JOURNAL OF INTERNATIONAL ANALYTICS

МЕЖДУНАРОДНАЯ АНАЛИТИКА

2020 / ТОМ 11 / НОМЕР 4

НОВОЕ ДЕСЯТИЛЕТИЕ: ТЕХНОЛОГИЧЕСКИЙ ФАКТОР В МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

21–38 И.В. ДАНИЛИН
Концептуализация стратегии США в технологической войне против КНР: экономика, политика, технонационализм

72–90 Г. САЙМОНС
Эволюция концепции смены режима и информационные войны в XXI веке

122–136 З.А. МАМЕДЬЯРОВ
Стратегическое значение фармацевтической отрасли в условиях пандемии коронавируса

147–170 О.И. ШАКИРОВ
Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве

ISSN (print) 2587-8476 ISSN (online) 2541-9633

ИМИ МГИМО МИД РОССИИ
2020

2020 / VOLUME 11 / No. 4
Meždunarodnaâ analitika

CHIEF EDITOR

Sergey Markedonov
MGIMO University (Russia)

DEPUTY EDITOR

Akhmet Yarlykapov
MGIMO University (Russia)

EDITORIAL BOARD

Andrew Kuchins – American University of Central Asia (Kyrgyzstan)
Benedict Harzl – University of Graz (Austria)
Bjorn Wittrock – Uppsala University (Sweden)
Erkin Baydarov – R.B. Suleimenov Institute of Oriental Studies (Kazakhstan)
Irina Busygina – National Research University Higher School of Economics (Russia)
Kimitaka Matsuzato – University of Tokyo (Japan)
Marlene Laruelle – George Washington University (USA)
Mitat Celikpala – Kadir Has University (Turkey)
Richard Sakwa – University of Kent (UK)
Sanjay Deshpande – University of Mumbai (India)
Sayed Mohammad Kazem Sajjadpour – Institute for Political and International Studies (Iran)
Viacheslav Morozov – University of Tartu (Estonia)
Zhao Huasheng – Fudan University (China)
Alexander Chechevishnikov – MGIMO University (Russia)
Andrei Sushentsov – MGIMO University (Russia)
Dmitriy Pobedash – Ural Federal University (Russia)
Ilya Tarasov – Immanuel Kant Baltic Federal University (Russia)
Larisa Deriglazova – Tomsk State University (Russia)
Lyubov Fadeeva – Perm State University (Russia)
Michael Rykhtik – Lobachevsky State University of Nizhni Novgorod (Russia)
Natalya Eremina – Saint-Petersburg State University (Russia)
Oleg Mikhalev – Voronezh State University (Russia)
Pavel Parshin – Moscow State Linguistic University (Russia)
Valeriy Konyshev – Saint-Petersburg State University (Russia)
Viktor Apryshchenko – Southern Federal University (Russia)
Viktor Larin – Institute of History, Archaeology and Ethnology, the Far Eastern Branch of Russian Academy of Sciences (Russia)
Yakov Grishin – Kazan Federal University (Russia)

The journal publishes research results in the field of international relations and world politics, regional studies, and the history of international relations.
Published since 2010, 4 times a year.

The journal is included in Russian Science Citation Index.

Mass media registration certificate
PI No. FS77-65736 of May 20, 2016

DOI Prefix 10.46272
ISSN (print) 2587-8476
ISSN (online) 2541-9633

FOUNDER

Federal State Autonomous Educational Institution of Higher Education “Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation”

EDITORS

Dmitry Tkach
Grant Beglarian
Natalia Samoylovskaya
Nikita Neklyudov
Vladimir Pavlov

COMPUTER LAYOUT

Alexey Talalaevsky

DESIGN

Veronika Levitskaya

2020 / ТОМ 11 / № 4

ГЛАВНЫЙ РЕДАКТОР

Сергей Мирославович Маркедонов
(МГИМО МИД России)

ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА

Ахмет Аминович Ярлыкапов
(МГИМО МИД России)

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Бенедикт Гарцль – Университет Граца (Австрия)
Бьёрн Виттрок – Уппсальский университет (Швеция)
Вячеслав Евгеньевич Морозов – Тартуский университет (Эстония)
Еркин Уланович Байдаров – Институт востоковедения имени Р.Б. Сулейменова (Казахстан)
Ирина Марковна Бусыгина – НИУ ВШЭ (Россия)
Кимитака Мацузато – Токийский университет (Япония)
Марлен Ларюэль – Университет Джорджа Вашингтона (США)
Митат Челикпала – Университет Кадир Хас (Турция)
Ричард Саква – Кентский университет (Великобритания)
Сайед Мохаммед Казем Саджадпур – Институт политических и международных исследований (Иран)
Санджай Дешпанде – Университет Мумбаи (Индия)
Чжао Хуашэн – Фуданьский университет (Шанхай)
Эндрю Качинс – Американский университет в Центральной Азии (Киргизия)
Александр Леонидович Чечевишников – МГИМО МИД России (Россия)
Андрей Андреевич Сушенцов – МГИМО МИД России (Россия)
Валерий Николаевич Конышев – Санкт-Петербургский государственный университет (Россия)
Виктор Лаврентьевич Ларин – Институт истории археологии и этнографии народов Дальнего Востока Дальневосточного отделения Российской академии наук (Россия)
Виктор Юрьевич Апрыщенко – Южный федеральный университет (Россия)
Дмитрий Иванович Победаш – Уральский федеральный университет имени Б.Н. Ельцина, Екатеринбург (Россия)
Илья Николаевич Тарасов – Балтийский федеральный университет имени И. Канта (Россия)
Лариса Валерьевна Дериглазова – Томский государственный национальный исследовательский университет (Россия)
Любовь Александровна Фадеева – Пермский государственный национальный исследовательский университет (Россия)
Михаил Иванович Рыхтик – Нижегородский государственный национальный исследовательский университет имени Н.И. Лобачевского (Россия)
Наталья Валерьевна Еремина – Санкт-Петербургский государственный университет (Россия)
Олег Юрьевич Михалёв – Воронежский государственный университет (Россия)
Павел Борисович Паршин – Московский государственный лингвистический университет имени Мориса Тореза (Россия)
Яков Яковлевич Гришин – Казанский федеральный университет (Россия)

В журнале публикуются результаты исследований в области международных отношений и мировой политики, регионоведения, а также истории международных отношений.
Издается с 2010 г.
Выходит 4 раза в год.

Журнал включен в РИНЦ.

Свидетельство о регистрации средства массовой информации ПИ № ФС77–65736 от 20 мая 2016 г.

DOI Prefix 10.46272
ISSN (print) 2587-8476
ISSN (online) 2541-9633

УЧРЕДИТЕЛЬ

Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации»

РЕДАКТОРЫ ВЫПУСКА

Владимир Владимирович Павлов
Грант Артурович Бегларян
Дмитрий Николаевич Ткач
Наталья Александровна Самойловская
Никита Яковлевич Неклюдов

КОМПЬЮТЕРНАЯ ВЕРСТКА

Алексей Владимирович Талалаевский

ДИЗАЙН

Вероника Евгеньевна Левицкая

W

СОДЕРЖАНИЕ

СЛОВО РЕДАКТОРА

«Крылья» международных отношений: технологии в современном мире
С.М. МАРКЕДОНОВ 7

ИНТЕРВЬЮ

Новые формы и методы дипломатии
Р.О. РАЙНХАРДТ 11

ИССЛЕДОВАТЕЛЬСКИЕ СТАТЬИ

Концептуализация стратегии США в технологической войне против КНР: экономика, политика, технонационализм
И.В. ДАНИЛИН 21

Решение стратегического уравнения: интеграция противоракетной обороны и обычных вооружений в российско-американский режим контроля над вооружениями
А.А. БАКЛИЦКИЙ 39

Угроза применения обычных видов вооружений для ядерной безопасности: новая реальность с точки зрения сдерживания
П. РАУТЕНБАХ 56

Эволюция концепции смены режима и информационные войны в XXI веке
Г. САЙМОНС 72

Анализ примеров использования хэштегов как средства координации протестных движений
А.В. АЛЕКСЕЕВ 91

Ислам и прогресс: между традицией и современностью
Ю. РОКНИФАРД О. ГАФАРЛЫ Л. ТЕРЕБЕССИ 104

ОБЗОРНЫЕ СТАТЬИ

Стратегическое значение фармацевтической отрасли в условиях пандемии коронавируса
З.А. МАМЕДЬЯРОВ 122

Смертоносные автономные системы с искусственным интеллектом: как избежать превосходства
Н.А. САМОЙЛОВСКАЯ 137

Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве
О.И. ШАКИРОВ 147

РЕЦЕНЗИЯ

О теории космической мощи
Д.В. СТЕФАНОВИЧ 171

CONTENT

EDITORIAL NOTE

The "Wings" of International Relations: Technology in Today's World
S. MARKEDONOV 7

INTERVIEW

New Forms and Methods of Diplomacy
R. REINHARDT 11

RESEARCH ARTICLES

Conceptualizing American Strategy in the Technology War Against China: Economy, Geopolitics, Techno-Nationalism
I. DANILIN 21

Solving the Strategic Equation: Integrating Missile Defense and Conventional Weapons in U.S.–Russian Arms Control
A. BAKLITSKIYV 39

The Threat of Conventional Weapons to Nuclear Security: A New Reality for Deterrence
P. RAURENBACH 56

The Evolution of Regime Change and Information Warfare in the 21st Century
G. SIMONS 72

Hashtagging as an Identifier of Political Transformations in the Digital Age
A. ALEKSEEV 91

Islam and Progress: Between Tradition and Modernity
J. ROKNIFARD O. GAFARLI L. TEREBESSY 104

RESEARCH ESSAYS

Strategic Role of the Pharmaceutical Industry in the Context of the Global Pandemic
Z. MAMEDYAROV 122

LAWS with AI: How to aBANdon the Superiority
N. SAMOYLOVSKAYA 137

Whoever Comes to Us with a Cyber Sword: Russian and U.S. Approaches to Deterrence in Cyberspace
O. SHAKIROV 147

REVIEW

On Theory of Space Power
D. STEFANOVICH 171

«Крылья» международных отношений: технологии в современном мире

https://doi.org/10.46272/2587-8476-2020-11-4-7-10

Первую главу своей знаменитой книги-прогноза американский футуролог Элвин Тоффлер назвал «Конец постоянства»[1]. Эта метафора как нельзя лучше передает то состояние, в котором пребывает современный мир. Турбулентность и непредсказуемость внутри-и внешнеполитических процессов существенно увеличивается. Привычные иерархии, альянсы ставятся под сомнения, устоявшиеся ценности оспариваются. И даже вокруг событий прошлого ведутся интенсивные «войны памяти» за право устанавливать «единственно правильные» исторические нарративы[2]. Понятие «новой нормальности», применяемое изначально к определенным социально-экономическим особенностям развития (низкие темпы роста и высокая безработица), перекочевало в общественные науки и стало использоваться в оценке стремительно меняющихся реалий[3].

