AI-July-2018_v2.pdf (дата обращения: 23.09.2019).

[172] См.: New players join race for offensive cyber abilities // Oxford Analytica. 2018. 20 August. URL: https://dailybrief.oxan.com/Analysis/DB236921/New-players-join-race-for-offensive-cyber-abilities- (дата обращения: 20.09.2019).

наступательного подхода к обеспечению безопасности в киберпространстве навязывается международному сообществу именно США.

Так, еще в октябре 2018 г. в рамках годовой программы Научный совет МО приступил к исследованию перспектив сохранения военного превосходства Америки перед лицом форсированного наращивания вероятными противниками США инновационных возможностей в оборонной сфере. Тогда же заместитель министра обороны по НИОКР М. Гриффин указал, что на современном этапе Соединенные Штаты должны найти принципиально новые способы противоборства с их конкурентами на мировой арене. В частности, отмечена необходимость глубокого анализа мотивации оппонентов США, а именно ключевых ценностных установок и интересов зарубежных политических элит, влияющих на принятие государственных решений. Научному совету также начал изучение способов противодействия мероприятиям по оказанию влияния и информационным операциям соперников Соединенных Штатов, включая «борьбу с вражеским нарративом»[173].

В складывающихся условиях можно ожидать дальнейшего количественного и качественного усиления интенсивности процессов информационного противоборства (от рассылки спама в целях выявления личной информации о крупных политических деятелях до осуществления атак типа «отказ в обслуживании»), направленных прежде всего на вывод из строя жизненно важных объектов критической инфраструктуры. Позитивными факторами на этом фоне являются дальнейшее совершенствование технологий кибернетической защиты.

В условиях форсированных процессов цифровизации информационное противостояние между специалистами по цифровой безопасности и кибервзломщиками открывает широкие возможности использования в целях информационного противоборства технологий искусственного интеллекта и машинного обучения. С 2014 по 2017 г. инвестиции в

[173] *Sherman Jason.* Griffin looking beyond guns, bombs to ensure future U.S. military superiority // Inside Defense. 2018. October 31 URL: https://insidedefense.com/inside-pentagon/griffin-looking-beyond-guns-bombs-ensure-future-us-military-superiority (дата обращения: 21.08.2019).

искусственный интеллект в мире выросли в три раза и составили около 40 млрд долларов. В 2018 г. показатель достиг уровня в 21,5 млрд долларов; предполагается, что к 2024 г. соответствующие инвестиции составят почти 140 млрд долларов[174].

До недавнего времени угрозы в области непосредственно информационной безопасности применительно к технологиям искусственного интеллекта не выделялись в самостоятельную область научного исследования. Однако в последние годы стало очевидно, что использование таких технологий ИИ путем целевого высокотехнологичного информационно-психологического воздействия на массовое сознание представляет большие риски социальной и политической стабильности.

Такая ситуация обусловлена тем, что, с одной стороны, в последнее время большинство кибератак были реализованы на высоком профессиональном уровне именно с привлечением средств ИИ. Данные технологии могут быть весьма успешно задействованы в целях маскировки подозрительных действий субъектов информационного противоборства и преодоления ими систем цифровой защиты. С другой стороны, искусственный интеллект способствует совершенствованию систем киберзащиты. Средства искусственного интеллекта позволяют определять характерные особенности поведения кибервзломщиков и затем использовать такие обобщенные образцы для выявления готовящихся сетевых атак. По прогнозам французских экспертов консалтинговой компании «Капгемини» *(Capgemini*), если до настоящего времени ИИ для обеспечения кибернетической безопасности использовали порядка 20 % государственных и частных организаций, то в 2020 г. это показатель возрастет приблизительно втрое.

Примечательно, что еще в 2012 г. в Управлении перспективных исследований в сфере разведки США была запущена программа «Распознавание

---

[174] См.: Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации. 2019. 10 октября. URL: http://publication.pravo.gov.ru/Document/View/0001201910110003?index=0 (дата обращения: 21.10.2019).

событий на основе ранних моделей с использованием суррогатов» (*EMBERS*). Целью разработки являлось прогнозирование массовых протестов посредством использования систем искусственного интеллекта с определением даты, места, протестующей группы населения.

По состоянию на июль 2019 г. только в Управлении перспективных исследований МО США развивалось уже более 20 проектов, посвященных применению искусственного интеллекта в целях информационно-психологического воздействия на массовое сознание, и более 60 – посвященных кибербезопасности. Один из них, запущенный в июле 2018 г. под названием «Исследования в области анализа потенциала искусственного интеллекта» (*Artificial Intelligence Exploration*), направлен на разработку так называемых инструментов третьей волны, способных привносить «контекстную осведомлённость в технологии, не понимающие мир, который они описывают»[175].

Примечательна также программа, нацеленная на автоматизацию извлечения научных знаний (*Automating Scientific Knowledge Extraction*). Скорее всего, этот принципиально важный для развития науки инструмент будет автоматически определять местонахождение новых данных и научных ресурсов, анализировать их для получения полезной информации, сравнивать результаты с существующими исследованиями, а затем генерировать новые модели.

Следует отметить, что государственные ведомства США, в частности руководство Командования сил специальных операций, проявляет высокий интерес к проектам в области анализа тональности – класса метода контент-анализа в компьютерной лингвистике, предназначенного для автоматизированного выявления в текстах эмоционально окрашенной лексики и оценочных суждений авторов. Анализ тональности обеспечивается широкой совокупностью источников (блоги, статьи, форумы, опросы и т. д.), что может

[175] *Sherman Jason.* Griffin looking beyond guns, bombs to ensure future U.S. military superiority // Inside Defense. 2018. October 31 URL: https://insidedefense.com/inside-pentagon/griffin-looking-beyond-guns-bombs-ensure-future-us-military-superiority (дата обращения: 21.08.2019).

быть весьма эффективным инструментом информационно-психологического воздействия на массовое сознание[176].

Согласно результатам расширенного мониторинга состояния национальной обороны, проведенного МО США в 2019–2020 гг. с целью определения ресурсов для высокоприоритетных проектов американского военного ведомства, которые могут быть развернуты против Китая и России, искусственный интеллект назван «опорной инновацией» среднесрочной перспективы с точки зрения обеспечения национальной безопасности Америки. Более того, эксперты Пентагона назвали ИИ «ключевой технологией военного дела», которая потенциально применима во всем спектре миссий Минобороны. Предполагается, что усиленное внимание к развитию ИИ поспособствует созданию в Соединенных Штатах «военно-технологического фундамента будущего», однако для этого потребуется наладить бесперебойную кооперацию государственных органов с промышленностью и научным сообществом страны, которая существенно ослабла в последние годы[177].

Западные эксперты едины во мнении, что ускорение темпов развития программ искусственного интеллекта в США связано с наращиванием темпов соответствующих разработок в государствах, которые якобы стремятся оспорить мировую гегемонию Америки. Основную угрозу поддержанию собственного технологического лидерства Соединённые Штаты видят в Китае и России.

Существенная часть китайских НИОКР относится к технологиям двойного назначения и осуществляется не только в целях улучшения экономических позиций страны в мире, но также усиления её обороноспособности. В Вашингтоне с беспокойством отмечают, что фокус внимания Пекина постепенно смещается от «информационных» к «умным» системам вооружений. К таковым американцы относят оружие космического базирования, беспилотные

---

[176] См. подр.: О разработках в области информационной войны в США // Научно-исследовательский центр проблем национальной безопасности. 2019. Март. URL: https://nic-pnb.ru/informacionnoe-protivoborstvo/o-razrabotkah-v-oblasti-informatsionnoj-vojny-v-ssha/ (дата обращения: 23.05.2019).

[177] См.: China’s AI Giants Can’t Say No to the Party // Foreign Policy. 2018. August 2. URL: https://foreignpolicy.com/2018/08/02/chinas-ai-giants-cant-say-no-to-the-party/ (дата обращения: 12.12.2018).

летательные аппараты, оружие направленной энергии, электромагнитные пушки, разделяющиеся головные части с блоками индивидуального наведения[178].

По оценкам специалистов, комплексный анализ гражданских и военных прорывных технологий Китая, результаты слушаний в Комиссии по американо-китайскому экономическому сотрудничеству и рассмотрению вопросов безопасности, а также отчёт по углублённому анализу вооружений КНР свидетельствуют о примерном паритете Вашингтона и Пекина в развитии технологий. Американские эксперты в докладе Исследовательской службы Конгресса США под названием «Искусственный интеллект и национальная безопасность», опубликованном 26 апреля 2018 г., отмечают, что Вашингтон имеет в лучшем случае десятилетие для расширения собственных возможностей в области искусственного интеллекта и выработки концепции противодействия военным разработкам Китая в этой сфере[179].

Подобной позиции придерживается руководство американского Управления перспективных исследований в сфере разведки. Там убеждены, что, хотя сегодня Соединённые Штаты и являются лидером на мировой арене в области разработок на базе ИИ, конкуренция со стороны других держав (в частности Китая и РФ) нарастает стремительнее, чем могли ожидать в Пентагоне. Кроме того, развитие этой индустрии в КНР встретит, по всей видимости, меньше барьеров, чем в США, с точки зрения возможности сопряжения потенциала военного и коммерческого секторов. Это определяет объём работы для американских военных разработчиков на обозримую перспективу, так как усилит риски конфронтации между конкурентами в будущем[180].

Военное и разведывательное сообщество США выражает серьезное беспокойство в связи с нарастанием угроз со стороны научно-технической

---

[178] См.: China in "full-speed" push for "intelligentized" weapons to defeat U.S. // Geostrategy-Direct. 2018. 15 May. URL: http://geostrategy-direct-subscribers.com/china-in-full-speed-push-for-intelligentized-weapons-to-defeat-u-s/ (дата обращения: 10.12.2018).

[179] Artificial Intelligence and National Security // Congressional Research Service. 2018. April. URL: https://fas.org/sgp/crs/natsec/R45178.pdf (дата обращения: 28.11.2018).

[180] См.: Bertuca *T.* Intel research chief wants to maintain "healthy" U.S. lead over China in AI race // Inside Defense. 2018. March. URL: https://insidedefense.com/daily-news/intel-research-chief-wants-maintain-healthy-us-lead-over-china-ai-race (дата обращения: 28.11.2018).

разведки КНР. Так, в апреле 2018 г. на конференции в Институте Аспена глава Национального центра контрразведки и безопасности У. Иванина отметил, что в последние годы официальная позиция Поднебесной сводится к массовому направлению на учёбу и работу в Соединённые Штаты исследователей, занимающихся изучением высоких технологий (в том числе разработок в сфере искусственного интеллекта). В Америку прибывает около 350 тыс. китайских студентов ежегодно. По его мнению, вытекающие из такой политики Китая угрозы безопасности США очевидны, но пока недооцениваются военно-политическим руководством страны. У. Иванина указал на необходимость ужесточения визового режима для прибывающих из КНР учёных и студентов, несмотря на то что большинство лиц этой категории находятся в стране на законных основаниях и вносят существенный вклад в развитие американской экономики[181].

Опасения по поводу широкого присутствия в научно-исследовательских кругах Соединённых Штатов представителей КНР высказываются и в профильных комитетах Конгресса США. Так, выступая в апреле 2018 г. в подкомитете палаты представителей, бывшая сотрудница американской контрразведки М.В. Клив отметила, что Китай на государственном уровне проводит подрывную программу. Ее суть сводится к сбору за рубежом информации, касающейся разработки и применения прорывных наукоемких технологий[182].

Такого мнения придерживается и член Комиссии по американо-китайскому экономическому сотрудничеству и рассмотрению вопросов безопасности М. Вессель. Он указывает, что уже в 2006 г. Пекин запустил «Проект 111» и «Программу тысячи талантов», которые призваны привлечь около 4 тысяч работающих за рубежом исследователей (желательно из числа этнических

---

[181] См.: White House report details Chinese theft of "future of the world" technology // Geostrategy-Direct. 2018. June. URL: http://geostrategy-direct-subscribers.com/white-house-report-details-chinese-theft-of-future-of-the-world-technology/ (дата обращения: 11.12.2018).

[182] См.: Van Cleave: U.S. a spies' paradise, national-level counterintelligence eliminated // Geostrategy-Direct. 2018. April. URL: http://geostrategy-direct-subscribers.com/van-cleave-u-s-a-spies-paradise-national-level-counterintelligence-eliminated/ (дата обращения: 10.12.2018).

китайцев) к решению задач национальной безопасности КНР. В связи с этим следует отметить, что сегодня уже порядка 20 % постоянных сотрудников лаборатории искусственного интеллекта при Калифорнийском университете в Беркли имеют китайское происхождение. В исследовательской группе «Бинг» (*Bing*) при Мэрилендском университете (*University of Marylend*) 30 из 38 докторантов и аспирантов – выходцы из КНР[183].

Во многом с учётом нарастающих угроз извне в рассматриваемой области Вашингтон активизирует совместные проекты в сфере искусственного интеллекта с союзниками. В мае 2018 г. американская сторона присоединилась к инициативе Великобритании по изучению возможностей и рисков применения технологий искусственного интеллекта в военных целях, включая машинное обучение и интеллектуальный анализ больших данных. На открытии Лаборатории по исследованию оборонных и наукоёмких технологий на военном объекте британского Минобороны в Портон-Дауне со стороны Соединённых Штатов присутствовали экс-глава компании Гугл Э. Шмидт, экс-главный советник министра обороны США С. Доннелли и вице-президент по науке и инновациям компании «Объединенные технологии» (*United Technologies*) М. Маккуэйд. Как заявлял экс-министр обороны Великобритании Г.Уильямсон, при открытии данной структуры ей было выделено более 20 млн фунтов стерлингов для проведения исследований, касающихся искусственного интеллекта, и в перспективе эта сумма будет увеличиваться[184].

В целом, следует сказать, что в настоящее время сетевые структуры во всем мире находятся в состоянии переломного момента, обусловленного технологическим прогрессом, в частности внедрением более совершенного оборудования и программного обеспечения на базе искусственного интеллекта и машинного обучения. По мере того, как средства искусственного интеллекта

---

[183] Ibid.

[184] Flagship AI Lab announced as Defence Secretary hosts first meet between British and American defence innovators // GOV.UK. 2018. May. URL: https://www.gov.uk/government/news/flagship-ai-lab-announced-as-defence-secretary-hosts-first-meet-between-british-and-american-defence-innovators (дата обращения: 28.11.2018).

совершенствуются, приобретают комплексный характер и синергетический эффект, и одновременно они становятся доступными для рядовых пользователей интернета. Как полагают специалисты в области информационного противоборства, в настоящее время влияние на политические процессы посредством применения технологий ИИ на просторах социальных сервисов интернета осуществляется в основном в двух формах:

1. в виде распространения через социальные сети фальшивых новостей и других сведений, направленных на дискредитацию и компрометацию политических режимов, элит или отдельных политических деятелей;

2. как кибервзломы компьютерных сетей национальных и региональных электоральных систем, а также систем отдельных политиков.

Специалисты в области информационной безопасности ожидают, что обе приведенные формы ведения информационного противоборства имеют большой потенциал совершенствования в условиях стремительного развития цифровых технологий и потребуют не только дополнительных затрат ресурсов на развитие соответствующих технологий противодействия, но и активизации мер по осведомленности граждан о существующих сетевых угрозах. Для противодействия фальшивому контенту эксперты предлагают создавать автоматическую или действующую в ручном режиме систему фильтрации ложной информации и пропаганды путем анализа контента и исходных данных с тем, чтобы своевременно выявить распространителей дезинформации и источники использованных сведений. В связи с этим государственные ведомства ведущих государств мира, а также крупные коммерческие компании (например, «Фейсбук» и «Гугл») сегодня вкладывают значительные средства в создание технологий, позволяющих выявлять лживые сведения политического характера на основе обобщения образцов такого рода контента, а также устанавливать факты их распространения в рамках соответствующей пропагандистской кампании.

Существующие в цифровом пространстве вызовы и угрозы в области информационной безопасности в значительной мере масштабируются в результате возрастающего политического и экономического противоборства

между государствами, условно разделяющимися на Запад (во главе с США) и Восток (под эгидой Китая). В данных условиях надежды на действующую без всяких ограничений и границ информационно-коммуникационную сеть постепенно размываются. Два указанных центра силы стремятся вовлечь в орбиту своего влияния как можно больше государств, тем более развитых или многонаселенных. В действительности корпорации и фирмы, которые обеспечивают развитие пользование интернетом во всевозможных вариациях, обязаны соблюдать законы национальных государств и вести свою работу в рамках рекомендаций национальных правительств. В результате политическое и экономическое противостояние между сверхдержавами и государствами регионального значения, включая торговые войны и разногласия внутри Евросоюза, находят свое отражение во всемирной сети. Например, Китай и Иран уже достаточно давно ввели цензуру контента в интернете и блокируют доступ своих граждан к внешним источникам информации. Не так давно такой путь избрала и Россия, подвергнувшись мощной волне критики со стороны «либеральных» стран Запада. Между тем в 2019 г. сами США запретили сотрудничество национальных компаний с крупнейшей китайской телекоммуникационной компанией «Хуавей». В результате возникновения подобных барьеров в последние годы существенно ухудшилось технологическое и правовое взаимодействие между странами в области обеспечения информационной безопасности.

Достаточно явственно новые витки информационного противоборства между ведущими государствами мира проявились в период распространения коронавируса нового типа в первой половине 2020 г. Уже с января 2020 г. США начали активную информационную кампанию против Китая. Так, социальные сервисы интернета наводнили язвительные комментарии и сатирические карикатуры антикитайского содержания, размещаемые как официальными лицами (президент США Д. Трамп), неправительственными организациями, а также другими субъектами информационного противоборства, пожелавшими остаться в глобальной сети анонимными. Руководство КПК обвиняли в попытках

сокрытия информации и неспособности контролировать ситуацию, а граждане страны описывались как нецивилизованные любители экзотических продуктов[185].

В связи с частым употреблением в трансграничном информационно-коммуникационном пространстве словосочетания «китайский коронавирус» в общественном сознании населения многих стран мира сформировалось впечатление, что каждый азиат является потенциальным носителем новой опасной болезни. Это привело к усилению недоброжелательного отношения к гражданам КНР во многих странах мира. Информационная кампания достигла такого размаха, что уже 2 февраля 2020 г. Всемирная организация здравоохранения заявила о начале «массовой инфодемии», подчеркнув опасность чрезмерного потока информационных сообщений как правдивого, так и ложного содержания о распространении COVID-19.

Как отметил в связи с этим генеральный директор ВОЗ Т. А. Гебрейесус, избыток информации во время кризисной ситуации может вводить в заблуждение или даже наносить вред. По его мнению, большие объемы информации могут быть опасными для здоровья людей по следующим причинам:

– они затрудняют поиск четкой и обоснованной фактическими данными информации о здоровье и рекомендаций по защите здоровья;

– в силу своего масштаба, доступности и повсеместного присутствия они способствуют возникновению тревоги, волнений и других проблем с психическим здоровьем;

– они подталкивают людей к выполнению вводящих в заблуждение или даже опасных рекомендаций;

– они вызывают у людей утомление, утрату интереса и враждебность к информации, поступающей от служб общественного здравоохранения;

– они дают почву для ксенофобии, ненависти и отторжения.

---

[185] Трамп заявил, что коронавирус – из китайской лаборатории. Разведка с ним не согласна // Би-би-си. 2020. Май. URL: https://www.bbc.com/russian/news-52440326 (дата обращения: 18.05.2020).

Примечательно, что в период распространения коронавируса нового типа инфодемия стала такой важной проблемой для международного сообщества, что что ВОЗ приняла решение о проведении первой глобальной конференции по инфодемиологии, в июне-июле 2020 г. Как планируется, на данном мероприятии будут обсуждаться примеры действий и инструменты для противодействия инфодемии, а также будет положено начало формированию сообщества экспертов-практиков и исследователей[186].

Китайское руководство умело включилось в информационное противоборство, усмотрев в нынешней ситуации возможность развернуть навязываемый странами Запада информационный нарратив в свою пользу, что могло бы поспособствовать изменению условий противостояния Китая с Соединенными Штатами Америки. Власти КНР резко активизировали информационную работу по нейтрализации ущерба имиджу страны как ответственного международного партнера. Китайские посольства и консульства за рубежом начали широко продвигать тезисы о том, что данный коронавирус изначально возник не в КНР, а эффективная борьба с ним руководства страны только поспособствовала защите населения остального мира от этой угрозы, позволив властным элитам зарубежных стран выиграть время для подготовки государственной системы к распространению вируса. Для этих целей использовались даже специально открытые официальные страницы политиков Китая в социальной сети «Твиттер», при том, что данная платформа там запрещена, и ранее китайские дипломаты воздерживались от ее использования[187].

Примечательно, что во время пандемии коронавируса нового типа европейцы остро негативно отреагировали на достаточно сильное информационное воздействие Пекина на Брюссель. Информационная политика

---

[186] Бороться с инфодемией вместе // Всемирная организация здравоохранения. 2020. URL: https://www.euro.who.int/ru/health-topics/Health-systems/e-health/news/news/2020/6/working-together-to-tackle-the-infodemic (дата обращения: 17.05.2020).

[187] *Yixiang Xu.* Reviving China's Health Silk Road Initiative? Battle of Narratives and Challenges for Transatlantic Leadership // American Institute for Contemporary German Studies, 2020. March. URL: https://www.aicgs.org/2020/03/reviving-chinas-health-silk-road-initiative-battle-of-narratives-and-challenges-for-transatlantic-leadership/ (дата обращения: 03.05.2020).

КНР на европейском направлении в данный период детально проанализирована в научном докладе «COVID-19 и китайско-европейские отношения», опубликованном 29 апреля 2020 г. объединенной сетью европейских «мозговых центров» по исследованию политики Китая *(European Think-tank Network on China*) [188].

В указанном документе отмечается, что в период распространения болезни «мягкая сила» КНР в Европе варьировалась от низкоуровневой (Румыния или Латвия) до наступательной (Польша, Португалия, Италия, Испания), и даже агрессивно-провокативной (Германия и Франция). Авторы доклада приходят к выводу о резко возросших рисках для европейских бизнесменов в случае их активизации на китайском направлении, что обусловлено жесткой установкой национальных элит, подверженной влиянию США, на укрепление кооперации с КНР[189].

Одновременно в период пандемии COVID-19 на Западе развернулась мощная информационная кампания, имеющая выраженный антироссийский характер. Так, в апреле 2020 г. авторитетная американская НПО Атлантический совет опубликовала аналитический доклад, где утверждается, что российские власти якобы активно воспользовались возможностями национальных СМИ в период пандемии, с тем чтобы нарастить влияние страны в зарубежных государствах, в частности в Литве, Латвии, Эстонии. Кроме того, как отмечается в докладе, Россия якобы нацелилась на обрушение экономик указанных стран для того, чтобы усилить их экономическую и политическую зависимость от Москвы[190].

---

[188] Covid-19 in Europe-China Relations // European Think-tank Network on China. 2020. April. URL: https://www.ifri.org/en/publications/publications-ifri/ouvrages-ifri/covid-19-europe-china-relations (дата обращения: 01.05.2020).

[189] Covid-19 in Europe-China Relations // European Think-tank Network on China. 2020. April. URL: https://www.ifri.org/en/publications/publications-ifri/ouvrages-ifri/covid-19-europe-china-relations (дата обращения: 01.05.2020).

[190] *Burrows M.J., Engelke* P. What world post-COVID-19? Three scenarios // Atlantic Council. 2020. April. URL: https://www.atlanticcouncil.org/content-series/shaping-post-covid-world-together/what-world-post-covid-19-three-scenarios/ (дата обращения: 18.05.2020).

На фоне подобных алармистских суждений специалисты Атлантического совета также указывает на то, что пророссийские силы якобы «вбрасывают» в информационное пространство прибалтийских стран следующий тезис: пандемия коронавируса является подходящим поводом для сближения восточноевропейских стран с Россией. Он резюмирует, что это может стать актуальным для восточноевропейцев на фоне проявления дисфункциональности во время распространения новой опасной болезни как общеевропейских институтов, так и заокеанского патрона стран Прибалтики – США. Авторы доклада делают вывод, что все публикации подобного рода имеют политические цели, поскольку являются «проплаченными информационными вбросами в медиапространство стран Прибалтики»[191].

Западные политологи также активно включились в информационную компанию, нацеленную на формирование и закрепление в общественном мнении точки зрения о том, что Россия якобы намеренно способствует угнетению демократических и либеральных ценностей в странах Запада, продвигая там идеи авторитаризма. В частности, РФ, мол, эксплуатирует тему пандемии коронавируса в целях подрыва консолидации не только внутри ЕС, но и на треке сотрудничества Европа – трансатлантический союзник. Это, по мнению аналитиков, способствует не только разрушению основ мирового порядка, сложенных в интересах стран англосферы после Второй мировой войны, но и сближению таких крупных центров силы со сходным видением проблем геополитического масштаба, как Россия и Китай. Американские эксперты резюмируют, что к альянсу данных держав, взявших курс на выстраивание альтернативного существующему механизма глобального управления, вполне могут примкнуть другие «государства-изгои», а после так называемая неопределившаяся часть международного сообщества[192].

---

[191] *Burrows M.J., Engelke* P. What world post-COVID-19? Three scenarios // Atlantic Council. 2020. April. URL: https://www.atlanticcouncil.org/content-series/shaping-post-covid-world-together/what-world-post-covid-19-three-scenarios/ (дата обращения: 18.05.2020).

[192] Ibid.

Кроме того, зарубежные специалисты в области информационного противоборства использовали время пандемии COVID-19 для противодействия Исламской Республике Иран. Так, в цифровом пространстве сети интернет начало функционировать так называемое виртуальное посольство США в Тегеране (*Virtual Embassy Tehran*), в том числе представленного страницей на сайте официального американского внешнеполитического ведомства, а также аккаунтами USAdarFarsi на таких интернет-платформах, как «Фейсбук», «Телеграм», «Твиттер», «Гугл+», «Ютуб», «Инстаграм»[193].

Примечательно, что впервые проект «виртуального посольства» был запущен в декабре 2011 г. для «поддержания прямого диалога» гражданами Ирана. В период нынешней вспышки коронавируса, сильно ударившей по многим странам мира, в том числе Исламской Республике, данная платформа активно использовалась властями США в пропагандистских целях с тем, чтобы разместить на ней информацию, компрометирующую действующий политический режим ИРИ, а также, напротив, для получения информации, обличающей властные элиты Ирана. В начале 2020 г. Госдепартамент США разместил в своей учетной записи USAdarFarsi на фарси анонимную анкету, состоящую из 37 вопросов, основной целью которой являлось выяснение как можно более точной информации о количестве зараженных и умерших в этой стране. По данным американских властей, опубликованных на официальной странице госсекретаря США М. Помпео в «Твиттере», менее чем за месяц данный опрос прошли более 7 тысяч иранцев[194].

Следует отметить и то, что в марте 2020 г. внешнеполитическое ведомство США задействовало в целях информационного противоборства с ИРИ свой официальный канал в сети «Телеграм», созданный еще в 2019 г. во время массовых протестов в Иране и предназначавшийся для получения сведений о

---

[193] *Atwood K.* US uses encrypted app to connect with Iranians as coronavirus sweeps their country // CNN. 2020. March 18. URL: https://edition.cnn.com/2020/03/18/politics/state-department-coronavirus-iran-outreach/index.html (дата обращения: 17.05.2020).

[194] State Dept. using app to connect with Iranians on coronavirus // FreePress. 2020. March 19. URL: https://freepressinternational.org/2020/state-dept-using-app-to-connect-with-iranians-on-coronavirus/ (дата обращения: 17.05.2020).

действиях властей по подавлению манифестаций. В период пандемии 2020 г. шифрованное приложение использовалось для стимулирования иранцев к передаче сведений о реальных масштабах распространения коронавируса в их стране, причем в качестве доказательств рассматривались как текстовые материалы, так и фото и видеоматериалы. В связи с этим американские дипломаты заявляют, что благодаря возможностям цифровой среды, в частности созданных на ее просторах сервисах для общения, у официальных властей США и мирового сообщества в целом появилась возможность получать постоянный поток информации от тысяч простых граждан, проживающих в самых разных странах мира[195].

В целом нынешняя кризисная ситуация обусловила мощную волну информационных кампаний в развитых государствах Запада, нацеленных на дискредитацию политических режимов в отдельных оппонирующих США странах. При этом мессенджеры, мобильные приложения и другие интернет-ресурсы активно использовались американскими официальными властями и представителями специальных служб, позволяя вести работу в рамках информационного противоборства более последовательно и планомерной.

В условиях усиления роли невоенных методов противоборства на современном этапе мирового развития, отмеченного тектоническими сдвигами геополитического характера, **существующие проблемы в сфере обеспечения информационной безопасности и возникающие в свете стремительной цифровизации социально-политической реальности риски могут значительно обостриться в силу нехватки квалифицированных кадров соответствующего профиля.** Например, даже в Америке в последние годы произошли кадровые потери в критически важных областях, в том числе связанных с обеспечением кибербезопасности. В Стратегии национальной

[195] *Atwood K.* US uses encrypted app to connect with Iranians as coronavirus sweeps their country // CNN. 2020. March 18. URL: https://edition.cnn.com/2020/03/18/politics/state-department-coronavirus-iran-outreach/index.html (дата обращения: 17.05.2020).

безопасности США, принятой в декабре 2017 г., ситуация в области кибернетической безопасности в стране оценивается как «крайне сложная»[196].

В указанном документе отмечается, что американские военные структуры не успевают адаптироваться к возникающим на современном этапе угрозам, в том числе, связанным с появлением новых технологий. В частности, по оценкам специалистов, цифровая инфраструктура США (включая сети федерального правительства), от которой зависит функционирование объектов жизнеобеспечения и бизнеса, а также быт граждан, нуждается в существенной модернизации. Одной из причин этого в стратегии названа забюрократизированность американской системы закупок вооружений и военной техники[197].

Соответственно, важным направлением деятельности федеральных американских ведомств в области обеспечения кибербезопасности критической инфраструктуры является активизация сотрудничества государства с частным сектором в целях максимального использования их совокупного потенциала при построении эшелонированной обороны в киберпространстве. И хотя в интересах решения указанной проблемы Белый дом предпринимает меры по усилению государственной поддержки деятельности технических вузов и программ профессионального обучения высококвалифицированных специалистов с ориентацией на их последующее привлечение к обеспечению функционирования наукоемких отраслей, пока эти меры малоэффективны.

По оценкам экспертов, в 2020 г. количество вакансий на этом участке занятости возрастет до трех с половиной миллионов сотрудников по сравнению с одним миллионов, зафиксированным в 2015 г. В результате вполне может возникнуть ситуация, когда невозможно будет найти достаточное количество специалистов указанного профиля, способных эффективно противодействовать операциям влияния в глобальной сети, многочисленным злоумышленникам,

---

[196] National Security Strategy of the United States of America // Whitehouse. 2017. December. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 17. 05.2020).

[197] Ibid.

похищающим информацию, фальсифицирующим персональные данные пользователей и выступающим от их имени в рамках мошеннических схем, а также реализующим политические кампании по дезинформации и оказанию влияния на ход политических процессов[198].

В данных условиях России целесообразно увеличить затраты на профессиональную подготовку соответствующих специалистов в области цифровой безопасности с тем, чтобы улучшить их навыки по противодействию деятельности в области информационного противоборства, в частности, по противодействию и нейтрализации кибератак. Необходимо также привлекать дополнительно квалифицированных экспертов данного профиля, способных прогнозировать формирование новых угроз в области информационного противоборства. В противном случае как деловой мир, так и политические режимы большинства государства понесут колоссальные убытки.

2.3. Информационное противоборство в цифровой сфере и перспективы трансформации миропорядка

В последние годы в практике международных отношений все более явно проявляется тезис, выдвинутый в Стратегии национальной безопасности США, принятой в начальный период президентства Д. Трампа. Согласно данному тезису, определяющей чертой современных политических процессов, находящихся под воздействием форсированных процессов цифровизации, является межгосударственная конкуренция, которая в условиях наличия оружия массового уничтожения и высокого уровня развития обычных систем вооружений и военной техники ведется в основном методами информационного противоборства[199].

---

[198] *Bertuca T.* Intel research chief wants to maintain "healthy" U.S. lead over China in AI race // Inside Defense. 2018. March. URL: https://insidedefense.com/daily-news/intel-research-chief-wants-maintain-healthy-us-lead-over-china-ai-race (дата обращения: 28.11.2018).

[199] National Security Strategy of the United States of America // Whitehouse. 2017. December. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 17. 05.2020).

Понятие мирового порядка – одно из наиболее распространенных в политической теории и практике. В научный оборот его ввел в 1977 г. классик британской школы международных отношений Х. Булл. Ученый описал мировой порядок как «характер (состояние) или направление внешней активности, обеспечивающей незыблемость тех целей сообщества государств, которые являются для него, с одной стороны, необходимыми, с другой – жизненно важными, с третьей – общими для всех»[200].

На протяжении последних 70 лет миропорядок формировался и в определенной мере поддерживался в равновесном состоянии благодаря деятельности многосторонних институтов, созданных после окончания Второй мировой войны, в частности Организации Объединенных Наций. При этом после распада Советского Союза и окончания холодной войны США на правах гегемона однополярного мира активно способствовали безальтернативному утверждению во всех странах «политического либерализма и демократии», а также добивались универсализации прав человека. До недавнего времени данные постулаты навязывались международному сообществу Вашингтоном в качестве ключевых общемировых ценностей.

Однако в последние годы Пекин взял курс на создание нового, во многом альтернативного американскому формата международного взаимодействия. Примечательно, но в этой деятельности он опирается именно на действующие международные структуры (ООН, ВТО и пр.), сужая для Белого дома спектр традиционных легитимных возможностей противодействия КНР. Действуя согласно этой парадигме, китайское руководство, видимо, будет стремиться к «дозированному» изменению мирового порядка, с тем чтобы представить международному сообществу в позитивном свете свое видение концепции цифрового суверенитета, с тем чтобы создавать условия для становления новой – цифровой – системы управления. Специалисты из США трактуют это как попытки КНР экспортировать «цифровой авторитаризм», который уже в

[200] *Bull Hedley*. The Anarchical Society: A Study of Order in World Politics. New York: Columbia University Press, 1977. 335 p.

обозримом будущем может подорвать демократические принципы управления в том числе на глобальном уровне, а также поставить под вопрос фундаментальные права человека и гражданина[201].

Китайские документы стратегического планирования свидетельствуют о том, что Пекин будет выстраивать все проекции цифровой геополитики строго по своим собственным правилам[202]. КНР, видимо, продолжит добиваться форсированного научно-технологического развития, способствовать региональной экономической взаимозависимости, инвестировать в цифровую инфраструктуру. По мнению западных специалистов, такой комплексный подход может сыграть решающую роль в формировании нового мирового порядка в интересах Китая и одновременно, с учетом соблюдения им действующих международно-правовых норм и принципов, позволит ему избежать прямого вооруженного конфликта с Соединенными Штатами Америки.

Текущие политические тренды демонстрируют, что США отнюдь не готовы смириться с потерей звания глобального гегемона и нацелены на сохранение своего лидерства любой ценой, в том числе посредством переформатирования мирового порядка. Особо острая конкуренция наблюдается между Соединенными Штатами и Китаем, которые борются не только за региональное, но и за глобальное влияние. **Крупные западные политологи придерживаются позиции, что ключевое значение в усилении американо-китайского соперничества, исход которого во многом предопределит контуры нового мирового порядка, будут иметь технологические прорывы, в частности успехи в формировании архитектуры цифровой среды.**

Как свидетельствует политический опыт, относительно стабильный мировой порядок возникает после сильных потрясений, которые создают условия

---

[201] *Lewis James.* How Will 5G Shape Innovation and Security: A Primer // Center for Strategic and International Studies. 2018. December 6. URL: https://www.csis.org/analysis/how-5g-will-shape-innovation-and-security (дата обращения: 01.02.2020).

[202] *Ding J., Triolo P., Sacks S.* Chinese Interests Take a Big Seat at the AI Governance Table // New America. 2018. June. URL: https://www.newamerica.org/cybersecurityinitiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/ (дата обращения: 25.01.2020).

для договоренностей о новых правилах международных отношений. Примерами таковых являются Вестфальский мирный договор, Венский конгресс, Парижский мирный договор и сформированный после Второй мировой войны биполярный мир. Последний формат прекратил свое существование с окончанием холодной войны, и наступила эра глобального доминирования США.

В свете развития цифрового соперничества между ведущими акторами мировой политики наметились качественные изменения в превалирующем с 1990–х гг. мироустройстве. Некоторые ученые даже высказывают предположения о возможном разрушении государственно-центристской модели организации власти, связывая это не только со спецификой современного этапа развития мировой политики, но именно с качественными преобразованиями модели функционирования общества, обусловленными форсированным технологическим рывком человечества[203].

Современная геополитическая конкуренция между ослабевающими и возвышающимися центрами силы сопровождается их соперничеством за завоевание технологического лидерства в том числе в деле создания и апробирования на практике инновационных средств и методов информационного воздействия. Фактически форсированные процессы цифровизации являются важным фактором, который стимулирует развитие межгосударственной борьбы, оказывая влияние на переход мирового порядка в новое состояние. Одновременно цифровизация является и отличительной чертой современных тенденций трансформации мироустройства, которые проявляются в форме технологической конкуренции. Зарубежные аналитики сходятся во мнении о том, то такая конкуренция во многом обусловлена повышенным полезным эффектом от

[203] *Брега А.В.* Политический риск в сетевом обществе: новая конфигурация // Социально-гуманитарные знания. 2018. № 3. С. 221–229; *Шутов А.Д.* Исторические прозрения. М.: ЮНИТИ-ДАНА, 2017. 463 с.

внедрения инноваций в социально-экономическую и политическую деятельность человека[204].

В последние годы соперничество за обладание цифровыми ресурсами спровоцировало не только новый виток глобализации, но также возвышение одних акторов мировой политики и ослабление других. Следствием развернувшегося противоборства за достижение технологического лидерства уже стало размывание сдерживающих механизмов применения силы при повышении вероятности ее использования нетрадиционными методами, что привело к разбалансировке самого каркаса миросистемы и ослаблению ее устойчивости[205].

Следует отметить тот факт, что дилемма об обретении так называемого цифрового суверенитета для многих государств актуализировалась в период распространения новой для человечества болезни COVID-19. Западные эксперты даже выдвинули гипотезу, что основным долгосрочным вызовом для человечества может стать «цифровая пандемия» и ее последствия. Подобные суждения обусловлены широким и успешным опытом применения передовых технологий (прежде всего искусственного интеллекта и систем связи 5G) во время распространения нового коронавируса. При этом разрешения указанной дилеммы пока не предвидится, что обусловлено все возрастающими амбициями в мировой технологической иерархии КНР и США, которые базируются на мощном цифровом потенциале[206].

В целом приведенные выше явления и процессы целесообразно считать маркерами, во многом обнажившими несоответствие формата постбиполярного миропорядка современным политическим реалиям, которые характеризуются обострением межгосударственной конкуренции в условиях всепроникающих процессов цифровизации. В зависимости от различных комбинаций

---

[204] См.напр.: *Миловидов В.Д.* Управление инновационным процессом: как эффективно использовать информацию. Нефтяное хозяйство, 2015, № 6. С. 10–16; *Миловидов В.Д.* Услышать шум волны: что мешает предвидеть инновации? Форсайт, 2018, т. 12, № 1. С 88–97.

[205] *Booth K., Wheeler N.* The Security Dilemma: Fear, Cooperation and Trust in World Politics. N.Y.: Palgrave McMillan, 2008. P. 1–18.

[206] *Bodansky Yossef.* After the Corona Virus // Institute for Strategic, Political, Security and Economic Consultancy. 2020. March. URL: https://www.ispsw.com/wp-content/uploads/2020/03/679_Bodansky.pdf (дата обращения: 03.04.2020).

традиционных и относительно новых моментов, обозначим, хотя и весьма условно, наиболее вероятные сценарии перехода мирового порядка в более или менее стабильные «стационарные состояния», которые, могут стать фундаментом будущего мироустройства.

Новая однополярность

Эксперты Исследовательской службы Конгресса США отмечают, что в настоящее время монополюсный (американоцентричный) миропорядок, который позиционируется также как «либеральный миропорядок» (*liberal order*), «открытый миропорядок» (*open order*) или «миропорядок, основанный на правилах» (*rules-based international system*), находится в предкризисном состоянии. В американской политической элите превалирует точка зрения, что такая ситуация обусловлена деятельностью Китая и России, а также других «ревизионистских держав» по пересмотру и подрыву основных принципов сложившегося в интересах Вашингтона мироустройства[207].

В начале президентства Д. Трампа в США были приняты Стратегия национальной безопасности (декабрь 2017 г.) и Национальная оборонная стратегия (январь 2018 г.). Авторы документов указывают на «новую геополитическую ситуацию», которую они называют «соперничество великих держав» (*great-power competition*). При этом американские власти декларируют готовность использовать всевозможные меры (экономические, политические, дипломатические, военные, ресурсы информационного пространства и пр.) для противостояния возможным противникам с целью сохранения США позиций мирового гегемона[208].

Между тем ряд специалистов в области международных отношений указывают, что «точка невозврата» для Америки уже пройдена. В частности, автор концепции «мягкой силы» Дж. Най сомневается, что «либеральный

---

[207] *O'Rourke Ronald, Moodie Michael.* U.S. Role in the World: Background and Issues for Congress // Congressional Research Service. 2019. URL: https://fas.org/sgp/crs/row/R44891.pdf (дата обращения: 04.04.2020).

[208] Renewed Great Power Competition: Implications for Defense – Issues for Congress // Congressional Research Service. 2019. August 5. URL: https://fas.org/sgp/crs/natsec/R43838.pdf (дата обращения: 03.04.2020).

порядок» переживет трудности нынешнего этапа мирового развития. По его мнению, причина современного кризиса заключается в том, что однополярный порядок в значительной степени был ограничен кругом государств-единомышленников, сконцентрированных по обе стороны Атлантики и «не включал в свою орбиту страны незападного мира – Китай, Индию и государства советского блока»[209].

Не исключено, что по указанной причине в деятельности нынешней администрации США прослеживается стремление трансформировать доминировавшую до недавнего времени модель миросистемы – и не обязательно с упором на либеральные ценности или при поддержке союзников и партнеров. Об этом, в частности, свидетельствует «ломка» учрежденного самим Вашингтоном после Второй мировой войны принципов «мирового общежития». По сути, стратегия действующего американского истеблишмента отражает понимание того, что либеральный миропорядок движется к своему закату и создавать нечто новое Соединенным Штатам необходимо заблаговременно, лишь в интересах Америки, пока еще обладающей решающим голосом в утверждении международных реалий.

Данный внешнеполитический курс вызывает неприятие европейских союзников Вашингтона, вписанных (в отличие от Китая и России) в «миропорядок, основанный на правилах» и честно действующих в его рамках. Например, это прослеживается в «германском манифесте», опубликованном в 2017 г. группой экспертов по внешней политике, представляющих ФРГ. В частности, в публикации отмечается, что действия президента Д. Трампа «ставят под угрозу мировой порядок, нанося тяжелый удар по нормативным основам западного либерализма». Авторы документа акцентируют внимание на целесообразности сохранения политического статус-кво во взаимоотношениях трансатлантических партнеров, однако прогнозируют дальнейшее расхождение

[209] *Nye Joseph.* Will the Liberal Order Survive? The History of an Idea // Foreign Affairs. 2017. Vol. 96, № 1. p. 10–16.

интересов Германии и США относительно вопросов энергетической, миграционной, климатической политики и пр. [210].

Между тем многие западные эксперты указывают на то, что кризис «либерального мирового порядка» возник задолго до избрания Д. Трампа президентом США. Так, автор критического анализа «германского манифеста» Дж. Бэсби указывает, что нынешний глава Белого дома явился лишь порождением такого кризиса. По мнению Дж. Бэсби основные причины краха либерального миропорядка связаны «с фундаментальными изменениями в мировой политике, в частности, ростом числа негосударственных акторов, фрагментацией глобального управления, появлением новых идей и норм, многие из которых не являются частью либерального проекта управления, расширением глобальной и функциональной взаимозависимости». Автор констатирует, что в современных реалиях возврат к «либеральному порядку» является уже невозможным[211].

Дискуссии относительно будущего американоцентричного мироустройства еще более усилились в свете вспышки нового коронавируса, в 2020 г. обострившей многие социальные, экономические и политические проблемы во многих странах мира. В западном сообществе явственно выплеснулось наружу ожидание тектонических сдвигов сложившихся ранее структур миропорядка и формирования новой геополитической расстановки сил.

В условиях нынешней пандемии в фокусе внимания отечественных и зарубежных политологовоказался прежде всего вопрос об ускорении эрозии глобальной мощи США ввиду их неспособности справиться с общей для человечества угрозой. Например, крупные американские международники К. Кэмпбелл и Р. Доши прямо указали, что Соединенные Штаты находятся в преддверии своего «суэцкого момента», намекая на окончательный закат

---

[210] In Spite of It All, America. A Transatlantic Manifesto in Times of Donald Trump – A German Perspective // New York Times. 2017. October. URL: http://trotzdem-amerika.de (дата обращения: 04.04.2020).

[211] *Busby Josh.* Entering the Global Multilogue – A Replique to the German ZEIT Manifesto // Duck of Minevra. 2017. URL: https://duckofminerva.com/2017/10/entering-the-global-multilogue-a-replique-to-the-german-zeit-manifesto.html"https://duckofminerva.com/2017/10/entering-the-global-multilogue-a-replique-to-the-german-zeit-manifesto.html (дата обращения: 03.04.2020).

Британской империи по итогам известных событий 1956 года. Аналитики обосновали свой тезис тем, что со времен Второй мировой войны влияние США определялось не только их экономической мощью, но также стабильностью системы государственного управления и способностью скоординировать оптимальное распределение ресурсов в условиях кризиса. В период пандемии 2020 г. Америка продемонстрировала слабость, тогда как Китай, «воспользовавшийся возникшим вакуумом глобальной власти», фактически занял позицию мирового лидера[212].

Таким образом, в западном экспертном сообществе превалирует точка зрения, что американоцентричный миропорядок близится к своему закату в свете динамичного упадка традиционных и возвышения новых центров силы. Вместе с тем специалисты указывают, что нестабильное и переходное состояние текущей международной ситуации учитывается вашингтонской элитой. Но ее методы становления «обновленной однополярности» слишком радикальны для государств, привыкших следовать букве международного права. Они соответствует видению нынешнего американского руководства, но не традиционных союзников и партнеров США.

Полицентричный миропорядок

Актуальные тенденции мировых политических процессов не исключают установления какого-либо формата многополярного мира. Западные и отечественные политологи называют это по-разному: «кооперативная многополярность», «новая Вестфальская система», «многоплановый миропорядок» и пр. Вместе с тем следует отметить, что большая часть специалистов связывает возможность полицентричности с достаточно усеченным историческим периодом.

---

[212] *Campbell Kurt M., Doshi Rush.* Coronavirus Could Reshape Global Order // Foreign Affairs. 2020. March 18. URL: https://www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order?utm_campaign=Center%20for%20Northeast%20Asian%20Policy%20Studies&utm_source=hs_email&utm_medium=email&utm_content=85459036 (дата обращения: 03.04.2020).

На уязвимость однополярности указал еще в 2014 г. американский ученый и дипломат Г. Киссинджер в своей книге «Мировой порядок». Он связывал это с растущей несогласованностью деятельности многосторонних институтов в условиях форсированной глобализации, а также отсутствием эффективного механизма экстренного реагирования на глобальные проблемы. Соответственно, Г. Киссинджер усмотрел возможность эволюционной (невоенной) адаптации однополюсного миропорядка в четырехстороннюю модель, которая учитывала бы базовые цивилизационные ценности и исторические традиции государств:

1. Европейская система – основанная на Вестфальской модели суверенных государств с наделением равным статусом внутри системы;

2. Исламская система – идея об общем мире на основе законов исламской религии;

3. Китайская система – традиционные идеи «срединного царства»;

4. Американоцентричная система – с привлечением сторонников напористой политики США и под их началом[213].

В 2017 г. в киссинджеровском духе сформулировал концепцию «мультиплексного мира» американский политолог индийского происхождения А. Ачария. Ученый описал нынешний этап мирового развития как «мультиплексный мир», в котором «элементы либерального порядка выживают, но включаются в комплекс множества пересекающихся международных порядков». Он подчеркивал, что речь идет именно о многосоставном, а не многополярном миропорядке, понимая под этим «систему с множеством модернов, где западная либеральная современность (и ее предпочтительные пути к экономическому развитию и управлению) является лишь частью того, что предлагается международному сообществу». Ученый не исключал, что в скором будущем мир трансформируется в комплекс перекрестных, если не конкурирующих «глобализмов». Между тем на данном этапе развития возвышающиеся державы, по мнению А. Ачария, не способны форсировать

[213] *Киссинджер Г.* Мировой порядок [пер. с англ. В. Желнинова, А. Милюкова]. М.: Издательство АСТ, 2018. 512 с.

переход мира в полицентричный, поэтому единственным средством для них останется сохранение действующих международных институтов[214].

Современные труды американского ученого неореалиста Дж. Миршаймера также сводятся к возможности развития мировых политических процессов в сторону многополюсности. В статье «Обреченный на неудачу. Подъем и падение либерального международного порядка», Дж. Миршаймер выдвигает тезис, что в новом многополярном мире проявятся различные типы «подчиненных и взаимозависимых порядков»[215].

Ученый прогнозирует, что в обозримом будущем в мире утвердится три реалистических порядка: «слабый» (*thin*) международный порядок и два «жестко ограниченных» (*thick bounded*) порядка: один во главе с Китаем, другой – с Соединенными Штатами. Формирующийся «слабый» порядок будет касаться главным образом вопросов стратегической стабильности, функционирования мировой экономики, изменений климата и пр. Между двумя «жестко ограниченными» порядками Дж. Миршаймер полагает вероятным экономическое и даже военное противостояние. При этом он не исключает сохранение переплетения международных экономических связей между США и Китаем, хотя последний и «будет стремиться к чрезмерному наращиванию своей мощи».

Пекин, согласно взглядам аналитика, попытается создать новые институты, соответствующие его интересам, а также вовлечь в свою орбиту азиатских и европейских партнеров. Главным финансовым инструментом сотворения китайского «жесткого ограниченного» порядка станет Азиатский банк инфраструктурных инвестиций (*Asian Infrastructure Development Bank*), от участия в деятельности которого Вашингтон отказался. В целом соперничество между блоками, возглавляемыми Китаем и США, будет напоминать биполярный мир периода холодной войны, однако с существенно большей автономией государств, примыкающих к полюсам.

---

[214] *Acharya Amitav.* After Liberal Hegemony: The Advent of a Multiplex World Order. Ethics & International Affairs. 2017. Vol. 31. No. 3. P. 271–285.

[215] *Mearsheimer John J.* Bound to Fail. The Rise and Fall of the Liberal International Order // International Security. 2019. Vol. 43. No. 4. P. 7–50.

С точки зрения ученого, Россия попытается остаться в стороне от присоединения к проектам Соединенных Штатов и Китая и попытается создать свой собственный порядок на основе региональных институтов, находящихся под ее влиянием. Вместе с тем в случае серьезного экономического ослабления не исключается возможность интеграции (хотя и незначительной) РФ в «жесткий миропорядок» США. Если Москва выберет сторону Пекина, то ее степень вовлеченности в «сильный ограниченный» порядок Китая будет незначительной. Соответственно, по мнению Дж. Миршаймера, США должны приложить усилия к тому, чтобы «вытянуть» Россию из орбиты влияния КНР и интегрировать ее в американский порядок.

В подобном ключе желательную для англосаксов расстановку сил в треугольнике США – Россия – Китай анализирует британский историк Н. Фергюсон. Он обращает внимание мирового сообщества на ожидаемую в 2021 г. 50-летнюю годовщину тайной поездки Г. Киссинджера в Пекин, ставшей «ключевым моментом холодной войны»: тогда раскол в отношениях между КНР и СССР был использован, чтобы объединить Вашингтон и Пекин против Москвы. Соответственно, по мнению Н. Фергюсона, американской элите необходимо заново освоить уроки дипломатии конца XX века. Окончательная цель американской стратегии 2020-х гг. должна состоять в том, чтобы добиться зеркального отражения маневра Г. Киссинджера, разобщив российского и китайского лидеров и подтолкнув Россию в западную конфигурацию, якобы «спасая ее от поглощения динамичным Китаем». Пока же указанные державы, наряду с Индией и ЕС, будут, видимо, выступать в качестве полюсов формирующейся полицентричности[216].

В целом зарубежные эксперты не исключают утверждения в обозримом будущем какой-либо проекции многополюсного мира. Отмечается, что государства и международные объединения, которые смогут предложить

[216] *Ferguson Niall.* Donald Trump must split up Putin and Xi, the new odd couple // The Times. 2020. January. URL: https://www.thetimes.co.uk/article/donald-trump-must-split-up-putin-and-xi-the-new-odd-couple-7rtgcb2qc (дата обращения: 07.04.2020).

конкурентоспособную концепцию экономического и общественно-политического развития, гарантирующую взаимоприемлемую базу для интеграции ее потенциальных участников при сохранении их национальной безопасности и цивилизационного своеобразия, смогут претендовать на роль ядра интеграции в каждом из центров многополярного мира. Однако ряд политологов опровергают жизнеспособность такой системы, утверждая, что она может стать лишь неким «переходным состоянием» к более стабильному устройству – одно– или двухполюсному порядку.

Биполярная система

Авторитеты зарубежной политологической мысли признают возможность возврата мира к двухполюсному антагонизму в международных отношениях, центрами которого выступят Соединенные Штаты Америки и Китай. Но такой сценарий вряд ли повторится в его исконной форме ввиду отсутствия явного американо-китайского идеологического противостояния, присущего конфликтности СССР и США. Не меньшую роль в развитии антагонизма двух держав играет и экономическая взаимозависимость Вашингтона и Пекина, обусловленная их сильной вовлеченностью в глобальные торговые и инвестиционные процессы. Кроме того, утверждение новой биполярности может осложниться присутствием в мировой экономике и политике других центров силы, обладающих значительным геополитическим потенциалом (Евросоюз, Россия, Индия и пр.), которые не всегда будут готовы следовать моделям, предлагаемым США или Китаем.

Одними из первых перспективы двухполюсного мира, основанного на американо-китайском противостоянии, описали упомянутые выше британский историк Н. Фергюсон («Кимерика», Chimerica = China + America, 2008 г.) и американский политический деятель Зб. Бжезинский («Большая двойка» – G2, 2009 г.). Хотя еще в 1997 г. Зб. Бжезинский указывал, наиболее серьезной и долгосрочной угрозой мировой гегемонии США может стать «великая коалиция» Китая и России, «объединенная не идеологией, а взаимодополняющими обидами».

Влиятельный дипломат вернулся к этому тезису двадцать лет спустя, в 2017 г.[217]. Однако вскоре концепцию Зб. Бжезинского раскритиковал крупный американский китаист О.Шелл. В статье под названием «Позорный крах Кимерики», опубликованной в апреле 2020 г. в американском журнале «Форейн полиси», аналитик указал на тектонические сдвиги, с которыми столкнется мир в связи с пандемией коронавируса. Примечательно, что в качестве движущих сил этих сдвигов ученый назвал американо-китайское противоборство. Его движущей силой может стать, по мнению О. Шелла, то, что Пекин вышел из кризиса пандемии «еще более самовластным, агрессивным и склонным к конфликтам с либерально-демократическим, «основанным на правилах» порядком», тогда как Америка продемонстрировала лишь собственную слабость[218].

В книге бывшего замминистра обороны США Г. Эллисона под названием «Обреченные на войну: смогут ли Америка и Китай избежать ловушки Фукидида?» проанализированы 16 конфликтов между новой, находящейся на подъеме державой и уже существующей, которые имели место в мировой истории. Американский стратег выяснил, что в 12 случаях такое соперничество приводило к военным конфликтам. Г. Эллисон констатировал, что применительно к современному противостоянию США и Китая «риски Фукидида» существенно возрастают в связи с «цивилизационной несовместимостью», усугубляющей конкуренцию держав. Подобное несоответствие якобы налицо проявляется в глубоких разногласиях американцев и китайцев в оценке роли государства, экономики, личности, отношений между странами и даже сущностной природы времени[219].

---

[217] Цит. по.: *Allison Graham*. China and Russia: A Strategic Alliance in the Making // The National Interest. 2018. December 14. URL: https://nationalinterest.org/feature/china-and-russia-strategic-alliance-making-38727 (дата обращения: 03.04.2020).

[218] *Schell Orville.* The Ugly End of Chimerica // Foreign Policy. 2020. April. URL: https://foreignpolicy.com/2020/04/03/chimerica-ugly-end-coronavirus-china-us-trade-relations/ (дата обращения: 09.04.2020).

[219] *Allison Graham.* China vs. America. Managing the Next Clash of Civilizations // Foreign Affairs. 2017. September/October. URL: https://www.foreignaffairs.com/articles/united-states/2017-08-15/china-vs-america (дата обращения: 04.04.2020).

Повышенное внимание перспективам американо-китайского противоборства уделяет американский экономист, профессор экономики Нью-Йоркского университета Н. Рубини в статье под названием «Глобальные последствия китайско-американской холодной войны». По его мнению, в обозримом будущем соперничество между США и КНР неизбежно. Однако обе стороны, полагает Н. Рубини, могли бы управлять этим соперничеством конструктивно, допуская сотрудничество по одним вопросам и конкуренцию– по другим. Пока же в Вашингтоне отсутствует осознание того обстоятельства, что новой державе, которая находится на подъеме, должна быть предоставлена «определенная роль в формировании глобальных институтов и правил международного общения». Американский экономист прогнозирует, что в будущем мир разделится на два несовместимых между собой экономических блока – проамериканский и прокитайский. Исход борьбы за привлечение на свою сторону союзников (прежде всего России и Евросоюза) во многом повлияет на то, кто в конечном итоге – США или КНР – станет мировым гегемоном[220].

Представитель китайской геополитической мысли, декан Института международных отношений в Университете Циньхуа Я. Сюэтун в статье «Эпоха непростого мира. Китайская сила в разделенном мире» также прогнозирует утверждение биполярного американо-китайского порядка. Однако, по мнению представителя Поднебесной, для такого альянса будут характерны временные союзы государств, нацеленные на решение насущных проблем, а не устойчивые противостоящие друг другу блоки, разделенные несовместимой идеологией. Он полагает, что риск прямого военного столкновения между США и Китаем «ничтожно мал», соответственно, ни одна из сторон не будет выстраивать или поддерживать обширную и дорогостоящую сеть альянсов, которым ни Пекин, ни Вашингтон сегодня не способны предложить объединяющую привлекательную идею.

---

[220] The Global Consequences of a Sino-American Cold War // Project Syndicate. 2019. May 20. URL: https://www.project-syndicate.org/commentary/united-states-china-cold-war-deglobalization-by-nouriel-roubini-2019-05?barrier=accesspaylog (дата обращения: 09.04.2020).

Ученый Я. Сюэтун приходит к выводу, что в перспективе американо-китайская биполярность вряд ли будет выглядеть как «идеологический экзистенциальный конфликт по поводу фундаментального характера мирового порядка». Скорее, это примет форму конкуренции за потребительские рынки и технологические преимущества, которая выплеснется наружу в спорах о нормах и правилах торговли, инвестиций, трудоустройства, обменных курсов и интеллектуальной собственности. Взамен образования военно-экономических блоков большинство стран возьмет на вооружение «внешнюю политику двух путей», занимая сторону Америки по одним вопросам, КНР – по другим. Причем такой итог, по мнению китайского эксперта, предопределен военно-экономической мощью двух государств и не зависит от того, «восстановятся ли Соединенные Штаты от лихорадки эпохи Д. Трампа и возглавят ли они новый виток устремлений к либерализму»[221].

Примечательно, что все чаще перспективы становления биполярности находятся в фокусе интересов американских специалистов. Так, в докладе Н. Роллан из Национального бюро азиатских исследований США (*The National Bureau of Asian Research*) обращается особое внимание на усиливающуюся из КНР критику современного мироустройства. По мнению автора документа, это свидетельствует о попытках выстраивания Китаем фундамента новой системы мировой политики, которая будет функционировать в интересах действующих властей этой страны, а не действующего глобального гегемона[222].

Говоря о попытках Поднебесной создать условия для формирования новой системы международных отношений, Н. Роллан отмечает, что действующее руководство этой страны не стремится взять на себя чрезмерные обязательства. Оно якобы намерено выстроить порядок, где Китай пользовался бы частичной гегемонией, но в преференциальных для него сферах, прежде всего

---

[221] *Xuetong Yan* . The Age of Uneasy Peace. Chinese Power in a Divided World // Foreign Affairs. 2019. January/February. URL: https://www.foreignaffairs.com/articles/china/2018-12-11/age-uneasy-peace (дата обращения: 03.04.2020).

[222] *Rolland Nadege.* China’s Vision for a New World Order // The National Bureau of Asian Research. NBR Special Report № 83. 2020. January. URL: https://www.nbr.org/publication/chinas-vision-for-a-new-world-order/ (дата обращения: 09.04.2020).

экономической. По прогнозу американского аналитика, даже при таких «усеченных» амбициях КНР путь к становлению новой системы международных отношений будет неизбежно ознаменован борьбой между действующим и возвышающимся гегемонами и примыкающим к ним «лагерями». Таким образом, по мнению автора доклада, в обозримой перспективе не только развивающиеся, но и развитые страны станут своеобразным «полем битвы» между Вашингтоном и Пекином. Соответственно, можно ожидать долговременного процесса становления двухполюсной системы, где наиболее продвинутые в отдельных областях государства постепенно разделятся на проамериканский и прокитайский блоки. Н. Роллан прогнозирует, что с учетом выделенных китайскими властями ресурсов на изменение мировой архитектуры, в более отдаленном будущем можно прогнозировать не только грядущую потерю США роли глобального гегемона, но также потенциальную эрозию основных «демократических» прав и свобод человека и гражданина, а также международного права в целом.

В целом в последние несколько лет проявления новой, хотя и несколько «деформированной» биполярности усилились. К ним, например, относится растущее давление администрации Д. Трампа на Пекин, в том числе выражающееся в попытках затруднить реализацию жизненно важной для Поднебесной инициативы геополитического масштаба «Пояс и путь». В качестве рубежа, после пересечения которого эскалация противоречий между Соединенными Штатов с Китаем будет только наращиваться, можно рассматривать пандемию COVID-19. Соответственно, с позиций сегодняшнего дня тенденция усиления противостояния между теряющими силу США и укрепляющей мощь КНР, даже вне зависимости от результатов президентских выборов в Америке в 2024 гг., выглядит необратимой.

Бесполюсный мир

Некоторые зарубежные специалисты в области международных отношений придерживаются позиции о несостоятельности формирования некого нового мироустройства с рельефно выделяющимися полюсами, хотя фактически эпоха однополярности завершилась. Они обосновывают вероятность формирования

мира без полюсов принципиально новым качеством международной жизни, которое характеризуется потерей глобального управления. В пользу данного предположения поспособствовала пандемия коронавируса, ставшая эпохальным событием современной истории.

В 2008 г. президент американского Совета по международным отношениям Р. Хаас предложил теорию неполярного мира. Он объяснил наступление новой эпохи тремя факторами. Первый фактор, по мнению Р. Хааса, связан с естественными процессами подъема и упадка государств и появлением в мировой политике «акторов вне суверенитета». Второй фактор он связал с провалами политики самих Соединенных Штатов, ослабивших собственные позиции и ускоривших появление в мире альтернативных центров силы (примечательно, что в 2019 г. данный тезис стал ведущим и в обосновании смены миропорядка американского политолога Ф. Закария). Наконец, бесполярность, по Р. Хаасу, стала неизбежным следствием глобализации (и даже гиперглобализации), которая, создав трансграничный мир, привела к разрушению миропорядка и поспособствовала утверждению бесполюсной политической системы[223].

В 2011 г. упомянутый выше американский экономист Нуриэль Рубини также предположил, что мир движется к состоянию бесполюсности. Его идея «мира большого нуля» проистекает из тезиса о том, что международные форумы и организации (в частности, G20) стали неэффективными применительно к современным политическим реалиям. Соответственно, любые попытки решить в их рамках глобальные проблемы мирового развития являются не более чем «результатом с нулевой суммой» [224].

Несмотря на внешнюю реакционность концепций бесполюсного мира, распространение в 2020 г. новой для человечества болезни – COVID-19 – приблизило именно такой тип мироустройства. Так, акцентируя внимание

---

[223] *Хаас Р.* Эпоха бесполярного мира // Россия в глобальной политике. 2008. 20 июля. URL: https://globalaffairs.ru/number/n_11144 (дата обращения: 08.04.2020).

[224] *Roubini Nouriel.* Our G-Zero World // Project Syndicate. 2011. February 11. URL: https://www.project-syndicate.org/commentary/our-g-zero-world?barrier=accesspaylog (дата обращения: 08.04.2020).

международного сообщества на перспективах трансформации миропорядка после вспышки коронавируса, Г. Киссинджер назвал пандемию 2020 г. «рубежным событием», последствия которого будут иметь «колоссальный и разрушительный эффект» для всего международного сообщества. Дипломат призвал ведущих зарубежных лидеров прекратить «споры о прошлом», объединить усилия и приступить к формулированию принципов мироустройства будущего, а США – извлечь уроки из опыта плана Маршалла и Манхеттенского проекта.

По мнению Г. Киссинджера, политическим элитам следует предпринять усилия в трех направлениях. Во-первых, необходимо выйти на передовые рубежи науки и создать адекватные современности технологии планирования действий в чрезвычайных ситуациях. Во-вторых, сконцентрироваться на восстановлении мировой экономики. Наконец, американский дипломат указал на важность сохранения незыблемости принципов «либерального мирового порядка»[225].

В целом, первая часть предложений Г. Киссинджера выглядит вполне разумной: восстановление экономики и развитие науки. Однако удержание доминанты «либерального миропорядка», скорее всего, будет для США существенно затруднено, что обусловлено отсутствием привлекательного наполнения данной идеи, которая могла бы стать универсальной максимой для наиболее динамично развивающихся государств мира, прежде всего азиатских.

Согласно другим оценкам западных политологов и государственных деятелей, в условиях обострения глобальных проблем на фоне пандемии COVID-19 ее вероятным следствием может стать повышенная турбулентность в зонах латентной нестабильности и открытых военных конфликтов. Выступая перед американскими военнослужащими в марте 2020 г. тогдашний министр обороны США М. Эспер и председатель Объединенного комитета начальников штабов М. Милли отметили, что экстренные обстоятельтсва первой половины 2020 г. негативно скажется на устойчивости государственного управления в ряде стран

[225] *Kissinger Henry.* The Coronavirus Pandemic Will Forever Alter the World Order // The Wall Street Journal. 2020. April 03. URL: https://www.wsj.com/articles/the-coronavirus-pandemic-will-forever-alter-the-world-order-11585953005 (дата обращения: 08.04.2020).

мира. Сопутствующий этим процессам «дефицит безопасности» трансформируется в существенную угрозу национальным интересам отдельных мировых держав, прежде всего США. Одновременно, уточнил М. Эспер, коронавирус может вызвать спиралевидное погружение некоторых стран в состояние глубокой дестабилизации, которая выйдет далеко за рамки проблем здравоохранения и в итоге приведет к политическому хаосу[226].

Примечательно, что в качестве наиболее вероятных сценариев дстабилизации мировых политических процессов представители западной политической науки называют именнно усиление информационного противоборства в его разнообразных проявлениях между основными участниками мировой политики. К таковым они относят:

1. Кибератаку против одной из крупных держав (США, Китай, Россия, Иран), перерастающую в военный конфликт. Не исключается, что следствием подобного развития событий может стать масштабная техногенная катастрофа[227].

2. Крупную информационную операцию, которая может спровоцировать нверную и/или скоропалительную интерпретацию намерений и планов одной из крупных держав с последующим перетеканием в военный конфликт (по подобию сценария 1983 г., когда проведение военных учений НАТО было понято в СССР как начало агрессии и резко повысило риск конфликтной эскалации между странами)[228].

3. Военный инцидент с участием американских и китайских / американских и российских военных, вызванный накалом информационного противоборства на фоне кризисных проявления функционирования нынешней системы международных отношений. Вероятным местом подобных инцидентов называется Сирия, а также регионы Черного и Балтийского морей (Россия / США)

---

[226] COVID–19 – a trigger for global transformation? // Finnish Institute of International Affairs. 2020. March. URL: https://www.fiia.fi/wp-content/uploads/2020/03/wp113_covid-19_a-trigger-for-global-transformation.pdf (дата обращения: 08.04.2020).

[227] Developing Cybersecurity Capacity // RAND. 2018. December. URL: https://www.rand.org/pubs/research_reports/RR2072.html (дата обращения: 08.04.2020).

[228] Preparing for War in Korea // RUSI. 2017. September. URL: https://rusi.org/publication/whitehall-reports/preparing-war-korea (дата обращения: 08.04.2020).

либо акватория Южно-Китайского моря (КНР / США)[229]. Вероятность эскалации американо-китайского военного конфликта представляется зарубежным военным аналитикам более высокой по сравнению с американо-российским столкновением[230].

В сложившейся на фоне соперничества за цифровое превосходство характеризующейся высокой степенью нестабильности, дебютная часть каждого из приведенных вариантов развития возможна. Причем даже последствия этого могут привести к глобальным по своему масштабу последствиям. Тревожным сигналом в данном контексте является отсутствие (в киберсфере), разрушение (в области контроля над вооружениями и режима нераспространения) или игнорирование (в экономической сфере) соответствующих международно-правовых норм, формирующих механизмы стратегического сдерживания.

Таким образом, **современные процессы цифровизации ставят под вопрос возможность сохранения прежних моделей в мировой экономике и политике. Видимо, новая социально-политическая и экономическая реальность будет оформляться в самое ближайшее время с активным использованием инструментов информационного противоборства, прежде всего в виртуальной среде, но в итоге может спровоцировать полномасштабную ломку нынешнего формата мирового устройства.** В период трансформации можно ожидать повышенной вероятности возникновения новых «случайностей», более характерных для мира без полюсов.

Наиболее активны в рамках подготовки перехода к новому технологическому укладу Соединенные Штаты. В последние годы они исследуют возможности внедрения перспективных разработок в практику ведомств, обеспечивающих национальную безопасность. Одновременно Белый дом пытается прощупать пути более эффективного противодействия потенциальным

---

[229] *Cooper Julian.* If War Comes Tomorrow: How Russia Prepares for Possible Armed Aggression // RUSI. 2016. August. URL: https://rusi.org/publication/whitehall-reports/if-war-comes-tomorrow-how-russia-prepares-possible-armed-aggression (дата обращения: 07.04.2020).

[230] Water Wars: Disjointed Operations in the South China Sea // Lawfare. 2019. May 21. URL: https://www.lawfareblog.com/water-wars-disjointed-operations-south-china-sea (дата обращения: 08.04.2020).

противникам (прежде всего, Китаю и России) посредством навязывания национальным технологическим гигантам ограничений на торговлю с зарубежными конкурентами. Предпринимаемые США попытки создания административных завалов на перспективных направлениях демонстрируют давление на крупных китайских производителей цифровой инфраструктуры, с целью добиться долгосрочных преимуществ для Америки на рынке цифровых технологий.

В данной связи следует выделить тот факт, что в информационном противоборстве, которое развернулось между КНР и США на фоне споров о происхождении коронавируса, ЕС твердо поддержал позицию трансатлантического партнера. Американцы, решая собственные геополитические задачи, умело воздействовали на болевые точки Евросоюза, связанные с восприятием Китая. Они апеллировали к таким важным для Запада темам, как негативное влияние Пекина на процессы противостояния «либеральных демократий» и «авторитарных режимов» в Европе, нарастание проблем в области правозащитной проблематики, усиление экономической зависимости ЕС от КНР и пр.[231]

Вместе с тем в свете накопленных к настоящему времени проблем общемирового значения, зарубежные ученые полагают невозможным сохранения гегемонии США в прежней форме. По их оценкам, так называемый либеральный порядок нестабилен и близок к состоянию кризиса. В качестве альтернативы аналитики нередко видят многополярность, которая воспринимается ими как сообщество относительно равноправных международных партнеров, принципы взаимодействия между которыми обеспечивает ООН, а в более отдаленной перспективе, возможно, и другие, новые международные институты. Утверждению такого сценария способствует растущая настоятельность запроса

[231] *Yixiang Xu.* Reviving China’s Health Silk Road Initiative? Battle of Narratives and Challenges for Transatlantic Leadership // American Institute for Contemporary German Studies, 2020. March. URL: https://www.aicgs.org/2020/03/reviving-chinas-health-silk-road-initiative-battle-of-narratives-and-challenges-for-transatlantic-leadership/ (дата обращения: 03.05.2020).

населения многих государств на некое «справедливое» мировое управление взамен жесткому диктату Вашингтона.

В данных условиях Китай взял курс на создание альтернативного американскому формата миропорядка. Примечательно, но в своей деятельности руководство КПК опирается на действующие международные структуры (ООН, ВТО и пр.), сужая для Белого дома спектр легитимных возможностей противодействия Пекину. Действуя в рамках этой парадигмы, китайские власти стремятся к дозированной трансформации нынешней модели управления экономическими и социально-политическими процессами. По мнению американских специалистов, такой подход может сыграть решающую роль в формировании системы международных отношений в интересах КНР. Одновременно, с учетом соблюдения Пекином действующих норм и принципов международного права, указанная линия поведения позволяет ему политически лавировать, не допуская втягивания в открытый вооруженный конфликт с Вашингтоном и его сателлитами[232].

Китайские документы стратегического планирования свидетельствуют о том, что Пекин будет «выстраивать все проекции цифровой геополитики строго по своим собственным правилам»[233]. КНР избрала курс на форсированное научно-технологическое развитие внутри страны. Одновременно китайский бизнес под патронажем госструктур активно инвестирует в развитие цифровой инфраструктуры в Азиатско-Тихоокеанском регионе и в Африке. Китай категорически не устраивает ситуация, при которой функционирование интернета регулируется специализированными западными технологическими корпорациями якобы международного значения. Это подталкивает китайские власти к принятию мер по укреплению роли КНР в управлении глобальным информационно-коммуникационным пространством. Одним из средств достижения указанной

[232] *Harding Brian.* China's Digital Silk Road and Southeast Asia // Center for Strategic and International Studies. 2019. February 15. URL: https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia. (дата обращения: 13.10.2020).

[233] *Ding J., Triolo P., Sacks S.* Chinese Interests Take a Big Seat at the AI Governance Table // New America. 2018. June. URL: https://www.newamerica.org/cybersecurityinitiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/ (дата обращения: 13.10.2020).

цели является развернутая Пекином активность по разработке и внедрению нового интернет-протокола (New IP) вместо существующего TCP/IP[234].

Важность приятия нового интернет-протокола мировым сообществом китайская сторона объясняет именно стремительным развитием цифровых технологий и ожидаемым в ближайшем будущем экспоненциальным ростом интернета вещей[235], появлением виртуальной и дополненной реальности, новых возможностей в области квантовой связи, искусственного интеллекта и пр. Соответственно, уже в обозримом будущем человечество столкнется с необходимостью высокоскоростной, безошибочной и бесперебойной передачи огромных массивов данных, при то что практически исчерпавшая свой потенциал в условиях стремительной цифровизации архитектура TCP/IP этого обеспечить не сможет.

Кроме того, Пекин считает принципиально важным реализацию в рамках New IP концепции «цифрового суверенитета» (в терминологии западных экспертов – «цифрового авторитаризма»). В рамках данной концепции государства смогут более эффективно регулировать национальное киберпространство и контролировать интернет-трафик, блокируя интернет-ресурсы вредоносного или неизвестного наполнения, отказывая в доступе к сети анонимным и неблагонадежным абонентам, что существенно снижает риски кибератак.

По оценкам зарубежных политологов, Пекин якобы нацелился на то, чтобы представить международному сообществу в позитивном свете собственное видение концепции «цифрового суверенитета» для установления системы глобального управления, соответствующей реалиям политического управления и экономики в условиях происходящей технологической революции. Вашингтонские аналитики трактуют это как попытки КНР «экспортировать

---

[234] TCP/IP – разработанный в 1972 г. пакет базовых протоколов Интернета, описывающий способ передачи данных в цифровом виде от источника к получателю. В названии использованы аббревиатуры двух важнейших протоколов – Transmission Control Protocol (TCP) и Internet Protocol (IP).

[235] Интернет вещей – концепция вычислительной сети физических предметов, оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и социально-политические процессы, исключающее из части действий и операций участие человека.

цифровой авторитаризм, который уже в обозримом будущем может подорвать реализацию демократических норм в международной политике, а также поставить под вопрос фундаментальные права человека и гражданина»[236].

В данных обстоятельствах, несмотря на внутриполитические трудности, США демонстрируют, что они отнюдь не готовы смириться с потерей звания глобального гегемона. В свете форсированной цифровизации они нацелились на сохранение своего технологического лидерства любой ценой, в том числе путем утверждения контроля над глобальным информационно-коммуникационным пространством. Поэтому надежды на действующую без всяких ограничений и границ глобальную информационно-коммуникационную сеть постепенно рассеиваются. Цифровые корпорации США и КНР воспринимаются, скорее, не как глобальные игроки, а как часть национальных экономик. Другим странам и их компаниям приходится трансформировать свою политику в технологической сфере в зависимости от геополитических предпочтений. Во многом это обусловлено тем, что корпорации и фирмы, которые обеспечивают развитие пользование интернетом во всевозможных вариациях, обязаны соблюдать законы национальных государств и вести свою работу в рамках рекомендаций национальных правительств.

В целом западные политологи сходятся во мнении о том, что даже при «усеченных» амбициях курс КНР на становление новой системы международных отношений будет реализовываться наряду с борьбой между действующим и возвышающимся гегемонами и примыкающим к ним «лагерями». Два указанных центра силы стремятся вовлечь в орбиту своего влияния как можно больше государств, особенно экономически развитых и многонаселенных. Обе стороны демонстрируют стремление к использованию поля мировой коммерции и логистических цепочек в качестве инструмента трансформации международной

[236] *Lewis James.* How Will 5G Shape Innovation and Security: A Primer // Center for Strategic and International Studies. 2018. December 6. URL: https://www.csis.org/analysis/how-5g-will-shape-innovation-and-security (дата обращения: 13.10.2020).

технологической, торговой и финансовой инфраструктуры для дальнейшего продвижения собственных интересов во все более поляризующемся мире[237].

По мере эскалации американо-китайского противостояния будущее мирового сотрудничества в области высоких технологий представляется экспертам все более мрачным. Аналитики «Евразия групп» (Eurasia Group) полагают, что в обозримой перспективе не только развивающиеся, но и развитые страны могут стать своеобразным «полем битвы» между Вашингтоном и Пекином. Соответственно, можно ожидать довольно оживленного процесса становления двухполюсной системы, разделенной «виртуальной Берлинской стеной» в технологической сфере, где наиболее продвинутые в отдельных областях государства размежуются на проамериканский и прокитайский блоки[238]. Это повысит вероятность фрагментации региональных технологических рынков и мирового технологического поля в принципе. В результате ухудшится и правовое взаимодействие в технологической сфере, формируя барьеры коммуникации между государствами, что только углубит дефицит безопасности. При реализации такого сценария можно прогнозировать окончательную эрозию действующего корпуса норм и принципов международного права.

В целом отсутствие критической массы предпосылок для успешной кооперации вероятных претендентов на активное участие в решении глобальных проблем создают комфортную среду международного общения все менее возможной, заставляя государства выбирать в пользу «меньшего из зол» – ослабленного, но близкого гегемона или возвышающегося, но пока еще чуждого. Данный выбор, видимо, будет сложным, поскольку, вопреки теории, ключевым разрушителем постбиполярного мироустройства сегодня выступает не новый претендент с собственными геополитическими амбициями, а нынешний «мировой

---

[237] *Kennedy Scott.* The Fat Tech Dragon: Benchmarking China's Innovation Drive // Harvard University. 2018. August. URL: https://fairbank.fas.harvard.edu/events/scott-kennedy-the-fat-tech-dragon-commercial-and-strategic-implications-of-chinas-hi-tech-drive/ (дата обращения: 13.10.2020).

[238] *Triolo Paul, Allison Kevin, Brown Clarise.* Eurasia Group White Paper: The Geopolitics of 5G // Eurasia Group. 2018. November 15. URL: https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public%281%29.pdf (дата обращения: 03.02.2020).

полицейский», который, по идее, должен бы стремиться сохранить статус-кво нынешнего порядка, однако сам провоцирует его ломку.

В отдельных регионах мира следствием политики ведущих акторов мировой политики по завоеванию технологического превосходства в условиях становления цифровой реальности уже стало размывание сдерживающих механизмов применения силы при повышении вероятности ее использования нетрадиционными методами. Несомненно, это ведет к разбалансировке самого каркаса миросистемы, ослаблению ее устойчивости.

В складывающихся обстоятельствах России было бы целесообразно в принципе остаться вне американо-китайского технологического противостояния. Однако ввиду заявленного курса на поддержку КНР, а также настоятельной необходимости выйти из-под диктата западных технологических корпораций, это представляется маловероятным. Необходимо активизировать фундаментальные и прикладные научные исследования в области высоких технологий, равно как и на практике внедрять соответствующие технологии в жизнедеятельность государства. Важно уделять больше внимания профессиональной подготовке отечественных специалистов с тем, чтобы поднять на более высокий уровень их знания, умения и навыки в области информационного противоборства, причем как в информационно-психологической, так и информационно-технической плоскости. Необходимо привлекать к научной и аналитической работе квалифицированных экспертов данного профиля, способных прогнозировать формирование новых вызовов и угроз в области информационного противоборства.

Указанные и прочие меры по купированию рисков, связанных с нынешним витком технологического соперничества между КНР и США, вероятно, позволят урегулировать для РФ проблему эрозии безопасности в условиях становления цифровой реальности, однако вряд ли поспособствуют ее окончательному решению в международном формате.

Глава 3. ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В УСЛОВИЯХ СТАНОВЛЕНИЯ ЦИФРОВОЙ РЕАЛЬНОСТИ

3.1. Современные разработки в области манипулирования социальными массами

Социальные массы использовались в качестве объекта политической и конкурентной борьбы на протяжении всей истории человечества. Однако в современных условиях «виртуализации» человеческой жизнедеятельности методики информационно-психологического воздействия стали развиваться форсированными темпами: эксперты обнаружили, что процессы социального управления можно технологизировать на новом уровне.

Одним из наиболее влиятельных экспертов в этой области является американский ученый А. Пентланд, бывший эксперт Национального управления по аэронавтике и исследованию космического пространства США. В настоящее время этот ученый возглавляет лабораторию динамики человека в Массачусетсском технологическом институте.

В 2014 г. А. Пентланд предложил концепцию социальной физики. В своем исследовании ученый отмечает: «После установления поведения в группах, компаниях и целых городах оказалось, что модель коммуникации и, в частности модель смешивания поведения между разными группами, что я называют движением идей, был единственным существенным фактором, как для инновации, так и для продуктивности»[239].

На состоявшемся в 2015 г. семинаре А. Пентланда по социальной физике указывалось, что подробные данные о поведении человека, полученные благодаря социальным сетям, сотовым телефонам, кредитным картам и другим подобным источникам, предоставляют ученым возможность отследить динамику социального научения человека и процесс принятия им решений. В основном, для

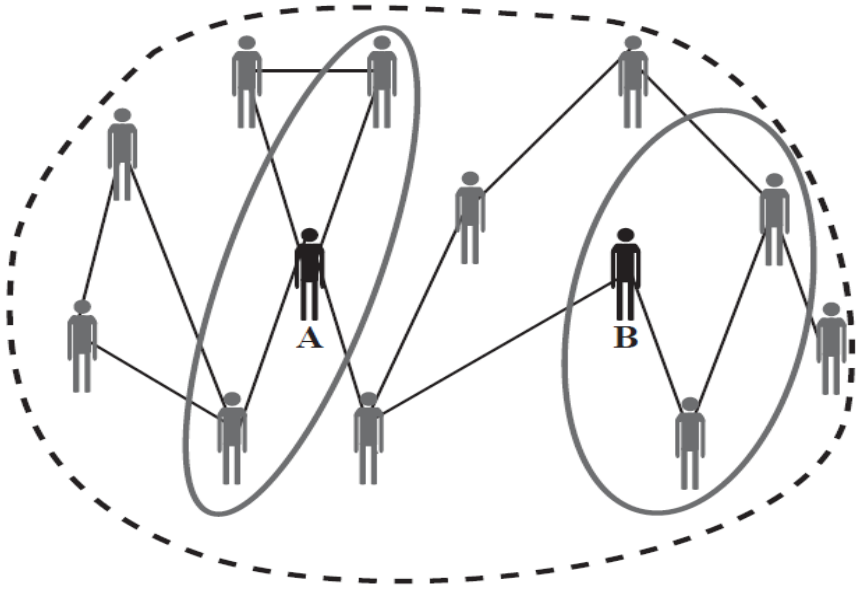
[239] Pentland A. Social physics. How good ideas spread — the lessons from a new science // Science Book a Day. 2014. URL: https://sciencebookaday.com/2014/08/01/science-book-a-day-interviews-alex-pentland/ (дата обращения: 19.04.2019).

решения таких задач используется потенциал гетерогенных стохастических сетевых моделей. Ученые также могут разработать механизмы стимулирования, которые будут влиять на поведение конкретной личности: «Такой подход поможет решить множество современных социально-политических и социально-экономических проблем, в частности, повысить производительность отдельных организаций или даже целых городов. В рамках исследований по данной проблематике будут проводиться эксперименты в масштабах от сотен до миллионов людей»[240]. В качестве применения результатов этой работы указывалось на возможность их применения в целях формирования новых моделей потребления и создания экономических кризисов.

Во многих работах, посвященных социальному управлению в условиях цифровой среды, А. Пентланд отмечает целесообразность создания государственной системы постоянного мониторинга и анализа процессов, развивающихся в виртуальном пространстве, посредством современных ИКТ. Он убежден, что в свете повышения социально-политических рисков необходим определенный диалог между властью и обществом. Используемый для этих целей анализ больших данных может с достаточно высокой степенью точности продемонстрировать связи, которые вызывают те или иные события в любой сфере жизнедеятельности человека»[241].

[240] Social Physics // Santa Fe Institute. 2015. URL: https://www.santafe.edu/events/social-physics (дата обращения: 19.04.2019).

[241] Science Book a Day Interviews Alex Pentland // Science Book a Day. 2014. URL: https://sciencebookaday.com/2014/08/01/science-book-a-day-interviews-alex-pentland/ (дата обращения: 21.06.2019).



Источник: Составлено по: *Pentland A.* Social physics. How good ideas spread — the lessons from a new science. — New York, 2014.

Рисунок 3.1 – Структура социальных коммуникаций по А. Пентланду

На Рисунке 3.1 продемонстрировано, что в условиях цифровой реальности **применение потенциала больших данных обусловливает расширение спектра возможностей для прогнозирования развития социально-политических процессов, однако макросоциальные последствия такого подхода пока изучены недостаточно.**

В целом в настоящее время на территории США действуют около 20 национальных лабораторий, где основными темами исследований являются:

- моделирование устойчивого развития человеческого общества;
- моделирование инноваций;
- динамика инфекционных заболеваний в условиях городской среды;
- непредвиденные ситуации в сложных эволюционных системах;
- динамические и количественные исследования человеческого поведения;
- организация и динамика живых систем[242].

Крупные проекты в указанной области ведет Управление перспективных исследований Минобороны США, призванное обеспечить сохранение технологического превосходства американских вооруженных сил. В частности,

[242] См. напр.: Experimental evidence of massive-scale emotional contagion through social networks // PNAS. URL: http://www.pnas.org/content/111/24/8788.full (дата обращения: 19.04.2019).

оно финансирует программы по исследованию потенциала социальных сетей. Например, в программе по исследованию роли социальных сетей в стратегической коммуникации *(Social Media in Strategic Communication)* принимали участие такие компании, как «Фейсбук», «Твиттер», «Пинтерест» *(Pinterest)* и «Кикстартер» *(Kickstarter).* В рамках эксперимента анализировалась активность пользователей указанных социальных сетей для построения в перспективе системы связей между людьми. Посредством манипулирования новостными потоками изучались индивидуальные процессы восприятия информации. По каждому пользователю сети был составлен профиль, отражающий порядка 150 характеристик. В результате конструировался механизм распространения в интернете необходимых потенциальному заказчику сведений[243]. Можно предположить, что подобные проекты реализуются прежде всего с целью выявления потенциала социальных сетей как пространства для ведения проправительственной пропаганды.

Управление перспективных исследований Минобороны США также активно выделяет гранты на разработку новых биометрических технологий. Это производится с целью изучения поведения личности, для чего применяются методы автоматической идентификации, основанные на физиологических или поведенческих характеристиках. В частности, именно в США было создана новаторская программа поведенческой биометрии *(Behavioral Biometrics).* В отличие от традиционных методов идентификации, адаптированных под нужды и особенности компьютеров (пароль и логин), современные позволяют компьютеру опознавать пользователя по его поведению. Они предложили именовать этот класс новаторских подходов к опознанию активной аутентификацией *(Active Authentication).*

Указанный набор концепций и моделей «поведенческого анализа» позволяет компьютерным системам без использования сложных паролей

[243] Цит. по: US military studied how to influence Twitter users in Darpa-funded research // The Guardian. 2014. July. URL: https://www.theguardian.com/world/2014/jul/08/darpa-social-networks-research-twitter-influence-studies (дата обращения: 18.04.2019).

самостоятельно распознавать пользователей по тем видам активности, которые строго индивидуальны для обычной деятельности отдельно взятого человека. В качестве примера можно назвать клавиатурный почерк, особенности движений пальцев при работе с мышью, экраном, сенсорной панелью и прочими манипуляторами. По утверждению создателей таких проектов, в дальнейшем их наработки могут быть использованы для создания технологической системы управления массами практически любой размерности[244].

Американцы ставят вопрос о расширении возможностей человеческого мышления. Изучению данного аспекта подчинено еще одно направление деятельности Управление перспективных исследований МО США, призванное создать устройства, имитирующие работу мозга человека (*Brain Initiative)*[245]. Эта сфера привлекает представителей Пентагона тем, что кора головного мозга успешно решает задачи распознавания образов в реальном времени и с достаточно низкими энергозатратами. Это, по их мнению, позволит в будущем эффективнее управлять не только пилотируемыми и беспилотными аппаратами, но и поведением человека. В частности, в рамках этой инициативы запланированы проекты, касающиеся реабилитации повреждений нервной системы, создания искусственного интеллекта, функционирующего подобно человеческому мозгу, и разработки эффективных интерфейсов человек – компьютер, позволяющих осуществить перевод мыслей индивида в цифровую форму и обратно. Как отмечают в ведомстве, поставленные перед учеными цели предполагают создание подобных технологий к 2020 г., и их запуск в массовое производство в последующие несколько лет.

Значительная роль в проведении подобных исследований отводится американским неправительственным организациям («мозговым центрам»). Большинство из них занимаются изучением военно-политических проблем, а

---

[244] См.: *Waitt T.* SecureAuth unveils behavioral biometric technology in partnership with DARPA-endorsed BehavioSec // AST. URL: https://americansecuritytoday.com/secureauth-unveils-behavioral-biometric-technology-in-partnership-with-darpa-endorsed-behaviosec/ (дата обращения: 18.04.2019).

[245] DARPA and the Brain Initiative // DARPA. URL: https://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative (дата обращения: 18.04.2019).

также вопросами строительства и применения вооруженных сил, результаты которых находят отражение практически во всех концептуальных документах Пентагона. Наиболее авторитетными организациями, работающими по перечисленным направлениям, являются: близкий к Пентагону исследовательский центр «Корпорация РЭНД», Массачусетский технологический институт, Институт Санта-Фе, Центр прикладного интеллекта и когнитивных наук при Университете Тафтса и пр.[246]

В качестве примера можно назвать разработки созданного в июне 2015 г. Пентагоном совместно с Инженерной школой Университета Тафтса Центра прикладного интеллекта и когнитивных наук. Он объединил экспертов в области психологии, неврологии, информационных технологий и робототехники с целью определения инновационных подходов к мониторингу мыслительных и физиологических процессов военнослужащих, изучения влияния различных состояний на их поведение в оперативной обстановке и оптимизация этого поведения посредством мультимодальных интерфейсов и роботизированных платформ**.**

Исследования разделены на четыре основные сферы:

1. Изучение принципов, обеспечивающих взаимодействие человека и интеллектуальных поддерживающих систем, которые нацелены на оптимизацию мышления и физических возможностей бойцов.

2. Исследование возможности управления такими состояниями, как напряжение, тревога, умственные перегрузки, стресс, страх, неуверенность и пр.

3. Изучение выполнения военнослужащими умственных и физических задач в реальной боевой обстановке с учетом соответствующих требований.

4. Исследования поведения бойцов в команде[247]**.**

---

[246] См. напр.: A General Agent-Based Model of Social Learning // RAND. 2017. URL: https://www.rand.org/pubs/research_reports/RR1768.html (дата обращения: 10.05.2018).

[247] См.: US Army, Tufts team up to advance cognitive science // DefenceTalk. 2018. URL: https://www.defencetalk.com/us-army-tufts-team-up-to-advance-cognitive-science-64761/ (дата обращения: 19.04.2019).

Как отмечают специалисты, Центр прикладного интеллекта и когнитивных наук находится под кураторством агентства Управления перспективных исследований Минобороны США[248].

Таким образом, тематика, масштабы и объемы финансирования лишь некоторых трудов, проводимых военными и экспертно-научными структурами Соединенных Штатов, демонстрирует намерения Вашингтона обладать эксклюзивными технологиями социального управления, которые могли бы быть применимы для достижения целей национального развития страны.

Результатом исследовательской работы американских экспертно-научных и военных ведомств является создание **информационно-аналитических платформ по мониторингу и моделированию социально-политического пространства.** В настоящее время подобные разработки все активнее используются в сочетании с новейшими технологиями психологической и информационной борьбы.

В частности, интерес представляют компьютерные модели прогнозирования поведением толпы. Так, еще в 2007 г. группа ученых из Университета Аризоны представила промежуточные результаты проекта «Моделирование поведения толпы» (*Modeling Crowd Behavior)*[249]**.** Исследователи представили разработку, которая позволяет прогнозировать варианты поведения толпы в различной обстановке и ситуациях. В данной системе используется «агент-центрированная методология», которая предполагает, что агенты (люди) в индивидуальном порядке наделены рядом характеристик (пол, возраст, телосложение, особенности здоровья и язык телодвижений и пр.), а для толпы в целом принимаются во внимание различные коллективные эмоции (спокойствие, паника и пр.). В соответствии с заданными параметрами агенты оценивают поступающую информацию, заражаются «эмоциями толпы», предпринимают различные

---

[248] См. напр.: Engineering Humans for War // The Atlantic. 2015. URL: https://www.theatlantic.com/international/archive/2015/09/military-technology-pentagon-robots/406786/ (дата обращения: 19.04.2019).

[249] См.: Mind of the Mob: The Geosimulation of Crowd Control // Yale Scientific Magazine. 2013. URL: http://www.yalescientific.org/2013/05/mind-of-the-mob-the-geosimulation-of-crowd-control/ (дата обращения: 18.04.2019).

стратегии коллективной деятельности. Тем самым формируются варианты массового социального поведения.

По мнению руководителя проекта, доцента Университета Аризоны П. Торренса, специалиста в таких специфических областях знания, как городская география и кибергеография, методика «Моделирование поведения толпы» может применяться как высокореалистичная среда для создания различных ситуаций, связанных с возникновением опасности для посетителей общественных мест. Как отмечает автор, он также смог ее использовать «для воспроизведения распространяющихся через повседневные контакты заболеваний в толпе». Проект Торренса спонсировался Национальным научным фондом США.

Другим достижением американских специалистов можно считать представленную в 2010 г. разработку главного советника по науке ВВС США М. Мейберри под названием «Социальный радар» *(Social Radar*). По замыслу автора, данный проект должен стать системой, которая позволяет видеть то, что происходит «в сердцах и умах людей» [250].

Целью разработки «Социальный радар» является раннее обнаружение и прогноз возможности и вариантов политической нестабильности в других государствах. М. Мейберри отмечает, что создание данной системы стало возможным благодаря ряду обстоятельств:

– насыщению информационного пространства структурированной и неструктурированной информацией, созданию программных продуктов, обеспечивающих эффективный поиск, мониторинг, кластеризацию и агрегацию такой информации;

– созданию «гиперсоциальной сети», включающей в себя транснациональные сети типа «Фейсбук», а также различные национальные сети, повсеместному распространению платформы «Твиттер» и соответствующих средств ее мониторинга, извлечения, агрегации и многоконтурной обработки полученной из нее информации;

---

[250] См.: Air Force’s Top Brain Wants a ‘Social Radar’ to ‘See Into Hearts and Minds’ // Wired. 2012. URL: https://www.wired.com/2012/01/social-radar-sees-minds/ (дата обращения: 18.04.2019).

– экспоненциальному росту аудио и видео контента в сети, происходящему в первую очередь за счет контента, поступающего с различного рода мобильных устройств;

– опережающему росту в интернете данных, полученных от различных подключенных к интернету устройств, от видеокамер до бытовой техники. С учетом привязки практически всех существующих программ и социальных сетей к системе геолокации появляется возможность в режиме реального времени получать картину событий, относящихся не только к определенным странам и социальным группам, но даже к отдельным местам и личностям;

– переводу средств массовой информации в электронный формат, а также процессу оцифровки ранее опубликованных изданий;

– развитию глобальных систем радиоэлектронной разведки (*ECHELON*), позволяющих вести тотальный мониторинг всех телекоммуникационных систем мира;

– созданию и практической отработке систем, позволяющих агрегировать для анализа и синтеза структурированные и неструктурированные информационные потоки в любых форматах и из любых источников (примером такой платформы является система «Палантир»).

Таким образом, проект «Социальный радар» базируется на интеграции информационных и когнитивных технологий, последних достижениях прогностики и систем распознавания образов, биометрии, социометрии и ряда других разработок социального знания. В настоящее время, как отмечает куратор проекта, он уже используется военным ведомством США.

Следует обратить также внимание на то, что в июле 2017 г. сайт госзакупок Соединенных Штатов опубликовал информацию о тендере по поиску компании-подрядчика для создания службы мониторинга социальных сетей, СМИ, блогов и форумов на основных европейских языках, в том числе, русском. Заказчиком данного тендера выступает ВМС США. По замыслу подрядчик должен организовать командный центр по работе с социальными сетями и предоставлять для Главного управления ВМС информацию о событиях, «представляющих для

него интерес» [251]. Как отмечается в документе, данные будут отслеживаться в режиме реального времени «по ключевым словам, словосочетаниям и интересующим социальным показателям»[252].

Активизировали разработки в области социокультурного моделирования военные и разведывательные структуры, а также подведомственные Пентагону экспертно-аналитические институты[253]. Например, в 2017 г. военное ведомство объявило конкурс на преподавание военной терминологии спецподразделениям Национальной гвардии США на русском, французском, арабском и испанском языках. Уже в мае 2018 г. Конгресс США поручил министру обороны представить доклад о наличии в американских войсках специалистов, владеющих русским, китайским и корейским языками. В законопроекте о финансировании Пентагона и его политике в 2019 г. отмечается, что не позднее чем через 180 дней после вступления закона в силу руководство военного ведомства должно будет оценить проблему нехватки квалифицированных специалистов со знанием указанных иностранных языков и предложить законодателям план ее решения – как в ближайшем будущем, так и в более отдаленной перспективе[254].

В целом рассмотренные выше технологии изучения и моделирования социально-политической обстановки позволяют субъекту управления решать следующие задачи:

– обнаруживать проблемы на ранних стадиях, отслеживая их дальнейшее развитие;

---

[251] D--Social Data Analytics Subscription Service // Federal Business Opportunity. 2017. July 26. URL: https://www.fbo.gov/index?s=opportunity&mode=form&id=89f601f3b1631165d227daf85ee917c9&tab=core&_cview=1 (дата обращения 13.05.2018).

[252] Ibid.

[253] См. напр.: Broad Operational Language Translation (BOLT) // DARPA. 2018. URL: https://www.darpa.mil/program/broad-operational-language-translation; IARPA Launches “MATERIAL” Program // DNI.GOV. 2017. December 22. URL: https://www.dni.gov/index.php/newsroom/press-releases/item/1829-iarpa-launches-material-program (дата обращения: 10.05.2018).

[254] H.R. 5515—FY19 NATIONAL DEFENSE AUTHORIZATION BILL // White House.gov. 2018. May. URL: https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/wysiwyg_uploaded/FY19%20NDAA%20Chairman%27s%20Mark%20Final.pdf (дата обращения 13.05.2018).

– обнаруживать «проблемных» людей, отслеживая их контакты;

– создавать соответствующий фон информационной среды.

Важным аспектом развития технологий социального манипулирования является проведение НИОКР по линии «хай–хьюм» (*HighHum*) – современных гуманитарных технологий, призванных оказывать долгосрочное контекстуальное влияние на широкую совокупность факторов (информационных, социальных, когнитивных и пр.), под воздействием которых формируется система ценностей общества. Фундаментальным отличием формирования массового сознания от прочих информационно-пропагандистских воздействий является то, что деятельность субъекта управления должна быть направлена не столько на формирование прямых угроз конкретным политическим силам и структурам, сколько на создание стимулов, способствующих запуску процессов трансформации идентичности у тех или иных групп населения, политизации настроений в различных социальных средах.

Конечной целью такой деятельности является создание идеологизированного конструкта, то есть искусственно создаваемой идентичности, на основе нетрадиционных для страны ценностей (антиценностей), социального поведения и политической активности на деструктивной базе, трансформированного исторического сознания. Впоследствии созданная идентичность может являться основой для формирования мотивации к определенной форме социального поведения, когда представители отдельных слоев населения (от активистов студенческой молодежи до экспертных кругов и политических элит) действуют в пользу противника без прямых «команд» и вознаграждений, а в силу «имплантированного» в них чуждого мировоззрения.

Важная функция технологий «хай–хьюм» – установление устойчивых связей между людьми и побуждение последних к определенным коллективным действиям. Анализ, координация работ по этому направлению и практическое руководство ими осуществляется в основном Управлением перспективных исследований в сфере разведки США *(IARPA).* По имеющимся данным, только за

2014–2015 гг. американские инвестиционные структуры увеличили вложения в «хай–хьюм» приблизительно в 5–5,5 раз[255].

Как полагают американские ученые, «благодатную среду» для распространения определенных идей и культивирования ценностей представляют собой социальные сети, что обусловливает подход США к исследованиям в сфере гуманитарных технологий и существенно способствует культурно-информационной экспансии Вашингтона. Этому способствует то обстоятельство, что поисковые сайты, почтовые сервисы и социальные сети, не попадают под действие национальных законов о средствах массовой информации, хотя и предоставляют своим пользователям новостной контент.

Следует также отметить, что колоссальный потенциал «мягкого» культурно-информационного воздействия заключают в себе социально ориентированные «образовательные» интренет-ресурсы. В этих целях широко применяются и так называемые вики-технологии. В частности, крупнейшая сетевая энциклопедия «Википедия» *(Wikipedia),* принадлежащая калифорнийской «благотворительной организации» *(Wikimedia Foundation),* сегодня претендует на роль главного источника знаний для рядовых пользователей сети всего мира. Благодаря популярности подобных ресурсов США формируют глобальную информационную повестку и транслируют свои политические ценности всему миру.

К процессам информационного противоборства, нацеленных на переформатирование социальных ценностей в конкретной социальной группе, стране или даже регионе, привлечены и непосредственно образовательные организации зарубежных стран. Например, с осени 2015 г. более десятка университетов США приступили к реализации в РФ программы «Обучение для всех» *(Teach For All).* Адаптацию программы под особенности российского населения осуществляла крупнейшая международная консалтинговая компания

[255] См. напр.: Угрозы безопасности России и перспективы отношений с НАТО и США: Сб. материалов / Под ред. д-ра экон. наук Г.Г. Тищенко, канд. полит. наук. А.В. Виловатых. М.: РИСИ, 2017. С.140–150.

«Бостон Консалтинг груп» (*Boston Consulting Group)* – крупный подрядчик Пентагона и разведсообщества США. За отбор кандидатов отвечает известная рекрутинговая компания «Оджес Бердстон» *(The Odgers Berdtson),* которая провела отбор кандидатов среди лучших выпускников российских ВУЗов в соответствии с запросами организаторов данного проекта. Их обучили основам педагогики, и в течение последующих двух лет они обучали российских школьников по методичкам «Обучения для всех», формируя «лидеров» российского общества по американскому образцу.

Важным элементом социального управления, реализующимся посредством цифрового прорыва человечества, являются современные интернет-сервисы, первоначально созданные в США. Они аккумулируют информацию о поисковых запросах пользователей по всему миру, нередко нарушая принцип конфиденциальности персональных данных, что открывает широкие возможности для применения технологий «цветных революций» и «управляемого хаоса». Это обусловлено тем, что военно-политические интересы госструктур США тесно переплетаются с коммерческими интересами крупных корпораций и неправительственных организаций. Например, базирующаяся в США Корпорация по управлению доменными именами и IP-адресами *(ICANN*), базирующаяся в Лос-Анджелесе, выполняет функции главного регулятора интернета, контролируя вопросы, связанные с присвоением доменных имен и выделением IP-адресов по всему миру.

В целом в настоящее время в американском правовом поле функционирует целый ряд компаний и ведомств, непосредственно решающих задачи по обеспечению национальной безопасности. В этой деятельности, например, участвуют:

– Компания «Гугл» совместно с венчурным фондом «Инкутел» развивают проект «Записанное Будущее» (*Recorded Future*) – платформу прогнозной аналитики по выявлению угроз и событий безопасности в сети интернет. Данная платформа вычленяет из контекста веб-страниц имена людей–объектов поиска,

упоминаемые ими места и события для того, чтобы анализировать «невидимые связи» этих личностей и прогнозировать их действия в будущем[256];

– частная компания «Палантир» развивает совместно с Управлением перспективных исследовательских проектов МО США программу «Тотальная осведомленность» *(Total/Terrorism Information Awareness*)[257]. Ее дочерние проекты *(Gothem, Metropolis*) также приспособлены для решения задач, поставленных государственными ведомствами Соединенных Штатов и рядом транснациональных корпораций;

– частная компания «Квик» (*Quid inc.)* – платформа осмысленного анализа информации – осуществляет моделирование ведения военных действий и боестолкновений в условиях плотной социальной среды[258];

– Социальные сети «Фейсбук», «Твиттер», «Ютуб» имеют обобщенную информацию о более чем 60 % активных пользователей интернет-сервисов в мире.

При этом следует отметить, что крупнейшие провайдеры больших данных обладают американской юрисдикцией. Это значит, что в случае соответствующих решений компетентных органов они обязаны предоставлять им все необходимые данные. Для этих целей на расчетную мощность выведен центр обработки данных Агентства национальной безопасности в штате Юта. Примечательно, что, согласно законодательству США, для предоставления обезличенных больших данных (в отличие от персональных данных), не требуется специальных судебных решений. Более того, большие данные должны предоставлять не только непосредственно американские компании, но также их провайдеры, брокеры данных и компании, котирующиеся на американском биржевом рынке – а это практически все крупные международные интернет-компании. В этой связи можно, например, отметить, то, что только компания маркетингового и

[256] Recorded Future, 2018. URL: https://www.recordedfuture.com/ (дата обращения 15.05.2018).

[257] Palantir Technologies, 2018. URL: http://www.palantir.com/ (дата обращения 15.05.2018).

[258] Quid inc, 2018. URL: https://quid.com/ (дата обращения 15.05.2018).

информационного сервиса «Аксиом» (*Axiom*) располагает данными приблизительно на 700 млн людей из разных стран. На каждого пользователя сети автоматически составляются профили, включающие до 150 характеристик.

Таким образом, в условиях утверждения цифровой реальности специалисты Пентагона и американские ученые активно работают над разработкой информационно-аналитических платформ по анализу и моделированию социально-политической обстановки в отдельных районах, странах и даже регионах мира. Все более широкое их использование в практике международных отношений позволяет высказать гипотезу о намерении элит Соединенных Штатов не только создать, но и более активно на деле применять технологии управления социальными массами для решения задач национальной безопасности.

Вместе с тем создание систем социального управления посредством инструментов цифровой реальности ведется не только в США, хотя они и являются ведущим актором по осуществлению такой деятельности. Все чаще многие зарубежные специалисты в области информационного противоборства указывают на то, что **в последние годы Китай активно работает над созданием собственных систем социального управления, функционирующих благодаря современным цифровым технологиям.** Такие оценки особенно распространены среди англосаксонских политологов, по мнению которых реконфигурация системы глобального управления с закреплением цифровой зависимости государств от концептуального и информационного ядра данной системы в Пекине способна отодвинуть США на второй план даже для их союзников.

В мае 2019 г. в Палате представителей Постоянного комитета по разведке США состоялись слушания под названием «Цифровой авторитаризм Китая: наблюдение, влияние и политический контроль». На дебатах специалисты сошлись во мнениях о глубинном замысле утверждаемой усилиями Компартии Китая цифровой стратегии, в основе которой – обеспечение политической и идеологической безопасности Поднебесной с прицелом на реформирование системы глобального управления. Они отмечали, что для расширения своей власти политическое руководство КНР стремится использовать «технологически

усиленный авторитаризм», позволяющий обеспечить защиту национального киберпространства от возникающих угроз, в частности «безграничного пространства идей». В связи с этим неоднократно упоминались термины «киберконфуцианство» и «китайский киберсоциализм». В целом эксперты признали «подрывной» стратегию политического руководства Поднебесной по созданию системы идеологических, политических, организационных мер, призванных заложить фундамент трансформации системы управления информационно-коммуникационным пространством, изначально функционирующей в интересах США[259].

В октябре 2019 г. ведущий аналитик Австралийского института стратегической политики *(Australian Strategic Policy Institute)* С. Хоффман опубликовала обзор, где подробно рассматривается деятельность КПК по созданию глобальной системы сбора данных на примере китайской компании Global Tone Communications Technology Co., Ltd. (*GTCOM*), контролируемой непосредственно Центральным отделом пропаганды Китая[260].

В приведенном документе австралийский ученый указывает на то, что КНР участвует в массовом сборе данных с целью систематизации информации для более надежного обеспечения государственной безопасности, в том числе политической безопасности КПК. Так, GTCOM разрабатывает способы распознавания объектов и человеческих лиц в сочетании с текстами и голосами для мониторинга рисков в режиме реального времени в целях обеспечения национальных интересов КНР, включая пропаганду, идеологическую и культурную безопасность. Кроме того, китайская компания подключена к созданию сети умных городов, что позволяет осуществлять сбор данных, которые

---

[259] China’s Tech-Enhanced Authoritarianism // U.S. Congress. 2019. May. URL: https://docs.house.gov/meetings/IG/IG00/20190516/109462/HHRG-116-IG00-Wstate-HoffmanS-20190516.pdf (дата обращения: 26.05.2020).

[260] *Hoffman S.* Engineering global consent: The Chinese Communist Party's data-driven power expansion // Australian Strategic Policy Institute. 2019. October 14. URL: https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion (дата обращения: 26.05.2020).

после соответствующей обработки могут быть использованы для разработки эффективной системы социального контроля.

Как полагает С. Хоффман, китайское руководство стремится преобразовать «по лекалам высокотехнологичного управления на базе традиционных конфуцианских ценностей» не только собственную страну, но и регулировать социально-политические и экономические процессы в других государствах. Об этом, отмечает эксперт, свидетельствуют следующее: используя лишь одну из своих многочисленных платформ, ориентированных на анализ данных в традиционных СМИ и социальных медиа, GTCOM собирает 10 терабайт данных в день (эквивалентно 5 трлн слов простого текста) и 2–3 петабайта в год (20 млрд фотографий в *Facebook*). На основании анализа материалов пленума и соответствующих партийных документов, автор доклада резюмирует, что уже в скором будущем КНР будет иметь возможность контролировать процессы, развивающиеся в трансграничном информационно-коммуникационном пространстве в глобальном масштабе.