В дискуссиях о «конце постоянства» значительное место занимает роль и значение научно-технологических достижений. По словам Тоффлера, «высокую скорость перемен можно отследить по многим факторам. Рост населения, урбанизация, меняющееся соотношение молодых и стариков, – все играет свою роль. Однако развитие технологий, очевидно, – решающий узел в сети причин; действительно, это узел, который активизирует всю сеть»[4]. Американский антрополог Эдвард Холл, размышляя о взаимовлиянии биологического и общественного развития, пришел к выводу о технологии как «продолжении биологической эволюции, способе человека отрастить себе крылья, ноги и хвост, не дожидаясь, пока это сделает за него природа»[5].

1 *Тоффлер, Э.* Шок будущего. – М.: АСТ, 2002. – 212 с.
2 Политика памяти в современной России и странах Восточной Европы. Акторы, институты, нарративы: коллективная монография / под ред. А.И. Миллера, Д.В. Ефременко. – СПб.: Издательство Европейского университета в Санкт-Петербурге, 2020. – 632 с.
3 *Юдаева, К.В.* New Normal для России. Научный доклад. – М.: Издательский дом «Дело» РАНХиГС, 2013. – 20 с.
4 *Тоффлер, Э.* Шок будущего.
5 Hall, Edward T. *Beyond Culture.* N.Y.: Anchor Books, 1989. P. 38

CC BY

В этом контексте важно понять и адекватно оценить, в какой степени технология является или может являться революционным фактором по отношению к международной политике. Можно ли говорить о том, что приход «цифрового века», растущее значение социальных сетей, радикальное обновление видов вооружений, появление новых видов вакцин отменяет или принципиально изменяет межгосударственные противоречия, национальные интересы, конфликты, военное и дипломатическое искусство? Речь в данном случае не о форме, а о содержании. Ряд исследователей совершенно справедливо указывают на растущее значение информационных технологий в сдерживании конкурентов и оппонентов на международной арене[1]. Но в данном случае мы говорим о меняющихся инструментах, а не о принципиальном изменении целеполагания. Компьютер отодвинул на второй (хотя и не вытеснил полностью) автоматическое оружие и артиллерийские системы. Но суть самого сдерживания от этого не поменялась: оно лишь стало более искусным научно и технически. Не менее популярным сегодня является и концепт «гибридной войны», понимаемой как использование непрямых действий для нанесения ущерба противостоящей стороне[2].

Но если вынести за скобки такие реалии современности, как киберпространство, разве поддержание внутренней нестабильности на территории противника через поддержку повстанцев, диверсии, коррупцию политического истеблишмента без объявления войны открыли в начале XXI в. и ничего подобного мы не видели раньше в диапазоне от французской Ла-Рошели до казачьих походов на Азов и Топкапы?

В свое время известный немецкий философ Юрген Хабермас, наблюдая за стремительным научно-техническим прогрессом, предложил формулу «деполитизации» традиционных идеологий[3]. На завершающем этапе холодной войны и в первые годы после нее большой популярностью пользовалась идея о технологическом прорыве, как важнейшей предпосылке глобализации, о стирании граней между государствами и традиционно понимаемыми национальными интересами[4]. Однако по прошествии тридцати лет мы видим, что новейшие научно-технические достижения никак не мешают США бороться за сохранение глобального доминирования, а Китаю и России – оспаривать его. Как следствие, появление в медийном, экспертном и академическом языке таких понятий, как «вакцинная дипломатия»[5] или конкуренция «техноэкономических блоков»[6]. При этом прикладное использование науки и техники нередко идет рука об руку с архаизацией общественных отношений, что блестяще продемонстрировал пример пресловутого «Исламского государства»[7].

Стремительное технологическое развитие гарантированно обеспечивает миру «конец постоянства». Но эти перемены совсем не обязательно радикально

1 *Смирнов, А.И.* Современные информационные технологии в международных отношениях. М.: МГИМО-Университет, 2017. – С. 10–11.
2 Hoffman, Frank G. *Conflict in the 21-st century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, 2007. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
3 *Хабермас, Ю.* Техника и наука как «идеология». – М.: Праксис, 2007. – С. 86, 92, 101.
4 *Альтерматт, У.* Этнонационализм в Европе. – М.: РГГУ, 2000. – 366 с.
5 "The Era of Vaccine Diplomacy Is Here," The New York Times, accessed March 4, 2021, http://surl.li/mtli.
6 Международные угрозы. Каждый за себя / Отв. ред. А.А. Сушенцов // МГИМО МИД России. [Электронный ресурс]. URL: https://mgimo.ru/upload/iblock/2ac/int-threats-2020.pdf (дата обращения 04.03.2021).
7 Организации, запрещенной в России.

трансформируют систему международных отношений. Они дают в руки конкурирующих игроков новые инструменты, но не отменяют самой конкуренции. И, несмотря на то что коммуникация становится глобальной, отдельные «коммуникаторы» не спешат отказаться от своих собственных интересов. Получается, что от болезней страдает все человечество, а борьба за более качественные рецепты их лечения превращается в еще одну арену для соперничества.

Представляемый читателю четвертый номер журнала «Международная аналитика» посвящен влиянию современных технологий на политические процессы глобального, межгосударственного и регионального характера. Его открывает интервью с Романом Райнхардтом, посвящённое новым формам и методам дипломатии. Оправдано ли с научной точки зрения появление конструктов «цифровая дипломатия» или «климатическая дипломатия», и не выглядят ли конъюнктурными дефиниции, ставшие ныне широко популярными? В интервью также рассматриваются такие вопросы, как сочетание «классической» и негосударственной дипломатии, влияние новейших научных изобретений на процесс формирования и принятия внешнеполитических решений.

В статье Ивана Данилина рассматривается американо-китайское технологическое соперничество. Весьма продуктивным представляется используемое автором понятие «технонационализм». С его точки зрения, технологический конфликт Вашингтона и Пекина «является новым феноменом, определяемым в том числе спецификой цифровых технологий и экономическими изменениями последних десятилетий, а также сохраняющим естественную преемственность с геополитическими и экономическими конфликтами прошлого и с существующими стратегиями и инструментарием».

Различным аспектам другого технологического соперничества, российско-американского, посвящены работы Андрея Баклицкого и Олега Шакирова. И если первый автор обращается к такой теме, как контроль над вооружениями, то второй – к сфере кибербезопасности. В статье Баклицкого рассматриваются две области, которые будут затронуты Москвой и Вашингтоном на будущих переговорах после продления договора СНВ-3. Это – противоракетная оборона и стратегические обычные вооружения. Шакиров фокусируется на вопросах интерпретаций концепции сдерживания в киберпространстве, имеющихся в США и в России.

Питер Раутенбах обращается к такому исследовательскому сюжету, как угроза со стороны новых обычных вооружений, привычному со времен холодной войны формату ядерного сдерживания. Автор полагает, что наличие у США систем обычных вооружений «Быстрый глобальный удар» по своей природе опасно, поскольку оно повышает как вероятность их применения, так и нанесения первого удара по системам ядерного сдерживания другого государства.

Пандемия коронавирусной инфекции актуализировала значение фармацевтической отрасли и ее научно-технологического влияния на международные процессы. Этому вопросу посвящен текст Заура Мамедьярова. Автор полагает, что ситуация с глобальным распространением COVID-19 четче высветила ранее существующие проблемы, среди которых наиболее важными являются эффективность распределения медикаментов среди граждан, роль государства в организации санитарно-эпидемиологических мер по сдерживанию пандемии,

наличие технологий, позволяющих минимизировать риски заболеваний и предотвращать их в будущем.

Различные аспекты современных информационных технологий и их воздействие на общественно-политические процессы рассматриваются в статьях Грега Саймонса и Александра Алексеева. Первый автор обращается к эволюции информационных войн и технологий смены режимов в начале XXI в. как способов непрямого воздействия на государства ради достижения национальных интересов их противников, тогда как второй автор – исследует феномен хэштэгов как технологий, стимулирующих протестные движения через социальные сети.

Науку, технический прогресс и религию обычно принято противопоставлять, хотя в действительности их взаимодействие и взаимовлияние намного сложнее. В статье Юлии Рокнифард, Орхана Гафарлы и Лесли Теребесси осмысливается отношение к прогрессу в странах исламского мира. Материал имеет два пласта: дискуссию мусульманских теологов и общественных мыслителей Востока о коллизиях между традицией и инновациями и тематические кейсы Ирана и Турции, которые авторы определяют, как «основные силы и идеологии» в исламском мире, «поощрявшие или препятствующие модернизации и технологическому прогрессу».

Проблемам военного применения искусственного интеллекта посвящена обзорная статья Натальи Самойловской. Автор рассматривает возможные политические последствия использования этой технологии, а также связанные с этим психологические и военные риски. Выход из ситуации Самойловская видит в разработке общей платформы и стандартов для применения искусственного интеллекта в военной области.

С того времени, как президент США Рональд Рейган объявил о программе «Стратегическая оборонная инициатива», получившей также известность как «Звездные войны», возможность ведения боевых действий в космосе стала не только сюжетом из научной фантастики, но и актуальным академическим и прикладным вопросом. Дмитрий Стефанович подготовил рецензию на книгу Бледдина Боуэна «Война в космосе. Стратегия, космическая мощь, геополитика».

Не исключено, что новые научно-технические достижения приведут не только к изменению форм конфронтации, конкуренции, кооперации, но и к существенным трансформациям их содержания. Пока же – вслед за Эдвардом Холлом можно сказать, что обретенные с помощью технологий крылья человека выросли и даже укрепились. Остается до сих пор не отвеченным вопрос, будет ли это укрепление во благо всему человечеству.

С.М. Маркедонов, главный редактор

Новые формы и методы дипломатии

https://doi.org/10.46272/2587-8476-2020-11-4-11-20

Интервью с Романом Райнхардтом, доцентом кафедры дипломатии МГИМО МИД России

АННОТАЦИЯ

Р.О. Райнхардт – доцент кафедры дипломатии МГИМО МИД России, специалист в области истории и теории дипломатии, руководитель и исполнитель ряда крупных проектов, посвященных дипломатической проблематике и поддержанных ведущими российскими научными фондами (РНФ, РФФИ). Его основные научные интересы охватывают такие темы, как экономическая дипломатия, научная дипломатия, международное научно-техническое сотрудничество в контексте российской внешней политики, а также внешних связей ЕС. Окончил МГИМО МИД России. В 2016 г. получил ученую степень кандидата экономических наук.

Беседу вел С.М. Маркедонов, главный редактор журнала «Международная аналитика»

Сергей Маркедонов: В настоящее время наблюдается рост многообразия различных форм и видов дипломатии. В специализированной литературе, не говоря уже о СМИ, можно встретить такие словосочетания как «научная дипломатия», «климатическая дипломатия», «цифровая дипломатия» и другие. Какие из данных понятий, с Вашей точки зрения, действительно имеют право на жизнь, а какие предстают, скорее, конструктами, которые едва ли пройдут проверку временем?

Роман Райнхардт: Как Вы совершенно верно отметили, со сравнительно недавних пор возникла мода на использование слова «дипломатия» в качестве своего рода «приставки» ко многим направлениями деятельности, где фактически или потенциально имеет место международное сотрудничество[1]. Отсюда не только те виды дипломатии, которые Вы перечислили, но также и «нефтяная», «долларовая», «спортивная» – вплоть до «дипломатии знаменитостей» (*celebrity diplomacy*)[2]. Иными словами, наблюдается некоторая «инфляция» этого изначально предельно узкого термина. В русле нарастающего перехода внешнеполитического нарратива в цифровую плоскость дипломатия становится, в известной

1 *Райнхардт, Р.О.* Настольная книга исследователя дипломатии // Мировая экономика и международные отношения. – 2017. – Т. 61 (4). – С.119–122.

2 Cooper, Andrew F. *Celebrity Diplomacy.* 1st Edition. London: Routledge, 2007.

CC BY

степени, хештегом, позволяющим различным деятелям набирать популярность путем аккумуляции лайков и репостов под лозунгом #ядипломат. При этом их отношение к дипломатии в классической трактовке может зачастую быть весьма опосредованным.

Если же рассматривать вопрос в историко-теоретическом ключе, то дипломатия – это, прежде всего, инструмент. Первые упоминания о дипломатии встречаются в древнейших образцах письменности: это и исторические памятники ранних цивилизаций, и литературные произведения (начиная, скажем, с «Истории Пелопонесской войны»), и дошедшие до нас религиозные источники, которые до сих пор не теряют своей актуальности. При этом методы дипломатии, описанные в те времена, несмотря на диктуемые процессом социального развития объективные метаморфозы, имеют свойство воплощать в себе некоторые константы.

Дипломатию однозначно можно отнести к самым древним и долговечным формам общественной и политической деятельности.

Например, эпизоды, трактуемые современными российскими и зарубежными исследователями в ключе так называемой дипломатии принуждения[1], описаны, в частности, в Пятикнижии Моисея. Упоминание, пусть и без глубокого анализа, торговых санкций, иногда относимых к арсеналу экономической дипломатии, присутствует на страницах названного труда Фукидида[2]. Институт проксенов, распространенный в Древней Греции, – прямой исторический предок нынешних почетных консулов. Все это частные примеры. В общем же плане допустимо говорить о том, что дипломатия как функциональное выражение внешней политики есть, по существу, реакция вневременного института на текущие события на международной арене.

С моей точки зрения, наиболее корректно было бы говорить не о «научной дипломатии», а об использовании дипломатических методов в международном научно-техническом сотрудничестве и так далее. Подобный подход может показаться педантичным, однако думается, что его применение в методологическом плане поможет избежать преумножения двусмысленностей. Согласитесь, что их пестрота иногда лишь запутывает исследователей – от экспертов до новичков – и рядовых читателей. Анализ предметного поля и его отдельных разделов показывает, что придать ему контуры с помощью «бритвы Оккама» было бы нелишним. Более того, с ростом числа работ по соответствующей тематике данная необходимость предстает все более острой для дальнейшего успешного развития теории.

С.М.: То есть, по Вашему мнению, уместнее говорить о дипломатии как о чем-то едином и универсальном, что по природе своей может применяться в любых сферах и, следовательно, не должно привязываться к ним. Например, дипломатия в области климатического, экономического сотрудничества и прочее.

Р.Р.: Совершенно верно. На основе глубокого изучения современной специализированной литературы можно сказать, что в последнее время многие ис-

1 *Зонова, Т.В.* Дипломатия принуждения. Казус Ливии // Международные процессы. – 2017. – Т.15 (1). – С.35–48.
2 Okano-Heijmans, Maaike. “Conceptualizing Economic Diplomacy: The Crossroads of International Relations, Economics, IPE and Diplomatic Studies.” In *Economic Diplomacy: Economic and Political Perspectives,* 2011. doi:10.1163/9789004209619_003.

следователи чересчур увлеклись анализом отдельных проявлений и форм международного сотрудничества. А вот синтеза, который бы позволил «увидеть лес за деревьями», пока что, как представляется, не хватает. Важно понимать, что дипломатия – будь то онлайн или офлайн, по классическим или новым трекам переговоров – все-таки едина. Более того, полагаю, что, рассуждая о ней, следует быть весьма аккуратным и острожным в терминах и формулировках.

Помню, когда готовил свою кандидатскую диссертацию по экономической дипломатии, первый, при этом весьма объемный параграф, пришлось посвятить анализу различных трактовок этого понятия[1]. И отечественные, и зарубежные работы, которые продолжают писаться сейчас, как правило, начинаются с определения экономической дипломатии как достижения экономических целей политическими средствами или наоборот. Либо же вовсе нечто иное. По сути, это напоминает схоластический и иногда, доходя до крайности, чуть ли не богословский спор: значение экономической дипломатии по Ги Каррон де ла Каррьеру[2], В. Щетинину[3], Д. Дегтереву[4], Р. Райнхардту[5] и т. д. Отталкиваясь же от того, что мы просто говорим о дипломатии во внешнеэкономических связях, можно сразу избежать подобных квази-теоретических диспутов. Более того, такой подход сразу позволит включить множественные труды, посвященные обозначенной проблематике, в которых, однако, сам названный термин не фигурирует. Другими словами, вопрос во многом касается тегирования и работы с метаданными.

Для простоты коммуникации внутри экспертного сообщества использование отдельных «дипломатий», как то: экономической, научной, климатической и т. п., вполне уместно.

Некоторые словосочетания уже прочно устоялись, другие, наоборот, – постепенно выходят из употребления. Что станет с третьими – покажет время. Вместе с тем стоит, по-моему, всегда держать в уме, что по смыслу речь здесь идет не об эпитетах дипломатии, но о ней как инструментарии внутри соответствующих сфер. Иначе говоря, не дипломатия принципиально различается в зависимости от точки ее приложения, но сами точки приложения имеют ту или иную специфику.

С.М.: А как же быть с «челночной дипломатией» Г. Киссинджера, упомянутой Вами «дипломатией принуждения» и, наконец, пресловутой «цифровой»? И к чему в таком случае сводится общий знаменатель всех перечисленных видов дипломатической активности – как было принято говорить раньше, к ее мирной и миротворческой природе в качестве антипода военной агрессии?

Р.Р.: Что касается первой части вопроса, то при попытке ответа на него есть риск погрязнуть в сугубо научной полемике с рассмотрением частных и заведо-

1 *Райнхардт, Р.О.* Сравнительный анализ систем экономической дипломатии в странах Европейского союза: автореферат диссертации на соискание ученой степени кандидата экономических наук / Московский государственный институт международных отношений (университет). – Москва, 2016. – 30 с.
2 *Каррон де ла Каррьер, Ги.* Экономическая дипломатия. Дипломат и рынок. Перевод О.И. Пичугина. – М.: РОССПЭН, 2003. – 294 с.
3 *Щетинин, В.Д.* Экономическая дипломатия: Учебное пособие. – М.: Международные отношения, 2001. – 280 с.
4 *Дегтярев, Д.А.* Экономическая дипломатия: экономика, политика, право. – М.: NAVONA, 2010. – 174 с.
5 *Райнхардт, Р.О.* Развитие теории экономической дипломатии в России 2000–2018 гг.: наукометрический и институциональный анализ // Научный диалог. – 2019. – №2. – С.283–295.

мо субъективных видений таких феноменов. Чтобы избежать этого, предлагаю относиться к перечисленным, равно как и другим схожим представлениям о дипломатии, которые можно встретить, не более чем как к журналистским клише. Широкой аудитории просто о дипломатии читать скучно. А вот какая-нибудь «дипломатия-катализатор»[1] или «твипломатия»[2] сразу вызывают интерес – что же это за новое слово и дело. Можно к этому относиться как угодно, но, как представляется, определенная доля скепсиса и критического восприятия не помешают. Впрочем, это лишь методологическое предостережение, носящее во многом проблемно-постановочный характер.

Относительно второй части вопроса – вновь соглашусь с Вами, однако с оговоркой о том, что в современной турбулентной среде становится все сложнее судить категорично, если подразделять все средства государственной внешней политики только на военные и на дипломатические. Именно по этому пути шел Г. Гроций и целый ряд других мыслителей. Мир в значении *реальность*, (здесь обращу ваше внимание на омонимичность и многозначность нашего языка, ибо в дореволюционной орфографии в этом значении слово было принято писать через «і десятеричное»: *мiр*ъ) безусловно, представляет собой не дихотомию черного и белого и даже не «оттенки серого», но целую палитру красок разной интенсивности. Те же экономические санкции можно рассматривать и как попытку цивилизованного разрешения имеющихся противоречий между государствами (не стреляют же!), и как форму гибридной войны.

Уже в 2009 г. на доктринальном уровне был обозначен переход от «мягкой силы» к «умной силе», не просто допускающей, но напрямую стимулирующей дипломатов к проведению информационных атак, направленных на дестабилизацию политических систем неугодных режимов.