В данной связи следует отметить, такие крупные технологические гиганты, как GTCOM, участвуют в реализации Программы создания системы социального кредита 2014–2020 гг. (ССК). Согласно замыслам Пекина, к 2020 г. каждый житель материкового Китая и все предприятия должны оцениваться ССК в режиме реального времени. Главная задача Программы: «оправдавшие доверие пользуются всеми благами, а утратившие доверие не смогут сделать ни шагу». Информация о жизни и деятельности гражданина (160 тысяч различных параметров) поступает из порядка 150 учреждений в один информационный центр, где обрабатывается с помощью технологии больших данных, по результатам чего рейтинг гражданина повышается либо снижается. Обладатель рейтинга более 1050 баллов – образцовый гражданин AAA, 1000 – AA, 900 – B, ниже 849 – подозрительный носитель рейтинга C (он уже не может находиться на службе в госструктурах). Гражданина, набравшего 599 баллов и менее, записывают в черный список с примечанием «человек D». Данный ярлык присваивается фактически изгоям общества, которых не берут почти ни на какую

работу, не дают кредиты, не продают билеты на скоростные поезда и самолеты и пр. Круг общения таких людей также ограничен, поскольку рейтинг социальных партнеров «человека D» стремительно снижается[261].

В общей картине цифровизации процесс социального управления, создаваемый китайским руководством в рамках ССК, нацелен прежде всего на предотвращение угроз государственной безопасности. С 2017 г. Пекин безвозмездно передал союзным странам и государствам, присоединившимся к инициативе «Пояс и путь», необходимые высобюджетные технологии, в частности отдельные модули ССК. Такие контракты подписаны с Никарагуа, Боливией, Эквадором, Танзанией, Мозамбиком, Эритреей и др., но с обязательным условием, что указанные системы будут обслуживаться специалистами из КНР. Как отмечают американские эксперты, к окончанию 2020 г. китайцы планируют завершить разработку полного пакета документации и технико-экономического обоснования систем социального рейтингования для Казахстана, Монголии и Киргизии. Фактически речь идет о наладке процессов социального управления КНР в зарубежных государствах, с тем чтобы не только обеспечить господство Пекина в региональном информационном пространстве, но превратить планету в ресурс для развития Поднебесной в принципе[262].

С учетом изложенного **страны англосферы во главе с США намерены существенно усилить критику политики Китая в сфере информатизации, указывая на то, что ставка Пекина на развитие цифровых технологий и внедрение их в жизнедеятельность государства – это прежде всего привлекательная завеса выстраиваемой авторитарной системы социального управления, которая в действительности реализуется на глобальном уровне.** Давление англосаксов на Поднебесную в международном масштабе, вероятно,

[261] New social credit code system to increase administrative efficiency // The State Council the People's Republic of China. 2015. June 17. URL: http://english.www.gov.cn/policies/latest_releases/2015/06/17/content_281475129090642.htm (дата обращения: 25.05.2020).

[262] ARIA In Action, Part 3: Implementation and the Indo-Pacific Strategy // United States Senate Committee on Foreign Relations. 2019. October 16. URL: https://www.foreign.senate.gov/hearings/aria-in-action-part-3-implementation-and-the-indo-pacific-strategy (дата обращения: 25.05.2020).

может затруднить цифровое сотрудничество КНР с ЕС, однако вряд ли серьезно повлияет на продвижение соответствующей повестки Нового шелкового пути в динамичных Африканском и Азиатско-Тихоокеанском макрорегионах.

Резюмируя, следует привести результаты панельного мониторинга программ исследований, проводимых в экспертно-аналитических учреждениях зарубежных стран. Он позволяет сделать обобщенный вывод о картине применения ведущими акторами мировой политики информационно-коммуникационных технологий для нужд управления массами практически любой размерности. Итак, лапидарный перечень подобных разработок за последние 15 лет включает следующие направления[263]:

1. технологии сбора, хранения, обработки и анализа больших объемов данных *(Big Data, Data Mining*);

2. визуализация данных *(Data Visualization*);

3. современные гуманитарные технологии *(HighHum*);

4. социокультурная разведка *(Sociocultural Behavior Engineering);*

5. разведка на основе открытых источников *(Open Source Intelligence*);

6. работа в социальных сетях *(Human Intelligence);*

7. методики анализа информации *(Structured Analytic Techniques*).

Таким образом, современные разработки ведущих государств мира демонстрируют общее возрастание значения «нелинейных» методов достижения превосходства над потенциальными противниками в ходе подготовки к ведению противоборства в современных условиях цифровизации социально-политической жизни. В настоящее время США и Китай создают технологические условия для нормального функционирования системы социального управления, соответствующей условиям формирующейся цифровой реальности. Итогом такого управления должно стать превращение субъектов мировой политики и экономики в объекты, находящиеся под внешним, руководящим воздействием.

---

[263] См. напр.: Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community // RAND. 2018. URL: https://www.rand.org/pubs/research_reports/RR1408.html (дата обращения: 19.04.2019).

3.2. Политологический анализ социального поведения в сети Интернет

На современном этапе мирового развития просторы социальных сервисов интернета стали оснвоным театром информационного противоборства между государствами и негосударственными участниками мировых политических процессов. В глобальной сети изучаются, затем апробируются новые методы информационно-психологического воздействия на общественное сознание, несмотря на существование объективных трудностей, в его политологическом исследовании. Они определяются природой и качествами феномена массового созанания, плохо поддающимися научному описанию. Как определял автор психоанализа З. Фрейд, массовое сознание «чувственно, заразно, мозаично, подвижно и изменчиво, конкретно, неоднородно, бесформенно, противоречиво, размыто»[264].

Отдельное место в исследовательском процессе занимают социальные сети и блоги информационно-коммуникационной сети, которые являются, по сути, глобальным поведенческим архивом. Там накапливается информация о привычках, предпочтениях, поступках и местоположении людей. Благодаря доступу к таким данным государственные элиты способны управлять социально-политическими процессами более эффективным образом, чем методами прямого воздействия. Практическим результатом такого управления являются информационные операции, проводимые государствами, лидирующими в моделировании цифровой социально-политической реальности.

Соответственно, с развитием современных ИКТ отечественные и зарубежные ученые все активнее исследуют комплекс феноменов, связанных с внутриличностными, межличностными, внутригрупповыми, межгрупповыми и социетальными механизмами восприятия информации, лежащими в основе популярности ресурсов интернета (в частности, блогов и социальных сетей).

Подобные труды в основном базируются на научной основе психометрии (психографии) – развивающемся с 1980-х гг. направлении психологической

[264] *Фрейд З.* Основные психологические теории в психоанализе / пер. М. В. Вульф, А. А. Спектор. М.: АСТ, 2006. 400 с.

науки, сосредоточенном на изучении деятельности, интересах и мнениях личности. В рамках данного научного направления разработана диспозициональная Пятифакторная модель (*Big Five Personality Model),* в основе которой лежат исследования Г. Оллпорта и Р. Кэттела.

Таблица 3.1 – Пятифакторная модель личности

Экстраверсия	*Невротизм*	*Открытость к опыту*	*Приятность в общении*	*Добросовестность*
экстраверт	+	+	+	+
Сердечность, общительность, активность, настойчивость, поиск положительных эмоций	Высокая самооценка, устойчивость к стрессу, самодостаточность, эмоциональная стабильность, пониженное чувство вины	Фантазия, эстетика, чувства, действия, идеи, ценности	Доверие, прямолинейность, альтруизм, уступчивость, скромность, мягкость	Компетентность, порядок, чувство долга, стремление к результату, самодисциплина, осмотрительность
интроверт	–	–	–	–
Спокойствие, сдержанность, пассивность, избегание внимания, замкнутость	Озабоченность, враждебность, депрессия, рефлексия, импульсивность, неустойчивость к стрессу	Консерватизм, нечувствительность, реалистичность, практичность, негибкость	Циничность, подозрительность, грубость, безжалостность, эгоизм, жадность	Безответственность, лень, непрактичность, небрежность, беспечность

Источник: Составлено по: *Goldberg L.R.* An alternative «description of personality»: The Big-Five factor structure. / L.R. Goldberg // Journal of Personality and Social Psychology. 1990. № 6. С.1216–1229.

Как продемонстрировано в Таблице 3.1 каждая личность характеризуется индивидуальными различиями в степени и форме адаптации к социальной среде с учетом пяти общих и относительно независимых факторов (диспозиций): экстраверсии, приятности в общении (способности прийти к согласию), добросовестности, невротизма (эмоциональной нестабильности), открытости к опыту. В работах современных зарубежных авторов достаточно убедительно доказывается, что переменные Пятифакторной модели связаны с поведением конкретной личности в социальных сетях.

В частности, крупные исследователи в области интеллектуального анализа больших данных М.Косински и Д. Стиллуэлл утверждают, что **информация из профилей пользователей интернет-сервисов («цифровые следы») предоставляет возможность посредством Пятифакторной модели выявить**

специфические характеристики личности и использовать их в манипулятивных целях.

Так, в 2016 г. на основе активности пользователей в социальных сетях эксперты британской компании «Кэмбридж Аналитика» (*Cambrige Analityca*), применяющей технологии глубинного анализа данных для разработки стратегической коммуникации в ходе избирательных кампаний в интернете, выделили 32 личностные категории, различающиеся между собой по уровню готовности отдать свой голос за кандидата в президенты Д. Трампа[265].

В целом легкодоступные цифровые записи поведения личности, такие как «лайки», могут быть использованы для автоматического и достаточно точного прогнозирования в том числе: пола, возраста, этнической принадлежности, религиозных и политических взглядов, личностных качеств, уровня интеллекта, сексуальной ориентации, состояния счастья и пр. Кроме того, благодаря информации, присутствующей в цифровом мире, личность может быть достаточно точно описана многими показателями, включая успехи в учебе, характер работы, социальный статус, здоровье, успех в романтических отношениях, политические взгляды, субъективное благополучие и пр.[266].

Помимо изучения личностных особенностей пользователей интернета ученые активно прибегают к исследованию базисных основ массового поведения в условиях цифровой среды. Теоретические наработки в этой области и проведенные эксперименты свидетельствуют, что человеческое поведение зависит не только от убеждений, а базируется на стереотипах и складывается под воздействием формальных и неформальных институтов. Даже в сложных ситуациях выбора от 50 до 90 % своих действий люди осуществляют

---

[265] *Weedon J., Nuland W., Stamos A.* Information Operations and Facebook // Facebook. 2017. April 27. URL: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf (дата обращения: 13.09.2019).

[266] См.: *Youyou W., Kosinski M., Stillwell D.* Computer-based personality judgments are more accurate than those made by humans // PNAS. 2015. January 27. URL: http://www.pnas.org/content/112/4/1036.full (дата обращения: 22.08.2019).

автоматически[267]. Соответственно, в условиях цифровой среды присутствуют широкие возможности использования потенциала управления социальным поведением.

В настоящее время **в интернет-пространстве активно применяется потенциал теории подталкивания (*nudge theory*), что предполагает возможность влияния на процесс принятия групповых и индивидуальных решений посредством положительного подкрепления и непрямых указаний**. При таком подходе подталкивание к действию не менее эффективно, чем силовое принуждение к действию или предписание.

Авторами теории подталкивания в ее оригинальном перцепте являются американские ученые Р. Талер и К. Санстейн. Их совместный труд «Nudge. Как улучшить наши решения о здоровье, благосостоянии и счастье»[268], выпущенный в 2008 г., был признан полезным государственными структурами США и Великобритании. В настоящее время в обеих странах созданы официальные структуры, исследующие возможности применения данной технологии для управления социальным поведением в условиях цифровой реальности. Среди зарубежных экспертов присутствуют предположения, что бывший британский премьер-министр Д. Кэмерон, равно как и экс-президент США Б. Обама использовали теорию подталкивания для достижения поставленных целей во внутренней и внешней политике[269].

В сфере государственного регулирования, такое подталкивание включает в себя, например, графические предупреждения на какой-либо продукции, плакаты о необходимости эффективного использования энергии или экономии топлива, информацию о пищевой ценности продукта. В категорию «подталкивания»

---

[267] См. напр.: *Harkins G.S., Szymanski K.* Social Loafing and Self-Evaluation with a social standard. Journal of Personality and social psychology. URL: https://www.researchgate.net/publication/247434281_Social_Loafing_and_Self-Evaluation_With_a_Social_Standard (дата обращения 21.01.2018).

[268] *Thaler R., Sunstein C.* Nudge: Improving Decisions about Health, Wealth and Happiness, Yale University Press. 2008.

[269] См. напр.: *Lewis, Carol*. Why Barack Obama and David Cameron are keen to ‘nudge’ you // The Times. 2008. July. URL: https://www.thetimes.co.uk/article/why-barack-obama-and-david-cameron-are-keen-to-nudge-you-pg0p3b5lqcq (дата обращения: 20.10.2018).

входит даже дизайн веб-сайтов, которые располагают на первом плане материалы крупным шрифтом.

Основное преимущество наджа, в противоположность ограничениям и запретам, состоит в том, что он избегает принуждения, а скорее ориентирует людей, задавая им определенное направление поведения. Таким образом, данная технология не принимает явную форму манипуляции или обмана. Между тем ряд влиятельных исследователей указывают, что подталкивание является эвфемизмом для названия психологических манипуляций, к которым прибегают в социальной инженерии[270].

Применительно к осуществлению подталкивания в интернет-пространстве надж базируется на следующих постулатах:

1. У отдельных социальных групп разные стереотипы, у людей – привычки, но обработка больших данных, присутствующих в интернете, позволяет обладать относительно верифицированной информацией о склонности конкретных групп и отдельных людей. Соответственно, большие данные способствуют прогнозированию социального поведения в различных масштабах.

2. Через поисковые сети, электронные выборы, платформы интернет-магазинов, где локализовано размещена конкретизированная информация, в цифровой реальности осуществляется «мягкое подталкивание» личности, возможное благодаря техническим возможностям интернет-сервисов. Такое подталкивание создает для человека ситуацию, когда самое легкое решение оказывается таким, какое нужно тому, кто эту ситуацию создает, то есть «подталкивателю».

При оказании воздействия на сознание масс и отдельной личности посредством надж-технологии эксперты предлагают учитывать ряд когнитивных искажений, определяющих эффективность такого воздействия. В частности, цеелесообразно учитывать, что информационно-психологическое воздействие в

---

[270] См. напр.: *Tapson Mark.* The Soft Totalitarianism of Nudging. FrontpageMag. 2013. August 13. URL: https://archives.frontpagemag.com/fpm/soft-totalitarianism-nudging-mark-tapson/ (дата обращения: 24.06.2019).

интернете реализуется и с учетом склонности личности отдавать предпочтение такой информации, которая согласуется с ее точкой зрения – этот феномен называется «предвзятость подтверждения» (*confirmation bias)*, что было выяснено еще в ходе экспериментов 1960-х гг.

Источник: Составлено по: *Harkins, S.G., Petty, R.E.* The multiple source effect in persuasion // Personality and Social Psychology Bulletin.
URL: http://journals.sagepub.com/doi/abs/10.1177/014616728174019 (дата обращения: 13.09.2019).

Рисунок 3.2 – Феномен «предвзятости подтверждения»

На Рисунке 3.2 показано, что феномен «предвзятости подтверждения» проявляется сильнее в отношении эмоционально значимых вопросов и глубоко укоренившихся убеждений. Склонность к подтверждению влияет на излишнюю уверенность человека в собственных суждениях, и может поддерживать и усиливать убеждения при получении доказательств обратного. Эти когнитивные искажения находят отражение в том числе в решениях, принимаемых в рациональных внешне политической и экономической сферах.

Труды современных ученых предоставляют возможность скорректировать выводы, сделанные в более ранних работах. В особенности это касается склонности людей проверять их гипотезы в предвзятом виде, фокусировать внимание только на одной возможности выбора и игнорировать альтернативные. Об этом свидетельствует исследование российского экономиста В.Д. Миловидова, где продемонстрировано, что равномерно распределенную в обществе или внутри конкретных социальных групп устойчивую ложную,

ошибочную убежденность в чем-либо – эффект «симметрии заблуждений» – крайне сложно выявить, поскольку массовое сознание отталкивает, отвергает любое несогласие с ним. Соответственно, люди склонны принимать неоднозначные свидетельства таким образом, чтобы поддерживалась их точка зрения[271].

Такая интерпретационная база обусловлена сущностью природы человека: ограниченной способностью перерабатывать информацию и склонностью принимать желаемое за действительное. Симметрия заблуждений обусловливает предвзятый поиск информации, особенности процессов запоминания, специфику толкования и пр. Соответственно, в условиях цифровой среды люди в большей или меньшей мере подвержены когнитивным искажениям более низкого порядка: «поляризации взглядов» (*attitude polarization*) – когда разногласия становятся ещё сильнее, несмотря на то что сторонам были представлены одни и те же свидетельства[272]; «стойкости убеждения» (*belief perseverance*) – когда мнение сохраняется даже тогда, когда поддерживающие его свидетельства были опровергнуты[273]; «первичность информации» (*primacy effect*) – склонности отдавать предпочтение информации, полученной первой[274]; «иллюзорность корреляции» (*illusory correlation*) – склонности видеть взаимосвязь между двумя явлениями или ситуациями там, где её нет[275] и пр.

Указанные феномены определяют высокую вероятность в возникновения в условиях специфичной информационно-коммуникационной среды эффекта «пузыря фильтров» (*filter bubble*) – технологии персонализированного подбора контента для интернет-пользователя, основанного на его месторасположении,

---

[271] *Миловидов В.Д.* О черных лебедях и человеческих ошибках // Коммерсант Наука. 2017. 5 сентября. URL: https://www.kommersant.ru/doc/3396747 (дата обращения: 12.10.2019).

[272] См.: *Kuhn, Deanna, Lao, Joseph.* Effects of Evidence on Attitudes: Is Polarization the Norm? // Psychological Science (American Psychological Society), March 1996. Т. 7 (2). С. 115–120.

[273] См.: *Nickerson Raymond S.* A Ubiquitous Phenomenon in Many Guises // Review of General Psychology (Educational Publishing Foundation), 1998. Т. 2 (2). p. 175–220.

[274] См.: *Baron Jonathan.* Thinking and deciding (3rd ed.), New York: Cambridge University Press, 2000.

[275] См.: *Fine, Cordelia.* A Mind of its Own: how your brain distorts and deceives, Cambridge, UK: Icon books, 2006.

прошлых нажатиях, предпочтениях, поиска, а также интересах и предпочтениях друзей.

Как отмечает автор приведенного термина блогер И. Парайзер в одноименной книге «Пузырь фильтров», потенциальным недостатком фильтрации поисковых запросов является то, что она «закрывает людей от новых идей, предметов и важной информации» и «создает впечатление того, что наши узкие собственные интересы и есть все, что существует и окружает нас»[276].

Источник: Составлено по: поисковая система «Яндекс».

Рисунок 3.3 – Эффект «пузыря фильтров»

[276] *Pariser Eli.* The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin Press, 2011.

На Рисунке 3.3 продемонстрирована негативная сторона персонализированного поиска. Она заключается в том, что информационные системы веб-сайтов выводят в поисковой строке лишь ту информацию, которая соответствует истории поиска конкретного пользователя, а другой контент, как правило, пользователю не выводится. В результате такой методики отбора подходящего контента человек оказывается в уютном «информационном пузыре», экранирующем от нарушающих гармонию его индивидуальной картины мира информационных раздражителей. Вполне возможно согласиться с выводом экспертов в том, что вредное воздействие «пузыря фильтров» может подрывать формирование гражданского общества и делать людей более уязвимыми для пропаганды и манипуляций.

Эффект «пузыря фильтров» схож с таким когнитивным искажением, как «парадокс релевантности». Этот феномен проявляется тогда, когда люди ищут информацию, которая изначально, исходя из цели такого поиска, кажется им важной, но в итоге она оказывается совершенно бесполезной или почти бесполезной. Одновременно они избегают информации, которая кажется им неправильной и несущественной, но оказывающейся полезной. Проблема появляется в связи с тем, что реальная значимость конкретного факта или понятия в этих случаях очевидна только после того, когда данный факт стал известен. Соответственно, в поисках информации пользователь интернета нередко не может узнать то, что ему действительно нужно, попадая в своего рода информационное слепое пятно[277].

Важным с точки зрения оказания информационно-психологического воздействия на личность в цифровой реальности является и формирование эффекта «эхо-камеры» (*echo chamber*), который способствует распространению в сети контента, соответствующего целям субъекта управления. Специалисты трактуют эффект «эхо-камеры» как ситуацию, при которой определенные идеи,

[277] См.: First Monday: What's on tap this month on TV and in movies and books: The Filter Bubble by Eli Pariser // USA Today. 2011. URL: https://usatoday30.usatoday.com/money/companies/management/monday/2011-04-29-first-monday-business-media-in-may_n.htm (дата обращения: 09.06.2019).

убеждения подкрепляются путем передачи сообщений или их повторением внутри закрытой системы (это может быть партия, круг единомышленников, субкультура, интернет-блог и пр.). Адресаты, находящиеся в такой закрытой системе, ориентируются на взгляды себе подобных (референтной группы). Магистральная логика обсуждений в блоге или в группе социальной сети нивелирует взгляды и убеждения личности, отклоняющиеся от принятой нормы, тем самым заключая его в изолированном коммуникативном социуме[278].

В условиях, когда человек окружает себя в социальных сетях участниками интернет-сообществ, придерживающихся позиции, аналогичной его собственной, а также под воздействием субъективного поиска, толкования и запоминания информации тренды массового поведения пользователей конкретной социальной сети или блога в определенной ситуации не только подкрепляют индивидуальную систему убеждений, но одновременно искажают целостную картину общественного мнения. Это условно формирует «информационного каскада».

Теория информационных каскадов была создана С. Бикхчандани, Д. Хиршляйфером и И. Велчем, а сам термин предложен в 1992 г.: «Оптимальным поведением индивида после изучения действий своих предшественников является копирование поведения предшественников без учета информации, имеющейся в собственном распоряжении»[279].

В условиях цифровой среды эффект «информационных каскадов» возникает в ситуациях, когда люди, не обладая полной информацией о происходящих процессах, имеющих для них определенную значимость, пытаются принять решение, наблюдая за поведением других интернет-пользователей данного конкретного сервиса. Влияние, которое оказывают на них решения интернет-окружения, настолько велико, что оно превышает влияние той информации, которая имеется в распоряжении самой личности. Информационные каскады во

---

[278] См.: The Echo Chamber Revisited // WNYC. 2011. June 17. URL: https://www.wnyc.org/story/143347-echo-chamber-revisited/#transcript (дата обращения: 13.09.2019).

[279] *Bikhchandani S., Hirshleifer D., Welch I.* A Theory of Fads, Fashion, Custom, and Cultural Change as Informational Cascades // Journal of Political Economy, 1992. p. 992–1026.

многом объясняют феномен стадного поведения в социальных сетях и других коммуникационных ресурсах интернета и этом плане примечательно высказывание социального философа Э. Хоффера: «Если людям предоставить возможность делать то, что им нравится, они, как правило, начинают имитировать действия друг друга»[280].

С учетом теоретического и практического изучения возможного воздействия описанных выше когнитивных искажений, некоторые из которых известны длительное время, другие – обнаружены непосредственно в связи с цифровизацией социально-политической реальности, в интернете все чаще применяются специально разработанные технологии.

В частности, в условиях цифровой среды широко используется технология точечного таргетинга *(targeting*) – механизма, который нацелен на идентификацию только той части аудитории, которая будет восприимчива к определенным аргументам. Данный механизм позволяет оказать воздействие именно на целевую группу, персонально обратившись к конкретным людям с учетом их индивидуальных характеристик (пол, возраст, профессия, увлечения и т.п.).

В настоящее время активно развиваются следующие виды таргетинга:

– Тематический таргетинг – показ рекламы на веб-сайтах, соответствующих определённой тематике.

– Таргетинг по интересам (контекстная реклама) – демонстрация рекламы в соответствии с интересами посетителей рекламной площадки;

– Географический таргетинг (геотаргетинг) – показ рекламы целевой аудитории, ограниченной некоторым географическим регионом, выбранным рекламодателем.

– Локальный таргетинг – рекламирование для целевой аудитории, находящейся в радиусе от 900 метров до 15 километров (с 2014 г. используется также понятие гиперлокальный таргетинг, обозначающее нацеливание рекламы на все устройства, оказывающиеся в определённой зоне вокруг какой-либо точки

[280] *Hoffer E.* The Passionate State of Mind, New York: Harper. 1955.

на местности, при этом радиус такой зоны технически может быть сколь угодно малым).

– Временной таргетинг – позволяет ограничить показ конкретного контента в СМИ по временному фактору (утро или вечер, будни или выходные).

– Социально-демографический таргетинг — по возрасту, полу, доходу, должности и т. д.

– Поведенческий таргетинг – внедрение механизма сбора информации о действиях пользователя в интернете с помощью cookie-файлов. Информация собирается в так называемых профилях и содержит данные о просмотренных сайтах, поисковых запросах, покупках в интернет-магазинах и пр. Получив такой профиль, рекламная служба может четко представить себе портрет объекта, узнать его привычки и пристрастия, стать владельцем контактных данных.

– Геоповеденческий таргетинг – суть которого сводится к обладанию информацией о перемещениях субъекта. Точное местоположение субъекта умеют определять современные геосоциальные сервисы, например, «Альтергео» (*AlterGeo*) и остановках («отметках» – *check-ins*) в некоторых точках. Постепенно можно достаточно четко выявить привычки и пристрастия объекта наблюдения[281].

Все большее применение в интернете находит такая технология воздействия на общественное сознание, как «троллинг» (*trolling),* способствующий созданию нового контента и распространению лживых сведений. В наиболее общем виде под этой деятельностью можно понимать процесс размещения на виртуальных коммуникативных ресурсах провокационных сообщений с целью нагнетания конфликтной обстановки путем нарушения социальных и этических норм интернет–взаимодействия.

Использование троллинга дает субъектам управления такие преимущества, как усиление эффекта массовости, возможность повысить уровень доверия к источнику «разоблачительной» информации, а также расширить круг ее

[281] См.: Facebook запускает гиперлокальную рекламу для тех, кто неподалёку // Apps4All. 2016. Июль. URL: http://apps4all.ru/post/10-08-14-facebook-zapuskaet-giperlokalnuyu-reklamu-dlya-teh-kto-nepodaleku (дата обращения: 10.10.2018).

получателей. Как полагают ряд зарубежных специалистов, уже в обозримом будущем троллинг может превратиться в востребованную специализацию целого ряда профессий в таких сферах, как журналистика, международная экономика, мировая политика и пр.[282]

В настоящее время все больше распространяется оплачиваемый троллинг. Под платным троллингом подразумеваются действия организованных групп интернет-пользователей, занимающихся за денежное вознаграждение формированием общественного мнения в сети в определенном направлении[283]. Так, например, в Соединенных Штатах широкая деятельность приписывается группе «Честный голос» (*Operation Earnest Voice*), находящейся непосредственно в подчинении Центрального командования вооруженных сил (*CENTCOM*). При этом в качестве основного соперника в информационно-коммуникационном пространстве американские специалисты называют в основном Российскую Федерацию и Китай.

Условно эксперты выделяют следующие сферы осуществления троллинга:

1.Политические тролли, применяющие в своей деятельности метод контент-анализа по поисковым словам (в зависимости от того, чьи политические интересы они представляют). Такие акторы интернет-среды часто активизируются в период предвыборных кампаний на всех уровнях властной иерархии.

2.Провокаторы стремятся отслеживать реакцию публичных персон на конкретные инициированные события с целью получить в свое распоряжение некорректный, абсурдный комментарий. Они выбирают в качестве инструмента провокации актуальные проблемы религии, этнической принадлежности, отношения к нововведениям в законодательстве и пр.

3.Вымогатели считаются наиболее технически продвинутой разновидностью пользователей интернета. Их целью является получение

---

[282] См. напр.: *Del Vicario M., Bessi A., Zollo F., et al.* The spreading of misinformation online // Proceedings of the National Academy of Sciences 2016. V. 113. N. 3. P. 554–559.

[283] См.: *Внебрачных Р. А.* Троллинг как форма социальной агрессии в виртуальных сообществах // Вестник Удмуртского университета. Философия. Социология. Психология. Педагогика. Ижевск: Удмуртский государственный университет, 2012. Вып. 1. С. 48–51.

конкретной информации (места работы, социального статуса, семейного статуса, номера телефона и пр.) с манипулятивным умыслом.

Зарубежные эксперты указывают, что вне зависимости от тематики виртуальные дискуссии в интернет-сообществах с применением троллинга значительно повышают выраженность негативных эмоциональных состояний и меняют убеждения пользователей к радикальным, крайним оценкам[284].

Примечательной технологией воздействия на общественное сознание является «астротурфинг» (*astroturfing*) – использование современного программного обеспечения либо специально нанятых оплачиваемых пользователей для искусственного управления общественным мнением. Как указывают западные специалисты, основная особенность астротурфинга, отличающая его от пропаганды – это имитация «низовой инициативы». Это призвано изобразить поддержку представителями общественности и политических сил, якобы с ними не связанных, но в реальности их финансирующих[285].

Эффективность астротурфинга во многом объясняется эффектом группового социального подкрепления *(communal reinforcement*), благодаря которому прочное убеждение внутри какого-либо социального сообщества формируется посредством повторения некого утверждения (идеи, концепции и пр.) его членами. Ученые доказали, что этот процесс происходит естественно, вне зависимости от подтверждения создаваемого убеждения достаточными эмпирическими или научными данными. Таким образом, даже широкая распространенность в интернет-сообществе какого-либо убеждения не является однозначным свидетельством его истинности или ложности. В наши дни это скорее зависит от усилий субъектов управления сформировать данное убеждение.

---

[284] См.напр.: *Parramore Lynn. T*he Filter Bubble // The Atlantic. 2010. 10 октября. URL: https://www.theatlantic.com/daily-dish/archive/2010/10/the-filter-bubble/181427/ (дата обращения: 10.10.2018).

[285] См.: *Stephen C. Webster*. Exclusive: Military's 'persona' software cost millions, used for 'classified social media activities' // Rawstory. 2011. February 22. URL: https://www.rawstory.com/wpcontent/uploads/2011/03/personamanagementcontract.pdf (дата обращения: 12.09.2019).

В настоящее время технология астротурфинга используется для вытеснения мнения реальных людей на веб-форумах либо для организации поддельных кампаний в интернете, которые создают впечатление того, что большое количество людей требуют или выступают против чего-либо. В основном такая деятельность характеризуется:

– созданием подставных групп для размещения сообщений в чатах, форумах, новостях – для продвижения или напротив осмеивания (особенно посредством «троллинга») конкретных идей;

– распространением в социальных сетях, блогах, на форумах идей, которые будут поддержаны и ретранслированы большим числом мнимых пользователей (реже – реальных, но введенных в заблуждение пользователей);

– технической «накруткой» количества просмотров той или иной информации в интернете для поднятия ее рейтинга и популярности[286].

По некоторым сведениям, технология астротурфинга активно применяется военными специалистами из США, ориентированным на проведение проамериканской пропаганды через социальные сети и различные блоги. С этой целью якобы регулярно создаются вымышленные виртуальные личности в соцсетях, которые по внешним признакам кажутся обычными пользователями из разных стран. Еще в марте 2011 г. на американском сайте госзакупок была опубликована информация, согласно которой армия США заключила контракт на сумму 2,76 млн долларов на поставку национальным вооруженным силам программного обеспечения для ведения проамериканской пропаганды за пределами национальной территории (в основном в странах Ближнего Востока) путем создания учетных записей в социальных платформах, маскируемых под

[286] См.: *Ratkiewicz J., M. D. Conover,* M. Meiss, B. Gonçalves, A. Flammini, F. Menczer. Detecting and Tracking Political Abuse in Social Media // Center for Complex Networks and Systems Research. Indiana University. 2011.

реальных людей и контролируемых анонимными операторами из числа американских военных[287].

Таким образом, как свидетельствует политическая практика информационного противоборства**, новейшие достижения нейробиологии и коммуникативистики в области генерирования специфических нарративов (новостных сообщений, видеоматериалов, высказываний) способны направить человеческую мысль по запрограммированному пути в том числе в глобальной сети интернет.** В условяих цифровой среды (прежде всего социальных сетях и блогосфере) регулярно апробируются новые методики информационного воздействия.

Широкую деятельность по исследованию и апробированию на практике разработок с целью эффективного воздействия на умонастроения масс в социокультурной среде потенциального противника ведут США. Например, в отчёте американского военного ведомства за 2013 г. «Анализ и проектирование социокультурного поведения в интересах Министерства обороны США» приводится целый ряд прикладных исследований, целями реализации которых явились: оптимальные методы устранения языкового барьера в новой социокультурной среде, моделирование социально-политической реальности и использование потенциала социальных сетей для нужд национального Минобороны и пр.[288]

Впоследствии указанные достижения применяться для анализа экономической, социальной, политической обстановки в отдельных странах и регионах, а также для подготовки общественного мнения к принятию важных политических решений. Это обусловливает развитие тенденции на качественно новую декомпозицию отношений между властью и обществом.

---

[287] См.: *Cho Charles H., Martens Martin L.,* Hakkyun Kim, Michelle Rodrigue. Astroturfing Global Warming: It Isn't Always Greener on the Other Side of the Fence // Journal of Business Ethics. 2011. № 4 (104). P. 571–587.

[288] См.напр.: Sociocultural Behavior Research and Engineering in the Department of Defense Context // U.S. Department of Defense. 2013. October. URL: https://info.publicintelligence.net/DoD-SocioculturalBehavior.pdf (дата обращения: 13.02.2018).

В этом контексте целесообразно отметить профильные исследования, проводимые зарубежными экспертными центрами по российской проблематике

– «Изучение российского интернет-пространства: коллективная деятельность в цифровой среде и сетевое пространство социума». Целью этого трёхлетнего проекта было «изучить влияние интернета на российскую политику, СМИ и общество». Использовались различные методы изучения интернет-активности: анализ и исследование структуры, сообществ и содержания блогосферы и контента в «Твиттере», опрос блогеров, контент-анализ различных СМИ.

– «Публичный дискурс в российской блогосфере: анализ политики и мобилизации в Рунете». В ходе этого двухлетнего исследования был проведен анализ русскоязычных блогов в целях выделения дискуссионных сетей, в которых обсуждаются политические и общественные темы. Изучив более 5 млн блогов, авторы выделили активное «дискуссионное ядро», состоящее более чем из 11 тыс. блогов. Эти блоги были сгруппированы в соответствии с паттернами цитирования внутри постов, а итоговая сегментация была проведена посредством автоматизированного контент-анализа, а также дополнена анализом экспертов.

– «Карта российского „Твиттера“». В рамках исследования было изучено порядка 50 млн русскоязычных твиттов, «дискуссионное ядро» которых составили 10 тысяч пользователей, сгруппированные на основе сочетания сетевых характеристик. Выявлены ключевые структуры динамики интеракции в русскоязычном «Твиттере» [289].

Резюмируя, отметим, что в последние годы вектор научно-исследовательской и экспертной деятельности в области изучения и апробирования возможностей информационно-коммуникационной сети интернет на массовое и индивидуальное сознание во многом сместился в сторону перспектив разработки политических технологий по управлению массовым

[289] См. напр.: Impact of the Internet on Russian Politics, Media, and Society // The Berkman Klein Center for Internet & Society. 2018. URL: https://cyber.harvard.edu/research/russia (дата обращения: 15.02.2018).

социальным поведением в условиях цифровой среды. Данным процессам способствует расширение научного инструментария и эмпирической базы подобного вида исследований: если ранее специалисты опирались прежде всего на классические методы психологии и социологии, когда результаты замеров на микрогруппах экстраполировались на макрогруппы, то в настоящее время такой экстраполяции зачастую не требуется. Многие необходимые сведения, которые используются ведущими акторами информационного противоборства, размещены в социальных сервисах интернета.

3.3. Потенциал меметики в информационно-психологическом воздействии на массовое сознание

Технологии воздействия на массовое сознание в условиях становления цифровой среды разрабатываются форсированными темпами. Активность в области исследований по проблематике поведения личности и социальных масс в виртуальной реальности обусловлена колоссальным, еще до конца не изученным потенциалом инноваций в области коммуникационных технологий.

Важную роль в восприятии обществом информации, циркулирующей в интернете, играют броские словосочетания, видео, графические изображения, которые принято называть «мемы». Например, именно они лежат в основе активно совершенствующихся в настоящее время технологий воздействия на массовое сознание, как «глубокие фейки». В этой связи потенциалу меметики, как базису перспективных наработок в рассматриваемой области, следует уделить особое внимание.

В 1898 г. В. М. Бехтерев в своей статье «Роль внушения в общественной жизни» предложил концепцию «ментальных микробов», которые, «подобно настоящим физическим микробам, действуют везде и всюду и передаются через слова и жесты окружающих лиц, через книги, газеты и пр.»[290] Между тем до повсеместного распространения средств массовой информации и коммуникации

[290] *Бехтерев В.М.* Избранные труды по психологии личности: в 2 т. Т. 2: Объективное изучение личности. СПб: Алетейя, 1999. С. 169.

(СМК) данная идея оставалась в тени дебатов учёных и не пользовалась большой популярностью среди политического и военного сообщества.

В 1976 г. английский биолог-эволюционист, этолог и популяризатор науки Р. Докинз в своей работе «Эгоистичный ген»[291] ввёл в научный оборот категорию «мем». По мнению исследователя, человеческая эволюция движима репликаторами[292] двух типов: биологическим и культурным. Для обозначения репликатора первого типа Р. Докинз применил категорию «ген» как частный случай молекулы особого рода, способной к самокопированию. Определения репликатора второго типа не существовало, поэтому для описания единицы передачи культурного наследия Р. Докинз использовал дефиницию «мем», прежде всего подчёркивая «способность» мема к самовоспроизведению, подобно гену.

В январе 1983 г. физик и информатик из США Д. Хофштадтер предложил назвать дисциплину, изучающую мемы, меметикой (по аналогии с генетикой)[293]. В 1988 г. термин «мем» был включён в Оксфордский словарь английского языка. С этого времени меметика стала предметом активных научных дискуссий.

В опубликованной в 1992 г. книге американского философа и когнитивиста Д. Деннета под названием «Объяснённое сознание» (Consciousness Explained) мемы описываются как культурные идеи («культурные вирусы»), которые могут деструктивно воздействовать на человеческое сознание, «паразитировать на личности», влияя в конечном итоге на ее поступки[294].

Примечательно, что активно работают в области меметики исследователи, не относящиеся к академическому мейнстриму. Так, в 1996 г. вышли в свет две фундаментальные работы в этой области знания: «Психические вирусы»[295] Р. Броуди, экс-менеджера компании «Майкрософт», и «Заражение мысли: как

---

[291] *Dawkins R.* The Selfish Gene. Oxford: OUP, 1976. 384 p.

[292] Под репликацией Р. Докинз понимал процесс самокопирования в максимальных количествах с учётом вариативности и селективности.

[293] См.: Metamagical Themas // Scientific American. URL: https://www.scientificamerican.com/author/douglas-r-hofstadter/ (дата обращения: 04.06.2018).

[294] *Фролов Д. А.* Меметика: к вопросу о культурных генах // Огарев-online. 2013. №7. URL: http://journal.mrsu.ru/wp-content/uploads/2013/11/Frolov.pdf (дата обращения: 06.09.2019).pdf (дата обращения: 06.09.2019).

[295] *Brodie R.* Virus of the Mind: The New Science of the Meme. Seattle: Integral Press, 1996.

вера распространяется в обществе»[296] А. Линча, математика и философа, много лет проработавшего инженером в Национальной ускорительной лаборатории им. Э. Ферми («Фермилаб»).

В указанных трудах авторы рассуждают на тему культурных вирусов, меметики религии, создания культа и даже дезинфекции социума. Приводятся три основных пути распространения мемов:

– повторение;

– когнитивный диссонанс, для разрешения которого вводится новый мем;

– генетическое реагирование (в качестве примера приводится апелляция к физиологическим и экзистенциальным потребностям: предупреждение об опасности, крики детей, сексуальная привлекательность и пр.).

В 1999 г. С. Блэкмор, психолог из Университета Западной Англии, опубликовала работу «Мем-машина», где произведён анализ идей Д. Деннета, А. Линча и Р. Броуди, а также сделана попытка их сравнения с различными подходами академических культурно-эволюционных дисциплин. Кроме того, основываясь на положениях меметики, в своей книге британский учёный представила новые теории эволюции языка и человеческого восприятия собственной «самости»[297].

С. Блэкмор определяет мем как любую информацию, скопированную от одной персоны к другой: привычки, предпочтения, навыки, песни, истории и пр. Как и основоположник термина «мем» Р. Докинз, британский исследователь утверждает, что мемы, подобно генам, следует рассматривать в качестве репликаторов, т.е. как информацию, воспроизводящуюся вариационно и селективно. По её мнению, они копируются путём имитации, обучения и других методов и борются за выживание в человеческой памяти, чтобы впоследствии реплицироваться вновь. Поскольку процесс обучения каждой отдельной личности имеет свои особенности, процесс имитации мемов также не может быть

[296] *Lynch A.* Thought Contagion: How Belief Spreads Through Society. N.Y.: Basic Books. 1996; *Smith J.M., Szathmary E.* The Major Transitions in Evolution. N.Y.: W.H. Freeman and Company Limited, 1995.

[297] *Blackmore S.* The Meme Machine. Oxford: OUP, 1999.

абсолютно точным. По С. Блэкмор, мемы, а значит, и пласты культуры развиваются по причине того, что выживают лишь некоторые вариации культурных единиц.

В связи с этим представляется возможным заметить, что заражение общества или его отдельных групп теми или иными идеями применимо практически к любой социальной сфере. По сути, речь идёт об управляемом создании в моде, публичной политике, экономике и прочих областях социальной деятельности различных «субкультур, живущих по своим собственным правилам». Например, даже в такой системе экономических отношений, как финансовый рынок, формируются свои мемы, пусть даже сугубо виртуальные. Как отмечает в этом контексте экономист В.Д. Миловидов, в своё время на финансовом рынке присутствовали, например, очертания субкультуры «алгоритмусов», или «алгоритмистов», занятых совершенствованием алгоритмической торговли. В указанной сфере, как и в любой другой области социальной деятельности, привнесённые образцы поведения копируются путём имитации, но лишь до тех пор, пока они сами не становятся мейнстримом (своего рода «болезнь роста»)[298].

Несмотря на обилие трудов в области меметики, накопленный к настоящему времени массив знаний всё ещё не позволяет учёным дать термину «мем» однозначное определение. Биологическое объяснение Р. Докинза гласит, что мем – это основная единица культурной передачи или инициации. Индонезийский учёный, специалист в области сложных социальных систем и интеллектуального анализа больших данных Х. Ситунгкир называет мемом единицу культурных комплексных систем. Психолог Г. Плоткин считает, что мем – элемент культурной наследственности, аналогично гену ему присуща внутренняя репрезентация знания. Таким образом, мем – сложная составная идея, которая самоорганизуется в отдельную запоминаемую единицу.

С учетом разночтений в существующих сегодня определениях того, что же такое мем, целесообразным представляется обратить внимание на труд ученых

[298] См. подр.: *Миловидов В.Д.* Философия финансового рынка. М.: Магистр, 2013. 270 с.

Д. Бека и К. Кована, обобщивших свойства мемов и представивших их ключевые характеристики:

– мемы влияют на совершаемый человеком выбор;

– в мемах проявляются глубинные образы мышления;

– мемы могут иметь деструктивный и позитивный характер (то есть способствовать или, напротив, препятствовать осуществлению какого-либо события);

– мемы влияют на принятие решений, но не формируют убеждения и ценности личности;

– мемы изменчивы – могут «разгораться» и «тускнеть», приобретая законченный и понятный обществу смысл лишь в рамках конкретного исторического контекста[299].

В условиях цифровой реальности для распространения мемов применяются визуальный канал информации, реже – аудиальный. Оформление мема может использоваться для негативного информационного воздействия и для формирования положительного образа продвигаемой идеи. Эмоционально окрашенные мемы лучше запоминаются, а значит, выполняют свою эволюционную функцию.

В качестве яркого примера использования мемов можно назвать деятельность С. Бертрама-Ли – британца, переехавшего в апреле 2016 г. из греческих Афин в Сирийский Курдистан с целью поддерживать Отряды народной самообороны[300]. В настоящее время он ведёт мем-каналы в социальных сетях с целью «поднятия боевого духа сирийских курдов»[301].

---

[299] См. подр.: *Бек Д., Кован К.* Спиральная динамика. Управляя ценностями, лидерством и изменениями в XXI веке / Д. Бек, К. Кован. М.: Открытый Мир, 2010. 424 с.

[300] Отряды народной самообороны (YPG) – вооружённое формирование Высшего курдского совета, входящее в оппозиционный альянс Сирийских демократических сил (SDF). Фактически является боевым крылом Партии демократического единства (PYD).

[301] См.: *Stutman G.* Making memes in a warzone // The Outline. 2017. 3 August. URL: https://theoutline.com/post/2052/making-memes-in-a-warzone?zd=1&zi=jn3rcyra (дата обращения: 15.06.2018).

Источник: facebook.com / Dank memes for Democratic Confederalist Dreams (дата обращения: 01.10.2019).

Рисунок 3.4 – Аватар сообщества, созданного С. Бертрамом-Ли

В настоящее время остается спорным статус меметики в корпусе научного знания. Здесь содержатся наиболее ощутимые противоречия, так как меметика вступает в конфликт с антропологией, социологией, лингвистикой, а более поздние работы по меметике – с нейронауками и кибернетикой.

Серьезное электронное издание – «Журнал меметики – эволюционные модели передачи информации» – просуществовало с 1997 по 2005 г. В последнем выпуске была опубликована заключительная статья ученого-меметиста Б. Эдмондса. С указанного периода исследования в области меметики стали фокусом разработок, связанных с происхождением культур, языка, усложнением социального поведения человека в процессе развития современных технологий. Для современной меметики важен скорее механизм процесса изменения, но не его объект, причины или условия.

В настоящее время разработки в сфере меметики, не присутствуя в научно-исследовательском пространстве, активно развиваются на стыке исследований политтехнологов и военных специалистов. Наиболее полно

прикладной аспект достижений меметики разработан государствами, входящими в состав НАТО, и непосредственно структурами Североатлантического альянса.

Считается, что впервые вопрос применения мемов в качестве «элементов организованного конфликта» поднял майор морской пехоты США М. Проссер в своём исследовании, опубликованном в 2006 году. В этой работе автор указывает, что каждый мем исходно является идеей, но не каждая идея может стать мемом (чтобы это произошло, она как минимум должна реплицироваться в сознании другой личности). Распространение мемов следует трактовать как болезнь ментального порядка, методов противодействия которой, с точки зрения М. Проссера, не выработано.

Как отмечает специалист, существует различие между направленностью информационных операций и меметических. Если информационные операции нацелены непосредственно на противника, то объектом меметических операций является состоящее из разнообразных пластов мирное население собственной страны и страны-оппонента.

Ссылаясь на исследования экспертных центров военного ведомства США, аналитик указывает, что мемы воспроизводятся и распространяются как эпидемии. По его мнению, «противоборство будущего потребует силовой структуры, закалённой для нелинейных операций. Пока же американские военные не имеют доктрины или рекомендаций для ведения боя в ментальном пространстве врага или некомбатантов. Однако с некоторыми модификациями можно достичь нового уровня понимания и возможности обеспечения превосходства в этой сфере»[302].

М. Проссер утверждает, что идеология в этом смысле должна рассматриваться как болезнь, а обладающие свойством саморепликации мемы – как метод её распространения или, напротив, как инструменты трансформации доминирующей идеологии (в зависимости от поставленных заказчиком целей).

[302] *Prosser M.* Memetics – A Growth Industry in US Military Operations // NATO. 2006. URL: https://www.sto.nato.int/publications/Lists/National_Catalogues/DispForm.aspx?ID=2638 (дата обращения: 04.06.2018).

Таким образом, используя логическую прогрессию связи мемов с популярными социальными идеями и политическими убеждениями масс, атака на идеологию должна предусматривать воздействие на центральную или трансцендентную идею (или группу идей) в качестве приоритетной цели субъекта управления.

В 2008 г. под руководством президента компании «Роботик Технолоджи» Р. Финкельштейна был завершён и опубликован масштабный труд, где на 1680 страницах собраны все публикации учёных, касающиеся применения меметики в военно-политических целях. Как отмечается в издании, данный проект подготовлен по заказу Управления перспективных исследований Министерства обороны США[303].

До того времени указанное ведомство уже проводило проекты в области изучения прикладного аспекта меметики, в частности:

– эпидемиология идей (*Epidemiology of Ideas),* 2006 г.;

– военная меметика (*Military Memetics*), с 2006 по 2009 г.;

– социальные медиа в стратегических коммуникациях (SMISC), с 2011 по 2015 г.;

– сюжетные сети (*Narrative Networks*), с 2011 по 2015 г.[304]

Так, целями проекта Социальные медиа в стратегических коммуникациях, согласно оригинальному описанию, были:

– обнаружение, классификация, измерение и отслеживание: а) образования идей и концепций (мемов), б) целенаправленного распространения сообщений и дезинформации;

– распознавание структур пропагандистских кампаний и операций влияния на сайтах и сообществах социальных медиа;

– идентификация участников и их намерений, измерение эффекта кампаний влияния;

---

[303] A Memetics Compendium // Robotic Technology Inc. 2008. May. URL: https://robotictechnologyinc.com/images/upload/file/Memetics%20Compendium%205%20February%2009.pdf (дата обращения: 05.06.2018).

[304] См.: Narrative Networks // DARPA. 2011. 7 October. URL: https://robo-hunter.com/uploads/files/560c1c5fe87df.pdf (дата обращения: 05.06.2018).

– противодействие враждебным кампаниям влияния с помощью контрсообщений.

Список технологий, которые специалисты Управления перспективных исследований Министерства обороны США рассматривали в качестве ключевых, для указанного проекта включал в себя лингвистический анализ, распознавание паттернов, эмоций, культурных нарративов[305], теорию графов[306], краудсорсинг, автоматическое создание контента, боты. Проект подразумевал создание программных средств отслеживания мемов, которые могли бы применяться в среде, где действуют американские вооруженные силы.

В целом, западные эксперты сходятся во мнении, что мемы представляют собой перспективный инструмент информационно-психологической борьбы. Проведенные российскими учеными экспериментальные исследования с использованием математического моделирования (в качестве исходных данных были использованы 3000 русскоязычных публикаций СМИ, обсуждаемые в социальных сетях) также доказывают, что **целенаправленное распространение мемов влечет за собой концептуальное изменение содержания информационного пространства социально-телекоммуникационной системы**[307].

По оценкам военных специалистов США, потенциал меметики можно расценивать не иначе как «революционный инструмент информационной войны, ведущейся на нейрокогнитивном уровне»[308]. Амекриканские эксперты даже ввели в обращение термин «военная меметика», что означает изучение и применение мемов для нужд национальной безопасности. Указывается, что в этом плане

---

[305] Нарратив – изложение взаимосвязанных событий, представленных читателю или слушателю в виде последовательности слов или образов.

[306] Теория графов – раздел дискретной математики, в котором изучаются свойства графов и их обобщений.

[307] См.напр.: *Артёмов А. А.* Эксперимент по моделированию процесса эволюции содержания информационного пространства социума (с применением мем-грамм-модели). Программная инженерия. 2016. № 7. С. 291–306.

[308] Tutorial: Military Memetics // Robotic Technology Inc. 2011. October 24–26. URL: https://www.robotictechnologyinc.com/images/upload/file/Presentation%20Military%20Memetics%20Tutorial%2013%20Dec%2011.pdf (дата обращения: 05.09.2019).

особый интерес представляют краткие мемы, поскольку они могут наиболее продуктивно использоваться в интернете и, в частности, в социальных сетях. Таким образом, для эффективного управления социально-политическими процессами американским госструктурам целесообразно моделировать динамику развития социальных сетей посредством меметических.

В информационно-аналитическом бюллетене военной разведки США за 2010 г. лейтенант Брайан Хэнкок рассматривает технологию применения мемов в качестве дополнительного элемента контрповстанческих операций, которые проводят в том числе и американские вооруженные силы. По его мнению, «меметическая теория предоставляет рамки для работы с наиболее важными социальными и военными проблемами на базовом причинном уровне»[309].

Б. Хэнкок называет мемы «вирусами сознания». Они, с точки зрения исследователя, образуют «невидимый, но достаточно реальный ДНК человеческого общества… Точно так, как гены организуют себя в ДНК, клетки и хромосомы как повторяемые элементы организуют себя в мемы, а также во взаимозависимые комплексы мемов (мемплексы)»[310].

С точки зрения обеспечения социально-политической стабильности основной принцип военной меметики состоит в вытеснении, или «перезаписи», опасных для социума патогенных мемов и мемплексов более мягкими единицами культурной информации. Для этого необходимо «идентифицировать, отследить, изолировать и уничтожить» мемы, формирующие основу конфликта, и только затем работать над созданием нового доброкачественного мема. Когда в целевой группе достигается критический уровень насыщения «позитивного» набора мемов, можно ожидать исчезновения нежелательных артефактов социального поведения. В этой связи идея Б. Хэнкока напоминает концепцию фреймов

[309] *Hancock B.J.* Memetic Warfare: The Future of War. Military Intelligence Professional Bulletin // FAS. 2010. April–June. URL: https://fas.org/irp/agency/army/mipb/2010_02.pdf (дата обращения: 04.06.2018).

[310] Ibid.

Дж. Лакоффа, согласно которой с введённым первично фреймом бороться труднее, чем ввести новый фрейм с нужным содержанием[311].

Военно-прикладной потенциал меметики изучается и профильными структурами Североатлантического альянса. Так, эксперт по социальным медиа из Стэнфордского университета Дж. Джиси в статье под названием «Время воспользоваться меметической войной», опубликованной в журнале Центра стратегических коммуникаций НАТО за 2015 г., отмечает, что такой вид противоборства является прежде всего «соперничеством за нарративы, идеи и социальный контроль на поле боя современных массмедиа»[312]. Меметическая война, по мнению исследователя, может быть полезна на уровне «большого нарратива» (повседневная деятельность средств массовой информации), в период протекания военного конфликта, а также при «особых обстоятельствах» (по всей видимости, автор имеет в виду конкретные информационные операции).

Как указывает Дж. Джиси, на современном этапе развития борьбу с применением мемов можно рассматривать как «цифровую» версию психологической войны. По его мнению, «ведение меметической войны – это одновременно этос и ремесло. Способность "говорить в интернете" в дополнение к пониманию нюансов целевой аудитории является важной для каждого, кто хочет участвовать в меметической войне»[313]. Отсюда эксперт делает вывод, что НАТО, помимо вложений в обеспечение кибербезопасности, следовало бы более активно инвестировать в потенциал меметической войны.

С учетом того обстоятельства, что ученые и государственные деятели США и стран Североатлантического союза первыми осознали всеобъемлющий характер и потенциал информационно-психологического воздействия в условиях цифровизации, наиболее тщательно рассматриваемые аспекты апробируются в

---

[311] См.: *Saletan W.* Neuro-Liberalism // The New York Times. 2008. June. URL: https://www.nytimes.com/2008/06/22/books/review/Saletan-t.html (дата обращения: 05.06.2018).

[312] *Giesea J.* It is time to embrace memetic warfare // Defence Strategic Communications journal. 2015. Winter. Vol. 1. No. 1. URL: https://www.stratcomcoe.org/academic-journal-defence-strategic-communications-vol1 (дата обращения: 05.06.2018).

[313] *Giesea J.* Memetic warfare. Part 2: Hacking hearts and minds. How the memetic warfare is transforming cyberwar. 2017.

политической практике именно американскими и натовскими экспертными структурами.

В 2017 г. авторитетный американский журнал в области международных отношений опубликовал материал «Может ли НАТО военизировать мемы?». В публикации отмечается, что сегодня даже обладающие колоссальной военной мощью Соединённые Штаты и Североатлантический альянс не способны обеспечить собственную безопасность без активной роли в формировании информационной реальности. Авторы указанных рекомендуют военно-политическому руководству США и НАТО быть передовиками на фронте новой «меметической войны» [314].

Соответственно, США и Североатлантический альянс активно проводят симуляционные игры и военные учения с применением потенциала мем-технологий. Например, в Организации Североатлантического договора проводилось исследование под названием «Юмор как инструмент коммуникации: проектирование для анализа»[315]. Эксперты НАТО проанализировали один из пластов современной культуры (назовем её условно – смеховой культуры). В данном случае анализу подвергалась деятельность российского КВН.

Во время состоявшихся в 2015 г. военных учениях Североатлантического военно-политического блока под названием «Трайдент» (*Trident Juncture*) оценивался потенциал социальных сетей как компонента ведения боевых действий в условиях современной цифровой реальности[316].

Разработчики указанного моделирования НАТО загрузили два приложения для социальной сети в пробный (вымышленный) интернет, а контролёры поощряли дружелюбных игроков во всех эшелонах к созданию там профилей. Оппозиционные силы и нейтральные игроки также создавали аккаунты.

[314] Can NATO Weaponize Memes? // Foreign Policy. 2017. April. URL: https://foreignpolicy.com/2017/04/13/nato-cyber-information-warfare-battle-of-ideas-memes-internet-culture/ (дата обращения: 05.06.2019).

[315] StratCom laughs: in search of an analytical framework // NATO Strategic Communications Centre of Excellence. 2016. URL: https://www.stratcomcoe.org/stratcom-laughs-search-analytical-framework (дата обращения: 05.06.2019).

[316] Trident Juncture shows NATO capabilities 'are real and ready'// NATO. 2015. November. URL: https://www.nato.int/cps/en/natohq/news_124265.htm%20 (дата обращения: 05.06.2019).

Большинство участников сразу же узнали формат двух приложений. Чат, похожий на «Твиттер» ограничивал количество символов до 120. Профиль, похожий на «Фейсбук», не ограничивал страницу участника определённым числом символов, он также включал опцию размещения фото и ссылок на другие сайты. Динамика этих приложений вызвала у организаторов учений необходимость использования обеих платформ в командных упражнениях. В итоге военные специалисты получили практические знания о последствиях позитивного и деструктивного влияния социальных сетей на информационное измерение войны.

По результатам проведенных маневров отмечалось, что для достижения информационно-психологического превосходства над средствами массовой информации противника во время современного военного конфликта оптимальным выглядит сотрудничество с крупной маркетинговой фирмой.

В последние годы Пентагон совместно с аналитическими научными центрами также провел ряд симуляционных игр и учений, связанных с применением мемов. Так, в декабре 2015 г., незадолго до операции по освобождению Мосула от ИГИЛ, были проведены игры с участием более 100 человек, разделённых на лагери. «Красные» представляли террористов, «белые» – гражданское население Мосула, а «синяя» команда получила задачу разработать стратегию «высокого уровня». В соответствии с этой стратегией предполагалось использование командой «синих» современных средств информационно-психологического противоборства для воздействия на население с учётом действий противника. Таким образом, «синие», имея в наличии данные, полученные в ходе социокультурной разведки, и информацию от технических экспертов, должны были выстроить процесс коммуникации с населением в ходе военного конфликта, реагируя на сообщения от «красных» (террористов ИГИЛ).

В специальном докладе по результатам указанных учений отмечается, что задачами этих манёвров, проведённых совместно Силами психологических операций США (*PSYOP)* и командой Университета Мэриленда, были:

1) апробация в реальных условиях методов контрпропаганды ИГИЛ;

2) интеграция последних нейрокогнитивных и социальных концепций для более точного выявления искомого контента с учётом современных информационно-коммуникационных возможностей;

3) анализ оперативной обстановки на поле боя с классификацией действующих там субъектов информационно-психологического противоборства как «нейтральных», «дружественных» и «вражеских».

Конечная цель экспериментаторов из Пентагона сводилась к получению возможности разработки военными в ходе конкретного боестолкновения «многопрофильного плана коммуникации с учётом знаний нейробиологии, политологии, социального моделирования и маркетинга». Авторы пришли к выводу, что сосредоточение специальных сил в процессе военного конфликта на психологических операциях как на основной деятельности, а не части полного спектра информационных, дипломатических или экономических мер может иметь достаточно эффективный результат[317].

В целом такие учения являются частью стратегии передовых коммуникаций США, включая анализ социальных сетей, управление социальным поведением мирного населения во время конфликтов и достижения нейробиологии, в целях проведения успешных информационных операций. Как известно, Пентагон работает с американскими и иностранными университетами и мозговыми центрами, оценивающими научные теории в когнитивном пространстве для проведения информационных операций.

К настоящему времени созданы программы, моделирующие политическую нестабильность в конкретной стране на основе анализа распространения «мемов» в социальных сетях. В качестве примера можно привести Программный комплекс эпидемиологического моделирования эволюции сообщений в социальных сетях

---

[317] См.: Counter-Da’esh Influence Operations Cognitive Space Narrative Simulation Insights // Whitepaper. 2016. June. URL: http://nsiteam.com/social/wp-content/uploads/2016/06/C-ISIL-Simulation-Whitepaper-Jun2016-Final5.compressed.pdf (дата обращения: 05.06.2019).

(*E-MEME*)[318], в основе которого лежит концепция распространения сообщений в информационном пространстве по аналогии с эпидемиями вирусных болезней. Только в данном случае эти «информационные вирусы» поражают общественное сознание, провоцируя людей на определенные действия.

Следует отметить и то обстоятельство, что в 2016 г. четыре крупных европейских вуза, включая Гарвардский университет, открыли двухлетние программы для изучения потенциала меметики. Год спустя учебные заведения Европы (в том числе один из старейших британских университетов – Кембриджский) запустили полноценные направления подготовки для желающих изучать интернет-мемы. Учебные программы данных вузов предусматривают подготовку к защите магистерской степени по эволюционной биологии, а их создатели говорят о «мем-революции».

Важно отметить и то, что в настоящее время, помимо госструктур, в процесс разработки и апробирования технологий информационно-психологического воздействия на массовое сознание включаются коммерческие интернет-сервисы.

В частности, в 2016 г. американские специалисты по информационной безопасности компании «Фейсбук» описали этапы проведения информационных операций посредством потенциала социальных сетей:

1.Целенаправленный сбор данных – хищение, а зачастую разглашение не публичных сведений, которые могут способствовать извлечению выгоды в политическом дискурсе.

2.Создание контента, ложного или истинного, через информационного оператора либо путем распространения историй журналистами и другими третьими лицам, в том числе фейковыми пользователями.

3.Усиление лжи – скоординированная деятельность фейковых аккаунтов с целью манипуляции политическим дискурсом (например, недопущение для

---

[318] См.: *Breden J.* Intell tool would track social media like a virus // GCN Magazine. 2013. URL: https://gcn.com/articles/2013/02/12/intell-tool-track-social-media-like-a-virus.aspx?s=BIGDATA_130313&admgarea=TC_BigData (дата обращения: 13.09.2019).

участия в политическом диалоге представителей определенных политических партий, усиление сенсационности одной информации над другой и пр.)[319].

В этом контексте примечательно выглядит труд американского военного аналитика Д. Эллсберга под названием «Машина Судного дня: исповедь ядерного стратега», где он предупреждает, что выданное в условиях повышенной социальной тревожности п «фейковые новости» (*fake news*) – политически мотивированное ложное сообщение – может стать причиной начала войны мирового масштаба[320].

В 2016 г. международная неправительственная организация «Бюро журналистских расследований» заявила, что в 2003 г. Пентагон профинансировал британскую пиар-компанию «Бэлл Поттингер» (*Bell Pottinger*) на сумму более 500 млн долларов для создания ее специалистами поддельных видеосюжетов о войне в Ираке, где запечатлены действия террористических группировок. Отмечалось, что в период оккупации группа сотрудников «Бэлл Поттингер» якобы размещалась вместе с американскими военными в военном лагере «Победа» (*Victory)* в Багдаде. Примечательно, что экс-руководитель пиар-компании Тим Белл подтвердил, что компания действительно выполняла такой подряд для американцев, который курировал генерал Д. Петреус. Впоследствии поддельные видеозаписи были зафиксированы не только в Ираке, но также в Иране, Сирии и даже в Соединённых Штатах Америки[321]. Это стало известно благодаря тому, что устройства, на которых они воспроизводились, автоматически маркировались.

Указанный случай был одним из первых в рядах масштабного использования невербальных средств подачи информации в условиях цифровизации, распространяющихся по принципу мем-технологий (прежде всего видео, реже – фото и аудио), с целью оказания сильного эмоционального

---

[319] *Weedon J., Nuland W., Stamos A.* Information Operations and Facebook // Facebook. 2017. April 27. URL: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf (дата обращения: 21.01.2018).

[320] См.: The Doomsday Machine by Daniel Ellsberg // San Francisco Chronicle. 2017. December. URL: http://www.sfchronicle.com/books/article/The-Doomsday-Machine-by-Daniel-Ellsberg-12413956.php (дата обращения: 13.01.2019).

[321] См.: Fake News and False Flags // The Bureau of Investigative Journalism. 2016. October. URL: http://labs.thebureauinvestigates.com/fake-news-and-false-flags/ (дата обращения: 12.10.2019).

воздействия на сознание пользователей глобальной сети. В свете форсированного развития цифровых технологий и исследований на базе психологии и социологии, политтехнологи при поддержке исследователей апробировали в политической практике еще более совершенные инструменты информационного воздействия.

В условиях, когда некоторые западные государства готовятся к «меметической войне» с потенциальным противником, научные разработки в области мем-технологий активно используются как инструмент информационно-психологического воздействия, в частности в форме сфальсифицированного контента. В последние годы количество фальшивых новостных сообщений, а также размещенного в интернете сфальсифицированногго фото- и видеоконтента, по мнению отечественных, так и зарубежных специалистов, достигло критического значения. Противодействие такой деятельности, которая ведется как легитимными, так и нелегитимными политическими акторами, представляет собой серьезную техническую, политическую, социальную и правовую проблему. Например, в настоящее время примерно 70 % населения Соединенных Штатов Америки считают, что проблема фейковых сообщений стала катализатором снижения доверия к органам государственной власти, и еще более половины опрошенных граждан США полагают, что фейковые новости является более серьезным вызовом для безопасности США, чем терроризм, нелегальная миграция, преступность или расизм[322].

В настоящее время большая часть дезинформации в интернет-пространстве все еще создается людьми, однако в последние годы стало появляться все больше фейков, сгенерированных с помощью технологий искусственного интеллекта. В настоящее время эксперты выделяют два оснвоных вида «фейков». К первому относятся фальшивые текстовые сообщения на различных сетевых ресурсах, включая и социальные сети, а ко второму – поддельный фото- и видеоконтент. Поддельные новости генерируются в основном людьми, но также растут и

[322] *Kelley M.* Sayler, Laurie A. Harris. Deep Fakes and National Security // CRS. 2019. URL: https://crsreports.congress.gov/product/pdf/IF/IF11333 (дата обращения: 05.12.2019).

масштабы их создания средствами искусственного интеллекта. Вместе с тем текстовые материалы, формируемые ИИ, все еще достаточно легко выявить, тогда как фото- и видеопродукты, создаваемые с помощью технологий ИИ, распознать весьма непросто. Более того, дезинформация такого рода, созданная на основе меметических технологий, приобретает большую популярность среди населения, поскольку формирует у людей полное впечатление истинности фото- или видеоряда.

Наибольшую опасность, по мнению специалистов из США, представляют перспективы применения в политической и военной практике «глубоких фейков» (*deepfakes*) – изображений объектов, где синтезированная картинка накладывается на реальную. Термин «глубокие фейки» образован путем сочетания терминов «глубокое машинное обучение» (*deep learning*) и «фейки». В основе технологии глубоких фейков лежит работа так называемых генеративных состязательных сетей (*generative adversarial networks*), когда наборы алгоритмов – нейросети – учатся выводить правила и повторять схемы, обрабатывая большие массивы данных. В ходе такого процесса пары алгоритмов объединяются друг против друга, где один алгоритм (генератор) создает ложный контент на основе имеющейся базы данных, а другой алгоритм (дискриминатор) пытается его выявить. В условиях, когда каждый из алгоритмов постоянно тренируется противостоять другому, происходит постепенное совершенствование качества создаваемого продукта. Как свидетельствует Рисунок 3.4, такая работа позволяет генеративным состязательным сетям производить очень реалистичный контент.

Источник: Hi-tech.mail.ru

Рисунок 3.5 – Фотографии несуществующих людей, созданных нейросетью

В апреле 2018 г. исследователи Вашингтонского университета опубликовали видео, получившее название «Обамапил» (*ObamaPeele*), – согласно именам его исполнителей. На видео экс-президент США Б. Обама якобы произносит речь; в действительности, текст для этого видео зачитывал актер Дж. Пил, который изначально не показан в кадре. Ролик наглядно продемонстрировал опасность данных технологий. Американские специалисты повторили подобный эксперимент с одним из выступлений Б.Обамы, состоявшегося в 2017 г., а затем представили его мировой общественности в сети интернет с подробным описанием того, по какому принципу создано такое видео[323].

Аналитики близкого к американским правительственным структурам экспертного центра Совет по международным отношениям (*Council on Foreign Relations)* считают, что большую опасность глубокие фейки представляют в период ухудшения межгосударственных отношений. В качестве примера они приводят фальшивый файл (фото, аудио или видео), претендующий на запись беседы российского и американского президентов в Финляндии летом 2018 г. (Хельсинки). К другим сюжетам подобной остроты, по оценкам американцев, можно причислить глубокие фейки, изображающие израильского

[323] Synthesizing Obama: Learning Lip Sync from Audio // Grail. 2017. October. URL: http://grail.cs.washington.edu/projects/AudioToObama/ (дата обращения: 20.10.2019).

военнослужащего, совершающего преступление в отношении палестинского ребенка или лидера народа рохинджа, выступающего против законных сил безопасности в Мьянме[324].

В свою очередь, крупные американские исследователи рассматриваемого феномена Р. Чесни и Д. Ситрон выражают опасение, что технологии глубоких фейков могут существенно усугубить социально-культурный раскол в США (по этническому, религиозному, расовому признакам). В основном такая деятельность связывается американскими учеными с иностранными силами, заинтересованными в дестабилизации Америки. В качестве примера они приводят размещение глубоких фейков с участием правоохранительных органов, превышающих свои служебные полномочия, и представителей группы меньшинств, размещенных в фальшивых аккаунтах[325].

Большое внимание западные специалисты уделяют возможности применения глубоких фейков в период электорального цикла. В аналитической записке Исследовательской службы Конгресса США «Глубокие фейки и национальная безопасность», опубликованной 14 ноября 2019 г., американские законодатели выражают опасение, что фальшивый контент может использоваться в целях радикализации населения, вербовки террористов или подстрекательства к насилию с учетом национального контекста. Кроме того, данные технологии якобы могут усилить инструментарий противников США в реализации ими операций влияния в ходе текущей предвыборной борьбы за пост главы государства[326].

В данном контексте следует отметить, что от американской и мировой общественности представители США замалчивают тот факт, что первое

---

[324] Disinformation on Steroids // Council on Foreign Relations. 2018. October 16. URL: https://www.cfr.org/report/deep-fake-disinformation-steroids?utm_medium=email&utm_source=twtw&utm_content=101918&sp_mid=57597773&sp_rid=ZXZyYXppYUBnbWFpbC5jb20S1 (дата обращения: 02.07.2019).

[325] *Чесни Р., Ситрон Д.* Глубокие фейки и новые войны дезинформации // Россия в глобальной политике. 2019. 18 января. URL: https://globalaffairs.ru/global-processes/Glubokie-feiki-i-novye-voiny-dezinformatcii-19918 (дата обращения: 20.10.2019).

[326] *Kelley M.* Sayler, Laurie A. Harris. Deep Fakes and National Security // CRS. 2019. URL: https://crsreports.congress.gov/product/pdf/IF/IF11333 (дата обращения: 05.12.2019).

«ознакомительное» распространение глубоких фейков состоялось именно на территории Америки, и там же в упредительном порядке началось создание механизмов по противодействию данной технологии[327].

Как нам представляется, мирвоому политическому сообществу важно учитывать, что в настоящее время технологии в указанной сфере активно совершенствуются, причем непосредственно под эгидой исследовательских подразделений военных и разведывательных структур отдельных стран мира. Например, по оценкам экспертов Управления перспективных исследований МО США, в будущем глубокие фейки могут быть снабжены такой опцией, как сопереживание аудитории, что поспособствует существенному изменению их восприятия. Кроме того, специалисты исследуют возможность на базе технологий искусственного интеллекта создания компьютерных программ, имитирующих не привязанную к конкретной ситуации речь человека[328].

В целом появление глубоких фейков целесообразно рассматривать в качестве эффективного инструмента инфомационного противоборства и, соответственно, долгосрочного вызова национальной безопасности. На данный факт обращают внимание авторы аналитического обзора, выпущенного Счетной палатой США[329] в декабре 2018 г. В этом документе указывается, что новая технология может быть использована против Соединенных Штатов и их союзников посредством создания полноценных политически мотивированных новостных сюжетов, а также дискредитации и шантажа дипломатов и служащих других госструктур, имеющих доступ к секретной информации и находящихся за рубежом[330].

В сентябре 2019 г. под эгидой Счетной палаты США был создан Центр стратегического прогнозирования (*Center for Strategic Foresight*), который

---

[327] Media Forensics (MediFor) // DARPA. 2016. URL: https://www.darpa.mil/program/media-forensics (дата обращения: 23.12.2019).

[328] Ibid.

[329] В США Счетная палата является ведущим аналитическо-следственным органом Конгресса.

[330] National Security: LongRange Emerging Threats Facing the United States as Identified by Federal Agencies // Government Accountable Office. 2018. URL: https://www.gao.gov/assets/700/695981.pdf (дата обращения: 23.12.2019).

объединил под руководством Дж. Блэквуда девять экспертов для анализа двух тем, имеющих принципиальное значение для будущей безопасности и благополучия страны. К таким темам отнесены космическая политика США, а также перспективы применения глубоких фейков для манипулирования взаимодействиями людей онлайн и в реальном мире[331].

В данной связи следует отметить, что в зарубежной экспертной среде практически не упоминается о рисках создания и применения в политической практике глубоких фейков негосударственными участниками мировой политики – повстанческими, террористическими, экстремистскими группировками, хакерскими и хактивистскими сообществами и пр., которые традиционно обращаются к невербальным методам воздействия на аудиторию. Вместе с тем данные технологии вполне могут использоваться ими в формате информационного противоборства ввиду относительно простого способа изготовления и размещения в социальных сервисах интернета, поскольку в условиях форсированной цифровизации социально-политической реальности в виртуальном пространстве довольно легко можно найти видео, фото и аудио любого человека, тем более публичного. Соответственно, в обозримой перспективе единственным сдерживающим фактором создания такого фальсифицированного контента станет доступ к обучающим материалам для нейросетей.

В свете появления угрозы нового типа ведущие государства мира, в частности Соединенные Штаты Америки, совершенствуют законодательную базу в сфере создания и распространения фейков. Так, опубликование в конце мая 2019 г. американскими СМИ фальшивого видео с главой Палаты представителей США Н. Пелози, которое успел даже прокомментировать в социальных медиа американский президент Д. Трамп, стало поводом к внесению в Конгресс нормативно-правового акта по борьбе с распространением дезинформации

[331] Deep Space & Deep Fakes: New "Center for Strategic Foresight" Launched // Government Accountable Office. 2019. URL: https://www.gao.gov/about/press-center/press-releases/center-for-strategic-foresight.htm (дата обращения: 23.12.2019).

посредством введения ограничений на технологии подделки видео с помощью глубоких фейков[332]. Вскоре США приняли другой закон, который обязует национальное министерство внутренней безопасности (*Department of Homeland Security)* ежегодно публиковать обзор, посвященный возможному негативному влиянию технологии глубоких фейков на национальную безопасность Америки[333].

Одновременно американцы изучают нормативно-правовую базу других государств по противодействию вызовам и угрозам, которые обусловлены применением меметических технологий в условиях цифровизации. В докладе, выполненном в апреле 2019 г. юристами Исследовательской службы Конгресса США, проанализированы меры 15 стран по противодействию фейковым новостям, и в том числе России[334]. Эксперт по политике РФ в данной области Астик Григорян дает весьма высокую оценку нормотворческим усилиям нашей страны в сравнении с другими рассматриваемыми государствами. Из документа следует, что одним из наиболее эффективных способов по противодействию фейкам является создание специальных онлайн-структур, призванных практически мгновенно опровергать фейковые новости и предоставлять населению правдивую информацию. В настоящее время по такому примеру действуют британское подразделение «Быстрый ответ» (*Rapid Response)* и китайская онлайн-платформа «Опровержение слухов» (*Refuting Rumors)*[335].

Кроме того, в США ищут технологические способы противобдействия уже созданным технологиям информационного противоборства. Так, в 2018 г. перед Национальным научным фондом США, Управлением перспективных

---

[332] Bill H.R. 3230 «To combat the spread of disinformation through restrictions on deep-fake video alteration technology» // Congress.gov. 2019. June 12. URL: https://www.congress.gov/bill/116th-congress/house-bill/3230/text (дата обращения: 02.07.2019).

[333] См.: *Goggin B.* From porn to 'Game of Thrones': How deepfakes and realistic-looking fake videos hit it big // Business Insider.2019. June 23. URL: https://www.businessinsider.com/deepfakes-explained-the-rise-of-fake-realistic-videos-online-2019-6. (дата обращения: 24.10.2019).

[334] Помимо анализа российского подхода к противодействию фейковым новостям, американцы изучали соответствующие меры Аргентины, Бразилии, Канады, Японии, Китая, Малайзии, Египта, Кении, Никарагуа, Израиля, Франции, Германии, Швеции и Великобритании.

[335] Initiatives to Counter Fake News in Selected Countries // CRS. 2019. URL: https://fas.org/irp/eprint/lloc-fake-news.pdf (дата обращения: 23.12.2019).

исследований Министерства обороны США и Управлением перспективных исследований в сфере разведки США поставлена задача обеспечить приемлемое купирование вызовов и угроз, связанных с созданием и применением в политической практике глубоких фейков. В частности, летом 2018 г. Управление перспективных исследований Министерства обороны США запустило проект, нацеленный на поиск возможного решения в деле различия поддельных и реально существующих видео с учетом того, что фальсификация:

1) выглядит как настоящий продукт;

2) создана при помощи искусственного интеллекта, соответственно, и анализ таких файлов также должен проводиться при помощи искусственного интеллекта.

Таким образом, если учитывать особенности ведения информационного противоборства в условиях современной цифровой среды (высокую скорость распространения информации в трансграничном формате; активное участие нелегитимных акторов мировой политики в создании и продвижении контента в глобальной информационно-коммуникационной сети; сильную подверженность аудитории эмоциональному воздействию и ее слабую восприимчивость к рациональным аргументам и пр.), то присутствуют все основания полагать, что уже в обозримом будущем общество во многих странах мира будет все чаще сталкиваться с распространением мем-технологий в фото- или видеоформате. В пользу этого свидетельствует возрастающая зависимость общества от цифровых медиаресурсов, а также восприятие их в качестве надежного источника информации. Кроме того, важным фактором является то, что технологии поизводства различного рода фейков совершенствуются с устрашающей скоростью, и бороться с ними становится все труднее, учитывая, что опасность сетевого поддельного контента усугубляется тем, что даже после его разоблаченя эффект от применения рассматриваемого инструмента информационного противоборства сохраняется весьма продолжительное время.

В данных обстоятельствах значимым фактором политики госструктур является скорость реагирования на процессы и события в информационно-

коммуникационном пространстве, причем не в ущерб возможности доходчивого разъяснения официальной позиции по значимым для социума вопросам. Последнее крайне важно в резонансных случаях, поскольку способствует убедительному опровержению фейковых новостей. При этом превентивное создание мемов и нарратива, отвечающих национальным интересам страны, может существенно минимизировать негативные последствия деятельности внешних сил в цифровой среде, стремящихся обычно заполнить ее «пустоты».

Глава 4. УПРЕЖДЕНИЕ ПОЛИТИЧЕСКИХ РИСКОВ СОВЕРШЕНСТВОВАНИЯ ПРАКТИК ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В ЦИФРОВУЮ ЭПОХУ

4.1. Вероятностные социально-политические последствия применения цифровых технологий в информационном противоборстве

В настоящее время социально-политический дискурс формируется в условиях постоянной гонки за интернет-трафиком, что заставляет как государственные, так и альтернативные средства массовой информации снизить планку внутренней цензуры, чтобы соответствовать в круглосуточном режиме функционирования интернет-форумов и социальных сетей ритму традиционных и новых акторов процессов информационного противоборства. Они действуют в логике «больше сенсации – больше просмотров – выше доход»[336], когда истина уже не рассматривается в качестве принципиально важной характеристики новостного сообщения. Вследствие такого изменения коммуникационной среды общества акценты в информационном пространстве все больше переносятся с качества информации на ее сенсационность. В данных условиях формируется новая социально-политическая реальность – в России и в мире в целом.

Соответственно, **прорывное развитие инновационных технологий, применимых для влияния на массовое сознание и формирования общественного мнения в условиях стремительной цифровизации, стимулирует возникновение новой коммуникативной реальности – вневременной и трансграничной среды, где ложная информация тесно переплетается с правдивой.** Это актуализирует применение в политологическом дискурсе понятия «постправды» (*post-truth era*) – информационного потока, намеренно конструируемого с помощью СМИ для создания виртуальной, отличной от действительности реальности с целью манипулирования общественным сознанием.

---

[336] См.: *Майка Р.* Как Трамп и фейки изменили медиа // РСМД. 2018. 4 июня. URL: https://russiancouncil.ru/analytics-and-comments/columns/united-states/kak-tramp-i-feyki-izmenili-media/?sphrase_id=28536647 (дата обращения: 14.04.2019).

Термин «постправда» был впервые использован американским исследователем Д. Робертсоном в статье для онлайн-издания «Грист» (*Grist*) 1 апреля 2010 г., в которой постправда определялась как политическая культура, где публичное содержание политики (общественное мнение и содержание новостей) практически полностью отрывается от законодательства[337].

В политологической и социологической теории постправда взаимопереплетается с категорией «симулякр», которую французский ученый Ж. Бодрияр применял к социальной реальности, описывая недобросовестность медиа при освещении реальных событий и медиаподделки[338]. Термин является семантическим эвфемизмом и подразумевает наличие в журналистских произведениях недостоверной или неточной информации. Чаще всего это носит сконструированный характер. Таким образом, постправда – суть нечто вместо правды, реальность, когда объективные факты являются менее значимыми при формировании общественного мнения, чем обращения к эмоциям и личным убеждениям[339].

В 2012 г. о постправде как социально-политической реальности упомянул американский экономист П. Кругман с целью охарактеризовать президентскую кампанию М. Ромни, в ходе которой последний обещал отменить сокращение расходов на оборону, состоявшееся при Б. Обаме, при том, что расходы на оборону в президентство последнего возросли[340].

Широкое распространение понятия «постправды» состоялось в 2016 г., ознаменованном американскими президентскими выборами и референдумом о членстве Великобритании в Европейском союзе. Авторитетный британский

---

[337] Цит. по.: *Harsin Jayson*. Regimes of Posttruth, Postpolitics, and Attention Economies. Communication, Culture & Critique. 2015. p. 327–333.

[338] Definition of post-truth in English // Oxford Dictionaries. Lexico Dictionaries. 2019. URL: https://www.lexico.com/en/definition/post-truth (дата обращения: 10.10.2019).

[339] См.: *Чугров Сергей.* Post-truth: трансформация политической реальности или саморазрушение либеральной демократии? // Полис. Политические исследования. 2017. № 2. С. 42–59.

[340] См.: *Gray Iain.* Iain Gray: Beware the black art of post-truth politics // The Scotsman. 2012. URL: https://www.scotsman.com/news/opinion/iain-gray-beware-the-black-art-of-post-truth-politics-1-2146059 (дата обращения: 25.09.2019).

Оксфордский словарь объявил термин «постправда» международным словом 2016 г., ссылаясь на 2000 % рост его использования в 2016 г. по сравнению с 2015 г.[341]

Одна из причин современной постправды – объемы обрушившихся на граждан фейковых новостей, когда люди часто неспособны противостоять информационному потоку и готовы охотнее верить придуманным, мимикрирующим под новости, сомнительным сообщениям, чем новостям авторитетных, крупных изданий, или по крайней мере сомневаться и проверять источники. Это происходит из-за того, что раздробленность источников новостей создаёт ситуацию, при которой сенсационная, эмоционально окрашенная лживая информация распространяется с необычайной скоростью.

Например, в ходе предшествовавшей Брекзиту кампании, организация «Голосуем за выход» (*Vote Leave*), лоббировавшая расставание Лондона и Брюсселя, неоднократно выступала с заявлениями, что Соединенному Королевству членство в Евросоюзе обходится в 350 млн фунтов в неделю. Спустя некоторое время представители указанной организации стали использовать факт финансовых выплат в том числе для обозначения переводимых Лондоном средств непосредственно в страны ЕС[342]. Несмотря на то обстоятельство, что институт фискальных исследований назвал эту сумму «заведомо неверной», «Голосуем за выход» продолжала использовать такие данные для проведения своей политики вплоть до дня проведения референдума[343].

Утверждению политики постправды способствует сама природа человека, который при переизбытке информации склонен доверять нерациональным, эмоциональным доводам в ущерб или даже взамен рациональной аргументации. На современном этапе это происходит в условиях четко выраженной сегментации

---

[341] См.: *Николаевич И. С.* Как нас обманывают СМИ. Манипуляция информацией. СПБ.: Питер, 2018. 320 с.

[342] См.: *Simons Ned.* Tory MP Sarah Wollaston switches sides in EU Referendum campaign. Huffpost politics. 2016. June. URL: https://consent.yahoo.com/collectConsent?sessionId=1_cc-session_aacf81e3-e862-4d14-bd5e-cbb861a13174&lang=en-gb&inline=false (дата обращения: 09.10.2019).

[343] Цит. по: The UK's EU membership fee // Full Fact. 2016. 25 февраля. URL: https://fullfact.org/europe/our-eu-membership-fee-55-million/ (дата обращения: 10.10.2019).

интернет-аудитории на отдельные группы, которые стремятся искать и публиковать преимущественно ту информацию, которая подтверждает и укрепляет их взгляды, игнорируя при этом конкурирующие мнения.

Происходящее в последние годы лавинообразное распространение фейковых новостей привело к усилению внимания к проблеме постправды региональных и международных организаций. Еще в 2017 г. специальный докладчик ООН по вопросам свободы слова и выражения мнения, Организация безопасности и сотрудничества в Европе и Организация американских государств опубликовали совместную декларацию «Свобода выражения мнений, фальшивые новости, дезинформация и пропаганда». В ней отмечались негативные социальные аспекты, связанные с рисками открытой информационно-коммуникационной среды, и в то же время указывалось на трудности ведения независимой журналистики в свете ужесточения стороны государственной цензуры[344].

Таким образом, если до недавнего времени технологические инновации в информационно-коммуникационной сфере оставались периферийным вопросом в международных взаимодействиях, однако сегодня использование возможностей интернета формирует качественно новую декомпозицию мировой политики. Ее основной особенностью становится отсутствие барьеров, традиционно присущих политико-дипломатической практике, – беспрецедентная доступность информации сочетается со столь же беспрецедентным ее переизбытком.

В этом контексте **на повестке дне ученых и государственных деятелей актуализируются вопросы о возникновении и развитии социальных, в частности протестных движений в условиях цифровой среды, а также управлении процессами информационного противоборства в данный период.**

Как показывают теоретические наработки и политическая практика, могут служить предпосылкой перетекания массового стихийного поведения из

[344] Amid rise of ‘fake news,’ authorities should ensure truthful info reaches public // United Nations. 2017. March 10. URL: https://news.un.org/en/story/2017/03/553122-amid-rise-fake-news-authorities-should-ensure-truthful-info-reaches-public-un (дата обращения: 08.10.2019).

виртуального пространства в реальную социально-политическую плоскость. Исследователи теории социальных движений трактуют этот феномен как «ряд дискуссионных перформансов, демонстраций и кампаний, с помощью которых простые люди осуществляют коллективные требования к другим»[345]. Так, американский социолог Ч. Тилли отмечал, что социальные движения являются основным средством привлечения людей к участию в государственной политике.

В свою очередь, идеолог «нового лейборизма», английский социолог Э. Гидденс определял социальные движения, как «коллективную попытку осуществить общие интересы или добиться общей цели посредством коллективного действия вне рамок установленных институтов». Примечательно, с позиции Э. Гидденса, что «теории революций и теории социальных движений с неизбежностью пересекаются»[346].

В современной социологической теории социальные движения рассматриваются как «массовые коллективные действия одной или нескольких социальных групп, связанные с обеспечением групповых или общественных интересов, потребностей (как материальных, так и духовных), и направленные на социальные изменения или сопротивления им в конфликтном противодействии с другими социальными группами»[347].

Очевидно, что масштабный географический охват социальных сетей, облегчающий трансграничное распространение информации и сочетающийся с широкими возможностями таргетирования аудитории имеют неоценимую важность для организаторов социальных движений. Обращению к возможностям интернет-пространства как к каналу, обеспечивающему доступ к целевой группе, способствует также сравнительно невысокая стоимость рекламного контакта и возможность практически бесплатного продвижения социально значимых проектов – за счет создания аккаунтов, постоянного генерирования актуального,

---

[345] *Tilly Charles.* Social Movements. Boulder, CO, Paradigm Publishers, 2004. p. 262.

[346] *Гидденс Э.* Социология / Пер. с англ.; науч. ред. В. А. Ядов; общ. ред. Л. С. Гурьевой, Л. Н. Посилевича. М.: Эдиториал УРСС, 1999. 703 с.

[347] *Грицанов А.А., Абушенко В.Л.,* Евелькин Г.М., Соколова Г.Н., Терещенко О.В. Социология: Энциклопедия. М., 2003. С. 789.

интересного и содержательного контента, сотрудничества с аналогичными виртуальными сообществами и т.д.

Кроме того, в пользу задействования преимуществ современного информационно-коммуникационного пространства в целях организации социальных движений свидетельствует и возможность получения быстрой обратной связи от целевых групп. Например, активность участия пользователей в электронных голосованиях, качество комментариев, количество «лайков» и «репостов», эмоциональность откликов позволяют сделать выводы о популярности идеи, важности и полезности информации для отдельных личностей (своеобразных лидеров общественного мнения), социальных слоев и общества страны в целом. Можно предположить, что именно с этой целью в виртуальных социальных сетях, как правило, создаются сообщества или публичные страницы («паблики»), где регулярно добавляются новости с возможностью их комментирования.

Широкому распространению в виртуальном мире информации о социальных движениях способствует использование современных мультимедийных технологий, в основе которых лежит сочетание текстового, музыкального, графического и видеоформатов контента, то есть взаимодополнение вербальных и невербальных каналов подачи информации. Таким образом, особенности интернет-пространства как коммуникативной среды и задействование соответствующих практик позволяют субъектам управления вполне уверенно ставить перед обществом определенную цель, как правило, связанную с выражением коллективного недовольства, поддержки или сопротивления каким-либо социальным изменениям. Об этом, в частности, свидетельствует использование потенциала социальных сетей в качестве инструмента управления обществом и его отдельными группами в недавних событиях в европейской политике, имеющих фактурное название – движение «жёлтых жилетов».

В отличие от предшествующих организованных французскими профсоюзами протестов движение «желтых жилетов» во Франции развивалось

посредством интернет-сервисов, в частности социальных сетей. Инициатива призыва к движению исходила от автомобилистки Ж. Муро из департамента региона Иль-де-Франс, опубликовавшей в мае 2018 г. онлайн-петицию к властям страны с призывом снизить цены на топливо. Данное обращение оставалось малозаметным до момента его опубликования 12 октября 2018 г. национальным изданием «Паризьен» (*Parisien*). Примечательно, что уже 25 октября онлайн-петиция Ж. Муро набрала почти четверть миллиона подписей французов (225 тысяч), а еще через месяц их количество превысило миллион[348].

Ведущую роль в популяризации движения «желтых жилетов» по всей Франции сыграли социальные сети, посредством которых люди координировали свои действия, блокируя ключевые узлы в разных точках страны и, соответственно, парализовали ответные действия власти. В этом плане примечательным фактором выступали названия групп, создаваемых в интернет-пространстве: «Граждане в гневе», «Желтые жилеты Руана», «Сердца жилетов: группа взаимопомощи участников движения», «Желтые жилеты: следующий этап – блокировка Парижа» и пр. В частности, как отмечал К. Тисье, модератор интернет–группы «Автомобилисты Нормандии в гневе», насчитывающей более 50 тысяч человек, идеальной платформой для организации акций «жёлтых жилетов» стал «Фейсбук». Он связывал это с тем, что когда участники движения нуждались в материально-техническом обеспечении, они его получали именно за счет функционирования сообществ в указанной соцсети[349].

Постепенно борьба участников движения «желтых жилетов» и французских властей распространилась на киберпространство. По оценкам экспертов, занимающейся вопросами кибербезопасности, со стороны протестующих происходили многочисленные инциденты типа «отказ в обслуживании» (DoS и

---

[348] См.: Qui sont les internautes à l'origine de l'appel aux blocages contre la hausse du prix du carburant? // Franceinfo. 2018. Novembre. URL: https://www.francetvinfo.fr/economie/automobile/essence/appel-aux-blocages-contre-la-hausse-du-prix-du-carburant-partout-en-france-les-gens-sont-prets-a-se-mobiliser_3003467.html (дата обращения: 10.10.2019).

[349] Un mois de prison avec sursis requis contre le « gilet jaune » Eric Drouet // Le Monde. 2019. 15 février. URL: https://www.lemonde.fr/societe/article/2019/02/15/eric-drouet-figure-des-gilets-jaunes-au-tribunal-vendredi_5423716_3224.html (дата обращения: 10.10.2019).

DDoS-атаки)[350] против сайтов французских госструктур. В частности, кибератакам подверглись официальные сайты Министерства юстиции и Бюро по сбору отчислений в фонд социального обеспечения и помощи семье Франции. Причем, как отмечают специалисты, участники движения «желтых жилетов» – далеко не единственные негосударственные субъекты информационного противоборства, кто применял такую тактику в киберпространстве: это уже происходило в Турции, в Каталонии и на Украине[351].

Социально-политическими последствиями деятельности «желтых жилетов» стала поляризация французского общества. Движение, первоначально возникшее как протест против налога на топливо, разделилось на группы с самыми разнообразными интересами и потребностями. Так, например, наряду с экономическими требованиями, одним из самых популярных стало требование политическое – признать «принцип народного референдума», когда важные реформы правительство должно выносить на всенародное голосование. Этому способствовал в том числе принцип функционирования социальных сетей, предполагающий разделение пользователей на дискриминированные сообщества по интересам.

Цифровые технологии явились ключевым инструментарием состоявшейся в 2014 г. в Гонконге «революции зонтиков», равно как и массовых протестов, вспыхнувших в 2019 г. Как указывают западные эксперты, в 2014 г. основными площадками протестующих стали социальные сети «Фейсбук» и «Твиттер». Например, в наиболее напряженный период противостояния власти и оппозиции

---

[350] DoS (*Denial of Service*) — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён; DDoS (*Distributed Denial of Service*) — аналогичная хакерская атака на вычислительную систему хорошо защищённой крупной компании или правительственной организации, выполняемая как правило одновременно с большого числа компьютеров.

[351] См. напр.: News Feed FYI // Facebook. 2019. URL: https://newsroom.fb.com/news/category/news-feed-fyi/ (дата обращения: 11.10.2019).

пользователи «Твиттера» публиковали 12 сообщений в секунду, а общее их число за время протестных акций достигло 1,3 млн сообщений[352].

В протестах, начавшихся в Гонконге летом 2019 г. в связи с началом процедуры правового слияния этой территории с материковым Китаем, цифровая среда стала идеальным пространством, а ее сервисы – инструментами для совершения массовых акций. Это обусловлено тем обстоятельством, что примерно 92 % жителей Гонконга имеют доступ в интернет и пользуются им ежедневно, а более 80 % населения причисляют себя к активным пользователям[353].

В противостоянии 2019 г. координация среди протестующих гонконгцев происходила уже не в социальных сетях, а в мессенджерах. Социальные сети служили в основном в качестве невербальной поддержки, где широко применялся потенциал меметических технологий с целью оказать максимальное информационно-психологическое воздействие на возможных участников протеста и подтолкнуть их к каким-либо действиям.

Смена инструментов интернет-сервисов обусловлена тем, что социальные сети не позволяют в полной мере сохранить анонимность их пользователей, в то время как мессенджеры имеют функцию шифрования и их пользователей существенно труднее без потери времени подвергнуть деанонимизации[354].

Среди наиболее используемых мессенджеров во время митингов в Гонконге следует назвать «Телеграм», «Вотсап» (*WhatsApp*), «Сигнал» (*Signal*) и «Фаерчат» (*FireChat*). Примечательно, что последний может быть использован даже при

---

[352] См.: *Chiu K.* From Facebook and Twitter to Telegram, WhatsApp and Signal: how protest technology has evolved since Occupy Central. SCMP. URL: https://www.scmp.com/news/hong-kong/article/3014255/ facebook-and-twitter-telegram-whatsapp-and-signal-how-protest (дата обращения 23.05.2019).

[353] См.: How many internet users does each country have? // Our World in Data. 2019. URL: https://ourworldindata.org/how-many-internet-users-does-each-country-have (дата обращения: 23.07.2019).

[354] См.: *Boehler L.* 'Off-the-grid' messaging application FireChat continues to ride Occupy boost // SCMP. 2019. URL: https://www.scmp.com/news/hong-kong/article/1611322/grid-messaging-application-firechat-continues-ride-occupy-boost (дата обращения: 23.08.2019).

отключении интернета и технологии беспроводной локальной сети Wi-Fi, поскольку работает по принципу «ячеечной сети»[355].

Взрывной прирост аудитории во время данных протестных акций наблюдался у мессенджера «Телеграм», который установили к тому моменту четверть всего населения Гонконга (1,7 млн человек). В этом сервисе публиковались наиболее агрессивные призывы по отношению к официальному Пекину; места протестных действий, что способствовало координации активистов; своеобразные зоны укрытия, где можно спрятаться от правоохранительных органов и пр.

Кроме того, как отмечают некоторые специалисты-китаеведы, важной платформой для коммуникации протестующих явились форумы, ведущиеся непосредственно на китайском языке. К таковым, например, они причисляют LIHKG[356]. Регистрация на указанном интернет-портале предполагает наличие адреса электронной почты с доменным именем одного из гонконгских интернет провайдеров или образовательных учреждений. Такой подход позволял автоматически отсеивать подавляющую массу иностранцев, к которым причисляются в том числе жители материкового Китая.

Важно отметить и относительно новый инструмент мобилизации протестующих – передача информации о местоположении посредством сервисов Wi-Fi или «Блютус» (*Bluetooth*). Этот инструмент в принципе может быть использован для политической пропаганды при распространении призывов выходить на митинг. Как свидетельствуют оценки участников оппозиционных выступлений, в местах крупного скопления людей один из 20–25 человек соглашался принять на телефон сообщение через «ЭйрДроп» (*AirDrop*). Кроме того, по их словам, эффективность использования указанного сервиса лучше всего проявляется при необходимости совершения единичного коллективного действия. Нередко это было связано с выполнением требований китайских

[355] Ibid.
[356] LIHKG. URL: https://lihkg.com/thread/1474430/page/1 (дата обращения: 06.10.2019).

властей с тем, чтобы воспрепятствовать обвинениям в адрес участников митингов в неподчинении.[357].

Протестующие в Гонконге стремились активно взаимодействовать с лидерами мнений западных стран (прежде всего Великобритании и США) с целью получить от них надежную поддержку в протестных начинаниях. В коммуникации с представителями зарубежных государств применялся в основном принцип взаимодействия на площадках социальных сетей, что обусловлено присутствием там лидеров мнения – журналистов, гражданских активистов, представителей НПО и пр. Этому поспособствовало то, что в Гонконге социальные сети в полной мере доступны для местного населения (в отличие от материкового Китая). Примечательно, что все видео–, фото–, и аудиофайлы сопровождались английскими субтитрами[358].

Западные эксперты зафиксировали на повышенную активность использования в период протестных акций бот-аккаунтов прокитайской направленности[359]. По их оценкам, активность таких ботов изначально находилась на довольно низком уровне, но после наращивания числа таких аккаунтов (август 2019 г.) их эффективность приблизилась к нулю. Англосаксонские специалисты указывают, что причина такого развития событий заключается в том, что изначально официальный Пекин старался игнорировать происходящее и, соответственно, потерял контроль над развитием общественных настроений. К тому моменту, когда стала очевидна целесообразность его активности, власти Китая не были готовы к координации массовой онлайн-компании в социальных медиа.

---

[357] См.: AirDrop requests are Gen Z’s way of passing notes on Apple devices – as Hong Kong protesters show // SCMP. 2019. URL: https://www.scmp.com/lifestyle/gadgets/article/3018133/airdrop-requests-are-gen-zs-way-passing-notes-apple-devices-hong (дата обращения: 23.09.2019).

[358] См.: Hong Kong: Ambulance Passes Through Sea of Protesters During Sunday’s Massive Rally // Spectee. 2019. URL: https://spectee.com/detail/22065 (дата обращения: 26.10.2019).

[359] См. напр.: 72 Insikt Group. Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion. 2019. URL: https://go.recordedfuture.com/hubfs/reports/cta-2019-0306.pdf (дата обращения: 06.10.2019).

Таким образом, хотя официальные власти КНР и смогли удержать контроль над патриотическим дискурсом внутри страны в ходе массовых протестных выступлений в Гонконге в 2019 г., применение протестующими всевозможных цифровых инструментов для решения собственных задач продемонстрировало высокую степень адаптивности социума к инновациям, появившимся сравнительно недавно, и одновременно пониженную готовность к отражению подобных угроз со стороны официальных властей.

В целом, сказанное демонстрирует открывающиеся перед политической элитой перспективы возможностей управления массовыми социальными движениями в обозримом будущем. По мере дальнейшей цифровизации социально-политического пространства, скорее всего, появятся новые риски, связанные с задействованием в социальной активности инновационных технологий на базе искусственного интеллекта. Не исключено, что как протестующие, так и властные элиты могут начать применять принципиально новый инструментарий для достижения собственных целей, акцентируя усилия на ресурсах цифровой среды[360].

Исследования, проведенные российскими учеными, указывают на специфичный состав социальной базы движений, организующихся в глобальной сети. Так, метод таргетингового анализа с переменными по полу, возрасту, месту проживания и ценностным ориентациям позволил выявить, что ядром протестного движения, развивающегося в виртуальном социуме, могут стать молодые мужчины в возрасте 18–34 лет, преимущественно жители крупных городов с населением свыше 1 млн населения. В целом при совокупной выборке 35 тысяч респондентов 15 тысяч заявляют о том, что точно войдут в протестное движение[361].

Гендерный состав исследуемого сообщества свидетельствует о более низкой социально-политической активности женщин по сравнению с мужчинами:

---

[360] См. подр.: *Рогачев С.В., Виловатых А.В.* Социальные движения в эпоху постправды // Проблемы национальной стратегии. 2020. № 1 (58).

[361] См. подр.: *Ушкин С.Г.* Вовлеченность пользователей социальных сетей в протестные движения // Власть. 2014. №8. С. 139–140.

женщины вдвое реже заявляют о своей готовности поддержать протестное социальное движение. Половина декларируемых участников протестной акции (51,0 %) – это люди от 25 до 34 лет; возраст каждого третьего пользователя (34,2 %) – от 18 до 34 лет. Другие возрастные категории представлены в существенно меньшей степени (от 1,6 % до 5,9 %).

Относительно детерминирующими для участия в социальном движении могут считаться три выраженных ценности: саморазвитие (8,6 %), семья и дети (6,3 %) и совершенствование мира (4,2 %). Другие ценностные ориентации (карьера и деньги, развлечения и отдых, наука и исследования, красота и искусство, слава и влияние) не играют существенной роли (от 0,8 % до 1,1 %). Примечательно, что большинство декларируемых участников протестной акции (76,1 %) предпочитают игнорировать заполнение данной информации в своем профиле.

Таким образом, сегодня постправда стала квазисредой, контекстом, который способствует распространению ложных новостей. Эта квазисреда возникает, когда люди игнорируют факты, и правда уже не играет существенной роли, уступая место популистской риторике. И хотя манипулирование массовым и индивидуальным сознанием не является чем-то новым в политической практике, новизна текущей ситуации заключается в том, что переполненность средств массовой информации и социальных сетей сфальсифицированными фактами превысила критический порог, что привело к появлению качественно нового феномена – искривленного информационного пространства.

Данные обстоятельства не могут не вызывать глубокую озабоченность в свете продвигаемых отдельными государствами попыток на международном уровне утвердить примат концепции неизбежного возникновения конфликтов в информационном пространстве. В стратегических документах ряда западных стран все более важная роль отводится нетрадиционным инструментам достижения военно-политических целей в информационной сфере и в том числе киберпространстве. Одновременно информационное противоборство в интернете (особенно в социальных сетях) все активнее практикуется государствами, их

прокси-силами, а также другими негосударственными акторами мировой политики.

В этом контексте **субъекты информационно-психологического воздействия, безусловно, учитывают, что современная информационно-коммуникационная реальность обладает большим аддитивным потенциалом**, то есть, значительным риском возникновения зависимости. Соответственно, важно рассмотреть и такое последствие цифровизации общественной жизни, как влияние современных информационно-коммуникационных технологий на психику личности. Данная проблема находится в фокусе внимания западных специалистов в связи с резким увеличением количества людей, зависимых от средств виртуального общения, но макросоциальные последствия этих процессов пока изучены недостаточно.

Прежде всего следует отметить, что широкие возможности интернет-пространства позволяют практически без ограничения доступа людей к информации и общению нивелировать статусные и нормативные барьеры, регламентирующие социальное поведение. Отсутствие преград в условиях цифровой среды облегчает для людей удовлетворение ряда потребностей[362].

В общепринятой иерархии, предложенной американским ученым А. Маслоу, потребности личности подразделяются на пять уровней: 1. Физиологические потребности – потребности в пище, сне, сексуальные и пр. 2. Потребности в безопасности – стабильности, защите, свободе от страха, тревоги и пр. 3. Потребности в любви и социальной принадлежности – семье, дружбе, референтной группе и пр. 4. Потребности в уважении и одобрении – признании, престиже, славе, поддержании статуса и пр. 5. Потребности в самоактуализации – развитии собственных способностей. Это нередко приводит к дисфункциям психического развития, в особенности интернет-зависимости (интернет-аддикции).

Интернет-аддикция определяется специалистами как непреодолимая тяга к использованию ресурсов глобальной сети. Проблема патологической зависимости

[362] См.: *Маслоу А.* Мотивация и личность. Санкт-Петербург: Евразия, 1999. 478 с.

возникает, когда стремление ухода в виртуальный мир начинает доминировать в сознании личности и в итоге приводит к отрыву от реальности[363]. К наиболее опасным проявлениям интернет-аддикции эксперты причисляют непреодолимое влечение к общению онлайн (участие в чатах, веб-форумах, большие объёмы переписки, новые знакомства); к посещению сайтов порнографического содержания (киберсексуальная зависимость); к поиску информации по новостным сайтам и в базах данных (информационная перегрузка); к покупкам в интернет-магазинах и участию в интернет-аукционах (онлайн-консьюмеризм); к компьютерным играм онлайн (игровая зависимость)[364].

Ученые не признают интернет-аддикцию в широком плане психическим расстройством – она рассматривается в качестве социальной девиации. Лишь в июне 2018 г. Всемирная организация здравоохранения включила отдельные ее проявления – зависимость от видео-игр и зависимость от азартных игр онлайн – в Международную классификацию болезней (МКБ-11). Документ запланирован к вводу в действие 1 января 2022 г., однако дискуссии специалистов о том, является ли игровая зависимость отдельным психическим синдромом или ее следует рассматривать в качестве симптома подлежащих проблем, таких как депрессия или синдром дефицита внимания и гиперактивности, продолжаются. В частности, наиболее авторитетная среди профильных специалистов Американская психиатрическая ассоциация (*American Psychiatric Association*) не признает игровое расстройство болезнью[365].

Игровой зависимости (в том числе азартным играм онлайн, где более рельефно выступает система вознаграждений) чаще подвержены мужчины, которым больше чем женщинам присуща нацеленность на успех. Социологи связывают их непреодолимое игровое влечение со стремлением компенсировать

---

[363] См.: The growing threat of internet addiction // European Science-Media Hub. 2019. January 9. URL: https://epthinktank.eu/2019/03/19/does-technology-exacerbate-social-polarisation/ (дата обращения: 22.07.2019).

[364] См. напр.: *Fischoff Stuart.* Media Psychology: A Personal Essay in Definition and Purview // Division 46. URL: https://www.apadivisions.org/division-46/about/fischoff-media-psychology.pdf (дата обращения: 22.07.2019).

[365] Internet Gaming // American Psychiatric Association. 2018. June. URL: https://www.psychiatry.org/patients-families/internet-gaming (дата обращения: 24.07.2019).

нереализованные в реальной жизни потребности в виртуальной среде. Это обусловлено исполнением традиционно мужских функций противоположным полом ввиду перераспределения социально-демографической структуры обществ в развитых странах, в том числе по гендерному, возрастному, этническому и прочим признакам.

В свою очередь, женщины, согласно статистике, более подвержены общению онлайн и конструированию собственной сетевой (виртуальной) идентичности. Под сетевой идентичностью понимаются компоненты облика личности, формируемого ей в рамках интернет-среды с целью самопрезентации[366]. По сути, сетевая идентичность – это проект личности, творчески раскрываемый ею в рамках возможностей интерфейса используемой онлайн-платформы, среди которых наиболее распространенными считаются социальные сети.

Специалисты указывают, что несоответствие реального и виртуального облика является причиной неадекватного самовосприятия женщин и провоцирует у них серьезные психические расстройства. В частности, исследование, проведенное в израильском Хайфском университете (*University of Haifa*), свидетельствует о том, что чем больше времени девушки подросткового возраста находятся в социальной сети, тем скорее у них развиваются синдромы расстройства приема пищи и неприятия своего образа тела[367]. Подобные результаты были получены в ходе эксперимента, состоявшегося в Университете штата Флорида (*University of Florida*), когда после проведения примерно двадцати минут в социальной сети экспериментуемые начинали беспокоиться о лишнем весе[368].

---

[366] См.: *Luskin Bernard J.* Defining and Describing Media Psychology // Psychology Today. 2012. November 30. URL: https://www.psychologytoday.com/intl/blog/the-media-psychology-effect/201211/defining-and-describing-media-psychology (дата обращения: 22.07.2019).

[367] Цит.по.: Facebook users more prone to developing eating disorders, study finds // ScienceDaily. 2011. February 7. URL: https://www.sciencedaily.com/releases/2011/02/110207091754.htm (дата обращения: 24.07.2019).

[368] Цит.по.: *Wilson June.* The Disillusionment with Social Media // The Amplifier. 2018. December 18. URL: https://div46amplifier.com/2018/12/18/the-disillusionment-with-social-media/ (дата обращения: 22.07.2019).

Нередко за рубежом публикуются исследования, свидетельствующие о позитивном влиянии сетевых технологий на психическое здоровье личности. В одном из таковых американские ученые констатируют, что пользование интернетом улучшает деятельность мозга у людей зрелого и пожилого возраста благодаря стимуляции центров, ответственных за принятие решений, а также контролирующих память, речь, зрение (якобы при чтении книг подобной активации соответствующих областей мозга не происходит). В свою очередь, австралийские специалисты утверждают, что общение в социальных сетях (исследование проводилось в сети «Фейсбук») способствует формированию у индивида чувства социальной связанности, позволяющего снизить риски депрессии и беспокойства. Критики подобных публикаций апеллируют в основном к их слабой доказательной базе[369].

Важным позитивным аспектом, связанным с развитием современных информационно-коммуникационных технологий, является их применение психологами и психотерапевтами. Эксперты Американской психологической ассоциации (*American Psychological Association*) считают подобные практики весьма эффективными ввиду возможности наблюдать поведение личности в виртуальном мире, которое зачастую отличается от ее поведения на медицинском приеме или в условиях стационара. Они также отмечают, что массив данных, присутствующий в цифровой среде, нередко позволяет сформировать более объективную характеристику личности по сравнению с информацией, которая предоставляется специалисту или в медицинское учреждение[370].

Однако нередко в цифровом мире личность создает желаемую виртуальную идентичность, существенно отличающуюся от реальной. В частности, исследование ученых Хельсинкского университета (*University of Helsinki*) свидетельствует об изменении онлайн поведения индивидов, вне интернета

---

[369] См. напр.: *Savastio Rebecca.* Facebook Causes Depression New Study Says // Guardian Liberty Voice. 2019. August 15. URL: https://guardianlv.com/2013/08/facebook-causes-depression-new-study-says/#PzRdcP38KPwjLoxo.9 (дата обращения: 22.07.2019).