При этом некоторыми акторами международных отношений сама категория миротворчества воспринимается в абстрактном, зачастую искаженном или, во всяком случае, субъективном ключе. Так, при взаимодействии с отдельными партнерами все чаще приходится сталкиваться с оригинальными интерпретациями дипломатической активности, равно как и этики. Яркий тому пример – концепция «трансформационной дипломатии», впервые представленная в 2006 г. К. Райс, занимавшей в то время должность госсекретаря США. Продвижение демократических ценностей (причем именно так, как их видят сами американцы) любыми средствами, не исключающее вмешательство во внутренние дела суверенных государств, фактически заложило основу для тех самых гибридных войн. Такой цинизм во многом определил вектор внешней политики двух предыдущих администраций Белого дома. В совокупности с другими факторами это привело к росту напряженности на международной арене, углубило и без того имеющиеся противоречия между странами.

1 Stone, Jeremy J. *Catalytic Diplomacy: Russia, China, North Korea and Iran.* Charleston: BookSurge Publishing, 2010.
2 *Рябинченко А.В.* Цифровая дипломатия вчера и сегодня // РСМД. 16 ноября 2018. [Электронный ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/columns/digitaldiplomacy/tsifrovaya-diplomatiya-vchera-i-segodnya/ (дата обращения 10.02.2021).

А с 2017 г. во внешнеполитическом нарративе стала широко употребляться очередная производная идеи Д. Ная, «острая сила» (*sharp power*), предполагающая еще более изощренное манипулирование общественным мнением за рубежом усилиями дипломатов[1]. Правда, используется эта категория почему-то в основном применительно к Китаю и России. Хочется надеяться, что новая вашингтонская администрация не продолжит следовать по тому же пути. Но стоит ли после всего этого удивляться разговорам о войне, мире и в конечном счете гибридной дипломатии?

С.М.: Худой мир лучше доброй ссоры. В этом контексте можно вспомнить и слова Н. Макиавелли о том, что войны нельзя избежать, но можно лишь отсрочить к выгоде противника, и формулу мирного сожительства В.И. Ленина, и мысль Р. Арона о солдате и дипломате как основных сменяющих друг друга действующих лицах мировой политики. При этом некоторые авторы придерживаются мнения о том, что раньше грань между этими проявлениями внешней политики была более явной, а дипломатия до того, как к ней подключились новые негосударственные акторы, – более эффективной. Согласны ли Вы с таким утверждением?

Р.Р.: Рассуждения о том, что раньше все было проще, понятнее и, стало быть, в чем-то лучше, на мой взгляд, принципиально неприемлемы. Во время Второй мировой войны, когда солдаты гибли миллионами, а крематории Освенцима и Бухенвальда работали на полную мощность, грань между добром и злом, между миром и войной была четкой и явной. Все было понятно, но эта осознаваемая всеми реальность была пропитана ужасом. Миссия дипломатии состоит в том, чтобы такая трагедия никогда не повторилась.

Как показала практика, перед лицом угроз и вызовов сегодняшнего дня усилий только классических дипломатов, т. е. сотрудников государственных органов внешних сношений, недостаточно, чтобы избежать катастрофы. Данное обстоятельство в известной степени обусловливает и, если угодно, легитимирует развитие так называемой общественной, гражданской, народной дипломатии (при желании синонимичный ряд можно продолжить). В роли участников дипломатических процессов, все чаще становящихся субъектами международных контактов, выступают новые институты, консолидирующие интересы различных социальных групп: делового, академического сообщества, религиозных объединений, наконец, частных лиц. В XXI в. эффективно бороться за мир можно только всем «миром», т. е. родом человеческим. Такая установка находит отражение не только в трудах исследователей, но и в стратегических документах, определяющих политику, в частности, в действующей Концепции внешней политики РФ[2]. Таким образом в миротворческую деятельность активно вовлекается широкий спектр протагонистов, а любой индивид становится не только «сапиенсом», но и, выражаясь фигурально, *homo diplomaticus.*

1 Cristopher Walker, and Jessica Ludwig, “The Meaning of Sharp Power. How Authoritarian States Project Influence,” Foreign Affairs, November 16, 2017, accessed February 10, 2021, https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

2 Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В.В. Путиным 30 ноября 2016 года // МИД РФ. 1 декабря 2016. [Электронный ресурс]. URL: https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2542248 (дата обращения: 10.03.2021).

Безусловно, по некоторым вопросам классические и даже секретные дипломатические переговоры способны дать бóльший результат, чем всеобщий мозговой штурм. Однако обозначенные упрощение и демократизация дипломатии – объективные процессы. По сути, это и представляет собой *modus vivendi* старого и нового, системного и несистемного. Попытки противостоять ему – как с одной, так и с другой стороны – несут в себе риски радикализации соответствующих групп интересов.

С.М.: То, что дипломатия за мир, про мир, о мире, и в нее вовлекается все большее число людей доброй воли, мы уяснили. Но все-таки, если цитировать классика, «вызывает антирес ваш технический прогресс». Общеизвестно, что наряду с развитием высоких технологий он выступает значимым фактором современных международных отношений. Это неоднократно анализировалось экспертами. Однако каким образом данные факторы влияют именно на дипломатические практики в прямом и узком значении этого понятия?

Р.Р.: Возьмем простой, но, с моей точки зрения, важный пример. В статье 36, пункте 2 Венской конвенции о дипломатических сношениях 1961 г. сказано, что «личный багаж дипломатического агента освобождается от досмотра, если нет серьезных оснований предполагать, что он содержит <запрещенные> предметы ...». Далее та же статья гласит, что если все-таки подозрения есть, то «такой досмотр должен производиться только в присутствии дипломатического агента или его уполномоченного представителя»[1].

Когда Конвенция писалась и ратифицировалась, особых сложностей в технической трактовке этого положения не возникало. Сейчас же, когда на государственных границах в условиях перманентной террористической угрозы применяются различные контролирующие устройства – от металлодетекторов и рентгеновских сканеров до тепловизоров и еще более высоких технологий – встает закономерный вопрос о том, является ли их использование по умолчанию нарушением личного иммунитета дипломата или нет. Проще говоря, имеет ли право сотрудник службы безопасности аэропорта или пограничной службы попросить носителя дипломатического паспорта пройти через рамку металлоискателя и проверить его багаж интроскопом. Сразу скажу, что сам, не имея специального юридического образования, неоднократно задавал этот вопрос экспертам по международному праву, как отечественным, так и зарубежным. Однозначного ответа не получил: мнения расходятся.

То же относится и к присутствию дипломатического агента или его полномочного представителя в случае, если досмотр все же будет иметь место. Должно ли присутствие обязательно быть физическим или может быть выбрана опция виртуального (онлайн, например, в режиме видеосвязи) присутствия. Вопрос открытый. Порядок регулирования подобных ситуаций на законодательном уровне пока что не определен.

Развивая тему, вспомним статью 22 той Конвенции, закрепляющую неприкосновенность помещений дипломатического представительства. А как

1 Венская конвенция о дипломатических сношениях. Принята 18 апреля 1961 года // ООН. [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/dip_rel.shtml (дата обращения 10.02.2021).

быть с цифровым сегментом его присутствия в стране пребывания? У каждого российского и у большинства иностранных загранучреждений есть аккаунты в социальных сетях. Это эффективный канал медийной политики, инструмент, при помощи которого осуществляется информационно-разъяснительная работа в качестве одной из функций посольства в соответствии со статьей 3 названного документа.

И тем не менее, социальные сети (от уже традиционного *Facebook* до новомодного *TikTok*) и иные ресурсы (хостинги, облачные хранилища данных и прочее) подчиняются не властям государства пребывания или аккредитующего государства, а частным корпорациям. Недавний резонансный скандал с блокировкой аккаунтов Д. Трампа – первая ласточка. В дальнейшем с таким явлением вполне могут столкнуться и, скорее всего, будут сталкиваться дипломатические органы.

Стратегия и тактика противодействия подобным мерам не так проста, как может показаться на первый взгляд. Хотя с чего начинать – понятно: с обновления законодательной базы и учета в ней новейших реалий дипломатической работы. Обратите внимание, что я говорил сейчас о статьях только одного, при этом ключевого нормативного документа международного дипломатического права.

С.М.: Да, инженеры-технологи, судя по всему, опережают юристов-международников. В результате коллизии налицо. Но предпринимаются или предприняты уже какие-либо конкретные шаги по частичному устранению таких коллизий – в частности, российским внешнеполитическим ведомством и профессиональным дипломатическим сообществом?

Р.Р.: Разумеется. На институциональном уровне в конце 2019 г. в МИД России был наконец создан Департамент международной информационной безопасности (ДМИБ). Его возглавляет опытный дипломат-практик А. Крутских, наряду с этим руководящий профильным Центром в МГИМО. Это направление, по-моему, одно из наиболее перспективных применительно к современной дипломатической повестке. Именно от того, насколько быстро и эффективно дипломаты научатся взаимодействовать друг с другом в цифровой среде, во многом будет зависеть международное сотрудничество в различных сферах: от коллективной безопасности до контактов в области науки и технологий, включая вопросы здравоохранения (наиболее актуальный ныне трек – вакцины), переговоров по климату и прочее.

Важную роль, как уже говорил, здесь играют вопросы кибербезопасности. Во время карантинов прошлого года, повлекших за собой переход на дистанционные формы работы, многие участники онлайн-конференций, включая дипломатов, столкнулись с таким банальным явлением, как подключение к ним незваных гостей. Были прецеденты подобных «визитов» и на высоком уровне – скажем, во время переговоров министров обороны ЕС в ноябре 2020 г.[1] В последнем случае речь, судя по всему, шла о примитивном недосмотре со стороны одного из

1 К секретному совещанию министров обороны ЕС подключился чужак // Вести. 20 ноября 2020. [Электронный ресурс]. URL: https://www.vesti.ru/article/2488505 (дата обращения 10.02.2021).

участников собрания, в результате которого любопытному журналисту удалось подобрать пароль. Однако знаменитые хакеры, причем не только русские, тоже не дремлют. Поэтому кибербезопасность занимает все более высокие позиции в списке приоритетов.

С.М.: В условиях продолжающейся пандемии такие значимые международные события, как 75-я сессия Генассамблеи ООН и Давосский форум 2021 г. прошли в режиме онлайн. В связи с этим, допустимо ли на текущем этапе давать предварительные оценки влияния пандемии на дипломатию, и если да, то каковы они могут быть? В свете того, что пандемия обнажила многие слабые стороны международного взаимодействия, уместно ли говорить о ней как о своего рода историческом водоразделе с дипломатией пре- и пост-?