[370] *Clay Rebecca A.* Moving assessment out of the clinic // American Psychological Association. 2019. July/August. URL: https://www.apa.org/monitor/2019/07-08/moving-assessment (дата обращения: 22.07.2019).

склонных к садизму. В ходе серии экспериментов выяснилось, что в социальных сетях они стремятся придерживаться поведения, положительно оцениваемого с точки зрения общественных и моральных норм[371].

В целом аналитики сходятся во мнении, что свобода интернета в ее нынешнем виде все чаще имеет негативные, а не позитивные для человека последствия[372]. За счет определения социально-психологических особенностей пользователей сети, которые они сами же афишируют на своих страницах в социальных сетях, руководствуясь удовлетворением акцентированных потребностей (потребность в идентификации; потребности в поддержании и повышении социального статуса и самооценки; потребность в успехе и пр.), в зоне особого риска оказываются дети и подростки, социальные установки которых лабильны ввиду несформированной или неустойчивой психики и отсутствия навыков самоконтроля[373].

С учетом вышесказанного во многих странах мира все чаще поднимается вопрос об ограничении пользования интернетом. В частности, на слушаниях в Палате представителей Конгресса США в феврале 2019 г. указывалось на целесообразность сохранения полностью открытого интернет-пространства только для целей потребления, ведения малого бизнеса и выражения свободы слова[374]. Рассматриваемая проблема активно обсуждается и в европейских государствах[375], но в целом в странах западного мира подобные дискуссии пока остаются вне правового поля.

---

[371] См.: *Suna P. Kinnunen, Marjaana Lindeman, Markku Verkasalo.* Help-giving and moral courage on the Internet // Journal of Psychosocial Research on Cyberspace. 2016. URL: https://cyberpsychology.eu/article/view/6279/5890 (дата обращения: 24.07.2019).

[372] См. напр.: Apple CEO to MIT grads: Tech without values is worthless // APNews. 2017. URL: https://www.apnews.com/466cbd4f2aaa4791bad6404dc92aab36 (дата обращения: 22.07.2019).

[373] См.: Does technology exacerbate social polarisation? // EPRS. 2019. March 19. URL: https://epthinktank.eu/2019/03/19/does-technology-exacerbate-social-polarisation/ (дата обращения: 22.07.2019).

[374] Цит. по: *Wheeler Tom.* Preserving an open internet for consumers, small businesses, and free speech // Brookings Institution. 2019. February 7. URL: https://www.brookings.edu/testimonies/preserving-an-open-internet-for-consumers-small-businesses-and-free-speech/ (дата обращения: 22.07.2019).

[375] См. напр.: Harmful internet use. Part 1, Part 2 // European Parliament. 2019. January. URL: http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624269/EPRS_STU(2019)624269_EN.pd

Вместе с тем в ноябре 2019 г. Государственное управление по делам печати и издательства КНР обнародовало документ, направленный на предотвращение формирования у несовершеннолетних пользователей интернета зависимости от современных информационно-коммуникационных технологий. Согласно концепции китайских законодателей, устанавливается общая ответственность провайдеров онлайн-игр, а также правительственных учреждений и общественности за совместный контроль над использованием интернет-ресурсов несовершеннолетними гражданами Китая. С этой целью всем пользователям глобальной сети предписывается в обязательном порядке зарегистрироваться, представив идентификационную информацию, а ответственность за исполнение этого требования несут государственные органы. Кроме того, вводится полный запрет на предоставление в интернете платных услуг детям в возрасте до восьми лет; детям до 16 лет разрешается израсходовать в течение месяца на внутриигровые покупки не более 28 долларов, а подросткам от 16 до 18 лет – не более 57 долларов. При этом лицам, не достигшим 18 лет, разрешено играть в сетевые проекты не более 90 минут в будний день и не более трёх часов в праздничные дни и выходные дни, а также им запрещено играть в онлайн-игры в ночное время (с десяти вечера до 8 утра)[376].

Можно предположить, что в перспективе внимание специалистов к рассматриваемому вопросу еще более возрастет ввиду динамичного развития информационно-коммуникационных технологий и, соответственно, их усиливающегося влияния на психическое развитие личности и социальное поведение в целом.

Соответственно, на современном этапе, сопровождающемся динамичным развитием новых практик информационного противоборства с применением инструментария цифровых технологий, на первый план для многих государств

---

f; http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624249/EPRS_STU(2019)624249_EN.pdf (дата обращения: 22.07.2019).

[376] См.: 90 Minutes a Day, Until 10 P.M.: China Sets Rules for Young Gamers // The New York Times. 2019. November 6. URL: https://www.nytimes.com/2019/11/06/business/china-video-game-ban-young.html (дата обращения: 08.11.2019).

выходит необходимость консолидации усилий органов государственной власти, средств массовой информации и неправительственных организаций для анализа существующих и вероятных социально-политических рисков. Не меньшее значение в этом плане имеет и разработка механизмов межгосударственного диалога по реагированию на современные и перспективные угрозы безопасности личности, обществу и государству в информационной сфере. При отсутствии таковых ускорится тенденция подрыва эффективности механизмов, сдерживающих применение силы, при одновременном повышении вероятности ее использования нетрадиционными методами. Сохранение и наращивание указанного тренда может спровоцировать ослабление самого каркаса миросистемы, и в конечном итоге разбалансировать ее устойчивость, причем такая опасность многократно возрастает ввиду того обстоятельства, что международно-правовые рамки в этой сфере формируются с заметным отставанием.

К настоящему времени многие аспекты процессы информационного протввоборства в системе международного права все еще остаются неурегулированными, в частности статус кибервойн. Но постепенно в зарубежном и отечественном экспертном сообществе утверждается согласие в вопросе о необходимости разработки юридически обязывающих норм и стандартов деятельности в информационной сфере.

Наиболее рельефно эта проблема проявилась в 2020 г, когда человечество столкнулось с распространением коронавируса нового типа. В этот период во многих странах мира существенно увеличились масштабы кибернетических атак. В частности, на рост киберпреступности указывается в опубликованном в августе 2020 г. отчете Интерпола, посвященном влиянию пандемии коронавируса на сферу кибербезопасности. Согласно документу, среди целей атак стало существенно больше государственных учреждений, объектов критически важной инфраструктуры, крупных корпораций. Участились случаи мошенничества с применением современных информационно-коммуникационных технологий в

области онлайн-продаж, прежде всего торговли медицинскими товарами, лекарствами, средствами индивидуальной защиты[377].

Количество кибератак на образовательные ресурсы с февраля 2020 г. возросло в среднем на 450 % по сравнению с аналогичным периодом прошлого года. Среди угроз следует отметить увеличение количества поддельных страниц и рассылок зараженных писем. Злоумышленники маскируются под популярные образовательные ресурсы: *Moodle, LNS, Blackboard, Zoom, Coursera* и пр. Эксперты выражают беспокойство в связи с тем, что образовательная индустрия не успевает адаптироваться к новым вызовам и обеспечить должный уровень информационной безопасности. Более того, изменение самой архитектуры кибернетических угроз, усугубленное пандемией коронавируса, создает дополнительную нагрузку на правоохранительные органы многих стран мира, при том, что количество атак растет весьма быстрыми темпами[378].

Гибридизация конфликтов порождает многие дополнительные проблемы этического и юридического характера. Авторитетные военные аналитики отмечают, что важными обстоятельствами любого политического и тем более вооруженного конфликта являются вопросы неприкосновенности государственных границ, соблюдения межгосударственных соглашений и международного законодательства в целом, а также последствий за нарушение таковых. Все это напрямую относится к цифровой сфере, поскольку кибератаки могут вызывать такие же физические разрушения, как оружие и боевая техника. Поэтому, с точки зрения ученых, действия в кибернетическом пространстве должны регламентироваться соответствующими договорами и стандартами по аналогии с Женевскими конвенциями. Пока международному сообществу не

---

[377] *Wright Thomas.* Stretching the international order to its breaking point // The Brookings Institution. 2020. April 6. URL: https://www.brookings.edu/blog/order-from-chaos/2020/04/06/stretching-the-international-order-to-its-breaking-point/?utm_campaign=Brookings%20Brief&utm_source=hs_email&utm_medium=email&utm_content=85914360 (дата обращения: 14.11.2020).

[378] *Newbury Charlotte. The* coronavirus ‘infodemic’: truth and conspiracy online // Public Technology. 2020. September 15.URL: https://www.publictechnology.net/articles/features/coronavirus-‘infodemic’-truth-and-conspiracy-online (дата обращения: 13.11.2020).

удалось выработать таковых, поскольку принятая в 2001 г. Будапештская конвенция не отвечает современным политическим реалиям.

Вместе с тем эксперты указывают на то, то при разработке норм и стандартов деятельности в указанной сфере следует принимать во внимание и присутствующие различия между традиционными военными действиями с применением кинетического оружия и кибернетическими операциями. По оценкам некоторых специалистов, в случае осуществления кибератак, вызывающих существенный физический ущерб, должны применяться нормы международного гуманитарного права и соглашений о правилах ведения вооруженных конфликтов. Когда же сетевые операции нарушают работу учреждений и уничтожают базы данных, то подобная деятельность попадает в зону правовой неопределенности. Кроме того, в традиционных боевых действиях есть разница между военными и гражданскими инфраструктурами, тогда как в кибервойне обе указанные составляющие используют одинаковые системы и технологии[379].

Современные тренды цифровизации свидетельствуют о том, что новая социально-политическая и экономическая реальность станет оформляться в самое ближайшее время в том числе с активным использованием цифровых технологий в информационном противоборстве, что в итоге может спровоцировать полномасштабную ломку нынешнего формата политического устройства мира.

По некоторым оценкам, **форсированное развитие не регламентированных международным правом цифровых технологий (например, искусственного интеллекта и сферы кибербезопасности) и применение их в практике информационного противоборства способно стать одной из главных причин формирования новых межгосударственных объединений и союзов, стимулируя развитие отдельных макрорегионов.** Не исключено, что каждый из таких кластеров станет развиваться на основании технологических разработок собственных научных школ и будет стремиться стать

[379] *Trendall Sam.* The fog of cyberwar // Public Technology. 2020. July. URL: https://www.publictechnology.net/articles/features/fog-cyberwar (дата обращения: 13.11.2020).

самодостаточным политическим и социально-экономическим образованием, особенно в условиях турбулентности, заданной пандемией COVID-19.

В пользу этого свидетельствует, как минимум, то, что в настоящий момент уже формируются первые международные объединения по линии развития искусственного интеллекта и кибербезопасности. Так, 15 июля 2020 г. увидело свет совместное заявление членов-основателей Глобального партнерства по искусственному интеллекту. В данную организацию вошли Австралия, Канада, Франция, Германия, Индия, Италия, Япония, Мексика, Новая Зеландия, Республика Корея, Сингапур, Словения, Великобритания и Соединенные Штаты Америки[380]. В сентябре 2020 г. Соединенные Штаты Америки и Великобритания подписали первую совместную Декларацию о сотрудничестве в области исследований и разработок в области искусственного интеллекта[381]. Согласно Стратегии развития искусственного интеллекта Германии, опубликованной в ноябре 2018 г., одной из главных задач Германии является комплексное сотрудничество с Францией в данной сфере научно-технического прогресса[382]. В декабре 2019 г. было озвучено обоюдное согласие Турции и Ирана сотрудничать в сфере развития ИИ[383]. В октябре 2020 г. Национальный центр искусственного интеллекта Саудовской Аравии (*NCAI*) объявил о подписании меморандума о взаимопонимании с китайской компанией «Хуавей» для обеспечения

---

[380] Guidance. Joint statement from founding members of the Global Partnership on Artificial Intelligence // GOV. UK. 2020. June. URL: https://www.gov.uk/government/publications/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence (дата обращения: 18.11.2020).

[381] Guidance. Declaration of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Artificial Intelligence Research and Development // GOV.UK. 2020. September 25. URL: https://www.gov.uk/government/publications/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-ai-research-and-development/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-artificial-intelligence-re (дата обращения: 13.11.2020).

[382] Strategie Künstliche Intelligenz der Bundesregierung // 2018. November. URL: https://www.bmbf.de/files/Nationale_KI-Strategie.pdf (дата обращения: 18.11.2020).

[383] Iran, Turkey to cooperate on artificial intelligence // IranPress. 2020. December. URL: https://iranpress.com/content/16886 (дата обращения: 18.11.2020).

стратегического сотрудничества в рамках Королевской национальной программы развития возможностей искусственного интеллекта[384].

Скорее всего, существующие в настоящий момент противоречия между крупными мировыми державами, форсированные пандемией нового коронавируса, в обозримом будущем лишь усугубятся вследствие ослабления традиционного гегемона (США) и возвышения Китая и, наконец, увеличения количества полюсов силы в принципе. По оценкам отдельных экспертов, стремление множества государств достичь лидерства в сфере ИИ и наращивание технологической конкуренции в деле создания новейших систем кибервооружений в совокупности с подобными процессами в иных научно-технических сферах, относящихся к шестому технологическому укладу, могут привести к конфликту глобального масштаба между различными по значимости и силе державами.

Тким образом, динамика процессов в технологической сфере ставит под вопрос возможность сохранения прежних моделей в мировой экономике и политике. Анализ взаимовлияния искусственного интеллекта и процессов, протекающих в кибернетическом пространстве, равно как и других связок информационного противоборства в политическом процессе важен для построения прогнозов развития международных отношений, теоретических моделей взаимоотношений различных центров силы. Достижение точности подобных прогнозов является высокоактуальной задачей в свете выстраивания новой модели мирового порядка на фоне заката мировой гегемонии США и планомерного восхождения Китая, при сохранении перспективы разделения мира на технологические макрорегионы.

Изучая основные направления информационного противоборства в политическом процессе ведущими странами Запада и возможности России в развитии соответствующих технологий, следует отметить, что у нашей страны,

---

[384] GlobalData Energy. Saudi Arabia signs artificial intelligence agreements // **Power Technology.** 2020. November 5. URL: https://www.power-technology.com/comment/saudi-arabia-signs-artificial-intelligence-agreements/ (дата обращения: 18.11.2020).

несомненно, присутствует потенциал, благодаря которому сохраняется возможность достижения определенных успехов в данном направлении. Так, целесообразно было бы учитывать, что по своему географическому положению Российская Федерация объективно является центром интеграционных процессов евразийского пространства, где информационная инфраструктура, которая, по всей видимости, станет основой шестого технологического уклада, еще только формируется. При выстраивании взаимовыгодного диалога с региональными державами (прежде всего Китаем) в перспективе РФ, обладая передовыми технологиями в некоторых областях (ВПК, атомная промышленность), вполне могла бы стать своего рода центровой державой евразийского пространства. Но для этого следовало бы, как минимум, проявлять большую активность в демонстрации государствам региона привлекательной информационно-коммуникационной модели развития цифровой среды, в том числе технологий, программно-аппаратных решений, правовых стандартов обеспечения кибербезопасности и пр. Вероятно, такую работу можно было бы усилить в рамках ШОС и БРИКС.

В целом с учетом появления новых, все более острых вызовов и угроз безопасности государства, обусловленных форсированным развитием и мимикрией информационно-коммуникационных технологий, для России возрастает потребность в перманентном совершенствовании системы обеспечения информационной безопасности страны, способной оперативно и эффективно реагировать на риски, порожденные цифровой реальностью, равно как и использовать ее преимущества.

4.2. Трансформация облика военных конфликтов будущего

Раскрытие потенциала цифровых технологий в целях ведения информационного противоборства, ведущегося вне пространственных и временных границ, ломает шаблонные схемы, присущие прежде политической динамике. Чрезвычайно быстро нарастает процесс политизации виртуального измерения. В решении политических проблем не остается «полутонов»,

поскольку виртуальная среда стала пространством для ведения информационных опреаций в мирное и военное время.

В условиях цифровизации социально-политической жизни и резким прогрессом в совершенствовании современных систем вооружений, усиливается тенденция ведения военнных конфликтов вкупе с политическими, экономическими и информационно-психологическими средствами воздействия на противника.

С учетом сказанного сегодня политики и военные указывают на изменение соотношения вкладов военных и невоенных способов противоборства в общий политический результат войны. По некоторым оценкам, такое соотношение составляет 1:4 в пользу не военных способов. Соответственно, **действенным способом предотвращения перетекания военных конфликтов в «горячую фазу» стало «размывание» их границ, то есть использование гибридного (смешанного) подхода к ведению противоборства.** Это обстоятельство является одним из важных факторов развития политических процессов – в России и в мире в целом[385].

Американские специалисты дают определение гибридной войны как военного конфликта, сочетающего регулярные («симметричные») боевые действия с элементами асимметричных войн. Например, военный теоретик Дж. МакКуен определяет гибридную войну как «комбинацию симметричной и асимметричной войн», однако при таком определении «все войны – потенциально гибридные»[386].

С свою очередь, исследователь Ф. Хоффман предлагает уточнение: в гибридных войнах асимметричная компонента имеет решающее оперативное значение на поле боя, в отличие от обычных войн, где роль асимметричных

---

[385] См. напр.: *Fleming, Brian P.* Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies (SAMS), U.S. Army Command & General Staff College, 2011.

[386] *McCuen, John J.* Hybrid wars // Military Review. 2008. URL: https://www.questia.com/library/journal/1P3-1458719761/hybrid-wars (дата обращения: 24.08.2019).

игроков (например, партизан) состоит в отвлечении сил противника на поддержание безопасности вдали от поля боя[387].

При этом западные и отечественные эксперты сходятся во мнении, что суть гибридизации военных конфликтов заключается в задействовании регулярных и иррегулярных силовых элементов при доминировании последних с конечной целью подрыва власти легитимного правительства зарубежной страны. Угрожающая актуальность такого конфликта в политических реалиях, характеризующихся хрупкостью в условиях форсированных процессов цифровизации, превращает гибридную войну в политическую реальность и форму протекания межгосударственного противоборства[388].

Специалисты в области информационного противоборства указывают на высокую вероятность гибридизации военных конфликтов будущего. Так, в докладе британского Минобороны «Глобальные стратегические тренды: будущее начинается сегодня», опубликованном в конце 2018 г., констатируется, что в среднесрочной перспективе использование дезинформации и пропаганды в средствах массовой информации и социальных сетях станет главной особенностью ведения гибридных войн. Такие методы противоборства будут, по оценкам англичан, все более активно применяться государствами и их коалициями (в том числе прокси силами), а также негосударственными акторами (частными военными компаниями, террористическими группировками и пр.), чему поспособствуют отсутствие физических границ в информационно-коммуникационном пространстве и недостаточная международно-правовая регламентация протекающих там процессов[389].

С учетом сказанного следует отметить, что в настоящее время новые импульсы приобретает международное измерение гибридных угроз.

---

[387] *Hoffman F.* Future Warfare: The Rise of Hybrid Warfare // U.S. Naval Institute. 2005. URL: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf (дата обращения: 23.09.2019).

[388] См. напр.: *Fleming, Brian P.* The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art. — Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies (SAMS), U.S. Army Command & General Staff College, 2011.

[389] Global Strategic Trends: The Future Starts Today // GOV.UK. 2018. 2 October. URL: https://www.gov.uk/government/publications/global-strategic-trends (дата обращения: 30.09.2019).

Показательной в этом контексте является состоявшаяся в Вене 19-20 сентября 2018 г. по инициативе ОБСЕ панельная дискуссия по теме «Понимание гибридных угроз и их влияние на пространстве ОБСЕ» с участием экспертов из России, Италии, Норвегии, Голландии и Бельгии. Участники пришли к выводу о необходимости развертывания широкой международной дискуссию по вопросам гибридных войн и угроз с выходом в перспективе на совместное понимание этих феноменов и формирование соответствующей нормативно-юридической базы, однако предшествующим процессом должна стать выработка на национальном уровне понятийного аппарата, отражающего особенности новых вызовов и угроз современности[390].

Данный вопрос затрагивается в недавней совместной статье бывшего генерального секретаря НАТО А. ф. Расмуссена и экс-министра внутренней безопасности США М. Чертоффа. По оценкам этих влиятельных политиков, союзники по обеим сторонам Атлантики постоянно совершенствуют технологии информационно-психологического воздействия на массовое сознание, и внастоящее время к ним целесообразно причислять «таргетирование информации, использование интернет-профилей пользователей, фэйковые новости, обращение к лидерам общественного мнения для тиражирования этих новостей и пр». В качестве характеристики всего спектра технологий гибридной войны, реализуемых в условиях цифровой реальности, предлагается термин «гипертенденциозный контент» *(hyper-partisancontent)*[391].

Большое внимание теме гибридных угроз уделяется в Североатлантическом союзе. В настоящее время в НАТО создана сеть центров передового опыта по обобщению данных о гибридных угрозах и тактиках противоборствующих сторон:

---

[390] См. подр.: *Бартош А.А.* ОБСЕ занялась гибридными угрозами // НВО. 2018. Сентябрь. URL: http://nvo.ng.ru/realty/2018-09-28/3_1015_osce.html (дата обращения: 26.08.2019).

[391] *Rasmussen A., Chertoff M.* The West Still Isn't Prepared to Stop Russia Meddling in Our Elections // Politico. 2018. June 05. URL: https://www.politico.com/magazine/story/2018/06/05/russia-election-meddling-prepared-218594 (дата обращения: 01.09.2019).

– Центр передового опыта НАТО в Латвии (Рига) в области стратегической коммуникации, который занимается вопросами информационной войны;

– Центр кибероперациий при штабе Объединенных вооруженных сил НАТО в Бельгии (Монс) вовлечен в разработку теории и практики действий в киберсреде;

– совместно с Центром кибероперациий действует Центр передового опыта НАТО по кибероборонев Эстонии (Таллин);

– Центр по противодействию гибридным угрозам в Финляндии (Хельсинки);

– Центр передового опыта НАТО по противодействию терроризму открыт в Турции (Анкара);

Кроме прочего, в НАТО созданы так называемые рабочие группы по борьбе с гибридными угрозами, которые функционируют при штаб-квартире альянса. Об их важности свидетельствует,например, то что на 2018–2020 гг. бюджет только рабочей группы по стратегическим коммуникациям Североатлантического союза (*StratCom Task Force*) составил 1,1 млн евро[392].

Большое значение в НАТО придается Европейскому центру передового опыта в области противодействия гибридным угрозам, официальное открытие которого состоялось в начале октября 2017 г. в Хельсинки (Финляндия). Данный центр взаимодействует с тремя натовскими Центрами передового опыта в столицах прибалтийских республик и недавно созданным Центром военного планирования и управления зарубежными небоевыми миссиями Евросоюза (Брюссель)[393].

Особенность Европейского центра передового опыта в области противодействия гибридным угрозам состоит в том, что он является первой подобного рода совместной структурой НАТО и Европейского союза, призванной

---

[392] См.: Countering Hybrid Warfare Project: Understanding Hybrid Warfare // GOV.UK. 2017. September. URL: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare (дата обращения: 20.09.2019).

[393] См.: New report: actors manipulating the online conversation are changing tactics // NATO. 2018. February 19. URL: https://www.stratcomcoe.org/new-report-actors-manipulating-online-conversation-are-changing-tactics (дата обращения: 05.09.2019).

синхронизировать усилия этих политических акторов. Его создание должно способствовать переводу в практическую плоскость положений Совместной декларации о сотрудничестве ЕС и НАТО, являющейся одним из важнейших итоговых документов натовского саммита в Варшаве (июль 2016 г.).

В целом следует резюмировать, что накопленные к настоящему времени объединенные ресурсы странНАТО позволяют мировому гегемону в лице США усиливать информационно-психологическое давление на неугодные политические режимы и одновременно «рекомендовать» стандарты поведения в информационно-коммуникационной сфере зарубежным странам. Например, как отметил на церемонии открытия хельсинского Центра тогдашний глава МИД Финляндии Т. Сойни, в Балтийском регионе НАТО и ЕС должны будут отработать «модели действий по противодействию исходящим от России гибридным угрозам, применимые также в других районах (в Средиземноморье и на Черном море)»[394].

Соответствующие сценарии были рассмотрены в недавнем докладе аналитического центра США «Корпорации РЭНД» под названием «Гибридная война в странах Балтии. Опасности и потенциальные ответы»[395]. В нем американские аналитики указывают, что главная угроза странам Балтии со стороны России будет носить конвенциональный характер (в связи с чем рекомендовано наращивание возможностей НАТО в регионе в интересах обычного сдерживания). Вместе с тем говорится о необходимости выработки комплексного подхода, сочетающего наступательные и оборонительные элементы, к выработке стратегии противодействия нашей стране в сфере информационной безопасности.

В указанном докладе американские эксперты придают ведущее значение конвенциональной угрозе, по их мнению, методы Москвы будут «более утонченными в стремлении оказать воздействие, которое будет достаточно

---

[394] EU and NATO welcome Hybrid CoE // Hybrid CoE. 2017. September 1. URL: https://www.hybridcoe.fi/news/eu-and-nato-welcome-hybrid-coe/ (дата обращения: 21.12.2017).

[395] Hybrid Warfare in the Baltics // RAND. 2017. URL: https://www.rand.org/pubs/research_reports/RR1577.html (дата обращения: 20.05.2019).

сильным, но не настолько, чтобы в действие была введена ст. 5 Вашингтонского договора (в частности, поддержка оппозиционных политических движений, ориентированная на этнические меньшинства пропаганда, ограничение подачи энергоносителей и т.д.)»[396].

Между тем в соответствии с решениями, принятыми еще в декабре 2015 г. на сессии Совета НАТО в формате министров иностранных дел, считается возможным задействование Сил реагирования альянса в ответ на гибридные угрозы. Однако их развертывание возможно только после принятия соответствующего политического решения (хотя главком Объединенных вооруженных сил НАТО в Европе может начинать соответствующие подготовительные мероприятия). По оценкам натовских чиновников, на сегодняшний день четкие критерии, на основании которых можно было принимать подобные решения, не разработаны. В связи с этим не случайно создание нового Управления разведки НАТО, функционал которого в плане противодействия гибридным угрозам планируется уточнить в 2021 г.

На последних сессиях Совета НАТО в формате министров обороны уже традиционно затрагивается проблема соответствия организационной структуры альянса условиям ведения гибридных войн. Важную роль в противодействии гибридным угрозам руководство Североатлантического союза отводит возможностям в сфере кибербезопасности. Еще с 2014 г. кибероборона признается составной частью коллективной обороны Североатлантического союза (признается, что к этой сфере применима ст. 5 Вашингтонского договора). Однако вопрос о выработке критериев, на основании которых Совет НАТО может принять данное решение, остается открытым.

Итоговыми документами Варшавского саммита 2016 г. подобная формулировка закреплена и в отношении гибридных угроз: возможность задействования механизмов коллективной обороны в ответ на «гибридную агрессию» не исключается. Кроме того, в соответствии с принятыми на саммите в

[396] Hybrid Warfare in the Baltics // RAND. 2017. URL: https://www.rand.org/pubs/research_reports/RR1577.html (дата обращения: 20.05.2019).

Варшаве «Обязательствами по обеспечению кибернетической обороны» предусматривается: обеспечение необходимого финансирования профильных программ; развитие взаимодействия между национальными структурами, задействованными в сфере информационных технологий; активизация обмена данными о соответствующих угрозах; отработка вопросов кибернетической обороны в ходе мероприятий оперативной и боевой подготовки. При этом киберпространство объявлено новой операционной военной сферой, а вопросы противодействия кибернетическим угрозам включены в рутинный процесс оперативного планирования Североатлантического союза. Таким образом, проблема переведена из области теоретических построений в практическую плоскость и становится частью четкого институционального процесса.

Следует подчеркнуть, что обеспечение устойчивости и формирование действенного потенциала в сфере кибербезопасности рассматриваются руководством альянса в качестве важнейших составляющих модели сдерживания недопущением/разубеждением *(deterrence by denial)*. В последние годы данная модель активно апробируется НАТО в странах, соседствующих с нашей страной, в частности в Балтийском регионе.

С точки зрения противодействия гибридным угрозам большое значение придается наращиванию возможностей гражданского сектора: обеспечению непрерывного функционирования органов государственного управления и бесперебойной работы важнейших национальных служб; повышению безопасности критически важных объектов инфраструктуры; оказанию эффективной поддержки вооруженных сил со стороны гражданских структур в сферах энергетики, транспорта и связи. Целый ряд докладов, подготовленных в 2015–2019 гг. западными аналитическими центрами, специально посвящен проблеме обеспечения устойчивости (боевой, а также связанной с защищенностью жизненно важных систем государства – социальной, политической, экономической и технологической) (*resilience; forward resilience*).

В феврале 2017 г. Центр передового опыта НАТО по кибероборонe в Эстонии выпустил переработанную версию «Руководства по международному

праву, применимому к ведению военных действий в киберпространстве» («Таллинское руководство»), опубликованную впервые в 2013 г. Обновление документа проходило под руководством координатора Государственного департамента по кибервопросам Кристофера Пэйнтера[397].

В обновленном «Таллинском руководстве» отмечается, что кибератаки должны использоваться против конкретных целей и объектов; «веерные атаки» должны быть под запретом. Государства имеют право применять различные контрмеры против незаконных кибероперациий. Контрмеры могут быть признаны незаконными, но только не в случае ответных действий. В целом документ закрепляет право альянса на начало боевых действий при обнаружении киберугрозы или в ответ на атаку с использованием цифровых технологий.

Примечательным выглядит также консолидация в сфере борьбы гибридными угрозами внутри Евросоюза. Об этом, например, свидетельствует то, что сентябре 2017 г. на саммите по цифровым технологиям президент Литвы Д. Грибаускайте выступила с инициативой «кибернетического Шенгена» – создания в рамках ЕС сил быстрого реагирования на кибернетические атаки. По ее мнению, данная структура будет дополнять НАТО в борьбе с гибридными угрозами, терроризмом и в помощи третьим странам. Уже в декабре участники европейской программы Постоянного структурированного сотрудничества в области обороны и безопасности одобрили оказание взаимопомощи для обеспечения кибернетической безопасности и создание кибер-группы быстрого реагирования, включив эту инициативу в число 17 утвержденных проектов. Как отмечают европейцы, создание таких сил выведет взаимодействие государств ЕС в кибернетической сфере на новый уровень, когда страны-участницы не станут ограничиваться национальным форматом[309].

Приведенные положения позволяют выдвинуть гипотезу, что **в среднесрочной перспективе знаковой чертов процессов информационного**

---

[397] См.: *Leetaru Kalev.* What Tallinn Manual 2.0 teaches us about the new cyber order // Forbes. 2017. June. URL: https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/ (дата обращения: 20.08.2019).

противоборства, скорее всего, станет повышение уровня конфликтности в киберпространстве. По мнению ведущих отечественных и зарубежных военных политологов, это способно в корне измененить процесс протекания военных конфликтов, причем уже в обозримом будущем[398]. Текущие тенденции трансформации облика военных конфликтов подводят экспертов к выводу, что в перспективе границы между состоянием войны и мира станут более размытыми[399].

В конце 2018 г. в Вашингтоне приступили к анализу возможностей приравнивания кибернетического оружия к традиционным видам оружия массового уничтожения. По оценкам чиновников Пентагона, кибероружие целесообразно ставить «на одну доску» с оружием массового уничтожения, поскольку с его помощью можно подорвать или уничтожить критическую инфраструктуру; поставить под угрозу сохранность больших баз данных (например, в сфере здравоохранения или в банковском деле); выявлять и подавлять сигналы спутниковой системы навигации; организовать с использованием соответствующих платформ в соцсетях кампании дезинформации, нацеленные на широкую аудиторию[400].

Для подготовки обоснования своей позиции военное ведомство США запросило национальные исследовательские институты собрать доказательства разрушительного потенциала кибероружия. Согласно этому запросу, ученым, помимо прочего, нужно будет выяснить, могут ли наступательные кибероперации применяться противниками Вашингтона в целях усовершенствования эффективности и увеличения поражающего действия оружия массового

---

[398] См. подр.: *Виловатых А.В*. Перспективы гибридизации военных конфликтов в условиях технологической революции // Международная жизнь. 2020.№ 3. С. 90–96.

[399] См. напр.: *Marton Péter.* Evolution in military affairs in the battlespace of Syria and Iraq // Corvinus Journal of International Affairs. 2018. Vol. 2. p.30.

[400] Recommendations to the President on Securing America's Cyber Interests and Deterring Cyber Threats Through International Engagement // U.S. Department of State. 2018. May. URL: https://www.state.gov/secretary/remarks/2018/05/282896.htm (дата обращения: 03.10.2019).

уничтожения, а также обеспечения замены традиционных видов такого оружия (ядерного, химического, радиологического, бактериологического[401].

Таким образом, предпринятые в последнее время американцами меры по кибернетической безопасности, свидетельствуют о решительном отходе Вашингтона от оборонительных действий в кибернетическом пространстве. Это подтверждает настрой США на поддержание своего доминирования на мировой арене, причем способ достижения данной цели противоречит позиции большей части государств международного сообщества. На практике реализация такой наступательной кибернетической концепции будет сопряжена с открытым или завуалированным применением информационных технологий в военно-политических целях[402].

Следует отметить, что с учетом повышения рисков в сфере кибербезопасности в последние годы в Америке все больше внимания придают обеспечению кибербезопасности объектов национальной критической инфраструктуры. Под этим понятием подразумевается концепция и система практического обеспечения противодействия серьезным угрозам работы важных объектов инфраструктуры и объектов повышенной опасности на территории страны и в ее ближайшем окружении, особенно в условиях распространения информационных технологий и связанных с ними кибернетических угроз.

Первым шагом американских властей в указанном направлении было создание в 1996 г. Комиссии по защите жизненно важной инфраструктуры при президенте Соединенных Штатов[403]. Тогда же была поставлена задача разработать всеобъемлющую национальную стратегию по защите инфраструктуры от физических и кибернетических угроз[404].

---

[401] См.: *Pomerleau Mark.* Are cyber weapons similar to WMDs? DoD wants to know // Fifth Domain. 2018. December 20. URL: https://www.fifthdomain.com/dod/2018/12/20/are-cyber-weapons-similar-to-wmds-dod-wants-to-know/ (дата обращения: 03.10.2019).

[402] *Виловатых А.В.* Фактор России в развитии стратегии кибербезопасности США и их союзников // Вестник Академии военных наук. 2020. № 1.

[403] См.: Executive Order. 13010. Critical Infrastructure Protection. Federal Register. Vol. 61. №. 138. July 17. 1996. pp. 3747–3750.

[404] См.: Critical Foundations: Protecting America's Infrastructures // FAS. 1997. October. URL: https://fas.org/sgp/library/pccip.pdf (дата обращения: 05.10.2019).

После событий 11 сентября 2001 г. термин «критическая инфраструктура» был закреплен в Патриотическом акте 2001 г. Несколько лет спустя последовало создание Министерства внутренней безопасности США, подразделения которого сегодня осуществляет основные функции по обеспечению безопасности критически важной для государства инфраструктуры [405].

Источник: Составлено по: Министерство внутренней безопасности США.

Рисунок 4.1 – Структура ведомств, вовлеченных в обеспечение кибербезопасности критической инфраструктуры США

Согласно стратегии кибербезопасности МВБ, в настоящее время к объектам критической инфраструктуры в США причисляется 16 секторов:1) химические объекты; 2) коммерческие предприятия; 3) системы связи; 4) предприятия непрерывного цикла; 5) плотины и дамбы; 6) оборонные промышленные объекты; 7) службы по ликвидации последствий чрезвычайных ситуаций; 8) энергетическая инфраструктура; 9) сектор финансовых услуг; 10) предприятия пищевой промышленности и сельского хозяйства; 11) правительственные учреждения; 12)

[405] Secure Cyberspace and Critical Infrastructure // US Department of Homeland Security. 2019. July 5. URL: https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure# (дата обращения: 05.10.2019).

система здравоохранения; 13) информационные технологии; 14) ядерные реакторы, радиоактивные материалы и их отходы; 15) транспортные системы; 16) объекты водоснабжения и очистки сточных вод[406].

За разработку национальных стандартов США в области кибербезопасности отвечает Национальный институт стандартов и технологий. В соответствии с постановлением администрации Б. Обамы «Улучшение кибербезопасности критической инфраструктуры», в США разработана концепция, которая состоит из стандартов, методик, описания процедур и процессов[407].

Таблица 4.1 Концепция обеспечения кибербезопасности объектов критической инфраструктуры США

Функция	*Описание*
Выявление (Identify)	Идентификация рисков и реагирование на них в целях обеспечения кибербезопасности системы в целом, ее активов, данных и функциональных возможностей
Защита (Protect)	Разработка мероприятий по доставке сервисов для обеспечения киберзащиты важнейших объектов инфраструктуры
Обнаружение (Detect)	Разработка и проведение соответствующих мероприятий по распознаванию событий, диктующих необходимость практического обеспечения кибербезопасности
Ответные действия (Respond)	Осуществление соответствующих мероприятий в области киберзащиты при обнаружении событий кибербезопасности
Восстановление (Recover)	Приведение в исходное состояние нарушенных функций из-за событий кибербезопасности и обеспечение устойчивости работы системы

Источник: Составлено по: NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

В Белом доме объясняют избранную концепцию «упреждающей защиты» тем, что кибератаки якобы уже стали неотъемлемой частью современных военных конфликтов. Данный подход исходит прежде всего из идеи о необходимости сохранения доминирующего положения страны на мировой арене ввиду получения преимуществ в обретении инновационных технологий другими политическими акторами, в том числе Китайской Народной Республикой.

[406] Critical Infrastructure Sectors // US Department of Homeland Security. 2018. URL: https://www.dhs.gov/critical-infrastructure-sectors (дата обращения: 18.09.2019).

[407] Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology. February 12, 2014.

В стратегии кибербезопасности, опубликованной Министерством внутренней безопасности США 15 мая 2018 г, надежное обеспечение защиты критической инфраструктуры от кибернетических угроз обозначается как «необходимый шаг к достижению лидирующих позиций США во всех операционных средах»[408]. Согласно документу, перед ведомством ставятся следующие задачи в рассматриваемой области:

1. Внедрять инновации по обеспечению кибернетической безопасности с целью нейтрализации рисков критической инфраструктуре.

2. Расширять и углублять взаимодействие с национальными ведомствами в интересах поддержания в надлежащем состоянии кибернетической безопасности критической инфраструктуры, выработки защитных мер и накопления информации, способствующей обеспечению кибербезопасности объектов критической инфраструктуры.

3. Развивать возможности ведомства в области обеспечения кибербезопасности в конкретных секторах, предоставлять каждому из них услуги в проведении экспертизы проводимых мероприятий и разрабатывать соответствующие механизмы их технической поддержки.

Примечательно и то обстоятельство, что США работают над совершенствованием существующих и созданием новых инструментов, способных поставить под угрозу критическую инфраструктуру равных им по силе соперников (*peer adversaries*). Впервые публично об этом заявил, выступая весной 2018 г. на слушаниях в сенатском Комитете по вооруженным силам, глава национального Киберкомандования и Агентства национальной безопасности генерал-лейтенант П. Накасоне. Военачальник отметил, что в перспективе указанные меры станут базой для утверждения американской гегемонии не только

[408] DHS Cybersecurity Strategy // US Department of Homeland Security. 2018. May 15. URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (дата обращения: 18.09.2018).

в кибернетическом, но также в космическом, воздушном, наземном, надводном и подводном пространствах[409].

Однако риторика политического руководства и сформулированные в концептуальных американских документах в области национальной безопасности масштабные планы в кибернетической сфере могут встретить препятствия, связанные с формализмом и сложностью процедур, присутствующих в бюрократической системе Соединенных Штатов, а также нехваткой квалифицированных специалистов в области кибербезопасности, находящихся на службе в государственных ведомствах.

В отчете Счётной палаты США за 2018 г. указывается, что на современном этапе критические объекты американской инфраструктуры уязвимы для киберугроз[410]. Среди элементов, наиболее подверженных риску, составители документа называют электросети, морские порты, газо- и нефтепроводы Соединённых Штатов. Например, отмечается, что в последние годы защита электросетей от кибератак была сопряжена с такими вызовами, как мониторинг за внедрением стандартов кибербезопасности, установка средств защиты «умных» сетей и введение единых параметров безопасности в рассматриваемой сфере. Помимо этого, авторы отчета констатируют слабую защищенность от киберугроз американских газо- и нефтепроводов, электросетей и коммунальных предприятий, используемых для снабжения военных объектов[411].

Основные источники киберугроз для элементов критической инфраструктуры, согласно данным американских государственных ведомств, имеют российское, китайское или иранское происхождение. В частности, в отчете

---

[409] *Pomerleau Mark.* Are cyber weapons similar to WMDs? DoD wants to know // Fifth Domain. 2018. December 20. URL: https://www.fifthdomain.com/dod/2018/12/20/are-cyber-weapons-similar-to-wmds-dod-wants-to-know/ (дата обращения: 03.10.2019).

[410] Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation // Government Accountability Office. 2018 July 25. URL: https://www.gao.gov/assets/700/693817.pdf (дата обращения: 17.09.2019).

[411] GAO-16-885T. FEDERAL INFORMATION SECURITY: Actions Needed to Address Challenges. Testimony Before the President's Commission on Enhancing National Cybersecurity. P. 1–3 // United States Government Accountability Office. 2016. September 19. URL: http://www.gao.gov/products/GAO-16-885T (дата обращения: 18.09.2019).

Национальной разведки США отмечается, что соперники Америки стратегически нацелены на проведение кибератак против таких секторов в Соединенных Штатах, как энергетика, биотехнологии, оборона, предприятия непрерывного цикла, системы связи и информационно-коммуникационных технологий[412].

Прослеживается беспокойство американских государственных чиновников относительно обеспечения кибербезопасности информационного сектора страны, что, в свою очередь, продуцирует проблемы функционированию ряда американских организаций в энергетической, ядерной, водной, авиационной, строительной и пр. сферах. Например, руководитель группы специалистов по анализу систем промышленной безопасности Министерства внутренней безопасности Дж. Хомер заявил о произошедшем в 2017 г. серьезном взломе иностранными акторами сетей коммунальных служб США, считавшихся местными специалистами безопасными или изолированным. По словам чиновника, хакеры якобы осуществили техническое проникновение в диспетчерские пункты американских электроэнергетических компаний[413].

С учетом указанных обоснований американцы создают новые структуры, ответственные за обеспечение кибербезопасности. Так, 31 июля 2018 г. Министерство внутренней безопасности США объявило о создании Национального центра управления кризисными ситуациями (*National Risk Management Center*). Его основной задачей стало обеспечение кибербезопасности предприятий банковского и энергетического секторов, а также компаний других отраслей промышленности от атак, способных нанести вред критически важной инфраструктуре. На современном этапе Национальный центр управления кризисными ситуациями, действующий под руководством помощника министра внутренней безопасности Б. Коласки, активно сотрудничает с различными

[412] Цит. по.: DNI: China’s cyber theft of tech (also Russia’s and Iran’s) threatens U.S. edge // Geostrategy-Direct. Foreign Influence Operations and their use of Social Media Platforms. 2018. July 31. URL: http://geostrategy-direct-subscribers.com/dni-chinas-cyber-theft-of-tech-also-russias-and-irans-threatens-u-s-edge/ (дата обращения: 03.10.2019).

[413] DNI: China’s cyber theft of tech (also Russia’s and Iran’s) threatens U.S. edge // Geostrategy-Direct. Foreign Influence Operations and their use of Social Media Platforms. 2018. July 31. URL: http://geostrategy-direct-subscribers.com/dni-chinas-cyber-theft-of-tech-also-russias-and-irans-threatens-u-s-edge/ (дата обращения: 03.10.2019).

государственными структурами, прежде всего Кибернетическим командованием ВС США. Главный офис центра размещен в Арлингтоне (шт. Вирджиния), а его штат укомплектован работниками указанного министерства[414].

Кроме того, летом 2018 г. чиновники США объявили, что в стране планируется создание нового агентства, призванного стать своего рода объединённым центром обеспечения кибербезопасности в свете активности террористов из иностранных государств. На деятельность указанной структуры только в 2019 г. предполагалось выделить 15 млрд долларов[415]. К окончанию 2019 г. Агентство кибербезопасности и защиты инфраструктуры можно рассматривать в качестве ключевого межведомственного звена, координирующего процессы по обеспечению кибернетической безопасности критически важной инфраструктуры Соединенных Штатов[416].

Следует обратить внимание, что военно-политическое руководство США активизирует меры по обеспечению кибернетической безопасности критически важных объектов инфраструктуры страны, учитывая усиление взаимосвязи между функционированием таких объектов и инновационными технологиями в области искусственного интеллекта ввиду осуществления с помощью последних функций управления и контроля. Предпринимаемые Вашингтоном шаги в данном направлении американские правящие круги связывают в основном с растущими кибернетическими угрозами со стороны их вероятных противников. Такая политика в очередной раз свидетельствует об окончательном отходе США от оборонительных действий в кибернетическом пространстве.

---

[414] См.: U.S. intel leaders warn of ‘pervasive’ Russian intrusions in 2018 amid tension with White House // Geostrategy-Direct. 2018. August 7. URL: http://geostrategy-direct-subscribers.com/u-s-intel-leaders-warn-of-pervasive-russian-intrusions-in-2018-amid-tension-with-white-house/ (дата обращения: 14.09.2019).

[415] DHS' Kolasky to lead new cyber risk center announced at summit this week // Inside Cybersecurity. 2018. August 03. URL: https://insidecybersecurity.com/daily-news/dhs-kolasky-lead-new-cyber-risk-center-announced-summit-week (дата обращения: 18.09.2019).

[416] President Donald J. Trump Signed H.R. 3359 into Law // Whitehouse.gov. 2018. November 16. URL: https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-signed-h-r-3359-law/ (дата обращения: 03.10.2019).

В Вашингтоне призналют, что американский подход чреват рисками и для самих Соединенных Штатов. Ввиду большей, чем у других стран зависимости Америки от интернета она гораздо более уязвима для кибератак по сравнению с иными государствами. Кроме того, военные специалисты сходятся во мнении о том, что крен в сторону развития наступательных возможностей может привести к отвлечению людских и финансовых ресурсов Вашингтона от решения реальных задач в указанной сфере. На современном этапе это может отразиться на безопасности США[417].

Пробелы в защите национальной критической инфраструктуры обнаружились еще в ходе первого в истории США аудита МО, проведенного в конце 2018 г. В частности, именно тогда выявилось неудовлетворительное состояние кибербезопасности информационных систем самого ведомства. Как заявил в связи с этим ревизор Пентагона Д. Норквист, наибольшую озабоченность специалистов вызвало состояние систем компьютерной безопасности[418].

Минимизировать указанные риски в Белом доме рассчитывают благодаря ряду мер, в том числе с помощью применения прорывных разработок в области квантовых технологий[419]. По оценкам специалистов Пентагона, квантовые компьютеры позволят создавать новые сверхнадежные системы киберзащиты, а также взламывать используемые противником системы шифрования данных с минимальным участием человека. В декабре 2018 г. Палата представителей Конгресса США приняла законопроект о Национальной квантовой инициативе (*National Quantum Initiative Act).* Данная инициатива предполагает выделение на исследования в указанной сфере 1,2 млрд долларов в течение ближайших пяти лет. В рамках Министерства энергетики США планируется учредить две

---

[417] См. напр.: *Williams Lauren C.* DOD struggles with loss of cyber personnel // FCW. 2018 September 28. URL: https://fcw.com/articles/2018/09/28/cyber-workforce-dod-williams.aspx (дата обращения: 01.10.2019).

[418] Цит. по.: *Aaron Mehta.* The Pentagon failed its audit, but officials aren't surprised // DefenseNews. 2018. November 15. URL: https://www.defensenews.com/pentagon/2018/11/15/the-pentagon-failed-its-audit-but-officials-arent-surprised/ (дата обращения: 03.03.2019).

[419] См. подр.: *Селянин Я. В.* Технологическое лидерство, роль государства и неоднозначность цифр в высокотехнологичных областях // Проблемы национальной стратегии. – 2019. № 5. URL: https://riss.ru/bookstore/journal/2019-g/5-56/ (дата обращения: 10.11.2019).

лаборатории квантовых исследований, каждая из которых получит финансирование в размере 25 млн долларов в год. Также при Управлении научно-технической политики Белого дома появится Национальное координационное бюро по квантовым исследованиям (*National Quantum Coordination Office*)[420].

Повсеместная цифровизация социально-политической и социально-экономической активности, ускоренная пандемией COVID-19 2020 г., стала поводом для провозглашения новой политики и корректировки законодательства отдельных стран в области кибербезопасности. Например, в Белом доме связали нововведения с необходимостью адаптации страны к рискам и возможностям, вытекающим из технологических изменений Четвертой промышленной революции, в условиях форсированного размывания глобальной мощи США.

Почва для пересмотра политики Соединенных Штатов в кибернетической сфере оказалась уже подготовленной. В марте 2020 г. спешно завершила работу комиссия «Солярий» (*Cyberspace Solarium Commission*), учрежденная в августе 2018 г. сенатором-республиканцем Дж. Маккейном по аналогии с одноименным американским проектом Д. Эйзенхауэра от 1953 г. Главной целью ее функционирования явился анализ долгосрочных угроз, обусловленных деятельностью вероятных противников Соединенных Штатов в киберпространстве и выработка на этой основе всеобъемлющего подхода к обеспечению кибербезопасности страны[421].

Комиссия «Солярий» представила более 80 выводов и рекомендаций по обеспечению интересов США в кибернетической сфере, примерно 50 из которых потребуют законодательного утверждения. Американские власти заявили, что результаты работы экспертов станут основой для новой стратегии кибербезопасности. Примечательно, что выводы и рекомендации комиссии уже

---

[420] H.R.6227 – National Quantum Initiative Act // Congress. gov. 2018. 21 December. URL: https://www.congress.gov/bill/115th-congress/house-bill/6227 (дата обращения: 01.03.2019).

[421] The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence // Congressional Research Service. 2020. March 20. URL: https://fas.org/sgp/crs/natsec/IF11469.pdf (дата обращения: 15.04.2020).

выступили в качестве предмета слушаний комитета по вооруженным силам Сената США, проводимых в закрытом режиме[422].

Предполагается, что в обозримом будущем наступательную киберстратегию США, провозглашенную Д. Трампом в 2018 г., сменит концепция «многоуровневого киберсдерживания». Согласно отчетному докладу комиссии «Солярий», фундаментом «многоуровневого киберсдерживания» станет реформирование системы американских госведомств. Планируется учреждение комитетов по кибербезопасности в Сенате и Палате представителей США, поскольку комитеты по вооруженным силам и комитеты по разведке якобы не могут на постоянной основе компетентно оценивать соответствующие проблемы. Также предполагается создать должность директора по кибербезопасности, который войдет в состав исполнительного офиса президента США. Кроме того, эксперты рекомендуют возложить на МО США большую часть ответственности за обеспечение кибербезопасности национальной военно-промышленной базы, а также наделить дополнительными полномочиями Федеральное бюро расследований и Агентство по кибербезопасности и безопасности инфраструктуры для улучшения взаимодействия данных структур с иностранными партнерами Америки.

В качестве другой опоры концепции многоуровневого киберсдерживания выступит совершенствование законодательной базы в области обращения с цифровыми данными. Как ожидается, это должно способствовать минимизации рисков в деятельности государственных и частных структур, вовлеченных в сбор, анализ и обработку персональной информации, посредством четкой нормативной регламентации их прав и обязанностей. В пакете правовых мер также учитывается расширение требований к финансовой отчетности в сфере кибербезопасности. Кроме того, заявлено о целесообразности введения дополнительных ограничений на политическую рекламу в интернете для минимизации негативного влияния

[422] Findings of the Cyberspace Solarium Commission // U.S. Senate Committee on Armed Services. 2020. March 25. URL: https://www.armed-services.senate.gov/hearings/20-03-25-findings-of-the-cyberspace-solarium-commission (дата обращения: 15.04.2020)

внешних сил. Решение последней задачи будет возложено на Глобальный центр взаимодействия США (*Global Engagement Center*)[423].

Одним из приоритетов в сфере кибербезопасности эксперты комиссии «Солярий» признали обеспечение технологического рывка, необходимого для поддержания доминирующих позиций страны в мире. Наиболее значимыми технологиями в краткосрочной и среднесрочной перспективе названы искусственный интеллект и системы связи пятого поколения 5G. На их развитии планируется сделать особый акцент, поскольку от данных технологий во многом зависит как кибербезопасность национальной критической инфраструктуры, так и проведение наступательных кибероперациий. Такие оценки базируются на результатах Расширенного мониторинга состояния национальной обороны (*Defense Wide Review*), проведенного МО США в 2019–2020 гг. с целью определения ресурсов для высокоприоритетных проектов американского военного ведомства, которые могут быть развернуты для невоенной нейтрализации внешнеполитической активности Китая и России[424].

В частности, эксперты Пентагона назвали ИИ «ключевой технологией будущего», которая потенциально применима во всем спектре миссий Минобороны. Они также признали необходимость выделения американским военным ведомством бюджетных ассигнований на создание безопасных и устойчивых 5G-систем для нужд МО, причем в самое ближайшее время, и призвали в дальнейшем к их ускоренной апробации и принятию на вооружение. Предполагается, что усиленное внимание к развитию технологий ИИ и систем связи 5G поспособствует созданию в Америке «военно-технологического фундамента будущего», однако для этого потребуется наладить бесперебойную кооперацию государственных органов с промышленностью и научным

[423] The Global Engagement Center: Leading the United States Government's Fight Against Global Disinformation Threat // U.S. Senate Committee on Foreign Relations. 2020. March 5. URL: https://www.foreign.senate.gov/hearings/the-global-engagement-center-leading-the-united-states-governments-fight-against-global-disinformation-threat (дата обращения: 15.04.2020).

[424] Renewed Great Power Competition: Implications for Defense—Issues for Congress // Congressional Research Service. 2020. April 7. URL: https://crsreports.congress.gov/product/pdf/R/R43838 (дата обращения: 15.04.2020).

сообществом США, которая существенно ослабла в последние годы. В этом контексте обращает на себя внимание тот факт, что уже 25 марта 2020 г. США приняли стратегию развития систем связи пятого поколения[425].

В соответствии с подходом «многоуровневого киберсдерживания», важным элементом инициативных мер США в киберпространстве признано укрепление сотрудничества с союзными странами. В частности, предусматривается согласование позиций Соединенных Штатов и их государств – партнеров в отношении злонамеренной активности оппонирующих им в киберпространстве акторов. Планируется активизировать обмен разведывательными данными, взаимопомощь в атрибуции анонимных атак, принятие совместных публичных заявлений о взаимной поддержке и пр.

Таким образом, в обозримом будущем американцы продолжат придерживаться «наступательной кибероборонs» (так называемой передовой обороны) в противостоянии с вероятными противниками даже в ситуациях, не требующих вмешательства третьей стороны, исходя из норм и принципов международного права. Однако это потребует усиления контроля государства над процессами, протекающими в киберпространстве. Признано необходимым проводить регулярные киберучения.

Основное внимание в новой американской киберстратегии планируется уделить противодействию кибернетической политике РФ и КНР. На мероприятии, организованном 15 апреля с.г. в целях презентации результатов деятельности комиссии «Солярий», указанные державы рассматривались как «основные геополитические субъекты, согласованно препятствующие сохранению технологического лидерства Соединенных Штатов». Члены комиссии связывали «угрозу со стороны России» с ее «чрезмерной вредоносной активностью» в киберпространстве, тогда как киберполитика Китая представлена в качестве источника «экзистенциальной угрозы» национальным интересам США.

[425] White House Releases National Strategy for 5G Security // NextGov. 2020. March 25. URL: https://www.nextgov.com/emerging-tech/2020/03/white-house-releases-national-strategy-5g-security/164109/ (дата обращения: 14.04.2020).

Специалисты признали, что недостаточная эффективность противостояния США с КНР и РФ в киберсреде во многом обусловлена нарастающими противоречиями между американскими ведомствами, в частности Министерством внутренней безопасности и Минобороны. Они резюмировали, что пандемия коронавируса стала своеобразным «11 сентября для киберсообщества США», но одновременно и наилучшей возможностью для оценки эффективности национального киберпотенциала[426].