Р.Р.: Пандемия коронавируса выступила мощным катализатором процессов, которые наблюдались в этой области и ранее, однако протекали медленнее. Тот же переход на онлайн – вплоть до открытия виртуальных дипломатических представительств – уже находил не только применение, но и описание в специализированной литературе. Среди прочего, в работах Т. Зоновой[1].

Не сказал бы, что пандемия, несмотря на свою беспрецедентность, привнесла что-то принципиально новое в международные отношения и, соответственно, в дипломатию.

Просто раньше инновации вызывали интерес преимущественно у специалистов, в то время как широкая публика, если и узнавала о чем-то подобном, воспринимала это как экзотику. В нынешних условиях за временным отсутствием традиционных альтернатив даже наиболее консервативные и критически настроенные к новшествам участники дипломатических процессов волей-неволей были вынуждены обратить на них внимание.

Те, кто и раньше имел склонность к цифровизации, продолжили двигаться в соответствующем направлении, в известной мере воспользовавшись сложившейся ситуацией. В результате увеличился разрыв технологически продвинутых и, если можно так выразиться, несколько отстающих или запаздывающих в этом отношении. В данном плане дипломатия едва ли отличается от любых других сфер.

Что касается сценариев развития и трансформации дипломатических систем после завершения пандемии, с уверенностью можно сказать одно: полностью к докризисному состоянию они уже не вернутся. Полагаю, однако, что некоторые новшества, привнесенные в 2020 г. в дипломатические практики, сохранятся, даже когда в них уже не будет столь острой, как сейчас, необходимости. В частности, цифровые следы. Уж слишком большую экономию ресурсов дает то, что уже с легкой подачи журналистского сообщества окрестили «зумпломатией»[2]. Так что не исключено, что и здесь мы в конечном итоге придем к очередному гибриду.

1 *Зонова, Т.В.* Дипломатия: модели, формы, методы. – М.: Аспект-Пресс, 2018. – 350 с.
2 Daniel Shapiro, and Daniel Rakov, "Will Zoomplomacy Last?" Foreign Policy, May 18, 2020, accessed February 10, 2021, https://foreignpolicy.com/2020/05/18/will-zoomplomacy-last/.

С.М.: Благодарю Вас за обозначенный прогноз. И напоследок вопрос о факторе личности в дипломатии. Есть мнение, что он уже не играет прежней роли. Иначе говоря, дипломатия обезличивается, чему как раз способствуют цифровые платформы, местами позволяющие вуалировать идентичность, местами и вовсе гарантирующие анонимность. Будет ли в новой цифровой среде место великим и ярким дипломатам?

Р.Р.: Думаю, что будет. Мы иногда со студентами проводим упражнения-игры: скажем, Венский конгресс 1814–1815 гг. в чате. И забавно, и дидактически полезно. С аватарками и прочей атрибутикой, из которой они потом делают мемы и «демотиваторы». Талант, как известно, бессмысленно симулировать, но и сложно скрывать. Поэтому в цифровой среде он себя обязательно проявит.

Как таковой фактор личности в дипломатии всегда играл важную роль. Достаточно вспомнить действия русского посла в Лондоне С. Воронцова, которые фактически позволили предотвратить общеевропейскую войну накануне второго раздела Польши. Или исторические достижении князя А. Горчакова, вернувшего России право держать военный флот в Черном море. Говоря о событиях уже XX в., нельзя обойти стороной вклад посла СССР в США А. Добрынина в вывод американских ракет с территории Турции, а также в целом в урегулирование Карибского кризиса.

Эти деятели служат ориентирами для современных дипломатов, равно как и для студентов, которых мы обучаем и которые в дальнейшем хотят попробовать себя на этом поприще. В лучшие свои минуты некоторые из нас ощущают себя будто бы их суммой – но всегда меньшей, чем любой из них в отдельности. Как любят повторять школьные учителя, история не знает сослагательного наклонения. Однако если представить себе альтернативную реальность, думается, что каждый из названных и многих других выдающихся дипломатов был бы, скорее всего, не менее успешен в переговорах в цифровом пространстве, чем в роскошных залах, где проводились живые конференции и решались судьбы мира.

Цитирование

Райнхардт, Р.О. Новые формы и методы дипломатии //
Международная аналитика. – 2020. – Том 11 (4). – С. 11–20.
https://doi.org/10.46272/2587-8476-2020-11-4-11-20

Сведения о финансировании

Материал подготовлен в рамках гранта МГИМО МИД России на выполнение
научных работ молодыми исследователями под руководством докторов или кандидатов наук.
Проект «Новые формы и методы дипломатии в условиях пандемии» XI конкурса
молодых ученых МГИМО «Научная идея».

For citation

Reinhardt, Roman O. "New Forms and Methods of Diplomacy."
Journal of International Analytics 11, no 4. (2020): 11–20.
https://doi.org/10.46272/2587-8476-2020-11-4-11-20

Funding

The material was prepared under the MGIMO grant for young researchers under the supervision
of doctoral or postdoctoral fellows.
The project "New Forms and Methods of Diplomacy under Pandemic Conditions"
of the XI MGIMO Young Researchers' Contest "Scientific Idea."

Концептуализация стратегии США в технологической войне против КНР: экономика, политика, технонационализм

Иван Владимирович Данилин

https://doi.org/10.46272/2587-8476-2020-11-4-21-38

АННОТАЦИЯ

В работе анализируется так называемая американо-китайская технологическая война 2017–2020 гг. в сфере прорывных цифровых технологий, ее истоки, факторы и иные аспекты с акцентом на рассмотрение американской стратегии по ограничению возможностей технологического развития КНР. Целью исследования является концептуализация американской стратегии технологической войны, а также оценка характера и перспектив технологических конфликтов. Статья представляет собой исследование с использованием компаративного, исторического подходов и элементов системного экономического анализа, отдельных элементов неореалистских и конструктивистских подходов. На основе изучения ключевых драйверов технологической войны (применительно к позиции США), а также сравнительно-исторического анализа наблюдаемых процессов и применяемых инструментов борьбы за технологическое лидерство сделан вывод о том, что технологический конфликт является новым феноменом, определяемым в том числе спецификой цифровых технологий и экономическими изменениями последних десятилетий, но сохраняющим естественную преемственность по отношению к геополитическим и экономическим конфликтам прошлого и к существующим стратегиям и инструментарию. С учетом особенностей нового конфликта и цифровых технологий сделан вывод о возможности описания американской политики в рамках скорректированной версии концепции неотехнонационализма (укрепление национального технологического потенциала и суверенитета посредством глобальных экономических инструментов). Отмечено, что в условиях цифровой революции и при анализе столкновения сверхдержав эта концепция предполагает достижение целей через обеспечение преференциального доступа к таким специфическим ресурсам развития, как глобальный человеческий капитал и большие первичные данные, формирование систем стандартов и проч. В заключении отмечается, что стратегия США при Д. Трампе, приведшая к более жесткому американскому курсу в технологической войне с КНР, определялась не только личностными характеристиками президента, но и объективными обстоятельствами. В частности, необходимостью слома старых неэффективных практик для формирования новых решений и подходов. Автор приходит к выводу о том, что в перспективе США сделают акцент на выстраивании техноэкономических режимов как более системной стратегии реализации технологического конфликта в адаптированной неотехнонационалистической логике.

КЛЮЧЕВЫЕ СЛОВА

передовые цифровые технологии, санкции, США, Китай, технонационализм

CC BY

Быстрое усиление научной, инновационной, промышленно-технологической и военно-технической мощи КНР в 2010-х гг. привело к росту обеспокоенности США, стремившихся сохранить свое экономическое и глобальное лидерство, снизить ущерб, связанный с утечкой производств и технологий в КНР и растущим торговым дисбалансом. Как следствие, с начала 2010-х гг. Вашингтон стал предпринимать все более системные меры по принуждению КНР к отказу от традиционных форм промышленной политики и протекционизма, защите интеллектуальной собственности США и – шире – ограничению доступа китайских компаний к американским технологиям и технологическим активам (в том числе через противодействие практике принуждения к трансферу технологий и ноу-хау)[1]. Обеспокоенность США и их давление на КНР усилились в результате успехов китайского технологического сектора и проактивной инновационно-технологической политики, в том числе программы *Made in China 2025* (с 2015), вызвавшей большой резонанс в США.

С приходом в Белый дом администрации Д. Трампа политика экономического сдерживания Китая перешла на принципиально новый уровень. С 2018 г. между двумя странами началась настоящая торговая война[2].

Особую роль в этом экономическом конфликте играют высокие технологии, прежде всего цифровые. В центре противостояния оказался целый ряд перспективных (*emerging*) цифровых технологий и решений: от телекоммуникационного оборудования стандарта 5G и искусственного интеллекта до онлайн-платформ и сервисов (*TikTok, WeChat* и проч.). В 2017–2018 гг. администрация последовательно развивала мероприятия по ограничению китайских технологических возможностей и глобальной экспансии в цифровой сфере[3]. Пик активности пришелся на 2019–2020 гг., когда были введены наиболее жесткие меры, что позволило некоторым обозревателям и аналитикам говорить о технологической войне (по аналогии с торговыми войнами).

Существовали как минимум три основные группы ограничений. Во-первых, на доступ ряда наиболее передовых в научно-технологическом отношении китайских предприятий в сфере электроники *(Huawei, ZTE, SMIC* и др.) к ключевым технологиям и техническим решениям в сфере разработки и производства передовых чипов, иной электронной продукции и обеспечивающим программным решениям. Во-вторых, на доступ китайских субъектов (компаний, академического сектора, государственных структур) к знаниям и профессиональному ресурсу США – через ограничения на академические обмены и научно-образовательную кооперацию, на китайские венчурные инвестиции в американские стартапы и проч. В-третьих, на доступ технологических субъектов КНР к американскому рынку (вплоть до принудительной замены телекоммуникационного оборудова-

1 См., например: Steinbock 2018; Салицкий, Семенова 2019; Qin 2019; Mascitelli, Chung 2019; Chen et al. 2020; Лексютина 2020, 89; "U.S. weighs restricting Chinese investment in artificial intelligence," Reuters, June 13, 2017, accessed November 25, 2020, https://www.reuters.com/article/us-usa-china-artificialintelligence/u-s-weighs-restricting-chinese-investment-in-artificial-intelligence-idUSKBN1942OX; Adam Segal, "When China Rules the Web," Foreign Affairs, September/October 2018, accessed November 25, 2020, https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web; Torsten Riecke, "Resilience and decoupling in the era of great power competition," China Monitor, MERICS, August 20, 2020, accessed November 25, 2020, https://merics.org/sites/default/files/2020-08/Merics_ChinaMonitor_PowerCompetition.pdf.

2 Steinbock 2018; Труш 2018; Evenett 2019a; Салицкий, Семенова 2019; Chen et al. 2020; Лексютина 2020.

3 Основные этапы и события технологической войны США и КНР изложены в: Sun 2019; Chen et al. 2020; Evans 2020; Данилин 2020.

ния *Huawei* и попыток запрета *TikTok* и *WeChat*), американскому венчурному капиталу и иным инвестиционным ресурсам (в том числе ужесточение требований к листингу и присутствию на американских фондовых биржах).

Учитывая огромное значение перспективных цифровых технологий для экономического развития и США, и КНР, а также долгосрочный характер американо-китайских противоречий (в том числе в инновационной и технологической сферах) возникает несколько важных исследовательских проблем. В частности, речь идет о концептуализации новой американской стратегии технологической войны, включая анализ ее ключевых мотивов и драйверов. Подобная работа, помимо прочего, позволит также определить, является ли данный феномен эволюцией уже существующих международных подходов и процессов, новым перспективным видом международного или геополитического / геоэкономического противостояния великих и региональных держав или же уникальным явлением, характерным для конкретного момента и / или группы перспективных технологий.

Обзор литературы

Статья представляет собой исследование с использованием компаративного, исторического подходов и элементов системного экономического анализа, отдельных элементов неореалистских и конструктивистских подходов. Свод научных и аналитических публикаций, необходимых для исследования и концептуализации стратегии США и американо-китайской технологической войны, имеет комплексный характер, соединяя в себе несколько различных блоков литературы: по торговым войнам, санкциям, развитию, а также технологическому противостоянию.

Изучение литературы по торговым войнам, включая и текущее противостояние США и КНР, имеет большое значение для понимания общего контекста этого противостояния, его основных этапов и – шире – основных мотивов экономического конфликта. Существующие работы сосредоточены либо на анализе общей динамики и истоков противостояния (подобный подход особенно характерен для российских работ[1]), либо (зарубежные публикации) на оценке и моделировании экономических эффектов для обеих сторон и других подобных вопросах[2]. Также были рассмотрены смежные работы, связанные с проблематикой защиты рынков и государства, развития и сопутствующих вопросов[3].

Сравнительно небольшое число теоретических и обобщающих работ по санкциям – прежде всего, труды таких классиков, как Г.К. Хафбауэр, У. Кэмпфер и А. Ловенберг[4] – весьма информативны для анализа логики, целей, стратегий и «механики» санкционных мероприятий (в том числе в технологической сфере), частично – отдельных международно-политических и геополитических аспектов технологических санкций. Не менее важны они и для систематизации мотивов

1 Труш 2018; Evenett 2019a; Салицкий, Семенова 2019; Лексютина 2020. В определенной степени обзорным можно считать, например, декабрьский выпуск *Journal of International Economic Law* за 2019 г.
2 См., например: Steinbock 2018; Li et al. 2020.
3 Почти классические примеры применительно к развивающимся странам: Эльянов 2005; Wade 2018; к развитым – Mazzucatto 2011; Wade 2014.
4 Kaempfer, Lowenberg 2007; Hufbauer et al. 2008; Hufbauer, Jung 2020.

санкций: от изменения внешнеполитического поведения режимов-«мишеней» для санкций до акцента на ограничении потенциала страны-оппонента и решения международных репутационных и внутриполитических задач страны-инициатора санкций.

Хотя вышеуказанные группы работ имеют непосредственное отношение к рамочным условиям и отдельным аспектам технологической войны, в целом они обладают иным фокусом исследования и напрямую не рассматривают ни феномен технологических конфликтов *per se*, ни обуславливающие их стратегии. По той же причине они в основном игнорируют связку геополитической / международно-политической и экономической проблематики, а также политических стратегий и дискурсов, важных для рассматриваемой темы.

В связи с этим нами был предпринят более широкий анализ литературы и аналитических материалов, включая работы по феномену технонационализма, все более часто упоминаемого в связи с американо-китайским конфликтом[1]. По сути, речь идет об осмыслении экономической проблематики (например, протекционизма, внешне ориентированного развития) в терминах и логике стратегий властных и экономических элит, потенциалов, частично политической психологии. Данные исследования имеют междисциплинарный характер (политология с элементами экономических методов), однако по некоторым акцентам предлагаемый подход максимально близок к международным исследованиям, особенно неореализму. Полезными оказываются и публикации, анализирующие проблематику секьюритизации технологий – самостоятельного направления исследований, де-факто, однако, связанного с вопросами санкций, геополитических и торговых противоречий. В совокупности эти две группы работ и связанных с ними концепций оказались наиболее полезны с учетом наработок по иным вышеуказанным блокам исследований.

Мотивы и движущие силы технологической войны

Прежде всего, целесообразно проанализировать мотивы и движущие силы американо-китайской технологической войны, определяющие стратегию США. Максимально упрощая и схематизируя наблюдаемые процессы, можно выделить три группы факторов: геополитическое противостояние и международно-политические противоречия, торговая война и протекционизм и, наконец, тесно связанные с ними (и с внутриполитическими факторами) проблемы секьюритизации технологий.

Наиболее очевидно геополитическое содержание, мотивы и драйверы американской стратегии и самой технологической войны. Они связаны с задачами

1 Ostry, Nelson 1995; Montresor 2001; Nakayama 2012; Kennedy 2013; Kim et al. 2020. См. также: Robert A. Manning, "Techno-Nationalism vs. the Fourth Industrial Revolution," Global Asia 14, no 1 (March 2019), accessed November 25, 2020, https://www.globalasia.org/v14no1/cover/techno-nationalism-vs-the-fourth-industrial-revolution_robert-a-manning; Alex Capri, "Techno-nationalism: The US-China tech innovation race," Hinrich Foundation, August 2020, accessed November 25, 2020, http://surl.li/jreb; Andreas Kuehn, and Bruce McConnell, "Weathering TechNationalism: A Security and Trustworthiness Framework to Manage," EastWest Institute, 2020, accessed November 25, 2020, https://www.eastwest.ngo/sites/default/files/ideas-files/weathering-technationalism.pdf; Alex Capri, "Techno-nationalism and diplomacy: The US-China race to reshape alliances, institutions and standards," Hinrich Foundation, October 2020, accessed November, 25, 2020, http://surl.li/jrek.

ограничения потенциала КНР – в том числе в логике «ловушки Фукидида»[1]. Удар по китайскому технологическому сектору был направлен, с одной стороны, на ограничение военно-технических возможностей Китая и его совокупного потенциала. Это вполне открыто заявлялось администрацией Д. Трампа, в том числе применительно к вопросу о «двойном» характере технологического развития КНР (включая так называемую военно-гражданскую интеграцию)[2]. С другой стороны, политика США направлена на снижение потенциала развития китайской экономики и предотвращение возможности ее перехода на более высокий уровень (как это и понимает китайская сторона[3]). Эта цель определяется ролью производства и экспорта цифровой продукции для экономики Китая, структурообразующим значением информационно-коммуникационных технологий (ИКТ) и крупнейших корпораций (*Huawei, ZTE, Alibaba, Tencent* и др.) для развития сектора хай-тек КНР и – шире – китайской инновационной системы. Говоря о геополитических факторах, любопытно отметить, что и сами дискуссии о 5G (в меньшей мере – по искусственному интеллекту и иным технологиям) ведутся с использованием едва ли не маккиндеровских геополитических формулировок (логика «кто контролирует цифровые технологии X, тот доминирует в мире»).

Далее, рационально обратиться к анализу технологического противостояния в контексте двусторонних торгово-инвестиционных противоречий.

Прежде всего, речь идет о международно-экономическом и глобальном измерениях национальной конкурентоспособности США: о борьбе за перспективные глобальные технологические рынки и контроль над ними, в том числе в части экспорта наукоемких цифровых услуг и оборудования, инвестиционной экспансии, включая поглощение стартапов, иных перспективных технологических компаний и проч. Отдельным вопросом в связи с этим является снятие барьеров на доступ технологических корпораций США на рынки КНР. Эта задача тем более значима, что в КНР до недавнего времени были де-юре и остаются до сих пор де-факто ограниченными возможности иностранных инвестиций во многие стратегические секторы экономики. Кроме того, по политическим (цензура) и экономическим (поддержка национальных компаний) причинам на китайском рынке запрещены или серьезно ограничены возможности работы американских интернет-сервисов *(Facebook, Google, Amazon* и др.). То же можно сказать и об импорте и реализации раз-

1 Опасения усиления КНР до уровня, когда она сможет сместить США с позиции ведущей сверхдержавы. О феномене «ловушки Фукидида» см.: Allison 2017. См. также: Steinbock 2018; Sun 2019; Chen et al. 2020.

2 Steinbock 2018; Sun 2019. См. работы в качестве примера официальной позиции США: Ana Swanson, Paul Mozur, and Steve Lohr, "U.S. Blacklists More Chinese Tech Companies Over National Security Concerns," The New York Times, June 21, 2019, accessed November 25, 2020, https://www.nytimes.com/2019/06/21/us/politics/us-china-trade-blacklist.html?auth=login-email&login=email; "Commerce Department Adds 24 Chinese Companies to the Entity List for Helping Build Military Islands in the South China Sea", The U.S. Department of Commerce, Press-release, August 26, 2020, accessed November 25, 2020, https://www.commerce.gov/news/press-releases/2020/08/commerce-department-adds-24-chinese-companies-entity-list-helping-build; "Chinese Technology Transfer Challenges to U.S. Export Control Policy," Remarks by Dr. Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, CSIS Project on Nuclear Issues, July 11, 2018, accessed November 25, 2020, https://www.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/chinese-technology-transfer-challenges-to-u-s-export-control-policy/; John R. Shane, and Lori E. Scheetz. "Commerce Department Further Restricts U.S. Exports to China, Russia, and Venezuela; Aims to Combat China's Military-Civil Fusion Strategy," Wiley, April 28, 2020, accessed November 25, 2020, https://www.wiley.law/alert-Commerce-Department-Further-Restricts-U-S-Exports-to-China-Russia-and-Venezuela-Aims-to-Combat-China-s-Military-Civil-Fusion-Strategy.