В целом в Вашингтоне придают большую значимость усилению кибернетических возможностей страны. По прогнозам американских специалистов, соперничество в киберпространстве может изменить сложившийся стратегический баланс сил в мире. Киберсреда расценивается как призма, опосредующая социальную деятельность во многих проявлениях. Причем, как предполагается, в обозримой перспективе зависимость общества от инноваций только усилится, и нынешняя пандемия коронавируса может послужить для этого своеобразным катализатором[427].

Соответственно, в Белом доме нацелились на принятие комплексных мер в сфере кибербезопасности, призванных способствовать сохранению глобального технологического лидерства США. Под завесой нового подхода скрываются еще более наступательные замыслы, чем в прежней редакции национальной киберстратегии, однако они затушеваны комплексом довольно взвешенных мер по ряду других направлений. Такая смена курса свидетельствует о том, что Соединенные Штаты Америки заблаговременно готовились к нейтрализации рисков, связанных с цифровизацией социальной реальности, в частности со становлением цифровой экономики и цифровой системы управления. В свете прогнозируемых вызовов, диктуемых пандемией COVID-19, пересмотр приоритетов в области кибербезопасности выглядит весьма своевременным.

---

[426] CSC Virtual Event: Layered Cyber Deterrence // Cyberspace Solarium Commission. 2020. April 15. URL: https://www.solarium.gov/#h.p_cEkideHVewUW (дата обращения: 14.04.2020).

[427] COVID-19 Exploited by Malicious Cyber Actors // CISA. 2020. April 8. URL: https://www.us-cert.gov/ncas/alerts/aa20-099a (дата обращения: 15.04.2020).

В целом избранный вашингтонской элитой подход к обеспечению безопасности киберпространства, являющегося своеобразной базой для проведения операций информационно-психологического воздействия, демонстрирует нацеленность Соединенных Штатов на удержание их доминирующего положения на мировой арене. Вместе с тем он объективно представляет собой серьезную угрозу стратегической стабильности. Поэтому важным аспектом с точки зрения поддержания информационной безопасности в международном контексте является привлечение внимания мирового сообщества к наступательному, а не оборонительному подходу США к обеспечению кибернетической безопасности в ущерб другим государствам. С учетом такого предпочтения в обозримой перспективе риски международной информационной безопасности в этой области, видимо, еще более возрастут.

С учетом форсированного совершенствования технологий искусственного интеллекта и появлением новых прорывных разработок в данном анправлении, которые могут применять как легитимные, так и нелегитимные акторы, мировые политические процессы, вероятно, приобретут характер пониженной прогнозируемости. Большая опасность тренда цифровизации процессов информационного противоборства таится именно в потенциале технологий ИИ и машинного обучения, которые, по оценкам специалистов, в определенный момент могут привести к исключению человека как звена цепи принятия решений.

Крупный американский военный эксперт Р. Уорк в докладе компании «Говини» *(Govini*), занимающейся обработкой и анализом данных по заказу правительственных структур, призвал Белый дом и Пентагон определить, в каких масштабах Соединённые Штаты будут наращивать исследования и разработки в области технологий, связанных с искусственным интеллектом, включая перспективные компьютерные системы, искусственные нейронные сети, большие данные, машинное обучение, автоматизированные системы и робототехнику. Р. Уорк указывал на то, что американские военные должны решить, хотят ли они

«возглавить предстоящую революцию или стать её жертвой»[428]. По его экспертному мнению, ответ на поставленный вопрос будет зависеть от того, как скоро Минобороны США осознает революционный военный потенциал искусственного интеллекта и передовых автономных систем.

Наиболее значимым проектом в американском военном ведомстве, апробирующим технологии искусственного интеллекта, является подразделение по ведению «алгоритмических боевых действий» (*Project Maven*). Оно было создано 26 апреля 2017 г. под руководством упомянутого выше Р. Уорка в целях ускоренной апробации машинного обучения и других технологий искусственного интеллекта в одной из сфер деятельности Пентагона. Каждые три месяца подразделение внедряет инновации в функционирование американских вооруженных сил. Как отмечает Р. Уорк, цель форсирования применения искусственного интеллекта в военном деле состоит в переходе от разовых попыток применения искусственного интеллекта для нужд национальной безопасности США к беспрерывности этого процесса[429].

Весной 2018 г. в Америке запущен процесс по учреждению Объединённого центра искусственного интеллекта (*Joint Artificial Intelligence Center*), который консолидирует усилия национального военного сообщества по разработкам в указанной сфере. настоящее время, помимо самостоятельных инициатив в данной области, в том или ином виде рассматриваемые технологии уже интегрированы в программы и планы Минобороны. Особенно влияние искусственного интеллекта проявляется в программе модернизации Большая шестерка (*Big Six*), где у

---

[428] AI, Big Data and Cloud Taxonomy // Govini. 2017. URL: https://www.govini.com/research-form/?post_title=DoD+ARTIFICIAL+INTELLIGENCE%2C+BIG+DATA+AND+CLOUD+TAXONOMY&post_link_redirect=https%3A%2F%2Fwww.govini.com%2Fresearch-item%2Fdod-artificial-intelligence-and-big-data-taxonomy%2F&post_id=4026 (дата обращения: 02.12.2018).

[429] Project Maven to Deploy Computer Algorithms to War Zone by Year's En // U.S. Department of Defense. 2017. 21 July. URL: https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/ (дата обращения: 28.06.2018).

ведущих направлений развития вооружения и военной техники присутствует важная «интеллектуальная» составляющая[430].

При развитии ИИ в США акцент предполагается сделать на развитии государственно-частного партнерства в указанной сфере. Национальным министерствам и ведомствам, внедряющим прорывные технологии, предписано привлекать к своей работе крупных американских ученых и экспертов, руководителей ведущих компаний (в частности, Google, Microsoft, IBM, Oracle, Qualcomm и пр.). В целом документ призван содействовать снятию в США барьеров для практического использования искусственного интеллекта, принятию технических стандартов, обеспечивающих кибербезопасность госструктур, ускорению подготовки следующего поколения разработчиков и пользователей новых технологий.

Примечательно, что на следующий день после опубликования указанного правового акта Пентагон выпустил собственную Стратегию в области искусственного интеллекта[431]. Документ повторяет положения утвержденных за последние годы оборонной и ядерной стратегий, где Китай и Россия названы главными противниками, а их сдерживание является важнейшей целью Соединенных Штатов. В нем присутствует положение, что Вашингтон возьмет на вооружение технологии искусственного интеллекта с целью удержания доминирующего положения на мировой арене и завоевания стратегического превосходства в военных конфликтах будущего.

Следует отметить и то, что в феврале 2019 г. ВМС США опубликовали аналитический доклад – политическую установку, где отмечается, что «ввиду апробирования в практике информационного противоборства технологий искусственного интеллекта информация стала более популярным оружием среди

---

[430] См.: Freedberg *S.* Army Sec. Esper’s 10-Year Plan Is A Big Bet On Budget // 2018. 6 June. URL: https://breakingdefense.com/2018/06/sec-esper-10-year-plan-is-a-big-bet-on-budget/ (дата обращения: 14.12.2018).

[431] Summary of the 2018 Department of Defense Artificial Intelligence Strategy // US DOD. 2019. 12 February. URL: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF?fbclid=IwAR0iPoHeBD-hjWG6spK_6C9nJjADlqguh9ZwV_gHYRpUrq7M0Zj7dsbvTEA (дата обращения: 01.03.2019).

стратегических конкурентов Америки, чем прежде». В связи с этим в документе вводится понятие «сообщество по информационным войнам», все элементы которого (включая разведчиков, связистов, криптологов, инженеров и пр.), должны участвовать в процессах информационного противоборства не самостоятельно, а как «полностью интегрированная система»[432].

Подобная поспешность внедрения в военно-политическую практику разработок на базе искусственного интеллекта повышает риски сокращения транспарентности военных программ, ведет к игнорированию международно-правовых принципов и норм, а также может поспособствовать распространению опасных технологий среди негосударственных субъектов. Присутствует опасность, что стремление к достижению технологического превосходства некоторых стран может привести к новой гонке вооружений в мире. В целом это может привести к усилению нестабильности и эскалации самых разнообразных для человечества рисков.

Сказанное выше является ключевым противоречием, свидетельствующим о перспективах развития искусственного интеллекта и одновременно угрозой таких технологий для человечества. Широкие возможности их применения в процессах информационного противоборства могут поставить под вопрос существующую архитектуру международной безопасности и мировой порядок в принципе. Более того, в условиях обострения отношений между ведущими государствами присутствует опасность развёртывания новой гонки вооружений в сфере создания боевых систем на базе искусственного интеллекта, разработка которых (в отличие от ядерного, химического, биологического оружия) остаётся в «серой зоне» международного права.

С активизацией на современном этапе НИОКР в области развития военного искусственного интеллекта в международном сообществе усиливается дискуссия об этичности и правомерности создания и применения таких систем. Так, в январе

[432] Цит. по.: О разработках в области информационной войны в США // Научно-исследовательский центр проблем национальной безопасности. 2019. Март. URL: https://nic-pnb.ru/informacionnoe-protivoborstvo/o-razrabotkah-v-oblasti-informatsionnoj-vojny-v-ssha/ (дата обращения: 23.05.2019).

2018 г. видные мировые учёные подписали открытое письмо, призывающее специалистов задуматься о стремлении создавать всё более сильный искусственный интеллект. «Мы рекомендуем проведение расширенных исследований, направленных на обеспечение надёжности и доброжелательности систем искусственного интеллекта с растущей мощностью. Системы искусственного интеллекта «должны делать то, что мы хотим, чтобы они делали»[433]. В марте 2018 г. около 300 исследовательских групп по всему миру начали проводить исследования по сохранению доброжелательности искусственного интеллекта.

Так, специалисты указывают на угрозы военного применения искусственного интеллекта, вытекающие из радикального сокращения времени на принятие стратегических решений в рамках деятельности в сфере военного управления и связи, а также при сборе и анализе разведывательной информации. Военные программы Пентагона нацелены на то, чтобы суперкомпьютеры взяли на себя работу по анализу различных данных и подготовке сценариев для политического и военного руководства[434].

Общественное внимание к использованию искусственного интеллекта в военных целях привело к переговорам в рамках Конвенции ООН о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие, под регулирование которой подпадают противопехотные мины и ослепляющие лазеры (Конвенция о негуманном оружии). В декабре 2016 г. 5–я Обзорная конференция Конвенции приняла решения сформировать группу правительственных экспертов по рассмотрению существующих проблем в области автономных боевых систем. Первая встреча этой группы состоялась в

---

[433] Autonomous weapons are a game-changer // The Economist. 2018. January. URL: https://www.economist.com/special-report/2018/01/25/autonomous-weapons-are-a-game-changer (дата обращения: 02.12. 2018).

[434] См. напр.: *Козюлин В.* Три группы угроз смертоносных автономных систем // РСМД. 2018. 1 ноября. URL: http://russiancouncil.ru/analytics-and-comments/analytics/tri-gruppy-ugroz-smertonosnykh-avtonomnykh-sistem/ (дата обращения: 10.12.2018).

декабре 2017 г., вторая – в апреле 2018 г. Однако к окончанию 2018 г. дипломатический процесс не привёл к каким-либо взаимным обязательствам[435].

Международные переговоры по этой проблематике вызывают мало интереса в Вашингтоне, который делает ставку на примат национального законодательства. В американском законе о Национальном оборонном бюджете на 2019 г. указывается допустимость использования вооруженными силами США «нетрадиционных технологий» – включая искусственный интеллект – с целью повысить состояние обороноспособности страны. Отмечается целесообразность развития партнёрства государственных структур с промышленностью, научными кругами и частными компаниями и использованию «более гибких процессов руководства и приобретения» в разработке и внедрении технологий искусственного интеллекта и машинного обучения для нужд американского Минобороны[436].

В складывающихся обстоятельствах, безусловно, важно на международном уровне адаптировать имеющееся или принять новое законодательство, регламентирующее соответсвующие вопросы, поскольку появление новых видов вооружения и военной техники, способных самостоятельно выбирать цели, свидетельствует о необходимости коррекции корпуса парва с учётом технологических особенностей оружия нового времени. Для предотвращения надвигающейся гонки вооружений между ведущими государствами мира, а также негосударственными акторами мировой политики необходим полный запрет смертоносных автономных систем. Кроме того, специалисты подчёркивают, что ответственность за применение смертоносных автономных систем при любых

---

[435] CCW Meeting of High Contracting Parties // The United Nations Office at Geneva. 2017. URL: https://www.unog.ch/80256EE600585943/httpPages)/A0A0A3470E40345CC12580CD003D7927?OpenDocument (дата обращения: 01.12.2018).

[436] См.: *Ионин Я.* Военный ИИ в США – с бюджетом, но без компромисса с Кремниевой долиной // РСМД. 2018. 21 августа. URL: http://russiancouncil.ru/analytics-and-comments/columns/military-and-security/voennyy-ii-v-ssha-s-byudzhetom-no-bez-kompromissa-s-kremnievoy-dolinoy/ (дата обращения: 10.12.2018).

условиях несёт человек, поэтому при их разработке должны учитываться риски и способы купирования таких рисков в будущем[437].

Таким образом, раскрытие потенциала Четвёртой промышленной революции приведёт к глубоким изменениям характера боевых действий в пользу смещения к невоенным методам противоборства. В частности, по прогнозам американских военных специалистов Школы международной службы Американского университета Д. Барно и Н. Бенсахель, всё более важную роль в конфликтах будущего станут играть такие операционные среды, как космос и киберпространство. При этом они отмечают, что искусственный интеллект и управление большими данными станет, видимо, использоваться как мощное оперативное преимущество[438].

Резюмируя, следует отметить, что происходящая на современном этапе мирового развития трансформация военного дела лишь в определенной мере затрагивает основное содержание войны, как фактора, оказывающего решающее влияние на ход и исход современных конфликтов. Но внимание, уделяемое западными аналитиками и военными деятелями исследованию основ гибридного противоборства, свидетельствует, что в будущем операции информационно-психологического воздействия с использованием цифровых технологий будут важным инструментом военно-политического руководства западных государств в борьбе за доминирование на мировой арене.

В целом адаптация к меняющемуся характеру войны на современном этапе является колоссальным вызовом для государственных и военных деятелей, и в ближайшие десятилетия масштабы этого вызова будут только нарастать по мере того, как будет раскрываться потенциал этой эпохи. Использование в боевых действиях слабо охваченных международным правом технологий Четвёртой промышленной революции может спровоцировать угрозы возникновения

---

[437] UN: Decisive action needed to ban killer robots – before it’s too late // Amnesty International. 2018. 27 August. URL: https://www.amnesty.org/en/latest/news/2018/08/un-decisive-action-needed-to-ban-killer-robots-before-its-too-late/ (дата обращения: 02.12. 2018).

[438] *Barno D., Bensahel N.* War in the fourth industrial revolution // War on the Rocks. 2018. 19 June. URL: https://warontherocks.com/2018/06/war-in-the-fourth-industrial-revolution/ (дата обращения: 02.12.2018).

неконтролируемой среды. Нельзя исключать и того, что поддержание стратегической стабильности в ближайшие десятилетия потребует пересмотра самих основ теории сдерживания.

4.3. Возможные меры России по купированию вызовов и угроз в области информационной безопасности

Разнообразие форм и способов достижения превосходства над противником является знаковой тенденцией развития международных отношений на современном этапе. Данная тенденция набирает обороты в условиях происходящей технологической революции, которая провоцирует усиление межгосударственной конкурентной борьбы. Геополитическое соперничество между мировыми центрами силы – в особенности между США и Китаем, США и Россией – сопровождается ускоренным внедрением ими инновационных технологий в разнообразные сферы жизнедеятельности социума, особенно в перспективных отраслях, определяющих национальную мощь и международное влияние страны[439].

Анализ состояния информационной обстановки вокруг Российской Федерации позволяет сделать вывод о постоянном проведении различными субъектами мировой политики мероприятий информационно-пропагандистского характера, направленных на подрыв суверенитета, политической и социальной стабильности, а также территориальной целостности России. В последние годы уровень таких усилий значительно возрос. Среди наиболее актуальных внешних угроз информационной безопасности Российской Федерации следует выделить:

– обострение международной конкуренции за обладание и контроль над стратегически важной информацией;

– расширение масштабов информационно-психологического воздействия на РФ со стороны иностранных государств и связанных с ними политических,

[439] См. подр.: *Шабров О.В.* Глобальные факторы современной политики // II Ежегодная Московская Конференция МРП СМП РАПН «Политические тенденции и явления: что определяет политику сегодня?». 2019. 6 апреля. URL: https://istina.msu.ru/conferences/188482207/ (дата обращения: 20.09.2019).

экономических, финансовых, общественных, религиозных и других организаций и их лидеров, представителей средств массовой информации, этнических, социальных, религиозных и других групп;

– стремление иностранных государств и международных террористических и экстремистских организаций к созданию новых и активному применению существующих видов информационного оружия;

– активизацию деятельности организаций, осуществляющих скрытый сбор информации о работе российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;

– наращивание рядом зарубежных стран возможностей информационно-технического воздействия на объекты критической инфраструктуры российского государства;

– проведение иностранными государствами мероприятий, направленных на снижение доверия населения Российской Федерации к политическому и военному руководству страны.

Противодействие вызовам и угрозам в информационной сфере, связанным с попытками внутриполитической дестабилизации России

В качестве долгосрочного проекта субъектов информационного противоборства, угрожающего национальной безопасности РФ, можно назвать применение современных гуманитарных технологий, призванных оказать долгосрочное контекстуальное влияние на широкую совокупность факторов (информационных, социальных, когнитивных и пр.), под воздействием которых формируется система ценностей российского общества. Это является одним из наиболее опасных вызовов национальной безопасности России.

По мнению отечественных специалистов, в краткосрочной перспективе именно трансформированная идентичность этнических групп и народов нашей страны может явиться основой сепаратистских идеологий и движений – от финно-угорской до калининградской. В зоне риска также находится историческое сознание населения РФ, которое может стать основой для экстремистских проявлений национализма. В это же русло вкладывается изменение религиозной

картины мира, которую оппоненты Российской Федерации желают видеть в качестве базы для формирования установок к участию в деятельности международных террористических организаций.

В этом контексте целесообразно учитывать, что внешнее управление возможно тогда, когда разрушена, забыта, намеренно выхолощена историческая традиция – религиозная, моральная, культурная и пр. Поэтому нужно заботиться о том, чтобы она всегда присутствовала в сознании российского населения. Это стержень, на котором держатся личность, общество и государство. Ее повсеместное сохранение – превентивная мера, позволяющая противодействовать любым попыткам установления контроля над индивидуальным и массовым сознанием. В первую очередь, речь идет о воспитании и образовании подрастающего поколения[440].

Для удержания инициативы в информационной сфере от РФ требуется использование ассиметричных способов противоборства. Реализация таких мер будет затруднена тем обстоятельством, что США в целях сохранения своего преимущества в информационном пространстве превентивно предпринимают шаги к недопущению расширения возможностей России по разъяснению зарубежной аудитории основных направлений государственной политики и доведению до массовой аудитории официального мнения по тем или иным значимым событиям. В частности, активно проводится информационная кампания по убеждению мирового сообщества в высокой эффективности «рупора российской пропаганды» и необходимости наращивания усилий по блокированию деятельности «прокремлевских» средств массовой информации.

Целесообразно учитывать, что многие государства пытаются дискредитировать образ Москвы в международных СМИ, и тем самым сформировать негативное восприятие нашей страны в мировом общественном мнении. Например, с ростом популярности мессенджеров и других социальных медиа, позволяющих создавать анонимные источники информации (как всем

[440] См. напр.: *Иванов В.Н.* Россия и русский мир. Экспертные суждения и оценки. М.: Академика, 2011. 112 с.

известные телеграм-каналы) и воспринимаемых общественностью как «независимые СМИ, заслуживающие доверия», сформировалась устойчивая угроза информационной безопасности Российской Федерации в сфере обороны. Она заключается в стремлении политических акторов получить инсайдерскую информацию для формирования предвзятого мнения о деятельности политического руководства страны, условно причисляемого к «силовому блоку»[441]. Обращению медиасубъектов к такого рода «инсайдерам» способствует «информационный вакуум», образующийся вокруг какой-либо внештатной ситуации вследствие несвоевременного либо некомпетентного доведения до российской и мировой общественности официальной информации.

В условиях стремительно меняющейся информационной обстановки и применения противоборствующей стороной новых форм и методов информационно-психологического и информационно-технического воздействия добиться более эффективного обеспечения национальной безопасности Российской Федерации можно будет путем перманентного совершенствования системы обеспечения информационной безопасности государства, способной оперативно и эффективно реагировать на возникающие вызовы и угрозы в информационной сфере. Это обусловлено тем, что агрессивные информационнные кампании в адрес нашей страны, реализуемые зарубежными правительствами, провоцируют сложные протестные настроения в российском социуме.

Соответственно, представляется важным в сжатые сроки осуществить комплекс наукоемких, высокотехнологичных мер, подкрепленных целым рядом обеспечивающих мероприятий, требующих затрат ресурсов и принятия новых юридических актов на государственном уровне. Как представляется, в условиях, когда отдельные государства стараются сделать глобальное информационное пространство зоной своего военно-политического влияния, необходимо

---

[441] New report: actors manipulating the online conversation are changing tactics // NATO. 2018. February 19. URL: https://www.stratcomcoe.org/new-report-actors-manipulating-online-conversation-are-changing-tactics (дата обращения: 05.09.2019).

выработать систему адекватных контрмер, направленных на обеспечение технологического, политического и культурно-информационного суверенитета государств. Необходимо комплексное импортозамещение американской ИТ-продукции и программного обеспечения (особенно в государственном секторе), а также динамичное развитие собственных интернет-сервисов, платежных систем и средств массовой коммуникации

Другим немаловажным фактором, который следует учитывать при совершенствовании системы информационной безопасности России, является многогранность и массированность действий противоборствующей стороны при проведении информационно-пропагандистских мероприятий. Ярким примером данного подхода является, в частности, проведение руководством США и их союзниками информационной кампании по формированию у мирового сообщества мнения о Российской Федерации как государстве, нарушающем положения Конвенции о запрещении химического оружия в контексте сирийского кризиса.

Искусственно сформированные в рамках информационных кампаний поводы используются американским руководством для осуществления действий, направленных на подрыв авторитета Российской Федерации на международной арене и формирование недоверия к нашей стране со стороны зарубежных партнеров. В частности, раскручивание странами Запада «дела Скрипалей» все еще используется для обоснования усиления санкционной политики в отношении России, в том числе для ущемления прав Российской Федерации в качестве полноценного субъекта международных отношений.

В этом контексте целесообразно открыто и своевременно представлять мировой общественности факты, свидетельствующие о целенаправленной деятельности западных структур по размещению на виртуальных коммуникативных ресурсах дезинформации или провокационных сообщений с целью нагнетания обстановки и разжигания конфликтов. Одновременно при проведении собственной информационной политики важно активнее применять этически допустимые технологии формирования общественного мнения. В этом

контексте можно было бы боолее внимательно отнестись к развитию цифровой дипломатии различных государственных ведомств, перспективным инструментом которой могут стать социальные медиа-платформы. В настоящее время они все чаще используются не только мировой общественностью, но и политическим сообществом.

При развитии и совершенствовании системы информационного обеспечения политической деятельности Российской Федерации важно избегать «слепого подражания» технологиям, применяемым западными странами. Это обусловлено прежде всего тем, что используемые США и их союзниками формы и методы опираются на весь потенциал имеющихся сил и средств, включающий в том числе расширенные возможности по оказанию влияния на ключевые медиаресурсы и международные организации.

Кроме того, повышению эффективности проводимых странами Запада мероприятий способствует англоязычное лингвистическое доминирование в мировом информационном пространстве. В связи с этим России стоило бы более внимательно отнестись к созданию системы убедительного опровержения так называемых «фейковых новостей». Несомненно, стоило бы отходить от простой реакции на происходящее к превентивному продвижению официальной линии государства, формированию собственного информационного контекста.

В целом, как представляется, для противодействия современным угрозам, связанным с негативным информационно-психологическим воздействием на население России, недостаточно задействовать возможности только непосредственных объектов дискредитации (в основном российских Минобороны и МИД). В целях нейтрализации соответствующих рисков важно скоординированное использование потенциала других органов государственной власти, СМИ и неправительственных организаций. Наращивание активных элементов системы обеспечения информационной безопасности России с обязательной координацией усилий по единому замыслу на государственном уровне поспособствует более надежному обеспечению интересов страны на

международной арене и обеспечит условия для ее динамичного социально-экономического развития.

Противодействие вызовам и угрозам, связанным с формированием антироссийского общественного мнения

В условиях, когда вызовы национальной безопасности любому государству могут быть смещены в сферу информационно-психологического давления, налицо активизация усилий ведущих стран Запада по раскручиванию антироссийской подрывной кампании с целью дискредитации, очернения имиджа и изоляции нашей страны на международной арене. Способом измерения эффективности влияния средств массовой информации и коммуникации на настроения в обществах отдельных государств являются социологические исследования. Эти же исследования негласно используются для манипулирования общественным мнением.

Проведенные после 2014 г. опросы населения различных служб и стран свидетельствуют, что в обобщенном виде субъекты информационного противоборства стремятся закрепить негативное восприятие России в мире. Динамика восприятия РФ в мировом общественном мнении за последние пять лет (2014-2019 гг.) демонстрирует, что в США и странах Западной Европы вместо отмечавшегося ранее нейтрального или даже относительно позитивного отношения к России ныне доминирует негативное. Такая же картина наблюдается в Латинской Америке, особенно, в Бразилии, Мексике и Перу. Центральная и Южная Европа, напротив, демонстрируют улучшение общественного восприятия РФ. Противоречивой выглядит ситуация на постсоветском пространстве и в Азиатско-Тихоокеанском регионе (АТР), где в дружественных к России государствах оценки населения начинают ухудшаться (в частности, Армении, Белоруссии, Индии). Позитивнее, чем раньше, Россию воспринимают в регионе Ближнего Востока и Северной Африки (особенно в Сирии, Ливане, Тунисе и Турции).

Depending on the country, U.S. or China is the more favored nation

Favorable view of ___

	Russia	U.S.	China	China-U.S. diff
Canada	27	43	**48**	5
Europe				
Netherlands	15	37	**49**	12
Spain	27	31	**43**	12
Greece	**64**	43	50	7
Germany	27	**35**	34	-1
France	36	**46**	44	-2
Sweden	18	**45**	41	-4
UK	26	**50**	45	-5
Hungary	39	**63**	38	-25
Italy	35	**61**	31	-30
Poland	21	**73**	42	-31
Asia-Pacific				
Australia	37	48	**64**	16
Indonesia	36	48	**55**	7
India	47	**49**	26	-23
Philippines	55	**78**	55	-23
South Korea	36	**75**	34	-41
Japan	26	**57**	13	-44
Vietnam	83	**84**	10	-74
Middle East				
Tunisia	39	27	**63**	36
Lebanon	47	34	**63**	29
Jordan	5	15	**35**	20
Turkey	32	18	**33**	15
Israel	35	**81**	53	-28

Источник: Globally, more people see U.S. power and influence as a major threat // Pew Research Center. 2017. August 1. URL: http://www.pewresearch.org/fact-tank/2017/08/01/u-s-power-and-influence-increasingly-seen-as-threat-in-other-countries/ (дата доступа 07.03.2018).

Рисунок 4.2 – Позитивное восприятие РФ, США и КНР в Европе, Азиатско-Тихоокеанском и Ближневосточном регионах

На Рисунке 4.4. приведены данные исследования американской службы Pew Research Center, согласно которому преимущественно отрицательное отношение к России высказывают жители 19 из 37 стран, где проводился опрос. В сравнении с Пекином или Вашингтоном Москву более негативно воспринимает население европейских государств (кроме Греции и Венгрии), стран Азии и Океании (за исключением Индии, Северной Кореи и Китая), всех стран Латинской Америки. Из 37 крупных государств мира только в Греции население относится к России лучше, чем к США или КНР.

Russia is more favored among young

Favorable view of Russia

	TOTAL %	18-29 %	30-49 %	50+ %	Young-old gap
Japan	26	53	33	16	+37
Brazil	35	57	34	20	+37
Australia	37	54	38	30	+24
South Korea	36	51	37	29	+22
UK	26	42	25	21	+21
Germany	27	39	29	22	+17
Spain	27	38	28	21	+17
U.S.	29	40	27	25	+15
Vietnam	83	89	82	74	+15
Canada	27	35	31	21	+14
Netherlands	15	25	13	12	+13
Turkey	32	37	31	26	+11

Источник: U.S. Image Suffers as Publics Around World Question Trump's Leadership // Pew Research Center, JUNE 26, 2017. URL: http://www.pewglobal.org/2017/06/26/u-s-image-suffers-as-publics-around-world-question-trumps-leadership/ (дата обращения:15.03.2018).

Рисунок 4. 3 – Позитивное восприятие России в отдельных странах с разбивкой по социально-возрастным группам

Вместе с тем, несмотря на негативизм в общих оценках, на Рисунке 4.5 продемонстрировано, что в последние годы динамика отношения населения ряда стран к Российской Федерации демонстрирует позитивную тенденцию среди молодежи.

Следует также отметить, что в государствах, причисляющих себя к Евроатлантическому сообществу, все сильнее проявляется зависимость от политических взглядов респондентов. Так, в США разное отношение к РФ демонстрируют сторонники демократического и республиканского лагерей (например, в качестве основной угрозы национальной безопасности Россию рассматривают примерно 61 % демократов и только 36 % республиканцев).

В Европе более позитивный образ РФ доминирует у приверженцев «партий, бросающих вызов» истеблишменту. В частности, идею налаживания связей между Европейским союзом и Российской Федерацией поддерживают 87 % немцев, при том что левые выступают за дружественные отношения вдвое чаще правых. В Польше такую позицию разделяют левые или центристы, во Франции – правые, социал-либералы и центристы.

Социологические исследования в Германии демонстрируют сдержанное улучшение отношения немцев к Российской Федерации при одновременном ухудшении отношения к США. Согласно опубликованным в декабре 2017 г. данным опроса немецкой исследовательской службы «АРД-тренд Германия» (*ARD-Deutschland-Trend),* уровень доверия немцев к политике России вырос до 28 %, и это самый высокий показатель с декабря 2011 г. Число не одобряющих политику Москвы немцев за последний год сократилось с 74 до 67 %. При этом рейтинг доверия немецкого населения к РФ как к партнеру ФРГ впервые превысил аналогичный показатель по отношению к США за все время наблюдений (с февраля 2007 г.)[442].

Несмотря на усиливающуюся антироссийскую пропаганду, положительные оценки в отношении России дает также население Финляндии. В декабре 2017 г. на вопрос социологов «Считаете ли вы развитие России угрозой для Финляндии» 51 % опрошенных ответили отрицательно, 36 % – положительно. Поддержка членства Финляндии в НАТО является самой низкой за последние годы и составляет 19 % (ранее доля сторонников сократилась с 26 % в 2014 г. до 21 % в начале 2017 г.). Против вступления страны в блок выступают 53 % граждан Финляндии[443].

Из государств Балканского полуострова активно внешнюю политику Москвы поддерживает Белград. В соответствии с приведенными результатами

---

[442] ARD-DeutschlandTREND Dezember 2017 - vollständiger Bericht .. Infratest dimap. 2017. Dezember. URL: https://www.infratest-dimap.de/umfragen-analysen/bundesweit/ard-deutschlandtrend/2017/dezember/ (дата обращения: 19.03.2018).

[443] Ylen kysely: Venäjän kehitystä uhkana pitävien määrä laskenut roimasti – asiantuntijan mielestä luku on silti korkea // Yle. 2017. URL: https://yle.fi/uutiset/3-9972311 (дата обращения: 19.03.2018).

опроса социологического агентства «Демостат», союз с Российской Федерацией предпочли бы 67,2 % граждан Сербии, тогда как вступление в ЕС – 50,9 %. Кроме того, опрос свидетельствует, что 41 % населения считают Россию «самым большим другом» республики. Большинство граждан выступает против создания на ее территории иностранных военных баз, но если они «необходимы», то больше всего сербов (20 %) поддержали бы создание именно российской военной базы[444]

Благоприятные оценки в отношении России высказывает и греческое общество. В исследовании, проведенном Университетом Македонии в октябре 2017 г. отмечается, что 57,3 % греков воспринимают нашу страну позитивно. Вместе с тем большинство греков выступают за укрепление связей с ЕС (47,5 %), тогда как на важность развития взаимодействия с Россией указывают 24,5 % опрошенных, с США – 9 %, со странами НАТО – 7,5 %[445].

В условиях, когда восприятие России в глазах мировой общественности раздроблено, а в некоторых странах начинает превалировать «эффект бумеранга» (противоположное навязываемой СМИ точки зрения социума или его отдельных групп на конкретную проблему), примечателен тренд на снижение международного влияния США. Американские специалисты весьма обеспокоены данными процессами, поскольку это проявляется практически в общемировом масштабе.

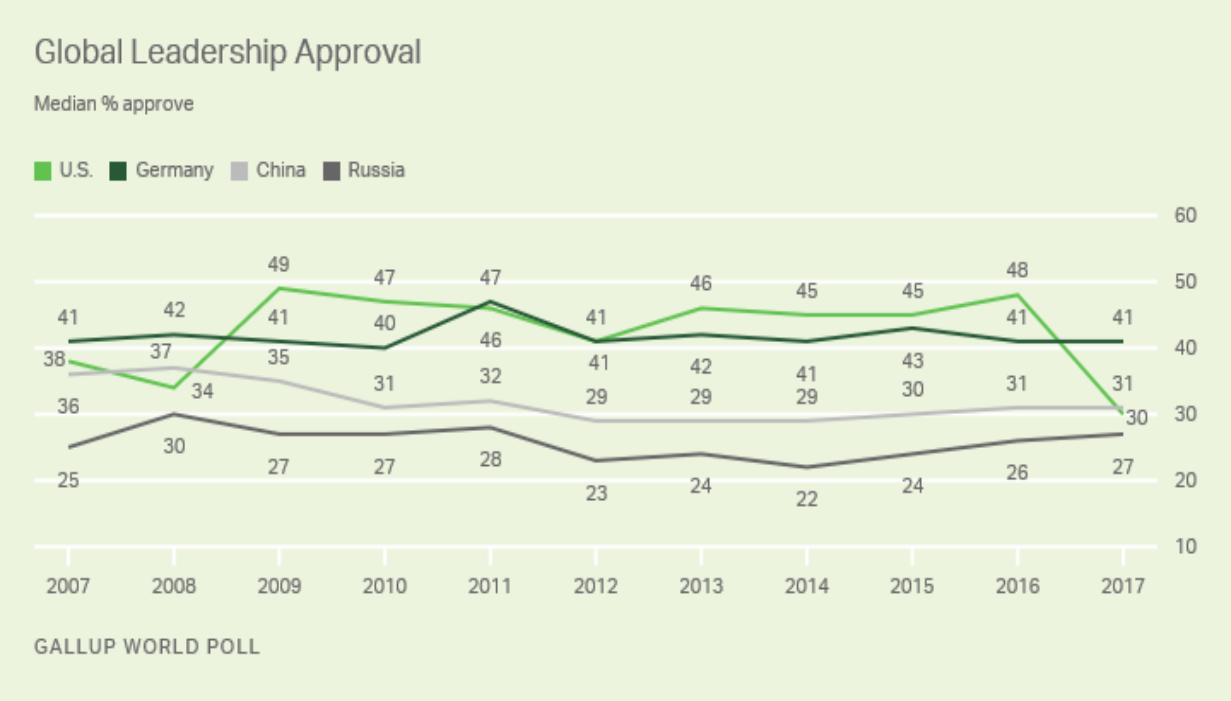
Так, согласно проведенному в январе 2018 г. в 134 государствах исследованию корпорации «Гэллап» (*Gallup*), количество респондентов, одобряющих лидирующую роль Америки в мире сократилось – с 48 % в 2016 г. до 30 % в 2017 г. Особенно заметно общественное мнение изменилось в Европе. Например, в Португалии, Бельгии, Норвегии, Великобритании, Дании, Франции

---

[444] См.: Western Balkans backsliding on democracy, says Lords committee // The Guardian. 2018. 10 January. URL: https://www.theguardian.com/politics/2018/jan/10/western-balkans-backsliding-on-democracy-says-lords-committee(дата обращения: 19.03.2018).

[445] Ibid.

негативные оценки в адрес Вашингтона содержали приблизительно до 60 % ответов, а в Германии – 72 %[446].



Источник: U.S. Leadership Image Suffers Most Among Friendly Nations // Gallup. 2018. February 20. URL: http://news.gallup.com/opinion/gallup/226997/leadership-image-suffers-among-friendly-nations.aspx (дата обращения: 13.03.2018).

Рисунок 4. 5 – Одобрение лидирующей мировой роли США, Германии, Китая и России

Опрос канадской компании «Глоубскан» (*GlobeScan*), охвативший около 18 тыс. граждан 19 стран, также продемонстрировал рост недовольства внешней политикой Соединенных Штатов. За период 2014–2017 гг. число отрицательных оценок увеличилось на шесть пунктов (с 43 до 49 %) в 17 странах, а количество позитивных – сократилось до 34 %. На 2017 г. пришлось наиболее резкое падение рейтинга Америки по сравнению с 11 другими оцениваемыми государствами[447].

С приходом в Белый дом Д. Трампа снизились показатели одобрения внешнеполитической активности США в странах Ближнего Востока и Северной Африки (БВСА). Результаты исследования эмиратской социологической службы

[446] U.S. Leadership Image Suffers Most Among Friendly Nations // Gallup. 2018. February 20. URL: http://news.gallup.com/opinion/gallup/226997/leadership-image-suffers-among-friendly-nations.aspx (дата обращения: 13.03.2018).

[447] Sharp Drop in World Views of US, UK: Global Poll // GlobeScan. 2017. July. URL: https://globescan.com/sharp-drop-in-world-views-of-us-uk-global-poll/ (дата обращения: 15.03.2018).

«Асда-Берстон Марстеллер» (*ASDA`A Burson-Marsteller*) продемонстрировали, что привлекательность политики Вашингтона в регионе сократилась с 25 % в 2016 г. до 17 % в 2017 г., при том что поддержка Москвы за этот же период выросла с 9 до 21 %[448]. Негативное отношение к Д. Трампу высказывают 83 % респондентов из стран БВСА (для сравнения: к Б. Обаме так относились 52 %, а к Дж. Бушу–младшему – 77 % арабов).

За последний год ухудшилось отношение к США также в странах Латинской Америки. Как свидетельствуют результаты опубликованного в ноябре 2017 г. опроса чилийской социологической службы «Латинобарометро» (Latinobarometro), проведенного в 18 государствах региона, усредненный показатель благоприятного восприятия Соединенных Штатов сократился там с 74 % в 2016 г. до 67 % в 2017 г. (наибольшее падение в Мексике – на 29 пунктов, Парагвае – 17, Уругвае и Гватемале – по 9). Рейтинг президента Трампа составил 2,7 по десятибалльной шкале (худший результат за время проведения исследований)[449].

Наиболее противоречивые оценки в адрес Америки зафиксированы в азиатском мире. Согласно итогам исследований автралийцев, опубликованным в сентябре 2017 г., 43 % китайцев, 44 % индонезийцев, 62 % австралийцев, 70 % южнокорейцев высказали мнение о том, что в период правления Трампа влияние США на обстановку в Индо-Тихоокеанском регионе будет скорее негативным. За более активную роль Вашингтона высказалось только население Индии (65 %), причем более половины респондентов в этой стране (53 %) выступили за наращивание военного присутствия Соединенных Штатов в регионе. Население КНР указало на высокую вероятность развязывания конфликта между Северной и Южной Кореей при посредничестве Пентагона (62 %). В свою очередь, 72 % респондентов из РК выразили опасение, что отношения их страны с Белым домом

---

[448] Arab Youth Survey 2017 // ASDA'A Burson-Marsteller. URL: http://www.arabyouthsurvey.com/pdf/2017-AYS-White-Paper-EN.pdf (дата обращения: 07.03.2018).

[449] Цит. по: U.S. Role in the World: Background and Issues for Congress // CRS. 2017. October 20. URL: https://fas.org/sgp/crs/row/R44891.pdf (дата обращения: 17.03.2018).

будут «плохими» (72 %), поскольку вмешательство американцев не будет способствовать урегулированию проблем Корейского полуострова[450].

Более того, в период нахождения в Белом доме Д. Трампа проявился и относительно новый тренд. Жители и лидеры ряда государств стали воспринимать Соединенные Штаты как источник угроз международной безопасности. Так, например, проведенное в конце 2017 г. американским центром «Пью» (Pew Research Center) в 30 странах мира исследование свидетельствует, что в настоящее время в среднем 38 % населения, проживающего в данных государствах, воспринимает Соединенные Штаты в качестве угрозы, тогда как в 2013 г. этот показатель равнялся 25 %. В целом за прошедшее пятилетие общественное отношение к Америке ухудшилось в 21 стране мира из 30, где проводились исследования[451].

Специалисты связывают ухудшение отношения мировой общественности к США с непрекращающимся американским вмешательством во внутренние дела других государств. Об этом, в частности, свидетельствует то, что восприятие американской внешней политики особенно изменилось после не санкционированных Советом Безопасности ООН военных ударов по территории Сирийской Арабской Республики; выхода Америки из многих международных соглашений; развязывания новых витков торговой войны с КНР и традиционным партнером США – Евросоюзом. Причем неодобрение проводимым курсом нынешнего главы Белого дома выражают, помимо общественности зарубежных стран, и сами американцы, которые считают, что под руководством Трампа Америка может быть втянута в международный конфликт[452].

---

[450] America's Role in the Indo-Pacific // The Perth USAsia Centre. 2017. May. URL: http://perthusasia.edu.au/getattachment/Our-Work/America-s-Role-in-the-Indo-Pacific/PU-20-ARIP-BOOK-WEB-(1).pdf.aspx?lang=en-AU (дата обращения: 23.05.2018).

[451] Globally, more people see U.S. power and influence as a major threat // Pew Research Center. 2017. August 1. URL: http://www.pewresearch.org/fact-tank/2017/08/01/u-s-power-and-influence-increasingly-seen-as-threat-in-other-countries/ (дата обращения: 07.03.2018).

[452] См.: The Iraq War continues to divide the U.S. public, 15 years after it began // Pew Research Center. 2018. March 19. URL: http://www.pewresearch.org/fact-tank/2018/03/19/iraq-war-continues-to-divide-u-s-public-15-years-after-it-began/ (дата обращения: 17.03.2018).

Динамика отношения мировой общественности к Соединенным Штатам показывает, что при реализации Вашингтоном тех или иных внешнеполитических инициатив расчет американского истеблишмента на традиционных союзников и партнеров может быть ошибочным. Произошедшее в период пребывания у власти в США Д. Трампа резкое снижение финансовой помощи США иностранным государствам (как по экономической и гуманитарной, так и по военной линиям) еще более усугубило указанные тенденции. С учетом же ориентации экс-главы Белого дома на «жесткие» (с применением военной силы) методы достижения внешнеполитических целей имидж США может не восстановиться до приемлемого уровня, что может быть обусловлено в том числе многовекторными усилиями Пекина утвердиться в качестве благонадежного торгового и экономического контрагента во взаимодействии с партнерами и союзниками Вашингтона.

В целом ситуация свидетельствует, что в настоящее время рост симпатий к России в мире контрастирует с ухудшением отношения к Соединенным Штатам. В данном контексте представляется важным комплексное наращивание усилий по закреплению позитивного образа политики России в мире. Примечательно в этом плане высказался российский ученый-международник М.А. Хрусталёв, когда вводил в научный оборот понятие «сознательное влияние»: «Говоря о влиянии, необходимо сделать некоторое уточнение. Оно может быть стихийным или сознательным. Первое есть продукт наличия материальных ресурсов, так как сила и богатство оказывают влияние уже самим фактом своего существования. Однако стихийное влияние не поддается регулированию и в лучшем случае принуждает, то есть потенциально содержит в себе угрозу. В отличие от него сознательное влияние убеждает»[453].

В складывающихся обстоятельствах Российской Федерации целесообразно использовать момент для наращивания такого «сознательного влияния» – экономического, военного, дипломатического, культурного, особенно в странах,

[453] *Хрусталев М.А.* Анализ международных ситуаций и политическая экспертиза: очерки теории и методологии. М.: НОФМО, 2008. С. 59.

где оценка внешней политики Белого дома последовательно ухудшается. Важным представляется более активное участие российских неправительственных организаций и средств массовой информации в формировании позитивного общественного мнения за рубежом о политике нашей страны, ее традициях и культуре. В целом позитивным шагом в этом контексте является привлечение максимально большого числа субъектов информационного противоборства (не только государств, но и региональных организаций, транснациональных корпораций, медиа-корпораций и пр.) к развитию диалога с Москвой.

Одновременно стоило бы проработать возможность наращивания численности подготовленных российских кадров для продвижения в штат международных организаций. Не следует исключать и обращение к позитивным аспектам зарубежного опыта ведения публичной дипломатии в условиях цифровой среды, который может существенно усилить потенциал России в данной области. Именно проактивный подход, отражающий реальные тенденции в мировом общественном мнении и опережающий в своем замысле концептуальные основы вероятных противников РФ, поспособствует утверждению позиций России в стратегически важных регионах мира.

Противодействие вызовам и угрозам, связанным с переносом информационного противоборства в нерегулируемую правом плоскость

Скоординированная деятельность отдельных акторов мировой политики по дискредитации России (в частности государств трансатлантического сообщества), существенно активизировавшаяся в последнее время, является следствием изменения концептуального подхода к обеспечению национальной безопасности в информационной сфере Соединенных Штатов Америки. С развитием прорывных информационно-коммуникационных технологий Белый дом окончательно избрал курс на агрессивную политику в области информационной сфере. Со временем это отразилось и на переоценке американцами угроз, исходящих из кибернетического пространства.

В принятых администрацией Д. Трампа доктринальных документах в области обороны и безопасности Российская Федерация фигурирует как

оппонирующая Соединенным Штатам держава, препятствующая реализации замыслов Вашингтона. Так, в Стратегии национальной безопасности США, вышедшей в декабре 2017 г., внешняя политика России рассматривается в качестве угрозы американскому влиянию, ценностям и политической системе. Большое значение в документе придается противоборству в информационном пространстве и обеспечению кибернетической безопасности страны[454].

Открытая часть Национальной оборонной стратегии, опубликованной Пентагоном в январе 2018 г., предусматривает применение всего комплекса мер (военных, экономических, дипломатических и пр.) в отношении вероятных противников Соединенных Штатов для поддержания американского доминирования на мировой арене. В частности, американская военная доктрина ставит в приоритет сдерживание России и Китая, настаивая в этой связи на существенном увеличении расходов на перспективные системы вооружений. Одновременно в документе обращается усиленное внимание на ведение в перспективе боевых действий в киберпространстве (и космосе). В среднесрочной перспективе предполагается завоевание безусловного технологического превосходства в данной сфере над возможными противниками США[455].

В новой национальной стратегии кибербезопасности Соединенных Штатов, опубликованной в сентябре 2018 г., прямо указывается, что американцы планируют в противостоянии с вероятными противниками придерживаться «проактивных оборонительных действий» (так называемой концепции передовой обороны) даже в ситуациях, не требующих вмешательства третьей стороны, исходя из норм и принципов международного права. Кроме того, что в целях предотвращения и сдерживания «злонамеренной деятельности» против США, их союзников и партнеров, а также для реагирования на таковую американские власти декларируют готовность использовать все доступные средства, в том числе

---

[454] National Security Strategy of the United States of America // Whitehouse. 2017. December. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 22.01.2018).

[455] Summary of the 2018 National Defense Strategy // US Department of Defense. 2017. December. URL: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (дата обращения: 22.01.2018).

дипломатические, информационные, военные (кинетические и кибернетические), финансовые, юридические, разведывательные механизмы и прибегать к публичной атрибуции кибератак.

В целом, налицо окончательный разворот стратегической парадигмы Соединенных Штатов по обеспечению национальных интересов в информационной сфере, свидетельствующий о переходе от оборонительных к наступательным действиям по обеспечению преимуществ в процессах информационного противоборства. Данный тезис зафиксирован во всех стратегических документах, принятых в президентство Д. Трампа. Актуальные тенденции политики Белого дома на российском направлении закрепляют указанный тезис на практике, а настроения вашингтонской элиты оставляют мало надежд на благоприятные перспективы российско-американских отношений.

В настоящее время под эгидой военного ведомства и Государственного департамента в сотрудничестве с иными министерствами и ведомствами правительства США разработан всеобъемлющий план противодействия «угрозе вредоносного воздействия со стороны Российской Федерации», включая перечень действий:

1) по осуществлению атрибуции, обороне и противодействию гибридным операциям;

2) по сдерживанию и (при необходимости) проведению ответных действий на вредоносную активность РФ в киберпространстве;

3) по идентификации и обороне от информационных операций в СМИ и социальных сетях.

Важная роль в руководстве, синхронизации и координации усилий правительства США по выявлению и противодействию пропаганде и дезинформации со стороны РФ (а также правительств иных государств и негосударственных структур) отводится Центру глобального взаимодействия, созданному в 2017 г. Государственным департаментом при содействии Пентагона.

Озабоченность вызывает сопряжение США с деятельностью Североатлантического союза, также принявшего на вооружение наступательную

стратегию достижения информационного превосходства над противником, прежде всего РФ. Организации Североатлантического договора предусматривает широкий спектр операций информационно-психологического воздействия в мирное и военное время. НАТО активно реализует комплекс мер по размыванию государственных интересов России в информационной сфере. Тем не менее, исходя из многочисленных принятых концепций, стратегий, доктрин передовиками достижения военно-политических целей посредством цифровых технологий будут, видимо, непосредственно американцы.

Одновременно и другие государства, причем даже относящихся к «развивающимся» на мировой арене, прилагают усилия к развитию оборонительных и наступательных возможностей ведения боевых действий в кибернетическом пространстве. Так, на современном этапе киберпространство и передовые технологии, акцентируемые Китаем в ходе реализации Цифрового шелкового пути, во многих отношениях слабо регулируются правовыми нормами. Ввиду их недавнего появления и форсированного совершенствования на данные сферы деятельности практически не распространены «жесткие», обязательные для исполнения положения международного права (в ряде случаев применяются так называемые мягкие нормы, вытекающие из конвенций, деклараций и пр.). Соответственно, Китай предпринимает усилия по продвижению своих национальных интересов посредством разработки «правил поведения» в области цифровой дипломатии и управления интернетом. Фактически политика Поднебесной сводится к созданию международных норм, соответствующих китайской концепции будущего, в том числе цифрового, мира.

В частности, КНР, как и Россия, отстаивает концепцию кибернетического суверенитета как организующего международного принципа управления процессами в интернет-среде. Китайское правительство трактует понятие киберсуверенитет как право отдельного государства избирать свой собственный путь развития кибернетической сферы, определять модель ее регулирования и государственной интернет-политики, а также участвовать в международном управлении киберпространством на равноправной основе. Как декларируется, ни

одна страна не должна стремиться к гегемонии в кибернетическом пространстве, вмешиваться во внутренние дела других государств, осуществлять, поддерживать кибердеятельность, подрывающую суверенитет других стран, или потворствовать таковой[456].

В целом подход КНР и России резко контрастирует с позицией США и их союзников, которые выступают за так называемый открытый интернет, менее подверженный регулированию. Западные страны поддерживают «распределенную модель управления интернетом», согласно которой в данном процессе участвуют технические органы, частный сектор, гражданское общество и государственные органы. Пекин, напротив, настаивает на государственно-ориентированном управлении процессами в киберпространстве[457].

Китай с успехом использует многосторонние институты, в том числе ООН, для продвижения своего видения кибербезопасности и киберсуверенитета. С 2014 г. КНР регулярно принимает у себя участников Всемирного интернет-форума для обсуждения проблем и перспектив развития всемирной информационно-коммуникационной сети. Кроме того, в последние годы Пекин активизирует дипломатические усилия по формированию международных кибернетических норм с опорой на группы правительственных экспертов ООН, что играет важную роль в усилиях Пекина по экспорту его концепции управления интернетом за рубеж. Распространение «модели ограниченного интернета» осуществляется им посредством разработки соответствующего законодательства, информационных систем, технологий и мониторинга нововведений. России важно ен отставать от этой деятельности, более того, превентивно формулироватьь идеи в области [458].

---

[456] International Strategy of Cooperation on Cyberspace // Ministry of Foreign Affairs of the People's Republic of China. 2017. March 1. URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (дата обращения: 01.02.2020).

[457] *Adee Sally.* The Global Internet is Disintegrating – What Comes Next? // BBC. 2019. May 15. URL: http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-next (дата обращения: 01.02.2020).

[458] *Nossel Suzanne.* Google is Handing the Future of the Internet to China // Foreign Policy. 2018. September 10. URL: https://foreignpolicy.com/2018/09/10/google-is-handing-the-future-of-the-internet-to-china/ (дата обращения: 03.02.2020).

С учетом отсутствия в настоящее время минимального корпуса международно-правовых мер по урегулированию инцидентов в киберпространстве, выход на боевые мощности данных структур может означать начало нерегламентированной конкуренции по наращиванию потенциала сил и средств для ведения информационного противоборства. Это обусловлено тем, что именно в социальных сервысах интернета зарождается новая идеология. Как полагают в этой связи американские эксперты, «борьба между либеральной демократией и цифровым авторитаризмом будет определяющей чертой XXI в., подобно тому как предыдущие периоды соперничества великих держав характеризовались конкуренцией политических идеологий»[459].

Процессы, обусловленные обострением конкуренции за сохранение доминирующего положения США в глобальной информационно-коммуникационной сети, ознаменованы также тем обстоятельством, что сегодня в мировую политику вовлечены так называемые акторы вне суверенитета. К таковым, безусловно, можно отнести военно-политические блоки, коалиции государств, террористические и экстремистские организации; хакерские и хактивистские группы; СМИ, неправительственные организации; коммерческие организации; блогеры и пр. Особую опасность в этом контексте, по мнению специалистов, представляет деструктивная преступная деятельность экстремистских и террористических группировок при том, что масштабы и интенсивность вовлечения таких субъектов в механизм информационного противоборства в последние годы все более усиливается.

С учетом изложенного российской стороне, как представляется, стоило бы обращать больше внимание на налаживание между государствами диалога по правовому регулированию процессов, развивающихся в кибернетическом пространстве. Готовность России к позитивному взаимодействию в указанной сфере, планомерно демонстрируемая на крупных форумах, способствовала бы

---

[459] *Wright Nicholas.* How Artificial Intelligence Will Reshape the Global Order // Foreign Affairs. 2019. July 10. URL: https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order?cid=nlc-fa_twofa-20180802 (дата обращения: 02.02.2020).

утверждению в мировом политическом сообществе более ответственного отношения к новым вызовам и угрозам, связанным с развитием технологий, находящихся пока в «серой зоне» международного права.

В этом контексте целесообразно учитывать, что на международном уровне остается открытым и вопрос о том, может ли кибернетическая атака квалифицироваться как «вооруженное нападение». По мнению экспертов ООН, в отношении информационно-коммуникационных технологий как средства ведения боевых действий, а также киберпространства как принципиально новой среды, возможность применения существующего корпуса норм международного гуманитарного права и права вооруженного конфликта неочевидна. Как отмечают специалисты, буквальное применение существующих базовых норм невозможно в силу технологической специфики инновационных технологий, применяемых в информационном противоборстве. Между тем в «Таллинском руководстве» НАТО указывается на использование в информационном пространстве тех же норм права, что и в любом другом – морском, воздушном и наземном.

Кроме того, концепция Устава ООН относительно «применения силы» не охватывает действия террористов и других негосударственных субъектов, которые часто стоят за нынешними актами киберагрессии. Причем эффективная адаптация международного законодательства к ведению боевых действий в новом информационном пространстве с участием как легитимных, так и нелегитимных акторов мировой политики не осуществляется во многом из-за позиции Вашингтона.

Стремясь избежать применения международного права к информационно-коммуникационной среде, США придерживаются толкования норм, обычаев и принципов, не накладывающего на государства дополнительных обязательств. В частности, это касается международного сотрудничества в области предотвращения использования информационно-коммуникационных технологий в военных целях, а также взаимодействия в целях предотвращения преступной, в том числе террористической, деятельности.

Соглашаясь с признанием обязанности по предотвращению использования своей территории для совершения международно-противоправных деяний с использованием современных технологий, американцы не видят смысла договариваться об установлении границ зон ответственности государств в цифровой среде. Такую же позицию США занимают в отношении процедуры объективизации данных при нарушении странами международных обязательств, порядка расследования международных инцидентов в информационно-коммуникационном пространстве на основе взаимодействия национальных групп реагирования на инциденты в области информационной безопасности.

Указанный выше подход развязывает Вашингтону руки в том, что касается бездоказательного обвинения России в дезинформировании мировой общественности, осуществлении кибератак, ведении онлайн-пропаганды и пр. В целом отсутствие минимального корпуса международно-правовых норм, регулирующих процессы в информационном пространстве, серьезно затрудняет для Российской Федерации обоснование ее непричастности к электоральным процессам на Западе. Как результат, там антироссийская риторика стала самодостаточной и успешно воспроизводит себя даже в отсутствие новых информационных поводов.

Соответственно, российской стороне следует последовательно акцентировать внимание на том, что агрессивный характер стратегических установок американского военно-политического руководства по достижению доминирования в киберпространстве представляет угрозу международной информационной безопасности, поскольку реализация такого подхода в практике международных отношений сопряжена с латентным или открытым применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе для осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета отдельных стран.

Кроме того, России, выступающей в качестве ответственного актора мировой политики, целесообразно настаивать на развитии международного диалога в борьбе с киберугрозами. Такая позиция, планомерно транслируемая в

массы и на крупных форумах, поспособствовала бы укреплению международного авторитета нашей страны как державы–миротворца.

В настоящее время деятельность в борьбе с киберпреступностью международным законодательством регламентирована слабо. Юридическим полем не охвачена в полной мере такая актуальная угроза, как хакерские атаки в интернете. В этом плане национальным интересам России соответствовало бы усиление взаимодействия с крупным государствами – прежде всего США и КНР – по снижению рисков, исходящих из кибернетического пространства. Предметами взаимодействия могли бы стать, как минимум, безопасность объектов критической инфраструктуры, борьба с хакерскими и хактивистскими атаками. Кроме того, можно было бы призвать открытые к диалогу страны к инициативе РФ о криминализации изготовления вредоносного программного обеспечения. Это позволило бы постепенно перевести борьбу с рисками в данной области на международную правовую основу, в том числе посредством создания гарантий безопасности информационно-коммуникационных технологий. В контексте того обстоятельства, что из Америки исходит целый спектр угроз безопасности РФ в рассматриваемой сфере, наши инициативы о взаимодействии, по возможности, целесообразно было бы доводить до мировой общественности.

Важным выглядит также активизация работы групп правительственных экспертов ООН, уже имеющих в своих наработках своеобразный «киберкодекс», но не сумевших в 2017 г. найти возможности для развития диалога. В качестве приоритетных мер развития взаимодействия на этом уровне выглядит выработка правил ответственного поведения государств в информационном пространстве и согласование механизмов предотвращения эскалации межгосударственных киберконфликтов.

В целом, в условиях, когда опасности и угрозы России в информационной сфере во многом определяются недостаточным международно-правовым контролем над положением в этой области, важным представляется концентрация усилий РФ и ее партнеров на предотвращении использования преимуществ цифровых технологий для достижения военных целей. Соответственно, требуется

более активно противостоять такой деятельности. Интересам Российской Федерации соответствовала бы проработка в ООН вопроса по подготовке правового акта, который регулировал бы порядок взаимодействия государств в борьбе с киберпреступностью и отвечал характеру современных угроз. Не менее важным представляется вопрос о единой интерпретации ключевых понятий существующей системы международного права, включая такие, как «использование силы» и «агрессия», с точки зрения более точной квалификации действий с применением информационно-коммуникационных технологий.

В стратегическом плане России целесообразно добиваться выработки комплексного обязательного для соблюдения режима ответственного поведения государств в сфере использования цифровых технологий. Его можно было бы зафиксировать в форме конвенции Организации Объединенных Наций либо обязывающего международного договора, открытого для присоединения всех стран и содержащего в себе механизмы верификации выполнения принятых обязательств.

Противодействие вызовам и угрозам в информационной сфере, связанным с форсированным технологическим прогрессом

В последнее пятилетие проявились два совершенно новых тренда использования технологий искусственного интеллекта в качестве оружия, угрожающего стабильности даже устойчивых к внешним информационно-психологическим воздействиям социальных систем.

Первый тренд – использование систем искусственного интеллекта на основе распределенных сетей и вычислительных ресурсов для решения задач управления в условиях плотной социальной и информационной среды.

Второй тренд тесно связан с первым, и его можно обозначить как военное применение информационно-аналитических платформ в сочетании с новейшими технологиями социальной, информационной и психологической войны.

Указанные тренды актуализированы в связи с тем, что в условиях трансформации миропорядка некоторые государства делают ставку на достижение технологического прорыва как на предпосылку своего дальнейшего

доминирования на международной арене. Это сопровождается ускоренным внедрением любых перспективных технологий в практическую деятельность, особенно в отраслях, которые определяют национальную мощь и влияние. Например, с подачи Вашингтона искусственный интеллект, кибернетическая и квантовая техника начинают непосредственно или опосредованно применяться в подготовке и отработке хода военных конфликтов будущего.

На базе масштабных социально-психологических исследований создаются соответствующие методики, позволяющие получить информацию об убеждениях, настроениях, поведении отдельных социальных групп с целью в перспективе смоделировать развитие социально-политической обстановки в отдельном районе, стране или регионе. Разработан ряд современных информационно-аналитических платформ, позволяющих более эффективно реализовывать идею сетецентрической войны.

В данных условиях управление социальными массами, анализ и моделирование социально-политических процессов вышли на совершенно новый уровень. В государствах трансатлантического сообщества создаются регулярные воинские формирования, специализирующиеся на информационных, психологических и кибероперациях. Разворачивающаяся технологическая гонка подталкивает военно-политическое руководство западных стран (прежде всего США) к ускоренному концептуальному обновлению национального и отчасти международного законодательства с дальней целью «подгонки» создаваемых правовых норм и принципов к их конкретным нуждам, диктуемым заботой о собственном превосходстве. Это весьма опасное явление с точки зрения поддержания международной безопасности, поскольку может нанести непоправимый урон стратегической стабильности.

Следует отметить, что упорно игнорируется тот факт, что имеющиеся у Вашингтона разработки по формированию общественного мнения и моделированию социально-политической обстановки посредством информационно-коммуникационных технологий всё чаще используются для реализации национальных интересов Америки в ущерб другим странам. Ввиду

нелдавнего появления таких технологий и недостаточной изученности последствий их использования подобная практика пока не охвачена международным гуманитарным правом.

С учетом все более активного включения в процессы информационного противоборства субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, повышаются риски разработки программ на базе искусственного интеллекта негосударственными акторами мировой политики. Повышается вероятность задействования таких программ в террористических и экстремистских целях в государствах и регионах мира с повышенной степенью социальной и психологической напряженности.

В среднесрочной перспективе операции информационно-психологического воздействия с использованием разнообразных технологий на базе искусственного интеллекта станут, вероятно, важным инструментом в арсенале американского военно-политического руководства. Их применение наращивается с разработкой и апробированием новых методик исследования и моделирования социально-политической обстановки. Цель американских стратегов остаётся прежней: изучать, чтобы контролировать; контролировать, чтобы управлять.

Например, в условиях цифровой реальности, когда все больше людей стали получать информацию из соцсетей, зависимых от пользователей, генерирующих нередко нефильтруемый контент, сфальцифицированные фото, аудио и видеозаписи могут распространяться очень быстро. Этому способствует то обстоятельство, что интернет-платформы подвержены эффекту «информационных каскадов», когда люди делятся информацией, не заботясь о ее подлинности, и из-за массовых репостов информация кажется надежной. Но нельзя исключать и того, что применение глубоких фейков спровоцирует появление так называемого дивиденда лжеца, когда людям будет проще подвергнуть сомнению реальные факты, апеллируя к их ложности.

Можно говорить о целесообразности противодействия новым разрушительным технологиям на базе искусственного интеллекта с учетом комплекса мер информационного, технологического и правового характера.

В качестве приоритетных мер представляются целесообразными:

– модернизация типовых алгоритмов информационного реагирования на распространение ложной информации с учетом особенностей угроз цифровой реальности;

– упредительное информирование общественности о новых технологиях на базе искусственного интеллекта, в том числе технологии фальсификации изображений;

– ознакомление с новыми технологиями воздействия на массовое сознание сотрудников правоохранительных органов РФ, равно и как иных государственных структур, которые могут столкнуться с последствиями применения таких технологий в профессиональной деятельности.

– разработка программно-технических средств и компьютерных криминалистических методик обнаружения признаков искажения фото/видео/аудио контента;

– стимулирование платформ социальных медиа предпринимать дополнительные усилия для выявления и удаления фальшивого контента;

– специальная криминализация либо закрепление гражданско-правовой ответственности действий, связанных с созданием глубоких фейков;

– ограничение доступа к информационным ресурсам интернета, которые распространяют фальшивый контент.

Вместе с тем, как представляется, помимо негативного смысла целесообразно обратить внимание и на позитивный потенциал применения подобных инновационных технологий на базе искусственного интелдлекта, в частности машинного обучения. В подобном ракурсе можно рассматривать и такие алгоритмы, как «Куил» (*Quill*), «Вордсмит» (*Wordsmith*) и «Хелиограф» (*Heliograf*), которые важно активнее использовать в многочисленных сферах жизнедеятельности человека – финансовой, здравоохранительной, военной,

духовной и пр. Они практически мгновенно преобразовывают статистику, таблицы данных, информацию в текстовые документы приемлемого качества[460].

Вероятно, по принципу глубоких фейков можно создать обучающие программы в области социально-гуманитарных дисциплин, в частности истории. С учетом того, что фото и аудио исторических деятелей присутствуют в архивах и интернете, из этого могла бы получиться образовательная технология. Человек, тем более ребенок, мыслит образами, лучше воспринимает невербальную информацию и подвержен сенсационности. В этом контексте технологии искусственного интеллекта могут иметь большие возможности.

Ускорение технологического прогресса диктует целесообразность проведения прикладных исследований в области социально-гуманитарных наук, которые способствовали бы более глубокому пониманию влияния новой информационной среды на социальные и политические процессы как в России, так и за рубежом. Необходимо сконцентрировать усилия и на изучении потенциального противника и развитии автоматизированных систем исследования и моделирования социально-политической обстановки. В качестве меры противодействия прогнозную аналитику могут использовать и отечественные государственные и наднациональные органы для предотвращения социальной напряженности (своевременного принятия социальных, экономических и политических мер, направленных на достижение стабильности в долгосрочной перспективе).

Необходимо поставить на повестку дня ООН вопрос о разработке эффективного механизма межгосударственного сотрудничества, направленного на предотвращение и минимизацию последствий злонамеренного использования искусственного интеллекта. Скорее всегно, сделать это будет крайне непросто, но важно, причем в достаточно сжатые сроки. Это обусловлено тем обстоятельством, что удержать технологии искусственного интеллекта двойного назначения в

[460] См.: Automated Insights and AP Increase Trading of Forgotten Firms // Automated Insights 2016. URL: https://automatedinsights.com/blog/automated-insights-and-ap-increase-trading-of-forgotten-firms/ (дата обращения: 21.10.2019).

рамках только национальной юрисдикции и контроля представляется практически невозможным в условиях повсеместного распространения интернета, социальных сетей, мобильной связи и пр.

На государственном уровне целесообразно обеспечивать своевременную подготовку специалистов, по своим компетенциям способных включиться в деятельность в указанной сфере[461]. Причем российским экспертам нужно стать передовиками в развитии фундаментальных и прикладных исследований в области искусственного интеллекта. В этом контексте можно было бы предусмотреть научные обмены, участие российских исследователей в российских и международных конференциях и пр. Это крайне важно в целях минимизации негативных возможных последствий для российских граждан, связанных с рисками отставания РФ от ведущих государств в рассматриваемой сфере.

В целом сумма новых технологий, накопленных только к настоящему времени, уже требует качественных изменений в российском обществе на уровне государственных и общественных институтов. Любая неопределенность, колебания, отсрочка назревших решений и, главное, отсутствие стратегического видения и соответствующих действий будут играть на руку асоциальным акторам информационного противоборства, нередко располагающим в своем арсенале колоссальным разрушительным потенциалом.

[461] См.: *Марченков В.И., Цибиков В.А.* О реализации возможностей сети интернет и программных средств в информационно-пропагандистской работе с военнослужащими / В.И. Марченков, В.А. Цибиков // Мир образования – образование в мире. 2015. № 3 (59). С. 197–204.

ЗАКЛЮЧЕНИЕ

На основе системного подхода, обобщения опыта зарубежных и отечественных трудов, посвященных информационному противоборству в политическом процессе, в диссертации выявлены и раскрыты тренды в сфере информационного противоборства, обусловленные форсированной цифровизацией. Теоретически обоснованы вероятные политические последствия и риски применения цифровых технологий в информационном противоборстве в контексте динамики современных социально-политических и военно-политических процессов.

В ходе диссертационного исследования подтверждена научная гипотеза, согласно которой при наращивании нелинейности развития современных мирополитических процессов можно ожидать существенного усиления социально-политических рисков с последующим утверждением «обществ риска», когда процессы трансформации мирового порядка могут приобрести существенно более скоротечный характер, а цена таких изменений может оказаться крайне высокой (вплоть до перетекания в «динамический хаос»), несмотря на использование участниками мировой политики прежде всего невоенных методов противоборства.

По итогам проведенного исследования представляется возможным сделать ряд выводов:

1. Деятельность в области информационного противоборства люди практикуют с глубокой древности. С появлением государства информационное противоборство утверждалось в качестве части межстрановых отношений не только в военное, но и в мирное время, являясь особым аспектом взаимодействия государственной власти с внутренними общественными силами, иногда выступающими в качестве ее противника. Первым военным столкновением, где целенаправленно и масштабно были использованы средства и методы информационно-психологического воздействия стала Первая мировая война. Уже к окончанию Второй мировой войны значительный практический опыт и

теоретическое осмысление ведения информационного противоборства позволило специалистам англосаксонских стран начать массированное информационно-психологическое воздействие на население Советского Союза. Создание оружия массового уничтожения поспособствовало разработке различного рода невоенных концепций ведения боевых действий. В свете процессов цифровизации появились принципиально новые методы и технологии информационного воздействия.

Соответственно, с течением времени деятельность политических субъектов в сфере информационного противоборства уверенно становится доминантой политических процессов новой мировой реальности. Цифровые технологии являются важным фактором развития современных политических процессов. В свете стремительных процессов цифровизации беспрецедентная доступность информации сочетается со столь же беспрецедентным ее переизбытком. Это обусловливает качественно новую декомпозицию отношений между властью и обществом, что существенно повышает уровень социально-политических рисков развития государства, прежде всего в сфере информационной безопасности.

2. Феномен информационного противоборства в политическом процессе отличается рядом характеристик:

– информационное противоборство в политическом процессе имеет латентный характер, поскольку оно представляет собой совокупность относительно самостоятельной скрытной деятельности политических субъектов (государств и их коалиций, а также социальных институтов, слоев и групп, политических лидеров) с целью упреждения намерений и подавления воли оппонирующей стороны в собственных политических интересах, которая в итоге способна вызвать как локальные, так и масштабные трансформации социально-политической системы;

– информационное противоборство как своеобразная форма протекания политических изменений на пересечении самых разнообразных сфер жизни общества (экономической, политической, социальной и духовной) обладает не только собственной ритмикой (повторяемостью), но и достаточно высокой степенью динамизма, отличающей его среди других политических процессов;

–в политическом пространстве информационного противоборства присутствует большое количество самых разнообразных политических акторов (легитимных и нелегитимных), обладающих собственными ресурсами трансформации политической системы, сочетание которых лишает процесс информационного противоборства строгой устойчивости в отличие от некоторых других политических процессов (например, избирательного процесса);

– процесс информационного противоборства реализуется как результирующая сумма политических воль, но в основном посредством соответствующих нормативно определенных технологий и процедур действий. Развитие процесса информационнного противоборства можно прогнозировать, но при наличии своевременной и достоверной информации о намерениях и планах участвующих в нем конкретных субъектов, применяющих привычные и чаще всего регламентированные способы и приемы деятельности.

По основанию объектного поля воздействия и защиты информационное противоборство включает в себя две основные составляющие: информационно-психологическую и информационно-техническую. Информационно-психологическое воздействие интегрирует совокупность информационных операций, связанных с воздействием на психику человека и общественное сознание. Информационно-техническое воздействие предполагает оказание влияния на разнородные информационно-технические системы: системы передачи данных, системы защиты информации, радиоэлектронную борьбу. По канонам политических установок большинства государств на современном этапе мирового развития информационное противоборство ведется в форме информационно-психологического воздействия в тесном взаимодействии с методами информационно-технического воздействия, особенно в период вооруженного конфликта.

В настоящее время среди разнообразных участников мировой политики деятельность по осуществлению информационных операций в рамках информационного противоборства наиболее полно регламентирована в

нормативно-правовых актах Североатлантического альянса, а также в национальном законодательстве входящих в него стран.

3. Социум практически любого государства окружен прорывным развитием инноваций, применимых для влияния на массовое сознание и формирования общественного мнения в условиях цифровой реальности. Это способствует установлению вневременной и трансграничной коммуникативной реальности, где ложная информация тесно переплетается с правдивой. Однако при всех объективных достоинствах применения цифровых технологий в интересах субъектов информационного противоборства вопросы развития цифровой дипломатии на практике целесообразно рассматривать в контексте рисков и угроз. Такие процессы, как показывают теоретические наработки и политическая практика, могут служить предпосылкой перетекания массового стихийного поведения из виртуального пространства в реально существующую социально-политическую плоскость. На повестке дне ученых и государственных деятелей возникают вопросы об осмыслении возникновения и развития социальных движений в условиях цифровой среды, а также управлении такими процессами.

В условиях утверждения цифровой реальности применение потенциала информационно-коммуникационных технологий и больших данных обусловливает большие возможности прогнозирования развития политических процессов, однако макросоциальные последствия такого подхода пока изучены недостаточно. В связи с этим усиливается значимость проведения фундаментальных политологических исследований в рамках указанной проблематики. Кроме того, повышается важность цифровой дипломатии, которая в условиях трансграничной цифровизации социально-политической жизни особенно эффективна как ресурс внешнеполитического ведомства. Наиболее успешно адаптировали информационное обеспечение государственной политики внутри страны и на внешней арене к условиям новой цифровой социально-политической реальности развитые западные государства.

4. В последнее время увеличивается состав политических акторов, являющихся одновременно и субъектами информационного противоборства,

которые связаны с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности. В условиях усиления геополитической конкуренции между ослабевающими и возвышающимися центрами силы ясно обозначается и соперничество между всеми акторами мировой политики за завоевание технологического лидерства в том числе в деле создания и апробирования на практике инновационных средств и методов информационной борьбы.

Использование легитимными и нелегитимнгыми акторами мировой политики информационно-коммуникационных технологий в военных и политических целях связывается в большинстве стран мира с серьезными угрозами национальной безопасности, при том что международно-правовые рамки в этой сфере формируются с заметным отставанием. Следствием этого является подрыв эффективности механизмов, сдерживающих применение силы, при одновременном повышении вероятности ее использования нетрадиционными методами, что ведет к разбалансировке самого каркаса миросистемы, ослабляет ее устойчивость.

В перспективе информационное воздействие в интернете (особенно в социальных медиа), скорее всего, станет все активнее практиковаться государствами, их прокси-силами, а также другими негосударственными акторами для достижения политических целей. При этом субъекты информационного противоборства, безусловно, учитывают, что современная информационно-коммуникационная реальность обладает большим аддитивным потенциалом, то есть, значительным риском возникновения зависимости. В этой связи обеспечение безопасности личности, общества и государства будет, видимо, становиться все более сложной, взаимосвязанной и многоаспектной деятельностью.

5. По мере достижения качественных прорывов в области современных цифровых технологий отдельные государства и негосударственные акторы мировой политики апробируют новые методики, направленные на изучение социума с целью определения доступности, уязвимости и восприимчивости к

поведенческому и установочному воздействию извне. В последние годы активно создаются регулярные воинские формирования, специализирующиеся на информационных, психологических и кибероперациях.

На базе масштабных политологических исследований разрабатываются соответствующие технологии, позволяющие моделировать развитие социально-политической обстановки в отдельном районе, стране или регионе на основе информации об убеждениях, настроениях, поведении людей в глобальной сети. К настоящему времени созданы технологические условия для манипулирования социальным поведением в условиях цифровой реальности. В ряде стран мира апробируются информационно-аналитические платформы по мониторингу и моделированию социально-политического пространства в предполагаемой стране-мишени.

Совершенствование практик в области информационного противоборства свидетельствуют об общем возрастании значения «нелинейных» методов достижения превосходства над потенциальными противниками в ходе подготовки к ведению противоборства в современных условиях цифровизации социально-политической жизни. В этом контексте углубленное изучение всего комплекса проблем, связанных с современными информационно-коммуникационными технологиями. Немаловажной представляется задача по обеспечению межведомственной стандартизации военно-политических и военных терминов, включая согласование четкого определения гибридной войны и ее составляющих. Это необходимо для изучения новых форм и способов межгосударственного противоборства, разработки эффективных способов противодействия им, составления сценариев развития военно-политической обстановки в важнейших регионах мира.

6. Политическая динамика последних лет способствует и смещению акцентов в деятельности государственных ведомств, связанной с совершенствованием национальной системы информационного противоборства. Например, в Вашингтоне отмечают, что переоценка приоритетов в указанной сфере связана с усилением противостояния США с Китаем и Россией, а также

набирающей обороты технологической революцией, которая, по мнению ученых и политиков, будет оказывать все возрастающее влияние на все сферы жизнедеятельности общества. В американских документах по обеспечению национальной безопасности все более важная роль отводится достижению военно-политических целей в информационной сфере и, в частности, киберпространстве. С целью обоснования наращивания собственных информационно-коммуникационных возможностей Вашингтон и его союзники апеллируют к якобы ведущейся деятельности своих вероятных противников (Китая, России, Ирана), одновременно блокируя принятие четких правовых норм в данной области.

Указанная тенденция не может не вызывать глубокую озабоченность в свете продвигаемых отдельными странами попыток на международном уровне утвердить примат концепции неизбежного возникновения конфликтов в информационном пространстве. Беспокойство в данной связи вызывает то обстоятельство, что в стремлении обеспечения лидерства в использовании достижений цифровых технологий Вашингтон не поддерживает полноценного международного сотрудничества для предотвращения использования информационно-коммуникационных технологий в военных целях, а также взаимодействия в целях предотвращения преступной, в том числе террористической, деятельности. Очевидно, что такой подход не способствует поддержанию информационной безопасности ни Соединенных Штатов, ни тем более других государств международного сообщества. Опасность многократно возрастает в условиях отсутствия минимального корпуса норм международного права, регламентирующего использование информационно-коммуникационных технологий в военных целях.

7. Ориентация отдельных государств мира на технологическое лидерство усиливает межгосударственную конкуренцию, форсируя размывание нынешнего формата миропорядка. В частности, применяемые США агрессивные методы обеспечения своего технологического превосходства с целью удержания позиций мирового лидера могут встретить жесткий отпор отдельных членов мирового

сообщества. В авангарде противостояния окажется, скорее всего, Пекин, не намеревающийся уступать Вашингтону в развертывающейся глобальной геополитической схватке. Конфронтационному развитию событий будут, видимо, способствовать накапливающиеся противоречия между Соединенными Штатами и их европейскими союзниками. Последние в условиях ухудшения собственных экономических перспектив и ужесточения торгово-политического курса администрации Д. Трампа столкнутся с необходимостью активного изыскания возможностей для минимизации потерь и рисков.

Однако пока ситуация благоприятствует американцам, прежде всего ввиду выстроенной ими на государственном уровне продуманной системы приоритетов инновационного технологического развития, а также двоякости толкования или отсутствия четкого международно-правового регулирования предпринимаемых США действий. Нельзя исключать, что в перспективе избранная Соединенными Штатами стратегия позволит им выйти на принципиально новый уровень обеспечения национальной безопасности и навязать международному сообществу соответствующую их видению новую модель миропорядка.

В целом отсутствие критической массы предпосылок для успешной кооперации наиболее вероятных претендентов на активное участие в глобальном управлении делают комфортную для всех среду международного общения все менее возможной, заставляя государства выбирать в пользу одного центра силы – ослабленного, но близкого или возвышающегося, но чуждого. Данный выбор, видимо, будет сложным, поскольку, вопреки теории, ключевым разрушителем постбиполярного порядка сегодня выступает не новый претендент с глобальными геополитическими амбициями, а еще действующий гегемон, который, по идее, должен бы стремиться сохранить статус-кво нынешнего миропорядка, однако сам провоцирует его ломку. Видимо, усилия Вашингтона будут и в дальнейшем сконцентрированы на подрыве существующей системы международных соглашений в области безопасности, в том числе с целью навязывания собственных правил поведения другим государствам. Такая целеустановка объясняется наличием у США передовой технологической базы,

благоприятствующей получению односторонних инновационных преимуществ. Для Вашингтона это чрезвычайно важно в условиях, когда однополярный миропорядок стремительно движется к упадку.

8. Для отражения вызовов и угроз нового типа России важно учитывать комплекс мер, которые способствовали бы более надежному обеспечению национальной безопасности. В качестве приоритетных целесообразно предусмотреть следующие:

– совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации;

– повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности России;

– совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности России;

– создание и модернизация программно-технических средств, отвечающих современным требованиям и тенденциям развития информационных технологий;

– полноценное развитие отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научно-технических организаций по разработке, созданию и эксплуатации средств обеспечения информационной безопасности страны;

– повышение качества подготовки специалистов в области информационной безопасности;

– совершенствование структуры, развитие сил и средств военной организации государства, участвующих в обеспечении информационной безопасности.

В целом, многовекторность вызовов и угроз безопасности государства, связанных с форсированными процессами развития технологий, обусловливают важность усиления внимания военно-политического руководства страны к обеспечению ее оборонным потенциалом, способным гарантировать достижение

поставленных в Стратегии национальной безопасности целей, включая создание благоприятных условий для технологического развития России в настоящем и будущем. Учитывая актуальные аспекты развития военно-политической ситуации вокруг России, формируемой под воздействием интенсивного проведения Соединенными Штатами и их трансатлантическими союзниками мероприятий в сфере информационной борьбы, а также прорывным развитием цифровых технологий, макросоциальные, политические и социально-экономические последствия совершенствования которых пока труднопрогнозируемы, на первый план для РФ выходит необходимость консолидации усилий органов государственной власти, средств массовой информации и неправительственных организаций по реагированию на современные и перспективные угрозы безопасности в информационной сфере.

СПИСОК ЛИТЕРАТУРЫ

1. *Алексеева Т.А.* Современные политические теории. М., 2000. С. 102.
2. *Аристотель.* Соч.: В 4 т./ Пер. С древнегреч. М.: Мысль, 1983. Т. 4. 830 с.
3. *Артёмов А. А.* Эксперимент по моделированию процесса эволюции содержания информационного пространства социума (с применением мем-грамм-модели). Программная инженерия. 2016. № 7. С. 291-306.
4. *Бартош А.А.* Конфликты XXI века. Гибридная война и цветная революция: монография / А. А. Бартош. Москва: Горячая линия-Телеком, 2018. 282 с.
5. *Бек Д., Кован К.* Спиральная динамика. Управляя ценностями, лидерством и изменениями в XXI веке / Д. Бек, К. Кован. М.: Открытый Мир, 2010. 424 с.
6. *Бехтерев В.М.* Избранные труды по психологии личности: в 2 т. Т. 2: Объективное изучение личности. СПб: Алетейя, 1999. С. 169.
7. *Блауберг И.В., Юдин Э.Г., Садовский В.Н.* Системный подход // Новая философская энциклопедия: В 4-х т.М.: Мысль, 2001. Т.3. С. 560.
8. *Больц Н.* Азбука медиа. М.: Европа, 2011. С. 29, 38.
9. Бороться с инфодемией вместе // Всемирная организация здравоохранения. 2020. URL: https://www.euro.who.int/ru/health-topics/Health-systems/e-health/news/news/2020/6/working-together-to-tackle-the-infodemic (дата обращения: 17.05.2020).
10. *Брега А.В.* Политический риск в сетевом обществе: новая конфигурация // Социально-гуманитарные знания. 2018. № 3. С. 221–229.
11. *Брега А. В.* Политический риск в обеспечении военной безопасности: теория и основы управления. Дисс. докт. полит. наук. Москва, 2007. 337 с.
12. *Будылин К.Ю.* Информационное противоборство в военной сфере: политологический анализ. Дис. канд. полит. наук. М., 2009, 169 с.
13. *Ветренко И.А*. Методологические особенности изучения политических процессов // Социум и власть. 2009. С. 45–48.
14. *Виловатых А.В.* Военная политика Великобритании: фактор Brexit // Проблемы национальной стратегии. 2017. № 6 (45). С.127–144.
15. *Виловатых А.В.* Информационная война: история и современность // Наука. Культура Общество. 2011. № 4. С. 73–83.
16. *Виловатых А.В.* Информационно-психологическое воздействие на массовое сознание в условиях новой политической реальности // Свободная мысль. 2019. № 6. С. 165–177.
17. *Виловатых А.В.* Искусственный интеллект как фактор военной политики будущего // Проблемы национальной стратегии. 2019. № 1 (52).С. 177–192.
18. *Виловатых А.В.* Использование информационно-коммуникационных технологий в военно-политических целях: социально-психологический аспект // Проблемы национальной стратегии. 2018. № 2 (47). С.197–211.

19. *Виловатых А.В*. Перспективы гибридизации военных конфликтов в условиях технологической революции // Международная жизнь. 2020.№ 3. С. 90–96.

20. *Виловатых А.В.* Фактор России в развитии стратегии кибербезопасности США и их союзников // Вестник Академии военных наук. 2020. № 1.

21. *Виловатых А.В., Михеев Е.А.* Стратегические установки США и НАТО по организации и проведению операций информационно-психологического воздействия // Наука. Культура Общество. 2018. № 2-3. С. 131–143.

22. *Виловатых А.В., Хряпин А.Л.* Современные разработки в области социального управления: опыт Соединенных Штатов Америки // Информационные войны, 2019. № 4 (52). С. 45–49.

23. *Внебрачных Р. А.* Троллинг как форма социальной агрессии в виртуальных сообществах // Вестник Удмуртского университета. Философия. Социология. Психология. Педагогика. Ижевск: Удмуртский государственный университет, 2012. Вып. 1. С. 48-51.

24. Военно-политическая ситуация в Северной Европе и угрозы безопасности России // Тищенко Г.Г., Абаев Л.Ч., Николайчук И.А., Виловатых А.В., Бекман Й. Проблемы национальной стратегии. 2016. № 6 (39). С.11–38.

25. *Волкогонов Д. А.* Психологическая война. М., 1986. 86 с.; *Живейнов Н. И.* Операция «PW»: «психологическая война» американских империалистов. М., 1996. 282 с.

26. *Воронцова Л.В., Фролов Д.Б.* История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006. 192 с.

27. *Гаман-Голутвина О.* Современная сравнительная политология перед вызовами развития // Интернет-портал «Перспективы». 2020. 13 мая. URL: http://www.perspektivy.info/misl/cenn/sovremennaja_sravnitelnaja_politologija_pered_vyzovami_razvitija_2020-05-13.htm (дата обращения 20.05.2020).

28. *Гидденс Э.* Социология / Пер. с англ.; науч. ред. В. А. Ядов; общ. ред. Л. С. Гурьевой, Л. Н. Посилевича. М.: Эдиториал УРСС, 1999. 703 с.

29. *Грин Р.* 48 законов власти и обольщения / Пер. с англ. Е. Я. Мигуновой. М.: РИПОЛ классик, 2005. 736 с.

30. *Грицанов А.А., Абушенко В.Л.,* Евелькин Г.М., Соколова Г.Н., Терещенко О.В. Социология: Энциклопедия. М., 2003. С. 789.

31. *Головин Н..И*. Информационная война. М.: Мир безопасности. 1998. № 8–9 (60). С. 79.

32. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 №646).

33. Дорожная карта развития «сквозной» цифровой технологии «Технология виртуальной и дополненной реальности» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. 2019. URL: https://digital.gov.ru/uploaded/files/07102019vrar.pdf (дата обращения: 18.06.2020).

34. *Иванов В.Н.* Россия и русский мир. Экспертные суждения и оценки. М.: Академика, 2011. 112 с.

35. *Ильин М.В.* Ритмы и масштабы перемен: О понятиях «процесс», «изменение» и «развитие» в политологии // Полис, 1993. №2. С. 75–77.

36. *Ильичева Л.Е., Кондрашов А.О.* Фейковые новости и информационная война // Государственная служба. 2018. № 6. С. 77–82.

37. *Ионин Я.* Военный ИИ в США – с бюджетом, но без компромисса с Кремниевой долиной // РСМД. 2018. 21 августа. URL: http://russiancouncil.ru/analytics-and-comments/columns/military-and-security/voennyy-ii-v-ssha-s-byudzhetom-no-bez-kompromissa-s-kremnievoy-dolinoy/ (дата обращения: 10.12.2018).

38. История политических и правовых учений. М.: Инфра-М, 1996. С.80.

39. *Караяни А.Г.* Информационно-психологическое противоборство в современной войне: учебное пособие. М.: Военный университет, 1997. 64 с.

40. *Карякин В.В.* Геополитика третьей волны: трансформация мира в эпоху Постмодерна: монография. М.: Граница, 2013. С. 25–26.

41. *Кефели И. Ф.* Асфатроника: на пути к теории глобальной безопасности: монография. СПб.: ИПЦ СЗИУ РАНХиГС, 2020. С. 20.

42. *Киссинджер Г.* Мировой порядок [пер. с англ. В. Желнинова, А. Милюкова]. М.: Издательство АСТ, 2018. 512 с.

43. *Клаузевиц К.* О войне. М.: Эксмо, 2007. 861 с.

44. *Клеандрова В.М., Яковлев Л.С.* История полиции, политического сыска и контрразведки в России в XVIII – начале XX века. С. 9, 36.

45. *Козюлин В.* Три группы угроз смертоносных автономных систем // РСМД. 2018. 1 ноября. URL: http://russiancouncil.ru/analytics-and-comments/analytics/tri-gruppy-ugroz-smertonosnykh-avtonomnykh-sistem/ (дата обращения: 10.12.2018).

46. *Кокошин А.А.* Методологические проблемы прогнозирования в интересах национальной безопасости России. М.: ИВ РАН, 2014. С.33.

47. *Кокошин А.А.*О системном и ментальном подходах к мирополитическим исследованиям. Краткий очерк. 2-е изд. М.: УРСС, 2008. С.17.

48. *Комиссина И. Н.* Современное состояние и перспективы развития робототехники в Китае // Проблемы национальной стратегии. 2020. № 1. С. 123–146.

49. *Комов С. Л.* Информационная борьба в современной войне: вопросы теории // Военная мысль. 1996. № 3. С.73.

50. Конвенция об обеспечении международной информационной безопасности (концепция) // Совет Безопасности РФ. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 14.03.2019).

51. *Конрад Н.И.* Сунь-Цзы. Трактат о военном искусстве. М., 1950. 404 с.

52. *Кочубей М.А.* Современные практики деструктивного воздействия на сознание как политическая технология // Российская ассоциация международных исследований. URL: http://www.risa.ru/ru/sections/359-1-3 (дата обращения: 07.10.2019).

53. *Куньщиков С.В.* Идеология в структуре политического процесса: сущность и динамика функционирования. Дис. канд. полит. наук. Екатеринбург, 2006. 149 с.

54. *Лайнбарджер П.* Психологическая война. Теория и практика обработки массового сознания. М.: Центрполиграф, 2013. 445 с.

55. *Лассуэлл Г. Д.* Психопатология и политика: Монография. М.: Издательство РАГС, 2005. 352 с.

56. *Лассуэл Г.* Техника пропаганды в мировой войне. М., 1929. С. 139–181.

57. *Лассуэлл Г. Д.* Язык власти // Политическая лингвистика. Екатеринбург, 2006. С. 264–279.

58. *Левашов В.К.* Глобализация и социальная безопасность // Социологические исследования. 2002. № 3. С. 24.

59. *Леонгард Г.* Технологии против человека. М.: АСТ, 2018 С. 21–28.

60. *Липпман У.* Общественное мнение / Пер. с англ. Т. В. Барчунова, под ред. К. А. Левинсон, К. В. Петренко. М.: Институт Фонда «Общественное мнение», 2004. 384 с.

61. *Майка Р.* Как Трамп и фейки изменили медиа // РСМД. 2018. 4 июня. URL: https://russiancouncil.ru/analytics-and-comments/columns/united-states/kak-tramp-i-feyki-izmenili-media/?sphrase_id=28536647 (дата обращения: 14.04.2019).

62. *Макиавелли Н.* Государь / Н. Макиавелли; Пер.с итал. К.А.Тананушко. Минск: ООО «Харвест», 2004. 703 с.

63. *Мамардашвили М. К.* Превращенные формы. (О необходимости иррациональных выражений). Москва, 1990. С. 315–398/

64. *Манойло А. В*. К вопросу о содержании понятия «Информационная война» // АШПИ. URL: http://ashpi.asu.ru/ic/?p=1552 (дата обращения: 23.08.2019).

65. *Марченков В.И., Цибиков В.А.* О реализации возможностей сети интернет и программных средств в информационно-пропагандистской работе с военнослужащими / В.И. Марченков, В.А. Цибиков // Мир образования – образование в мире. 2015. № 3 (59). С. 197–204.

66. *Маслоу А.* Мотивация и личность. Санкт-Петербург: Евразия, 1999. 478 с.

67. *Мелешкина Е.Ю.* Формирование партийных предпочтений избирателей в посткоммунистических странах Восточной Европы // Выборы в посткоммунистических обществах: Пробл.-тем. сб. / Отв. ред. Е.Ю. Мелешкина. М.: ИНИОН РАН, 2000. С. 51.

68. Методические рекомендации по разоблачению фейковых обвинений в адрес ВКС России в Сирии // Война и мир. 2018. Декабрь. URL: http://www.warandpeace.ru/ru/exclusive/view/135803/ (дата обращения: 12.10.2019).

69. *Миловидов В.Д.* О черных лебедях и человеческих ошибках // Коммерсант Наука. 2017. 5 сентября. URL: https://www.kommersant.ru/doc/3396747 (дата обращения: 12.10.2019).

70. *Миловидов В.Д.* Управление инновационным процессом: как эффективно использовать информацию. Нефтяное хозяйство, 2015, № 6. С. 10–16.

71. *Миловидов В.Д.* Услышать шум волны: что мешает предвидеть инновации? Форсайт, 2018, т. 12, № 1. С 88–97.

72. *Миловидов В.Д.* Философия финансового рынка. М.: Магистр, 2013. 270 с.

73. *Николаевич И. С.* Как нас обманывают СМИ. Манипуляция информацией. СПБ.: Питер, 2018. 320 с.

74. *Мельник В.А.* Современный словарь по политологии. Мн., 2004. С. 355.

75. *Модестов С.А.* Формирование геополитического пространства России: теоретические основы и методология исследования: Дисс. докт. полит. наук. Москва, 1998. 390 с.

76. Мультимедийная журналистика / ред. А. Г. Качкаевой, С. А. Шомовой. учебник для вузов. М.: Высшая школа экономики, 2017. С. 23.

77. Мысли Е. Месснера о сути современной мятежевойны // Milresource. 2006. URL: http://www.milresource.ru/Quotations-Messner.html (дата обращения: 19.09.2019).

78. *Николайчук И.А.* Политическая медиаметрия. Зарубежные СМИ и безопасность России: Монография. М.: РИСИ, 2015. 230 с.

79. *Николсон М.* Влияние индивида на международную систему. Размышления о структурах / Жирар М. (рук. авт. колл.) // Индивиды в международной политике. М., 1996. С. 133–136.

80. *О'Нил К.* Убийственные большие данные. Как математика превратилась в оружие массового поражения. М.: АСТ, 2018 С. 266–267.

81. О разработках в области информационной войны в США // Научно-исследовательский центр проблем национальной безопасности. 2019. Март. URL: https://nic-pnb.ru/informacionnoe-protivoborstvo/o-razrabotkah-v-oblasti-informatsionnoj-vojny-v-ssha/ (дата обращения: 23.05.2019).

82. *Олевский В.* Доктрина психологических операций НАТО // Зарубежное военное обозрение. 2016. №5. С. 12–20.

83. *Осипов Г.В.* Социология и общество. Социологический анализ российской смуты. М.: Норма, 2001. 848 с/

84. Оценка могущества Китая. «Один пояс, один путь»: полный текст речи Си Цзиньпина в Пекине // ИноСМИ. 2017. 19 мая. URL: https://inosmi.ru/politic/20170519/239391693.html (дата обращения: 21.02.2020).

85. *Панарин И.Н.* Информационная война и власть. М.: Мир безопасности, 2001. 223 с.

86. *Панарин И.Н.* Информационная война и Россия. М.: Мир безопасности, 2000. 159 с.

87. *Панарин И. Н.* СМИ, пропаганда и информационные войны // Либрус. URL: http://lib.rus.ec/b/358612/read#t32 (дата обращения: 20.08.2019).

88. *Пирумов В.С., Леин Е.Б., Евтеева Л.В.* Системный подход в современных исследовнаиях. Введение в теорию систем. Л.: Изд-во Военно-морской академии, 1973. С. 14.

89. Политическая мысль Новейшего времени. Персоналии, идеи, концепции: Краткий справочник. Чебоксары: ЧКИ РУК, 2010. С. 18.

90. Политология / А.Ю. Мельвиль и др. М.: МГИМО, 2008. С. 82.

91. *Поппер К.* Логика научного исследования // Поппер К. Логика и рост научного знания. М., 1983. С. 83.

92. *Почепцов Г. Г.* Информационные войны. М.: Рефл–бук, Киев: Ваклер, 2000. 573 с.

93. Проблемы информационной безопасности в международных военно-политических отношениях. Под ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН, 2016. С. 48.

94. *Рогачев С.В., Виловатых А.В.* Социальные движения в эпоху постправды // Проблемы национальной стратегии. 2020. № 1 (58). С. 90–105.

95. *Рогачев С.В.* Российская социальная реальность: интересы по критериям риска. Аналитический доклад. М.: ФГБУН ИСПИ РАН, 2017. 104 с.

96. *Рогачев С.В.* Цифровизация по критериям политического риска: научный доклад. М.: Издательство «Проспект», 2019. 52 с.

97. *Розов Н.С.* Философия и теория истории. М.: Логос, 200. Кн.1.: Пролегомены. С. 245.

98. *Свирский Я.И.* Нелинейный мир постнеклассической науки и творческое наследие Ж.Делеза. Дис. докт. полит. наук. М.: РАН, 2004.

99. *Селянин Я.В.* Технологическое лидерство, роль государства и неоднозначность цифр в высокотехнологичных областях на примере военно-промышленной политики США в области высокопроизводительных вычислений // Проблемы национальной стратегии. 2019. № 5. С. 137–167.

100. *Сидненко Г.Ф.* Информационное противодействие терроризму: политологический аспект. М.: Изд-во Триумф, Лучшие книги, 2019. 220 с.

101. *Смирнов А.А.* Негосударственные акторы в современных информационных войнах // Международная жизнь. 2018. № 5. URL: https://interaffairs.ru/jauthor/material/2020 (дата обращения: 04.10.2019).

102. Современная социальная теория: Бурдье, Гидденс, Хабермас. Новосибирск: Изд-во Новосиб. ун-та, 1995. С. 40–80.

103. Соглашение между правительствами государств - членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. // Бюллетень международных договоров. 2012. №1. С. 13–21.

104. *Соловьев А.И.* Политология: Политическая теория, политические технологии. М., 2003. С. 303.

105. *Сондерс Ф.С.* ЦРУ и мир искусств: культурный фронт холодной войны. М.: Институт внешнеполитических исследований и инициатив, Кучково поле, 2013. С. 117.

106. *Сорокин П. А.* Социальная и культурная динамика: Исследование изменений в больших системах искусства, истины, этики, права и общественных отношений. СПб: РХГИ, 2000. С. 80.

107. *Стёпин В.С.* Научное познание в ценности техногенной цивилизации // Вопросы философии. № 10, 1989. С.16.

108. Стратегия национальной безопасности Российской Федерации (Указ Президента РФ от 31.12.2015 № 683).

109. *Стрельцов А. А.* Информационная безопасность России. Основные понятия и определения: Учеб. пособие / Под общ. ред. проф. А. Прохожева. М.: РАГС, 1999. Ч. 1. С.34.

110. *Стюарт К.* Тайны дома Крю. Английская пропаганда в мировую войну 1914–1918 гг. М., 1928. 125 с.

111. *Суворов А.В.* Наука побеждать. М.: Изд. Центр «Анкил-Воин», 1996. С. 13.

112. *Сундиев И.Ю., Смирнов А.А., Костин В.Н.* Информационно-пропагандистская деятельность террористической организации «Исламское государство Ирака и Леванта» // Библиотека криминалиста. 2015. №1. С. 208–218.

113. Сунь-Цзы. Трактат о военном искусстве. М., 1950. 404 с.

114. *Тененбаум Б.* Великий Макиавелли: Тёмный гений власти: «Цель оправдывает средства?». М.: Яуза, Эксмо, 2012. 480 с.

115. *Тимофеева Л.Н.* Управление через сотрудничество государства и общества: проблемы обоюдной ответственности / Л.Н. Тимофеева // Государство и граждане в электронной среде. Выпуск 1 (Труды XX Международной объединенной конференции «Интернет и современное общество». СПб: Университет ИТМО.2017. С. 188-203.

116. *Толстых Е.А.* Пятая колонна. Made in USA // Литмир. 2019. URL: https://www.litmir.me/br/?b=655070&p=8 (дата обращения: 03.04.2019).

117. Трамп заявил, что коронавирус - из китайской лаборатории. Разведка с ним не согласна // Би-би-си. 2020. Май. URL: https://www.bbc.com/russian/news-52440326 (дата обращения: 18.05.2020).

118. *Траут Дж., Райс Э.* Маркетинговые войны. М.: Питер, 2018. 288 с.

119. Угрозы безопасности России и перспективы отношений с НАТО и США: Сб. материалов / Под ред. д-ра экон. наук Г.Г. Тищенко, канд. полит. наук. А.В. Виловатых. М.: РИСИ, 2017. С.140–150.

120. Указ Президента Российской Федерации от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации" // Официальный интернет-портал правовой информации. 2019. 10 октября. URL: http://publication.pravo.gov.ru/Document/View/0001201910110003?index=0 (дата обращения: 21.10.2019).

121. *Ушкин С.Г.* Вовлеченность пользователей социальных сетей в протестные движения // Власть. 2014. №8. С. 139–140.

122. *Фрейд З.* Основные психологические теории в психоанализе / пер. М. В. Вульф, А. А. Спектор. М.: АСТ, 2006. 400 с.

123. *Фролов Д. А.* Меметика: к вопросу о культурных генах // Огарев-online. 2013. №7. URL: http://journal.mrsu.ru/wp-content/uploads/2013/11/Frolov.pdf (дата обращения: 06.09.2019).pdf (дата обращения: 06.09.2019).

124. *Фролов И.Т.* Системно-структурный метод и диалектика // Вопросы философии. 1969. № 12. С. 153.

125. *Фриман Ч.* Технологии, государственное управление и неограниченная война // Россия в глобальной политике. 2018. 12 февраля. URL: http://www.globalaffairs.ru/number/Tekhnologii-gosudarstvennoe-upravlenie-i-neogranichennaya-voina-19349 (дата обращения: 29.08.2019).

126. Хаас Р. Эпоха бесполярного мира // Россия в глобальной политике. 2008. 20 июля. URL: https://globalaffairs.ru/number/n_11144 (дата обращения: 08.04.2020).

127. *Хрусталев М.А.* Анализ международных ситуаций и политическая экспертиза: очерки теории и методологии. - М.: НОФМО, 2008. С. 59.

128. *Хрусталев М.А.* Международные аспекты социально-политической стабильности // Международные процессы. М., 2008. Т.6. №2. С. 48–59.

129. *Цыгичко В.Н.* Модели в системе принятия военно-стратегических решений в СССР. М.: Империум Пресс, 2005. 94 с.

130. *Чесни Р., Ситрон Д.* Глубокие фейки и новые войны дезинформации // Россия в глобальной политике. 2019. 18 января. URL: https://globalaffairs.ru/global-processes/Glubokie-feiki-i-novye-voiny-dezinformatcii-19918 (дата обращения: 20.10.2019).

131. *Чугров Сергей.* Post-truth: трансформация политической реальности или саморазрушение либеральной демократии? // Полис. Политические исследования. 2017. № 2. С. 42–59.

132. *Шабров О.В.* Глобальные факторы современной политики // II Ежегодная Московская Конференция МРП СМП РАПН «Политические тенденции и явления: что определяет политику сегодня?». 2019. 6 апреля. URL: https://istina.msu.ru/conferences/188482207/ (дата обращения: 20.09.2019).

133. *Шутов А.Д.* Исторические прозрения. М.: ЮНИТИ-ДАНА, 2017. 463 с.

134. *Шутов А.Ю.* Политический процесс. М.: Изд-во Московского университета, 1994. 80 с.

135. A General Agent-Based Model of Social Learning // RAND. 2017. URL: https://www.rand.org/pubs/research_reports/RR1768.html (дата обращения: 10.05.2018).

136. A Memetics Compendium // Robotic Technology Inc. 2008. May. URL: https://robotictechnologyinc.com/images/upload/file/Memetics%20Compendium%205%20February%2009.pdf (дата обращения: 05.06.2018).

137. A new Industrial Strategy for a globally competitive, green and digital Europe // European Commission. 2020. March 10. URL: https://ec.europa.eu/commission/presscorner/detail/en/fs_20_425 (дата обращения: 25.05.2020).

138. *Aaron Mehta.* The Pentagon failed its audit, but officials aren't surprised // DefenseNews. 2018. November 15. URL: https://www.defensenews.com/pentagon/2018/11/15/the-pentagon-failed-its-audit-but-officials-arent-surprised/ (дата обращения: 03.03.2019).

139. *Acharya Amitav.* After Liberal Hegemony: The Advent of a Multiplex World Order. Ethics & International Affairs. 2017. Vol. 31. No. 3. P. 271–285.

140. Achieve and Maintain Cyberspace Superiority // U.S. Cyber Command. 2018. March 23. URL: https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf (дата обращения: 27.08.2019)/

141. Air Force's Top Brain Wants a 'Social Radar' to 'See Into Hearts and Mind s' // Wired. 2012. URL: https://www.wired.com/2012/01/social-radar-sees-minds/ (дата обращения: 18.04.2019).

142. AI, Big Data and Cloud Taxonomy // Govini. 2017. URL: https://www.govini.com/research-form/?post_title=DoD+ARTIFICIAL+INTELLIGENCE%2C+BIG+DATA+AND+CLOUD+TAXONOMY&post_link_redirect=https%3A%2F%2Fwww.govini.com%2Fresearch-item%2Fdod-artificial-intelligence-and-big-data-taxonomy%2F&post_id=4026 (дата обращения: 02.12.2018).

143. *Adee Sally*. The Global Internet is Disintegrating – What Comes Next? // BBC. 2019. May 15. URL: http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-next (дата обращения: 01.02.2020).

144. AirDrop requests are Gen Z's way of passing notes on Apple devices – as Hong Kong protesters show // SCMP. 2019. URL: https://www.scmp.com/lifestyle/gadgets/article/3018133/airdrop-requests-are-gen-zs-way-passing-notes-apple-devices-hong (дата обращения: 23.09.2019).

145. Allied Joint Doctrine for Psychological Operations.AJP-3.10.1 // GOV.UK. 2014. September. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (дата обращения 22.01.2018).

146. Allied Joint Doctrine for Psychological Operations.AJP-3.10.1(A) October, 2007. URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf. (дата обращения 21.01.2018).

147. Allison Graham. China and Russia: A Strategic Alliance in the Making // The National Interest. 2018. December 14. URL: https://nationalinterest.org/feature/china-and-russia-strategic-alliance-making-38727 (дата обращения: 03.04.2020).

148. *Allison Graham.* China vs.America. Managing the Next Clash of Civilizations // Foreign Affairs. 2017. September/October. URL: https://www.foreignaffairs.com/articles/united-states/2017-08-15/china-vs-america (дата обращения: 04.04.2020).

149. *Altmann J., Sauer F.* Autonomous Weapon Systems and Strategic Stability // Survival. 2017. № 5 (59). pp. 117–142.

150. America First Foreign Policy // The White House.2017. September 19. URL: https://www.whitehouse.gov/america-first-foreignpolicy (дата обращения: 18.05.2020).

151. America's Role in the Indo-Pacific // The Perth USAsia Centre. 2017. May. URL: http://perthusasia.edu.au/getattachment/Our-Work/America-s-Role-in-the-Indo-

Pacific/PU-20-ARIP-BOOK-WEB-(1).pdf.aspx?lang=en-AU (дата обращения: 23.05.2018).

152. Amid rise of ‘fake news,’ authorities should ensure truthful info reaches public // United Nations. 2017. March 10. URL: https://news.un.org/en/story/2017/03/553122-amid-rise-fake-news-authorities-should-ensure-truthful-info-reaches-public-un (дата обращения: 08.10.2019).

153. Apple CEO to MIT grads: Tech without values is worthless // APNews. 2017. URL: https://www.apnews.com/466cbd4f2aaa4791bad6404dc92aab36 (дата обращения: 22.07.2019).

154. Arab Youth Survey 2017 // ASDA’A Burson-Marsteller. URL: http://www.arabyouthsurvey.com/pdf/2017-AYS-White-Paper-EN.pdf (дата обращения: 07.03.2018).

155. ARD-DeutschlandTREND Dezember 2017 - vollständiger Bericht .. Infratest dimap. 2017. Dezember. URL: https://www.infratest-dimap.de/umfragen-analysen/bundesweit/ard-deutschlandtrend/2017/dezember/ (дата обращения: 19.03.2018).

156. ARIA In Action, Part 3: Implementation and the Indo-Pacific Strategy // United States Senate Committee on Foreign Relations. 2019. October 16. URL: https://www.foreign.senate.gov/hearings/aria-in-action-part-3-implementation-and-the-indo-pacific-strategy (дата обращения: 25.05.2020).

157. Artificial Intelligence and International Security // Center for a New American Security. 2018. July. URL: https://www.cnas.org/publications/reports/artificial-intelli gence-and-international-security (дата обращения: 20.04.2020).

158. Artificial Intelligence and National Security // Congressional Research Service. 2019. URL: https://fas.org/sgp/crs/natsec/R45178.pdf (дата обращения: 20.04.2020).

159. Artificial intelligence is transforming social media // The Washington Post. 2018. September. URL: https://www.washingtonpost.com/news/democracy-post/wp/2018/09/05/artificial-intelligence-is-transforming-social-media-can-american-democracy-survive/ (дата обращения: 16.06.2019).

160. *Atwood K.* US uses encrypted app to connect with Iranians as coronavirus sweeps their country // CNN. 2020. March 18. URL: https://edition.cnn.com/2020/03/18/politics/state-department-coronavirus-iran-outreach/index.html (дата обращения: 17.05.2020).

161. *Aum Dan*, *Silverberg Elliot*. Opportunity for the U.S. to Show Global Leadership // National Bureau of Asian Research. 2020. March 18. URL: https://www.nbr.org/publication/opportunity-for-the-u-s-to-show-global-leadership/ (дата обращения: 21.04.2020).

162. Automated Insights and AP Increase Trading of Forgotten Firms // Automated Insights 2016. URL: https://automatedinsights.com/blog/automated-insights-and-ap-increase-trading-of-forgotten-firms/ (дата обращения: 21.10.2019).

163. Autonomous weapons are a game-changer // The Economist. 2018. 25 January. URL: https://www.economist.com/special-report/2018/01/25/autonomous-weapons-are-a-game-changer (дата обращения: 02.12. 2018).

164. *Barno D., Bensahel N.* War in the fourth industrial revolution // War on the Rocks. 2018. 19 June. URL: https://warontherocks.com/2018/06/war-in-the-fourth-industrial-revolution/ (дата обращения: 02.12.2018).