3 См., например: Труш 2018; Лексютина 2020; Adam Segal, "Seizing Core Technologies: China Responds to U.S. Technology Competition," China Leadership Monitor, The Washington International Trade Association (WITA), January 06, 2019, accessed November 25, 2020, https://www.wita.org/nextgentrade/china-responds-u-s-tech-competition/.

личных американских аппаратных решений (ранее – в том числе мобильных телефонов), включая нетарифные ограничения в виде системы уникальных национальных технических стандартов[1].

Во-вторых, наряду с предотвращением нечестной конкуренции наблюдаются и классические протекционистские мотивы, связанные с защитой национального рынка и американского технологического бизнеса от китайской экспансии в принципиально важных для будущего экономики технологических областях[2]. Заметим в этой связи, что, хотя большинство американских цифровых корпораций проявляют очень сдержанную позицию относительно технологических санкций Белого дома (в силу собственных бизнес-интересов в КНР), часть из них объективно заинтересована в ограничении китайской конкуренции. Показательным примером в данном отношении является роль, приписываемая основателю и руководителю *Facebook* М. Цукербергу, в продвижении идей о запрете *TikTok* в США[3]. Другим важным индикатором значимости этого мотива является давно дискутируемый вопрос о дефиците США в торговле высокотехнологичной продукцией с КНР, хотя немалая его часть – импорт продукции американских фирм. В Вашингтоне как минимум с конца 2000-х гг. обсуждается проблема потерь американской экономики, включая сектор хай-тек, от агрессивной торговой политики КНР, усиленной скрытой господдержкой, демпингом, кражей интеллектуальной собственности и иными нечестными практиками[4].

Своего рода промежуточное положение между экономическими, геополитическими и отчасти дискурсивными (см. ниже) соображениями занимают мотивы, связанные с национальной экономической безопасностью. Для США в данном случае речь идет о стратегической независимости от неамериканских (особенно из страны-противника / оппонента) поставщиков критических технологий, минимизации рисков кибершпионажа[5].

Наконец, в качестве специфического мотива технологического противостояния США и Китая выступают процессы секьюритизации. Это касается как собственно прорывных цифровых гражданских и «двойных» технологий[6], так и научно-технологических ресурсов (кадры, компетенции, венчурный и иной умный капитал, образовательная система и проч.).

Не вызывает сомнений, что секьюритизация играет огромную роль в разматывании маховика американо-китайской технологической войны. Если говорить о США, то сами формулировки санкций и обеспечивающих решений связаны как раз с представлением и вербализацией китайской технологической мощи как угрозы.

Хотя формально проблематика секьюритизации занимает подчиненное положение относительно более общих геополитических факторов, в части прорывных технологий она приобретает до некоторой степени самостоятельное значение.

1 Kshetri et al. 2011; Shim, Shin 2016; Qin 2019; Kim et al. 2020.
2 Steinbock 2018; Sun 2019.
3 Georgia Wells, Jeff Horwitz, and Aruna Viswanatha, "Facebook CEO Mark Zuckerberg Stoked Washington's Fears About TikTok," The Wall Street Journal, August 23, 2020, accessed November 25, 2020, https://www.wsj.com/articles/facebook-ceo-mark-zuckerberg-stoked-washingtons-fears-about-tiktok-11598223133.
4 Помимо работ советника Д. Трампа П. Наварро, достаточно подробное изложение суммы претензий американской стороны к КНР можно найти, например, в работах влиятельного «мозгового центра» ITIF, специализировавшегося в том числе на анализе китайской технологической экспансии и ее угрозе для США. См., например: Atkinson, Ezell 2012.
5 См. об этом, в частности: Лексютина 2020, 89.
6 См., например, анализ данного феномена применительно к военным технологиям: Чеков 2020.

С одной стороны, речь идет о частном случае концепции «технологической неопределенности»[1]. Учитывая не вполне представимые пределы возможностей и угроз современных цифровых технологий, часть американских военных и властных элит опасается уязвимости перед растущей цифровой мощью КНР. Одновременно она стремится максимально капитализировать ситуацию пока еще сохраняющегося лидерства США в цифровом сегменте (включая его финансовые, институциональные и другие аспекты). Это, в свою очередь, стимулирует и геополитические, и торгово-экономические конфликты.

С другой – процесс секьюритизации цифровых технологий поддерживается с обеих сторон широкими и хорошо наблюдаемыми альянсами интересантов. Формально стратегические цели (доминирование США, новая роль Китая в глобальной иерархии) на поверку нередко оказываются еще и факторами сложной внутриполитической борьбы (для сравнения: китайская тема в предвыборной борьбе Д. Трампа и Дж. Байдена). В бизнес-сообществе, в свою очередь, актуальны мотивы нечестной конкуренции, усиления внутриэкономических позиций и / или формирования новых возможностей рентного поведения в рамках политики импортозамещения.

Технологическая война: Business as Usual?

Несложно заметить, что при всем различии рассмотренных факторов – даже с учетом доминирования условно-геополитических соображений – они вполне органично сочетаются друг с другом, формируя внутренне непротиворечивую базу системного противостояния КНР и стратегии США. Несмотря на то что в каждом случае технологическая тематика вписана в мотивы и процессы более высокого уровня, она имеет вполне самостоятельное значение и в ряде случаев обеспечивает логическое единство различных направлений политики США. В этом смысле технологическая война как самостоятельное направление стратегии США вопросов не вызывает. Однако имеем ли мы дело с новым феноменом или с новым проявлением хорошо известных процессов?

Формально наблюдаемая ситуация находит множественные исторические параллели и аналогии. Если говорить о торгово-экономическом измерении проблемы, то при всем огромном значении современных цифровых технологий как объекта противостояния подобный конфликт не уникален. Противоречия в технологической сфере, доходящие до протекционистских и иных ограничительных мер, были, например, характерны для взаимоотношений США и Японии в 1980-х гг.[2] Даже если говорить о технологических отношениях США – КНР[3], то история взаимных претензий, включая давление США по отмене китайских ограничений в сегменте хай-тек, прослеживается уже в 2000-х гг.[4]

1 Истомин 2020.
2 См. хотя бы: Robert Reich, “The Rise of Techno-nationalism: In the Emerging Debate about How to Restore America’s Technological Pre-eminence, We Are Misconstruing the Problem and Advancing the Wrong Solutions,” Atlantic Monthly, May 1987, p. 62–70, accessed November 25, 2020, http://surl.li/jvco; Nakayama 2012; Kim et al. 2020.
3 См., например: Kennedy 2013; Evenett 2019a. Характерно, что за более активное давление на КНР против протекционизма и иных архаичных форм промышленной политики призывали многие политические деятели и интеллектуалы. Ср. работы ITIF: Atkinson, Ezell 2012.
4 См., например: Shim, Shin 2016.

Неуникальны и протекционистские мотивы в политике США, хорошо вписывающиеся в тренды, актуальные для развитых стран начиная как минимум с кризиса 2008–2009 гг. (в том числе против КНР)[1]. Как представляется, помимо реакции на кризис в изменившихся реалиях глобальной экономики и торговли, а также в связи с ростом популизма, это является следствием переосмысления западными странами, и прежде всего Соединенными Штатами, баланса выгод и рисков либеральной модели глобализации, которая привела к незапланированному усилению КНР.

История санкций тоже дает нам богатую пищу для исторических аналогий, а стратегия США более-менее соответствует ее классическим примерам[2]. Налицо не буквальные, но все же параллели современной ситуации с технологическими ограничениями стран НАТО против СССР и стран Восточного блока в рамках деятельности Координационного комитета по экспортному контролю (*COCOM*). Однако и после 1991 г. технологические санкции оставались важным элементом сдерживания развития оппонентов, недопуска к новым военно-техническим возможностям, принуждения к уступкам. Характерным примером являются, например, санкции против Ирана[3]. КНР также неоднократно выступала объектом пусть и более мягких, но вполне значимых санкций. Помимо запрета европейскими странами и США экспорта вооружений и военной техники в Китай после событий на площади Тяньаньмэнь, можно указать на целый ряд иных мер. Например, ужесточение экспортного контроля США в сфере ракетных и спутниковых технологий с конца 1990-х гг. в ответ на утверждения о нелегальном доступе Китая к некоторым важным решениям в данной сфере, а также запрет, введенный в 2011 г. на тесное взаимодействие *NASA* с китайскими структурами[4].

Неудивительно, что, по мнению таких классиков изучения санкций, как Г. Хафбауэр, политика Д. Трампа против КНР является простой эволюцией существующих подходов и практик санкционного давления[5]. Вплоть до того, что в качестве *casus belli* против некоторых китайских технологических компаний использовались обвинения в нарушении прав человека, в том числе против национальных меньшинств в Синьцзян-Уйгурском автономном округе[6]. Примечательно, что, несмотря на расширение полномочий существующих надзорных органов и новой интерпретации старых нормативно-правовых актов, администрации Д. Трампа в ее технологическом «крестовом походе» против Китая не понадобился ни принципиально новый инструментарий, ни разработка новой нормативно-правовой базы[7].

Наконец, феномен секьюритизации технологий и научно-технологических ресурсов не является новым или уникальным – особенно для случаев геополи-

1 Evenett 2019a; Evenett 2019b; Sun 2019.
2 Kaempfer, Lowenberg 2007; Hufbauer et al. 2008.
3 Fakhari 2017.
4 См., например, об основных событиях: Pete Spotts, "NASA's Bolden walks tight rope on China trip," The Christian Science Monitor, October 16, 2010, accessed November 25, 2020, https://www.csmonitor.com/Science/2010/1016/NASA-s-Bolden-walks-tight-rope-on-China-trip; William Petland, "Congress Bans Scientific Collaboration with China, Cites High Espionage Risks," Forbes, May 7, 2011, accessed November 25, 2020, http://surl.li/jvdn; David Lague, "Special Report-In satellite tech race, China hitched a ride from Europe," Reuters, December 22, 2013, accessed November 25, 2020, http://surl.li/jvds; "U.S. Space industry 'deep dive' assessment: impact of U.S. export controls on the space industrial base," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, February 2014, accessed November 25, 2020, http://surl.li/jvdu.
5 Hufbauer, Euijin 2020.
6 См., например: David Shepardson, and Josh Horwitz, "U.S. expands blacklist to include China's top AI startups ahead of trade talks," Reuters, October 7, 2019, accessed November 25, 2020, https://www.reuters.com/article/us-usa-trade-china-exclusive/us-expands-blacklist-to-include-chinas-top-ai-startups-ahead-of-trade-talks-idUSKBN1WM25M.
7 Лексютина 2020, 91.