165. *Baron Jonathan.* Thinking and deciding (3rd ed.), New York: Cambridge University Press, 2000.

166. *Bendett Samuel.* Here's How the Russian Military Is Organizing to Develop AI // Defense One. 2018. July 20. URL: https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/ (дата обращения: 23.09.2019).

167. *Benedict R.* The Chrysanthemum and the Sword. Patterns of Japanese Culture. Boston, 1946. p. 324.

168. *Bertuca T.* Intel research chief wants to maintain "healthy" U.S. lead over China in AI race // Inside Defense. 2018. 14 March. URL: https://insidedefense.com/daily-news/intel-research-chief-wants-maintain-healthy-us-lead-over-china-ai-race (дата обращения: 21.02.2020).

169. *Bikhchandani S., Hirshleifer D., Welch I.* A Theory of Fads, Fashion, Custom, and Cultural Change as Informational Cascades. Journal of Political Economy. 1992. (100;5), pp. 992–1026.

170. Bill H.R. 3230 «To combat the spread of disinformation through restrictions on deep-fake video alteration technology» // Congress.gov. 2019. June 12. URL: https://www.congress.gov/bill/116th-congress/house-bill/3230/text (дата обращения: 02.07.2019).

171. *Blackmore S.* The Meme Machine. Oxford: OUP, 1999.

172. *Bodansky Yossef.* After the Corona Virus // Institute for Strategic, Political, Security and Economic Consultancy. 2020. March. URL: https://www.ispsw.com/wp-content/uploads/2020/03/679_Bodansky.pdf (дата обращения: 03.04.2020).

173. *Boehler L.* 'Off-the-grid' messaging application FireChat continues to ride Occupy boost // SCMP. 2019. URL: https://www.scmp.com/news/hong-kong/article/1611322/grid-messaging-application-firechat-continues-ride-occupy-boost (дата обращения: 23.08.2019).

174. *Booth K., Wheeler N.* The Security Dilemma: Fear, Cooperation and Trust in World Politics. N.Y.: Palgrave McMillan, 2008. pp. 1–18.

175. *Breden J.* Intell tool would track social media like a virus // GCN Magazine, 2013. URL: https://gcn.com/articles/2013/02/12/intell-tool-track-social-media-like-a-virus.aspx?s=BIGDATA_130313&admgarea=TC_BigData (дата обращения: 13.09.2019).

176. *Bremmer Ian, Thompson Nicholas.* The AI Cold War That Threatens Us All // Wired Magazine. 2018. October 23. URL: https://www.wired.com/story/ai-cold-war-china-could-doom-us-all/ (дата обращения: 20.04.2020).

177. Broad Operational Language Translation (BOLT) // DARPA. 2018. URL: https://www.darpa.mil/program/broad-operational-language-translation

178. *Brodie R.* Virus of the Mind: The New Science of the Meme. Seattle: Integral Press, 1996.

179. *Bull Hedley.* The Anarchical Society: A Study of Order in World Politics. New York: Columbia University Press, 1977. 335 p.

180. Burrows M.J., Engelke P. What world post-COVID-19? Three scenarios // Atlantic Council. 2020. April. URL: https://www.atlanticcouncil.org/content-series/shaping-post-covid-world-together/what-world-post-covid-19-three-scenarios/ (дата обращения: 18.05.2020).

181. *Busby Josh.* Entering the Global Multilogue – A Replique to the German ZEIT Manifesto // Duck of Minevra. 2017. URL: https://duckofminerva.com/2017/10/entering-the-global-multilogue-a-replique-to-the-german-zeit-manifesto.html"https://duckofminerva.com/2017/10/entering-the-global-multilogue-a-replique-to-the-german-zeit-manifesto.html (дата обращения: 03.04.2020).

182. *Campbell Kurt M., Doshi Rush.* Coronavirus Could Reshape Global Order // Foreign Affairs. 2020. March 18. URL: https://www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order?utm_campaign=Center%20for%20Northeast%20Asian%20Policy%20Studies&utm_source=hs_email&utm_medium=email&utm_content=85459036 (дата обращения: 03.04.2020).

183. Can NATO Weaponize Memes? // Foreign Policy. 2017. 13 April. URL: https://foreignpolicy.com/2017/04/13/nato-cyber-information-warfare-battle-of-ideas-memes-internet-culture/ (дата обращения: 05.06.2019).

184. CCW Meeting of High Contracting Parties // The United Nations Office at Geneva. 2017. URL: https://www.unog.ch/80256EE600585943/httpPages)/A0A0A3470E40345CC12580CD003D7927?OpenDocument (дата обращения: 01.12.2018).

185. Chambers J. Countering Gray-Zone Hybrid Threats. An Analysis of Russia's "New Generation Warfare" and Implications for the US Army // Modern War Institute at West Point. 2016. 18 October. URL: https://mwi.usma.edu/wp-content/uploads/2016/10/Coun tering-Gray-Zone-Hybrid-Threats.pdf (дата обращения: 10.11.2018).

186. *Cheney Clayton.* China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism // Pacific Forum. 2019. July. URL: https://www.pacforum.org/sites/default/files/issuesinsights_Vol19%20WP8FINAL.pdf (дата обращения: 03.02.2020).

187. China in "full-speed" push for "intelligentized" weapons to defeat U.S. // Geostrategy-Direct. 2018. 15 May. URL: http://geostrategy-direct-subscribers.com/china-infull-speed-push-for-intelligentized-weapons-to-defeat-u-s/ (дата обращения: 20.04.2020).

188. China's AI Giants Can't Say No to the Party // Foreign Policy. 2018. 2 August. URL: https://foreignpolicy.com/2018/08/02/chinas-ai-giants-cant-say-no-to-the-party/ (дата обращения: 12.12.2018)

189. China’s Digital Rise. Challenges for Europe// MERICS. 2019. May. URL: https://www.merics.org/en/events/chinas-digital-rise-challenges-europe (дата обращения: 02.02.2020).

190. China’s Tech-Enhanced Authoritarianism // URL: https://docs.house.gov/meetings/IG/IG00/20190516/109462/HHRG-116-IG00-Wstate-HoffmanS-20190516.pdf (дата обращения: 26.05.2020).

191. *Chiu K.* From Facebook and Twitter to Telegram, WhatsApp and Signal: how protest technology has evolved since Occupy Central. SCMP. URL: https://www.scmp.com/news/hong-kong/article/3014255/ facebook-and-twitter-telegram-whatsapp-and-signal-how-protest (дата обращения 23.05.2019).

192. *Cho Charles H., Martens Martin L.,* Hakkyun Kim, Michelle Rodrigue. Astroturfing Global Warming: It Isn’t Always Greener on the Other Side of the Fence // Journal of Business Ethics. 2011. № 4 (104). С.571–587.

193. *Clay Rebecca A.* Moving assessment out of the clinic // American Psychological Association. 2019. July/August. URL: https://www.apa.org/monitor/2019/07-08/moving-assessment (дата обращения: 22.07.2019).

194. Command and Control Warfare. Joint Publication 3-13.1. Washington D.C.: Joint Chiefs of Staff, Feb. 1996.

195. Competing in the Gray Zone // CSIS. 2018. October 24. URL: https://www.csis.org/analysis/competing-gray-zone-0 (дата обращения: 20.09.2019).

196. Cooper Julian. If War Comes Tomorrow: How Russia Prepares for Possible Armed Aggression // RUSI. 2016. August. URL: https://rusi.org/publication/whitehall-reports/if-war-comes-tomorrow-how-russia-prepares-possible-armed-aggression (дата обращения: 07.04.2020).

197. Corruption Perceptions Index 2018 // Transparency International. 2018. URL: https://www.transparency.org/cpi2018 (дата обращения: 14.07.2019).

198. Counter-Da’esh Influence Operations Cognitive Space Narrative Simulation Insights // Whitepaper. 2016. June. URL: http://nsiteam.com/social/wp-content/uploads/2016/06/C-ISIL-Simulation-Whitepaper-Jun2016-Final5.compressed.pdf (дата обращения: 05.06.2019).

199. Countering Hybrid Warfare Project: Understanding Hybrid Warfare // GOV.UK. 2017. 28 September. URL: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare (дата обращения: 20.09.2019).

200. COVID-19 – a trigger for global transformation? // Finnish Institute of International Affairs. 2020. March. URL: https://www.fiia.fi/wp-content/uploads/2020/03/wp113_covid-19_a-trigger-for-global-transformation.pdf (дата обращения: 08.04.2020).

201. COVID-19 Exploited by Malicious Cyber Actors // CISA. 2020. April 8. URL: https://www.us-cert.gov/ncas/alerts/aa20-099a (дата обращения: 15.04.2020).

202. Covid-19 in Europe-China Relations // European Think-tank Network on China. 2020. April. URL: https://www.ifri.org/en/publications/publications-ifri/ouvrages-ifri/covid-19-europe-china-relations (дата обращения: 01.05.2020).

203. Critical Foundations: Protecting America's Infrastructures // FAS. 1997. October. URL: https://fas.org/sgp/library/pccip.pdf (дата обращения: 05.10.2019).

204. Critical Infrastructure Sectors // US Department of Homeland Security. 2018. URL: https://www.dhs.gov/critical-infrastructure-sectors (дата обращения: 18.09.2019).

205. CSC Virtual Event: Layered Cyber Deterrence // Cyberspace Solarium Commission. 2020. April 15. URL: https://www.solarium.gov/#h.p_cEkideHVewUW (дата обращения: 14.04.2020).

206. D--Social Data Analytics Subscription Service // Federal Business Opportunity. 2017. July26. URL: https://www.fbo.gov/index?s=opportunity&mode=form&id=89f601f3b1631165d227daf85ee917c9&tab=core&_cview=1 (дата обращения 13.05.2018).

207. DARPA and the Brain Initiative // DARPA. URL: https://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative (дата обращения: 18.04.2019).

208. *Dawkins R.* The Selfish Gene. Oxford: OUP, 1976. 384 p.

209. Definition of post-truth in English // Oxford Dictionaries. Lexico Dictionaries. 2019. URL: https://www.lexico.com/en/definition/post-truth (дата обращения: 10.10.2019).

210. *Del Vicario M., Bessi A., Zollo F., et al.* The spreading of misinformation online // Proceedings of the National Academy of Sciences 2016. V. 113. N. 3. P. 554-559.

211. Department of Defense Cyber Strategy 2018 // US DOD. 2018. September. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_ (дата обращения: 01.10.2019).

212. Developing Cybersecurity Capacity // RAND. 2018. December. URL: https://www.rand.org/pubs/research_reports/RR2072.html (дата обращения: 08.04.2020).

213. DHS Cybersecurity Strategy // US Department of Homeland Security. 2018. May 15. URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (дата обращения: 18.09.2018).

214. DHS' Kolasky to lead new cyber risk center announced at summit this week // Inside Cybersecurity. 2018. August 03. URL: https://insidecybersecurity.com/daily-news/dhs-kolasky-lead-new-cyber-risk-center-announced-summit-week (дата обращения: 18.09.2019).

215. Digitalreport 2020. Berlin: European Center for Digital Competitiveness by ESCP Business School. Januar 2020. P. 15.

216. Disinformation, 'fake news' and the EU's response // EPRS. 2019. April. URL: http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/614584/EPRS_ATA%282017%29614584_EN.pdf (дата обращения: 05.09.2019).

217. Disinformation on Steroids // Council on Foreign Relations. 2018. October 16. URL: https://www.cfr.org/report/deep-fake-disinformation-

steroids?utm_medium=email&utm_source=twtw&utm_content=101918&sp_mid=57597773&sp_rid=ZXZyYXppYUBnbWFpbC5jb20S1 (дата обращения: 02.07.2019).

218. *Ding J., Triolo P., Sacks S.* Chinese Interests Take a Big Seat at the AI Governance Table // New America. 2018. 20 June. URL: https://www.newamerica.org/cybersecurityinitiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/ (дата обращения: 25.01.2020).

219. DNI: China's cyber theft of tech (also Russia's and Iran's) threatens U.S. edge // Geostrategy-Direct. Foreign Influence Operations and their use of Social Media Platforms. 2018. July 31. URL: http://geostrategy-direct-subscribers.com/dni-chinas-cyber-theft-of-tech-also-russias-and-irans-threatens-u-s-edge/ (дата обращения: 03.10.2019).

220. Does technology exacerbate social polarisation? // EPRS. 2019. March 19. URL: https://epthinktank.eu/2019/03/19/does-technology-exacerbate-social-polarisation/ (дата обращения: 22.07.2019).

221. *Downs A.* An economic theory of democracy. New York: Harper and Row. 1957. 320 p.

222. Engineering Humans for War // The Atlantic. URL: https://www.theatlantic.com/international/archive/2015/09/military-technology-pentagon-robots/406786/ (дата обращения: 19.04.2019).

223. EU and NATO welcome Hybrid CoE // Hybrid CoE. 2017. September 1. URL: https://www.hybridcoe.fi/news/eu-and-nato-welcome-hybrid-coe/ (дата обращения: 21.12.2017).

224. Executive Order. 13010. Critical Infrastructure Protection. Federal Register. Vol. 61. №. 138. July 17. 1996. pp. 3747-3750.

225. Experimental evidence of massive-scale emotional contagion through social networks // PNAS. URL: http://www.pnas.org/content/111/24/8788.full (дата обращения: 19.02.2020).

226. Facebook users more prone to developing eating disorders, study finds // ScienceDaily. 2011. February 7. URL: https://www.sciencedaily.com/releases/2011/02/110207091754.htm (дата обращения: 24.07.2019).

227. Fake News and False Flags // The Bureau of Investigative Journalism. 2016. October. URL: http://labs.thebureauinvestigates.com/fake-news-and-false-flags/ (дата обращения: 12.10.2019).

228. *Ferguson Niall.* Donald Trump must split up Putin and Xi, the new odd couple // The Times. 2020. January. URL: https://www.thetimes.co.uk/article/donald-trump-must-split-up-putin-and-xi-the-new-odd-couple-7rtgcb2qc (дата обращения: 07.04.2020).

229. Findings of the Cyberspace Solarium Commission // U.S. Senate Committee on Armed Services. 2020. March 25. URL: https://www.armed-services.senate.gov/hearings/20-03-25-findings-of-the-cyberspace-solarium-commission (дата обращения: 15.04.2020)

230. *Fine Cordelia.* A Mind of its Own: how your brain distorts and deceives, Cambridge, UK: Icon books, 2006.

231. *Fischoff Stuart.* Media Psychology: A Personal Essay in Definition and Purview // Division 46. URL: https://www.apadivisions.org/division-46/about/fischoff-media-psychology.pdf (дата обращения: 22.07.2019).

232. First Monday: What's on tap this month on TV and in movies and books: The Filter Bubble by Eli Pariser // USA Today. 2011. URL: https://usatoday30.usatoday.com/money/companies/management/monday/2011-04-29-first-monday-business-media-in-may_n.htm (дата обращения: 09.06.2019).

233. *Fleming, Brian P.* The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art. — Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies (SAMS), U.S. Army Command & General Staff College, 2011.

234. *Fleming, Brian P.* Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies (SAMS), U.S. Army Command & General Staff College, 2011.

235. Flagship AI Lab announced as Defence Secretary hosts first meet between British and American defence innovators // GOV.UK. 2018. 22 May. URL: https://www.gov.uk/government/news/flagship-ai-lab-announced-as-defence-secretary-hosts-first-meet-between-british-and-american-defence-innovators (дата обращения: 28.11.2018).

236. Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology. February 12, 2014.

237. *Freedberg S.* Army Sec. Esper's 10-Year Plan Is A Big Bet On Budget // 2018. 6 June. URL: https://breakingdefense.com/2018/06/sec-esper-10-year-plan-is-a-big-bet-on-budget/ (дата обращения: 14.12.2018).

238. GAO-16-885T. FEDERAL INFORMATION SECURITY: Actions Needed to Address Challenges. Testimony Before the President's Commission on Enhancing National Cybersecurity. P. 1–3 // United States Government Accountability Office. 2016. September 19. URL: http://www.gao.gov/products/GAO-16-885T (дата обращения: 18.09.2019).

239. *Giesea J.* It is time to embrace memetic warfare // Defence Strategic Communications journal. 2015. Winter. Vol. 1. No. 1. URL: https://www.stratcomcoe.org/academic-journal-defence-strategic-communications-vol1 (дата обращения: 05.06.2018).

240. *Giesea J.* Memetic warfare. Part 2: Hacking hearts and minds. How the memetic warfare is transforming cyberwar. 2017.

241. Globally, more people see U.S. power and influence as a major threat // Pew Research Center. 2017. August 1. URL: http://www.pewresearch.org/fact-tank/2017/08/01/u-s-power-and-influence-increasingly-seen-as-threat-in-other-countries/ (дата обращения: 07.03.2018).

242. *Goggin B.* From porn to 'Game of Thrones': How deepfakes and realistic-looking fake videos hit it big // Business Insider.2019. June 23. URL: https://www.businessinsider.com/deepfakes- explained-the-rise-of-fake-realistic-videos-online-2019-6. (дата обращения: 24.10.2019).

243. *Gray Iain.* Iain Gray: Beware the black art of post-truth politics // The scotsman. 2012. URL: https://www.scotsman.com/news/opinion/iain-gray-beware-the-black-art-of-post-truth-politics-1-2146059 (дата обращения: 25.09.2019).

244. H.R. 5515—FY19 NATIONAL DEFENSE AUTHORIZATION BILL // White House.gov. 2018. May. URL: https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/wysiwyg_uploaded/FY19%20NDAA%20Chairman%27s%20Mark%20Final.pdf (дата обращения 13.05.2018).

245. H.R.6227 – National Quantum Initiative Act // Congress. gov. 2018. 21 December. URL: https://www.congress.gov/bill/115th-congress/house-bill/6227 (дата обращения: 01.03.2019).

246. *Hancock B.J.* Memetic Warfare: The Future of War. Military Intelligence Professional Bulletin // FAS. 2010. April–June. URL: https://fas.org/irp/agency/army/mipb/2010_02.pdf (дата обращения: 04.06.2018).

247. *Harding Brian.* China's Digital Silk Road and Southeast Asia // Center for Strategic and International Studies. 2019. February 15. URL: https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia. (дата обращения: 24.04.2020).

248. *Harkins G.S., Szymanski K.* Social Loafing and Self-Evaluation with a social standard. Journal of Personality and social psychology. USA, 1987. URL: https://www.researchgate.net/publication/247434281_Social_Loafing_and_Self-Evaluation_With_a_Social_Standard (дата обращения 21.01.2018).

249. *Harkins S.G., Petty, R.E.* The multiple source effect in persuasion // Personality and Social Psychology Bulletin. URL: http://journals.sagepub.com/doi/abs/10.1177/014616728174019 (дата обращения: 13.09.2019).

250. Harmful internet use. Part 1, Part 2 // European Parliament. 2019. January. URL: http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624269/EPRS_STU(2019)624269_EN.pdf; http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624249/EPRS_STU(2019)624249_EN.pdf (дата обращения: 22.07.2019).

251. *Harsin Jayson*. Regimes of Posttruth, Postpolitics, and Attention Economies. Communication, Culture & Critique. 2015. pp. 327–333.

252. *Heilmann Sebastian.* Leninism Upgraded: Xi Jinping's Authoritarian Innovations // Mercator Institute for China Studies. 2016. URL: https://www.merics.org/sites/default/files/2018-03/Heilmann_Leninism_Upgraded_China_Economic_Quarterly_Dec.2016.pdf (дата обращения: 01.02.2020).

253. *Hoffman S.* Engineering global consent: The Chinese Communist Party's data-driven power expansion // Australian Strategic Policy Institute. 2019. October 14. URL: https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion (дата обращения: 26.05.2020).

254. *Hoffer E.* The Passionate State of Mind, New York: Harper. 1955.

255. Hong Kong: Ambulance Passes Through Sea of Protesters During Sunday's Massive Rally / Spectee. 2019. URL: https://spectee.com/detail/22065 (дата обращения: 26.10.2019).

256. *Hong Shen.* Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative // International Journal of Communication. № 12. 2018. URL: https://ijoc.org/index.php/ijoc/article/view/8405/2386 (дата обращения: 04.02.2020).

257. *Horowitz Michael.* Strategic Competition in an Era of Artificial Intelligence // Center for a New American Security. 2018. July. URL: http://files.cnas.org.s3.amazonaws.com/documents/CNAS-Strategic-Competition-in-an-Era-of-AI-July-2018_v2.pdf (дата обращения: 23.09.2019).

258. *Hosmer S.* Operations Against Enemy Leaders. Santa Monica: RAND, 2001. P.180.

259. House Intelligence Committee To Hold Open Hearing on Deepfakes and AI «The National Security Challenge of Artificial Intelligence, Manipulated Media, and "Deepfakes"» // House Permanent Select Committee on Intelligence. 2019. June 7. URL: https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=657 (дата обращения: 25.06.2019).

260. How to Stop Losing the Information War // Defense One. 2018. July 26. URL: https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/ (дата обращения: 20.08.2019).

261. *Hoffman F.* Future Warfare: The Rise of Hybrid Warfare // U.S. Naval Institute. 2005. URL: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf (дата обращения: 23.09.2019).

262. How many internet users does each country have? // Our World in Data. 2019. URL: https://ourworldindata.org/how-many-internet-users-does-each-country-have (дата обращения: 23.07.2019).

263. *Howe J.* Artificial Intelligence at Edinburgh University: a Perspective // The University of Edinburgh. 2007. 17 August. URL: http://www.inf.ed.ac.uk/about/AIhistory.html (дата обращения: 02.12.2018).

264. Hybrid Warfare in the Baltics // RAND. 2017. URL: https://www.rand.org/pubs/research_reports/RR1577.html (дата обращения: 20.05.2019).

265. IARPA Launches "MATERIAL" Program // DNI.GOV. 2017. December 22/URL: https://www.dni.gov/index.php/newsroom/press-releases/item/1829-iarpa-launches-material-program (дата обращения: 10.05.2018).

266. Information Warfare. Directive TS 3600.1. Washington D.C.: U.S. Department of Defense, 21 Dec. 1992.

267. IQT Labs // In-Q-Tel, Inc. URL: https://www.iqt.org/labs/ (дата обращения: 19.04.2019); Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community // RAND. URL: https://www.rand.org/pubs/research_reports/RR1408.html (дата обращения: 19.04.2019).

268. Impact of the Internet on Russian Politics, Media, and Society // The Berkman Klein Center for Internet & Society. URL: https://cyber.harvard.edu/research/russia (дата обращения: 15.02.2018).

269. In Spite of It All, America. A Transatlantic Manifesto in Times of Donald Trump – A German Perspective // New York Times. 2017. October. URL: http://trotzdem-amerika.de (дата обращения: 04.04.2020).

270. International Strategy of Cooperation on Cyberspace // Ministry of Foreign Affairs of the People's Republic of China. 2017. March 1. URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (дата обращения: 24.04.2020).

271. International tourist arrivals up 4% reach a record 1.2 billion in 2015 // UNWTO. 2016. URL: https://media.unwto.org/Press-release/2016-01-18/international-tourist-arrivals-4-reach-record-12-billion-2015 (дата обращения: 14.07.2019).

272. Internet Gaming // American Psychiatric Association. 2018. June. URL: https://www.psychiatry.org/patients-families/internet-gaming (дата обращения: 24.07.2019).

273. *James M. Dubik, Nic Vincent*. America's Global Competitions: The Gray Zone in Context // Institute for the Study of War. 2018. February. URL: http://iswresearch.blogspot.com/sites/default/files/The%20Gray%20Zone_Dubik_2018.pdf (дата обращения: 20.09.2019).

274. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington D.C.: Joint Chiefs of Staff, Dec. 1998.

275. Joint Publication 3-53. Doctrine for Joint Psychological Operation.5 September 2003. URL: https://www.hsdl.org/?abstract&did=472329. (дата обращения 21.01.2018).

276. *Kissinger Henry*. The Coronavirus Pandemic Will Forever Alter the World Order // The all Street Journal. 2020. April 03. URL: https://www.wsj.com/articles/the-coronavirus-pandemic-will-forever-alter-the-world-order-11585953005 (дата обращения: 08.04.2020).

277. Knowledge Graph // Google. 2018. URL: https://www.google.com/intl/es419/insidesearch/features/search/knowledge.html (дата обращения 13.05.2018).

278. *Kristof F*. However Much Trump Spends on Arms, We Can't Bomb Ebola // The New York Times. 2017. March 2. URL: https://www.nytimes.com/2017/03/02/opinion/however-much-trump-spends-on-arms-we-cant-bomb-ebola.html?_r=0 (дата обращения: 14.09.2019).

279. *Kuhn, Deanna, Lao, Joseph.* Effects of Evidence on Attitudes: Is Polarization the Norm? // Psychological Science (American Psychological Society), March 1996. — T. 7 (2): 115–120.

280. *Leetaru Kalev*. What Tallinn Manual 2.0 teaches us about the new cyber order // Forbes. 2017. 15 June. URL: https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/ (дата обращения: 20.08.2019)

281. *Lewis Carol*. Why Barack Obama and David Cameron are keen to ‘nudge’ you // The Times. 2008. July. URL: https://www.thetimes.co.uk/article/why-barack-obama-and-david-cameron-are-keen-to-nudge-you-pg0p3b5lqcq (дата обращения: 20.10.2018).

282. *Lewis James.* Cognitive Effect and State Conflict in Cyberspace // Center for Strategic and International Studies. 2018. September 26 URL: https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace (дата обращения: 20.02.2020).

283. *Lewis James.* How Will 5G Shape Innovation and Security: A Primer // Center for Strategic and International Studies. 2018. December 6. URL: https://www.csis.org/analysis/how-5g-will-shape-innovation-and-security (дата обращения: 01.02.2020).

284. *Luskin Bernard J.* Defining and Describing Media Psychology // Psychology Today. 2012. November 30. URL: https://www.psychologytoday.com/intl/blog/the-media-psychology-effect/201211/defining-and-describing-media-psychology (дата обращения: 22.07.2019).

285. *Lynch A.* Thought Contagion: How Belief Spreads Through Society. N.Y.: Basic Books. 1996; *Smith J.M.*, *Szathmary E.* The Major Transitions in Evolution. N.Y.: W.H. Freeman and Company Limited, 1995.

286. Machiavelli: Still Shocking after Five Centuries // National Interest. 2014. November. URL: https://nationalinterest.org/commentary/machiavelli-still-shocking-after-five-centuries-9126 (дата обращения: 12.09.2017).

287. *Marton Péter.* Evolution in military affairs in the battlespace of Syria and Iraq // Corvinus Journal of International Affairs. 2018. Vol. 2, iss. 2-3. pp. 30-41.

288. *McCarthy J.* What is Artificial Intelligence? // Computer Science Department. 2007. 12 November. URL: http://www-formal.stanford.edu/jmc/whatisai/whatisai.html (дата обращения: 03.12.2018).

289. *McCuen, John J.* Hybrid wars // Military Review. 2008. URL: https://www.questia.com/library/journal/1P3-1458719761/hybrid-wars (дата обращения: 24.08.2019).

290. *Mearsheimer John J.* Bound to Fail. The Rise and Fall of the Liberal International Order // International Security. 2019. Vol. 43. No. 4. P. 7–50.

291. Metamagical Themas // Scientific American. 1983. URL: https://www.scientificamerican.com/author/douglas-r-hofstadter/ (дата обращения: 04.06.2018).

292. Mind of the Mob: The Geosimulation of Crowd Control // Yale Scientific Magazine. 2013. URL: http://www.yalescientific.org/2013/05/mind-of-the-mob-the-geosimulation-of-crowd-control/ (дата обращения: 18.04.2019).

293. Monitoring Social Media. Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations // RAND. 2017. URL: https://www.rand.org/pubs/research_reports/RR1742.html (дата обращения 13.05.2018).

294. Multi-Domain Battle: Evolution of Combined Arms for the 21st Century. 2025–2040 // Army Capabilities Integration Center. 2017. October. URL: http://www.arcic.army.mil/ App_Documents/Multi-Domain-Battle-Evolution-of-Combined-Arms.pdf (дата обращения: 10.11.2018).

295. Narrative Networks // DARPA. 2011. 7 October. URL: https://robo-hunter.com/uploads/files/560c1c5fe87df.pdf (дата обращения: 05.06.2018).

296. National Science Foundation requests input on updating cyber research and development plan // Inside Cybersecurity. 2018. 12 November. URL: https://insidecybersecurity.com/daily-briefs/national-science-foundation-requests-input-updating-cyber-research-and-development-plan (дата обращения: 20.02.2020).

297. National Cyber Strategy of the United States of America // The White House. 2018. September. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 23.09.2019).

298. National Security Strategy of the United States of America, 2017 P. 12-13, 31–32. // The White House. 2017. December 18. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 02.10.2019).

299. New players join race for offensive cyber abilities // Oxford Analytica. 2018. 20 August. URL: https://dailybrief.oxan.com/Analysis/DB236921/New-players-join-race-for-offensive-cyber-abilities- (дата обращения: 20.09.2019).

300. New report: actors manipulating the online conversation are changing tactics // NATO. 2018. February 19. URL: https://www.stratcomcoe.org/new-report-actors-manipulating-online-conversation-are-changing-tactics (дата обращения: 05.09.2019).

301. New social credit code system to increase administrative efficiency // The State Council the People's Republic of China. 2015. June 17. URL: http://english.www.gov.cn/policies/latest_releases/2015/06/17/content_281475129090642.htm (дата обращения: 25.05.2020).

302. News Feed FYI // Facebook. 2019. URL: https://newsroom.fb.com/news/category/news-feed-fyi/ (дата обращения: 11.10.2019).

303. *Nickerson Raymond S.* A Ubiquitous Phenomenon in Many Guises // Review of General Psychology (Educational Publishing Foundation), 1998. – T. 2 (2). pp. 175–220.

304. Norway, Russia and Luxembourg take the lead for being the cheapest countries in the world to be a student // The Independent. 2015. URL: http://www.independent.co.uk/student/news/norway-russia-and-luxembourg-take-the-lead-for-being-the-cheapest-countries-in-the-world-to-be-a-a6799211.html (дата обращения: 16.07.2019).

305. *Nossel Suzanne.* Google is Handing the Future of the Internet to China // Foreign Policy. 2018. September 10. URL: https://foreignpolicy.com/2018/09/10/google-is-handing-the-future-of-the-internet-to-china/ (дата обращения: 03.02.2020).

306. Nye Joseph. Will the Liberal Order Survive? The History of an Idea // Foreign Affairs. 2017. Vol. 96. No. 1. P. 10-16.

307. One more term for Putin: Dark ambition, dim hopes // Brookings. 2018. March 20. URL: https://www.brookings.edu/blog/up-front/2018/03/20/one-more-term-for-putin-dark-ambition-dim-hopes/ (дата обращения 28.03.2017).

308. O'Rourke Ronald, Moodie Michael. U.S. Role in the World: Background and Issues for Congress // Congressional Research Service. 2019. URL: https://fas.org/sgp/crs/row/R44891.pdf (дата обращения: 04.04.2020).

309. Overall Best Countries Ranking Rankings // U.S. News & World Report. 2019. URL: https://www.usnews.com/news/best-countries/overall-rankings (дата обращения: 14.07.2019).

310. *Pariser Eli.* The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin Press, 2011.

311. *Parramore Lynn. T*he Filter Bubble // The Atlantic. 2010. 10 октября. URL: https://www.theatlantic.com/daily-dish/archive/2010/10/the-filter-bubble/181427/ (дата обращения: 10.10.2018).

312. *Patrick Stewart, Feng Ashley.* Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road // Council on Foreign Relations/ 2018. July 2. URL: https://www.cfr.org/blog/belt-and-router-china-aimstighter-internet-controls-digital-silk-road (дата обращения: 04.02.2020).

313. *Pentland A.* Social physics. How good ideas spread — the lessons from a new science. New York, 2014.Science Book a Day Interviews Alex Pentland // Science Book a Day. 2014. URL: https://sciencebookaday.com/2014/08/01/science-book-a-day-interviews-alex-pentland/ (дата обращения: 19.04.2019).

314. *Petrov N.* Understanding Methods of Elite Repression in Russia // Chatham House. 2019. 4 June. URL: https://www.chathamhouse.org/expert/comment/understanding-methods-elite-repression-russia (дата обращения: 19.09.2019).

315. *Pomerleau Mark.* Are cyber weapons similar to WMDs? DoD wants to know // Fifth Domain. 2018. December 20. URL: https://www.fifthdomain.com/dod/2018/12/20/are-cyber-weapons-similar-to-wmds-dod-wants-to-know/ (дата обращения: 03.10.2019).

316. *Prasso Sheridan.* China’s Digital Silk Road is Looking More Like an Iron Curtain // Bloomberg. 2019. January 10. URL: https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-likean-iron-curtain (дата обращения: 03.02.2020).

317. Preparing for War in Korea // RUSI. 2017. September. URL: https://rusi.org/publication/whitehall-reports/preparing-war-korea (дата обращения: 08.04.2020).

318. President Donald J. Trump Signed H.R. 3359 into Law // Whitehouse.gov. 2018. November 16. URL: https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-signed-h-r-3359-law/ (дата обращения: 03.10.2019).

319. Project Maven to Deploy Computer Algorithms to War Zone by Year’s En // U.S. Department of Defense. 2017. 21 July. URL: https://www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/ (дата обращения: 28.06.2018).

320. *Prosser M.* Memetics – A Growth Industry in US Military Operations // NATO. 2006. URL: https://www.sto.nato.int/publications/Lists/National_Catalogues/DispForm.aspx?ID=2638 (дата обращения: 04.06.2018).

321. Putin and Russia in 2018–24: What Next? // Chatham House. 2018. March 15. URL: https://www.chathamhouse.org/research/publications/putin-and-russia-2018-24-what-next (дата обращения 27.03.2017).

322. Putin's landslide election makes it seem like Russia is stable. Don't be fooled // CSIS. 2018. March 19. URL: https://www.csis.org/search?search_api_views_fulltext=russia%20elections&sort_by=field_publication_date&page= (дата обращения 27.03.2018).

323. Putin's New Term—From Brezhnev to Stalin // Cato Institute.2018. March 21. URL: https://www.cato.org/blog/putins-new-term-brezhnev-stalin (дата обращения 28.03.2017).

324. Qui sont les internautes à l'origine de l'appel aux blocages contre la hausse du prix du carburant? // Franceinfo. 2018. Novembre. URL: https://www.francetvinfo.fr/economie/automobile/essence/appel-aux-blocages-contre-la-hausse-du-prix-du-carburant-partout-en-france-les-gens-sont-prets-a-se-mobiliser_3003467.html (дата обращения: 10.10.2019).

325. *Rasmussen A., Chertoff M.* The West Still Isn't Prepared to Stop Russia Meddling in Our Elections // Politico. 2018. June 05. URL: https://www.politico.com/magazine/story/2018/06/05/russia-election-meddling-prepared-218594 (дата обращения: 01.09.2019).

326. *Ratkiewicz J., M. D. Conover,* M. Meiss, B. Gonçalves, A. Flammini, F. Menczer. Detecting and Tracking Political Abuse in Social Media // Center for Complex Networks and Systems Research. Indiana University. 2011.

327. *Raynor W.* Jr International Dictionary of Artificial Intelligence / 2nd ed. L.: Global Professional Publishing, 2008.

328. Recommendations to the President on Securing America's Cyber Interests and Deterring Cyber Threats Through International Engagement // U.S. Department of State. 2018. May. URL: https://www.state.gov/secretary/remarks/2018/05/282896.htm (дата обращения: 03.10.2019).

329. Reinventing society in the wake of big data // Edge Foundation. 2012. URL: https://www.edge.org/conversation/reinventing-society-in-the-wake-of-big-data (дата обращения: 19.04.2019).

330. Remarks by President Trump to the People of Poland // The White House. 2017. July 6. URL: https://www.whitehouse.gov/the-press-office/2017/07/06/remarks-president-trump-people-poland-july-6-2017 (дата обращения: 18.05.2020).

331. Renewed Great Power Competition: Implications for Defense—Issues for Congress // Congressional Research Service. 2019. August 5. URL: https://fas.org/sgp/crs/natsec/R43838.pdf (дата обращения: 03.04.2020).

332. *Rid T., Hecker M.* War 2.0: Irregular Warfare in the Information Age. Westport (Calif.): Praeger, 2007.

333. Rising to the China Challenge // Center for New American Security. 2020. January 28. URL: https://www.cnas.org/publications/reports/rising-to-the-china-challenge (дата обращения: 24.05.2020).

334. *Rolland Nadege.* China's Vision for a New World Order // The National Bureau of Asian Research. NBR Special Report № 83. 2020. January. URL: https://www.nbr.org/publication/chinas-vision-for-a-new-world-order/ (дата обращения: 09.04.2020).

335. Roubini Nouriel. Our G-Zero World // Project Syndicate. 2011. February 11. URL: https://www.project-syndicate.org/commentary/our-g-zero-world?barrier=accesspaylog (дата обращения: 08.04.2020).

336. *Russell S., Norvig P.* Artificial Intelligence: A Modern Approach // AIMA. 2003. URL: http://aima.cs.berkeley.edu (дата обращения: 02.12.2018).

337. Russia Is Our Adversary // The Atlantic. 2018. February 9. URL: https://www.theatlantic.com/politics/archive/2018/02/russia-is-our-adversary/552962/ (дата обращения 16.05.2018).

338. Russia Will Challenge US Military Superiority in Europe by 2025: US General // Defense One. 2018. URL: https://www.defenseone.com/threats/2018/03/russia-will-challenge-us-military-superiority-europe-2025-us-general/146523/ (дата обращения: 20.08.2019).

339. Russian New Generation Warfare Handbook / Asymmetric Warfare Group // Public Intelligence. 2017. 18 September. URL: https://info.publicintelligence.net/AWG-Rus sianNewWarfareHandbook.pdf (дата обращения: 15.11.2018).

340. S.2943 - National Defense Authorization Act for Fiscal Year 2017. SEC. 1287 // Congress.gov: URL: https://www.congress.gov/bill/114th-congress/senate-bill/2943 (дата обращения: 05.04.2018).

341. *Saletan W.* Neuro-Liberalism // The New York Times. 2008. 22 June. URL: https://www.nytimes.com/2008/06/22/books/review/Saletan-t.html (дата обращения: 05.06.2018).

342. *Savastio Rebecca.* Facebook Causes Depression New Study Says // Guardian Liberty Voice. 2019. August 15. URL: https://guardianlv.com/2013/08/facebook-causes-depression-new-study-says/#PzRdcP38KPwjLoxo.9 (дата обращения: 22.07.2019).

343. *Schwab K.* The Fourth Industrial Revolution // World Economic Forum. 2018. URL: https://www.weforum.org/pages/the-fourth-industrial-revolution-by-klaus-schwab (дата обращения: 02.12. 2018).

344. Science Book a Day Interviews Alex Pentland // Science Book a Day. 2014. URL: https://sciencebookaday.com/2014/08/01/science-book-a-day-interviews-alex-pentland/ (дата обращения: 21.06.2019).

345. Secure Cyberspace and Critical Infrastructure // US Department of Homeland Security. 2019. July 5. URL: https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure# (дата обращения: 05.10.2019).

346. Securing Communications in the Quantum Computing Age. Managing the Risks to Encryption // RAND Corporation. 2020. April. URL:

https://www.rand.org/pubs/research_reports/RR3102.html (дата обращения: 19.04.2020).

347. *Seely B.* A Definition of Contemporary Russian Conflict: How Does the Kremlin Wage War? // The Henry Jackson Society. 2018. 4 June. URL: http://henryjacksonsociety.org/wp-content/uploads/2018/06/A-Definition-of-Contemporary-Russian-Conflict-new-branding.pdf (дата обращения: 30.09.2019).

348. *Segal Adam.* When China Rules the Web // Foreign Affairs. 2018. September/October. URL: https://www.foreignaffairs.com/issues/2018/97/5 (дата обращения: 01.02.2020).

349. Shaping the digital transformation in Europe. Working paper: Economic potential // European Commission. 2020. February. URL: https://ec.europa.eu/digital-single-market/en/news/shaping-digital-transformation-europeworking-paper-economic-potentialIbidem (дата обращения: 25.05.2020).

350. *Schell Orville.* The Ugly End of Chimerica // Foreign Policy. 2020. April. URL: https://foreignpolicy.com/2020/04/03/chimerica-ugly-end-coronavirus-china-us-trade-relations/ (дата обращения: 09.04.2020).

351. Sharp Drop in World Views of US, UK: Global Poll // GlobeScan. 2017. 4 July. URL: https://globescan.com/sharp-drop-in-world-views-of-us-uk-global-poll/ (дата обращения: 15.03.2018).

352. *Sherman J.* Griffin looking beyond guns, bombs to ensure future U.S. military superiority // Inside Defense. 2018. 31 October. URL: https://insidedefense.com/inside-pentagon/griffin-looking-beyond-guns-bombs-ensure-future-us-military-superiority (дата обращения: 21.02.2020).

353. *Siddiqui Sabena.* BRI, BeiDou and the Digital Silk Road // Asia Times. 2019. April 9. URL: https://www.asiatimes.com/2019/04/opinion/bri-beidou-and-the-digital-silk-road/ (дата обращения: 02.02.2020).

354. *Simons Ned.* Tory MP Sarah Wollaston switches sides in EU Referendum campaign. Huffpost politics. 2016. June. URL: https://consent.yahoo.com/collectConsent?sessionId=1_cc-session_aacf81e3-e862-4d14-bd5e-cbb861a13174&lang=en-gb&inline=false (дата обращения: 09.10.2019).

355. *Slaughter Anne-Marie.* Connections, not armies, make countries powerful // Financial Times. 2016. April. URL: https://www.ft.com/content/21973144-0544-11e6-9b51-0fb5e65703ce (дата обращения: 23.07.2019).

356. *Slaughter Anne-Marie.* The real new world order // Foreign Affairs. 1997. September. URL: http://www.columbia.edu/itc/sipa/S6800/courseworks/real_new_slaughter.pdf (дата обращения: 23.09.2019).

357. *Smith-Goodson Paul.* Quantum USA Vs. Quantum China: The World's Most Important Technology Race // Forbes. 2019. October 10. URL: https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#6c1f5f6472de (дата обращения: 01.02.2020).

358. Social Physics // Santa Fe Institute. 2015. URL: https://www.santafe.edu/events/social-physics (дата обращения: 19.04.2019).

359. Society's Nervous System: Building Effective Government, Energy, and Public Health Systems. A. Pentland in Computer, Vol. 45, No. 1. January 2012. pp. 31–38.

360. Sociocultural Behavior Research and Engineering in the Department of Defense Context // U.S. Department of Defense. 2013. 31 October. URL: https://info.publicintelligence.net/DoD-SocioculturalBehavior.pdf (дата обращения: 13.02.2018).

361. StratCom laughs: in search of an analytical framework // NATO Strategic Communications Centre of Excellence. 2016. URL: https://www.stratcomcoe.org/stratcom-laughs-search-analytical-framework (дата обращения: 05.06.2019).

362. State Dept. using app to connect with Iranians on coronavirus // FreePress. 2020. March 19. URL: https://freepressinternational.org/2020/state-dept-using-app-to-connect-with-iranians-on-coronavirus/ (дата обращения: 17.05.2020).

363. *Stephen C. Webster*. Exclusive: Military's 'persona' software cost millions, used for 'classified social media activities' // Rawstory. 2011. February 22. URL: https://www.rawstory.com/wpcontent/uploads/2011/03/personamanagementcontract.pdf (дата обращения: 12.09.2019).

364. *Stutman G*. Making memes in a warzone // The Outline. 2017. 3 August. URL: https://theoutline.com/post/2052/making-memes-in-a-warzone?zd=1&zi=jn3rcyra (дата обращения: 15.06.2018).

365. Summary of the 2018 Department of Defense Artificial Intelligence Strategy // US DOD. 2019. 12 February. URL: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF?fbclid=IwAR0iPoHeBD-hjWG6spK_6C9nJjADlqguh9ZwV_gHYRpUrq7M0Zj7dsbvTEA (дата обращения: 01.03.2019).

366. Summary of the 2018 National Defense Strategy // US Department of Defense. 2017. December. URL: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (дата обращения: 22.01.2018).

367. *Suna P. Kinnunen, Marjaana Lindeman, Markku Verkasalo.* Help-giving and moral courage on the Internet // Journal of Psychosocial Research on Cyberspace. 2016. URL: https://cyberpsychology.eu/article/view/6279/5890 (дата обращения: 24.07.2019).

368. Synthesizing Obama: Learning Lip Sync from Audio // Grail. 2017. October. URL: http://grail.cs.washington.edu/projects/AudioToObama/ (дата обращения: 20.10.2019).

369. *Tapson Mark.* The Soft Totalitarianism of Nudging. FrontpageMag. 2013. August 13. URL: https://archives.frontpagemag.com/fpm/soft-totalitarianism-nudging-mark-tapson/ (дата обращения: 24.06.2019).

370. *Thaler R., Sunstein C.* Nudge: Improving Decisions about Health, Wealth and Happiness, Yale University Press. 2008.

371. The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence // Congressional Research Service. 2020. March 20. URL: https://fas.org/sgp/crs/natsec/IF11469.pdf (дата обращения: 15.04.2020).

372. The Doomsday Machine by Daniel Ellsberg // San Francisco Chronicle. 2017. 7 December. URL: http://www.sfchronicle.com/books/article/The-Doomsday-Machine-by-Daniel-Ellsberg-12413956.php (дата обращения: 13.01.2019).

373. The EU's response to the coronavirus 'infodemic' // European Parliament. 2020. June 12. URL: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2020)651963 (дата обращения: 04.06.2020).

374. The Echo Chamber Revisited // WNYC. 2011. June 17. URL: https://www.wnyc.org/story/143347-echo-chamber-revisited/#transcript (дата обращения: 13.09.2019).

375. The Global Engagement Center: Leading the United States Government's Fight Against Global Disinformation Threat // U.S. Senate Committee on Foreign Relations. 2020. March 5. URL: https://www.foreign.senate.gov/hearings/the-global-engagement-center-leading-the-united-states-governments-fight-against-global-disinformation-threat (дата обращения: 15.04.2020).

376. The growing threat of internet addiction // European Science-Media Hub. 2019. January 9. URL: https://epthinktank.eu/2019/03/19/does-technology-exacerbate-social-polarisation/ (дата обращения: 22.07.2019).

377. The Iraq War continues to divide the U.S. public, 15 years after it began // Pew Research Center. 2018. March 19. URL: http://www.pewresearch.org/fact-tank/2018/03/19/iraq-war-continues-to-divide-u-s-public-15-years-after-it-began/ (дата обращения: 17.03.2018).

378. The Growing Need to Focus on Modern Political Warfare // RAND. 2019 URL: https://www.rand.org/pubs/research_briefs/RB10071.html (дата обращения: 12.09.2019).

379. The Harvard Project on the Soviet Social System Online // Harvard Library. 2018. June 14. URL: https://library.harvard.edu/collections/hpsss/index.html (дата обращения: 03.04.2020).

380. The UK's EU membership fee // Full Fact. 2016. 25 февраля. URL: https://fullfact.org/europe/our-eu-membership-fee-55-million/ (дата обращения: 10.10.2019).

381. The US-EU Rivalry for Data Protection: Energy Sector Implications // IFRI. 2019. February. URL: https://www.ifri.org/en/publications/editoriaux-de-lifri/edito-energie/us-rivalry-data-protection-energy-sector-implications (дата обращения: 20.05.2020).

382. These Are the World’s Healthiest Nations // Bloomberg. 2019. URL: https://www.bloomberg.com/news/articles/2019-02-24/spain-tops-italy-as-world-s-healthiest-nation-while-u-s-slips (дата обращения: 15.08.2019).

383. The Global Consequences of a Sino-American Cold War // Project Syndicate. 2019. May 20. URL: https://www.project-syndicate.org/commentary/united-

states-china-cold-war-deglobalization-by-nouriel-roubini-2019-05?barrier=accesspaylog (дата обращения: 09.04.2020).

384. *Thomas R.* Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976. pp. 3–13.

385. *Tilly Charles.* Social Movements, 1768—2004, Boulder, CO, Paradigm Publishers, 2004. pp. 262.

386. Trident Juncture shows NATO capabilities 'are real and ready'// NATO. 2015. 4 November. URL: https://www.nato.int/cps/en/natohq/news_124265.htm%20 (дата обращения: 05.06.2019).

387. *Triolo Paul, Allison Kevin, Brown Clarise.* Eurasia Group White Paper: The Geopolitics of 5G // Eurasia Group. 2018. November 15. URL: https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public%281%29.pdf (дата обращения: 03.02.2020).

388. Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive // The Wall Street Journal. 2018. August 15. URL: https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721 (дата обращения: 23.09.2019).

389. Tutorial: Military Memetics // Robotic Technology Inc. 2011. 24-26 October. URL: https://www.robotictechnologyinc.com/images/upload/file/Presentation%20Military%20Memetics%20Tutorial%2013%20Dec%2011.pdf (дата обращения: 05.09.2019).

390. UN: Decisive action needed to ban killer robots – before it's too late // Amnesty International. 2018. 27 August. URL: https://www.amnesty.org/en/latest/news/2018/08/un-decisive-action-needed-to-ban-killer-robots-before-its-too-late/ (дата обращения: 02.12. 2018).

391. Un mois de prison avec sursis requis contre le « gilet jaune » Eric Drouet // Le Monde. 2019. 15 février. URL: https://www.lemonde.fr/societe/article/2019/02/15/eric-drouet-figure-des-gilets-jaunes-au-tribunal-vendredi_5423716_3224.html (дата обращения: 10.10.2019).

392. Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation // Government Accountability Office. 2018 July 25. URL: https://www.gao.gov/assets/700/693817.pdf (дата обращения: 17.09.2019).

393. US Army, Tufts team up to advance cognitive science // DefenceTalk. URL: https://www.defencetalk.com/us-army-tufts-team-up-to-advance-cognitive-science-64761/ (дата обращения: 19.04.2019).

394. U.S. intel leaders warn of 'pervasive' Russian intrusions in 2018 amid tension with White House // Geostrategy-Direct. 2018. August 7. URL: http://geostrategy-direct-subscribers.com/u-s-intel-leaders-warn-of-pervasive-russian-intrusions-in-2018-amid-tension-with-white-house/ (дата обращения: 14.09.2019).

395. U.S. Leadership Image Suffers Most Among Friendly Nations // Gallup. 2018. February 20. URL: http://news.gallup.com/opinion/gallup/226997/leadership-image-suffers-among-friendly-nations.aspx (дата обращения: 13.03.2018).

396. US ‘outgunned & outmatched’ by Russia in Europe, claims top general seeking budget increase // RT. 2018. 9 March. URL: https://www.rt.com/usa/420836-general-russia-outgunned-nato/ (дата обращения: 05.04.2018).

397. U.S. Role in the World: Background and Issues for Congress // CRS. 2017. October 20. URL: https://fas.org/sgp/crs/row/R44891.pdf (дата обращения: 17.03.2018).

398. Van Cleave: U.S. a spies’ paradise, national-level counterintelligence eliminated // Geostrategy-Direct. 2018. 17 April. URL: http://geostrategy-direct-subscribers.com/van-cleave-u-s-a-spies-paradise-national-level-counterintelligence-eliminated/ (дата обращения: 10.12.2018).

399. Vision and Actions on Jointly Building Silk Road Economic Belt and 21stCentury Maritime Silk Road // Reconasia-production. 2015. March. URL: https://reconasia-production.s3.amazonaws.com/media/filer_public/e0/22/e0228017-7463-46fc-9094-0465a6f1ca23/vision_and_actions_on_jointly_building_silk_road_economic_belt_and_21st-century_maritime_silk_road.pdf (дата обращения: 20.02.2020).

400. *Waitt T.* SecureAuth unveils behavioral biometric technology in partnership with DARPA-endorsed BehavioSec // AST. URL: https://americansecuritytoday.com/secureauth-unveils-behavioral-biometric-technology-in-partnership-with-darpa-endorsed-behaviosec/ (дата обращения: 18.04.2019).

401. Water Wars: Disjointed Operations in the South China Sea // Lawfare. 2019. May 21. URL: https://www.lawfareblog.com/water-wars-disjointed-operations-south-china-sea (дата обращения: 08.04.2020).

402. *Weedon J., Nuland W., Stamos A.* Information Operations and Facebook // Facebook. 2017. April 27. URL: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf (дата обращения: 13.09.2019).

403. Western Balkans backsliding on democracy, says Lords committee // The Guardian. 2018. 10 January. URL: https://www.theguardian.com/politics/2018/jan/10/western-balkans-backsliding-on-democracy-says-lords-committee(дата обращения: 19.03.2018).

404. What is WikiLeaks // WikiLeaks. 2015. November. URL: https://wikileaks.org/What-is-Wikileaks.html (дата обращения: 10.12.2018).

405. White House Releases National Strategy for 5G Security // NextGov. 2020. March 25. URL: https://www.nextgov.com/emerging-tech/2020/03/white-house-releases-national-strategy-5g-security/164109/ (дата обращения: 19.05.2020).

406. *Wheeler Tom.* Preserving an open internet for consumers, small businesses, and free speech // Brookings Institution. 2019. February 7. URL: https://www.brookings.edu/testimonies/preserving-an-open-internet-for-consumers-small-businesses-and-free-speech/ (дата обращения: 22.07.2019).

407. White House Releases National Strategy for 5G Security // NextGov. 2020. March 25. URL: https://www.nextgov.com/emerging-tech/2020/03/white-house-releases-national-strategy-5g-security/164109/ (дата обращения: 14.04.2020).

408. White House report details Chinese theft of "future of the world" technology // Geostrategy-Direct. 2018. 26 June. URL: http://geostrategy-direct-subscribers.com/white-house-report-details-chinese-theft-of-future-of-the-world-technology/ (дата обращения: 11.12.2018).

409. Why Virtual Embassy? // U.S. Virtual Embassy Iran. 2020. URL: https://ir.usembassy.gov/ (дата обращения: 17.05.2020).

410. Will Knight.The US military is funding an effort to catch deepfakes and other AI trickery // MIT Technology Review. 2018. May 23. URL: https://www.technologyreview.com/s/611146/the-us-military-is-funding-an-effort-to-catch-deepfakes-and-other-ai-trickery/ (дата обращения: 23.05.2019).

411. *Williams Lauren C*. DOD struggles with loss of cyber personnel // FCW. 2018 September 28. URL: https://fcw.com/articles/2018/09/28/cyber-workforce-dod-williams.aspx (дата обращения: 01.10.2019).

412. *Wilson June*. The Disillusionment with Social Media // The Amplifier. 2018. December 18. URL: https://div46amplifier.com/2018/12/18/the-disillusionment-with-social-media/ (дата обращения: 22.07.2019).

413. *Wright Nicholas.* How Artificial Intelligence Will Reshape the Global Order // Foreign Affairs. 2019. URL: https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order?cid=nlc-fa_twofa-20180802 (дата обращения: 22.04.2020).

414. *Xuetong Yan* . The Age of Uneasy Peace. Chinese Power in a Divided World // Foreign Affairs. 2019. January/February. URL: https://www.foreignaffairs.com/articles/china/2018-12-11/age-uneasy-peace (дата обращения: 03.04.2020).

415. *Yixiang Xu.* Reviving China’s Health Silk Road Initiative? Battle of Narratives and Challenges for Transatlantic Leadership // American Institute for Contemporary German Studies, 2020. March. URL: https://www.aicgs.org/2020/03/reviving-chinas-health-silk-road-initiative-battle-of-narratives-and-challenges-for-transatlantic-leadership/ (дата обращения: 03.05.2020).

416. Ylen kysely: Venäjän kehitystä uhkana pitävien määrä laskenut roimasti – asiantuntijan mielestä luku on silti korkea // Yle. 2017. URL: https://yle.fi/uutiset/3-9972311 (дата обращения: 19.03.2018).

417. *Youyou W., Kosinski M., Stillwell D.* Computer-based personality judgments are more accurate than those made by humans // PNAS. 2015. January 27. URL: http://www.pnas.org/content/112/4/1036.full (дата обращения: 22.08.2019).

418. 90 Minutes a Day, Until 10 P.M.: China Sets Rules for Young Gamers // The New York Times. 2019. November 6. URL: https://www.nytimes.com/2019/11/06/business/china-video-game-ban-young.html (дата обращения: 08.11.2019).