тического соперничества и сложных международно-политических отношений. Опустим вопрос о том, что технологии сами по себе являются лишь частным случаем секьюритизации стратегических ресурсов, будь то углеводороды (например, противоречия России и ЕС по вопросам энергетической безопасности начиная с 2000-х гг.) или даже пространства (как, например, в случае с Арктикой). Но и применительно к научно-технологической сфере секьюритизация была и остается широко распространенной практикой. Яркие примеры дает космическая сфера. Хорошо известен «эффект спутника» для внутри- и внешнеполитических, экономических и военных процессов и стратегий на Западе. Однако секьюритизация космических технологий была характерна и для вполне союзнических отношений США и стран Западной Европы. Европейские политики едва ли не с 1970-х гг. оценивали свою зависимость от американских космических возможностей как угрозу и уязвимость, поощряя развитие европейского космического сектора (от вывода грузов на орбиту до системы спутниковой навигации *Galileo*)[1]. Акценты секьюритизации космической отрасли прекрасно иллюстрируют слова президента Франции Ж. Ширака, заявившего в 1990-х гг., что без собственных космических возможностей Европа обречена быть «вассалом» Америки[2].

Поэтому тот факт, что объектом секьюритизации выступают цифровые технологии, является вполне закономерным. Будучи классическими технологиями широкого применения (*General Purpose Technologies*), имеющими критическое значение для экономического и военного потенциала страны и неясные пределы возможностей и рисков, они всегда являлись объектом дискурса вызовов и угроз, и за последние 20 лет этот тезис подтверждается эволюцией проблем кибербезопасности: от рассуждений о хакерских атаках и интернет-террористических актах в 1990-х гг.[3] до обвинений РФ в кибератаках против государств Запада[4]. По мере развития технологии «Интернета вещей», социальных сетей и иных сложных решений, где установление реального события априори проблематично, секьюритизация цифровых технологий становится все более актуальной, простой и политически удобной темой, нередко оказываясь идеальным выражением «теоремы Томаса».

Цифровое противостояние: новый феномен и новая реальность

Итак, казалось бы, нельзя говорить о новизне ни стратегии США, ни самого феномена технологической войны. В конечном счете, хотя технологии и оказывают существенное воздействие на международные процессы, балансы сил и т.д., но на длительных временных горизонтах радикально их не меняют вне более широкого комплекса ресурсных, институциональных и иных экономических и политических факторов[5].

Однако речь в данном случае идет не столько о долгосрочном изменении баланса сил, сколько о вполне конкретной стратегии в сфере противостояния

1 См. подробнее в: Johnson-Freese, Erickson 2006.
2 Ibid., 17.
3 Furnell, Warren 1999.
4 См., например, по ситуации в этой сфере до Крымского кризиса: Hansen, Nissenbaum 2009.
5 В частности, данная идея обосновывалась в исследовании И.А. Истомина и И.В. Данилина, по итогам которого был сделан совместный доклад «Меняют ли технологии международную систему?» на VIII Всероссийском конгрессе политологов (Москва, РАПН, 6–8 декабря 2018).

сверхдержав. И здесь ситуация заметно отличается от прошлых конфликтов и сильно выбивается из наблюдавшихся еще недавно экономических и политических трендов.

Во-первых, по сравнению с 1970–1990-ми гг. процессы долгосрочного экономического и военно-технического развития и взаимосвязанные с ними геополитические факторы стали намного теснее коррелировать с коммерческими технологиями и технологическими рынками. При этом США едва ли не впервые столкнулись с ситуацией наложения геополитического противостояния и рыночной конкуренции в сфере прорывных технологий – еще и с почти равным оппонентом.

Чуть более подробно поясним последний тезис. Если говорить о послевоенном противостоянии США и СССР, то Советский Союз был в каких-то областях сопоставим, в каких-то равен, а в чем-то превосходил США по важнейшим военным и «двойным» технологиям. Страны были сопоставимы и по масштабу, и по сложности экономики. Но, во-первых, разрыв по размеру номинального ВВП между США и СССР даже в середине 1980-х был почти в 1,2–1,4 раза выше, чем между США и КНР к концу 2010-х гг.[1] Во-вторых, СССР не конкурировал с США в сфере гражданских коммерческих технологий на мировых рынках, включая советский и американский. В условиях холодной войны это было неосуществимо, а СССР не претендовал на лидерство в коммерческой технологической сфере в силу специфики избранной экономической модели. Что касается конкуренции с Японией в 1970–1990-е гг., то, кроме десятилетия 1987–1996 гг., номинальный ВВП США превышал японский в 2 и более раз (то есть разрыв между ВВП двух стран был в 1,5–2 раза больше, чем между США и КНР в настоящее время). Что касается международной конкуренции, то ситуация была зеркальной отношениям США – СССР. Системная конкуренция в сфере коммерческого хай-тека была налицо (преимущественно в 1980-е – первую половину 1990-х), но затрагивала лишь ряд подотраслей микроэлектроники и электронной продукции (зато об американо-японском геополитическом противостоянии говорить не приходилось).

Во-вторых, налицо также коррекция подходов к экономической глобализации, стремление компенсировать «провалы» (с точки зрения интересов США и их стремления к сохранению лидерства) глобальных институтов регулирования. В частности, весьма специфично выглядит массовое использование достаточно специализированных инструментов технологических санкций и иных торгово-экономических ограничений, связанных с технологической сферой, протекционизма и вскрытия рынков, не практиковавшихся западными странами с 1980-х гг. Это тем более необычно, учитывая закономерности развития цифровой индустрии, где еще 5 лет назад представить себе сложившуюся ситуацию было вряд ли возможно.

Наконец, не стоит сбрасывать со счетов и специфику перспективных цифровых технологий в их взаимосвязи с международными процессами.

1 Огромной сложностью подобных вычислений являются статистические ограничения, в частности, слабая возможность сравнения ВВП двух стран по паритету покупательной способности. При сопоставлении разрывов в размерах ВВП относительно США и СССР, США и Японии использовались данные изданий CIA Factbook, данные Всемирного банка ("GDP (current US$)," World Bank, accessed November 25, 2020, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=chart.) и ООН по национальным счетам ("National Accounts – Analysis of Main Aggregates (AMA)," UN Statistics Division, accessed November 25, 2020, https://unstats.un.org/unsd/snaama/Index.).

В последние три десятилетия развитие глобального ИКТ-сектора отличалось высоким уровнем интернационализации, международной кооперации, мощными глобальными стоимостными цепочками с расширенным аутсорсингом. Помимо естественных процессов научно-технологической и производственной специализации, эксплуатации конкурентных преимуществ (для развитых стран – мощных компетенций, для развивающихся стран Тихоокеанской Азии – дешевой рабочей силы и проч.) и разделения рисков и издержек, интернационализация подпитывалась двумя трендами. С одной стороны, обеспечением глобального доступа к квалифицированным кадрам, инновационным предпринимателям, разработчикам, умному капиталу, сложившимся инновационным институтам, экосистемам и кластерам, определяющим конкурентоспособность и развитие ИКТ в будущем. С другой – для новых цифровых технологий (интернет-решения, искусственный интеллект, большие данные) – доступом к первичным данным как новому стратегическому ресурсу цифровой экономики. В условиях растущей конкуренции США и Китая ценность и значение этих ресурсов возрастают, а доступ к ним действительно становится одним из ключевых факторов реализации цифрового лидерства.

Таким образом, несмотря на очевидные исторические параллели, технологическая война США и Китая – это не обычная торговая война, «типичные» санкции или иные традиционные феномены. Это элемент системной борьбы сверхдержав в сравнительно новом глобальном пространстве критических коммерческих технологий и технологической ренты, имеющих большое значение для усиления потенциалов развития, структурирования международных отношений и решения иных задач лидерства. Другой вопрос, что в этом качестве он явно сохраняет преемственность по отношению к геополитическим и экономическим конфликтам прошлого, являясь, скорее, эволюцией существующих подходов и решений, учитывающей новую роль и значение цифровых технологий в современном мире.

Американская стратегия и технологическая война как проявление технонационализма

Анализ мотивов, политического и экономического содержания, исторического контекста американских действий в разворачивающейся технологической войне позволяет нам корректно концептуализировать стратегию США. Наиболее удобной в данном случае оказывается адаптированная концепция (нео)технонационализма.

Исторически термин «технонационализм» является не вполне точным переводом лозунга японского Министерства внешней торговли и промышленности «Построим нацию на основе науки и технологий» (“*kagaku gijutsu rikkoku*” – 科学技術立国), активно применявшегося в период укрепления японского национального промышленно-технологического потенциала[1]. Во второй половине 1980-х гг. он, однако, стал использоваться также американскими авторами для описания протекционистской политики США в ответ на японскую технологическую угрозу, как и

1 Nakayama 2012.

японских протекционистских технологических стратегий[1]. Этот термин тесно смыкался по смыслу с понятием «технологического меркантилизма» и его аналогами.

Хотя технонационалистические акценты были всегда характерны для развитых стран и самих США[2], в последние десятилетия фокус исследований и дискуссий по технонационализму сместился в сторону развивающихся стран Азии, где феномен получил наиболее яркие и характерные формы[3]. Именно на основе азиатских кейсов концепция и оформилась окончательно в 1990-е гг. Под технонационализмом понимался акцент элит на развитии национального научно-технологического потенциала и технологическом суверенитете в ключевых (под)отраслях. Это, в свою очередь, рассматривалось как один из важнейших факторов конкурентоспособности, национального развития и комплексной национальной экономической безопасности[4]. Заметим, что, хотя концепция изначально применялась преимущественно к экономической политике, некоторые авторы уже тогда считали правомочным включать в нее вопросы, связанные с усилением военно-технического потенциала, совокупной мощи и международного влияния[5].

В своей рыночно-экономической интерпретации технонационализм изначально противопоставлялся техноглобализму, который понимался как достижение конкурентоспособности и развития через интеграцию в глобальное разделение труда и стоимостные цепочки (ГСЦ), а также иные международные и транснациональные процессы.

Это, казалось бы, непротиворечивое концептуальное определение подверглось существенному испытанию в связи с опытом КНР в конце 1990-х и особенно в 2000-х гг. Ведущая роль прямых иностранных инвестиций, активное участие КНР в глобальном разделении труда и иные процессы привели западных авторов к переосмыслению феномена в виде формулы неотехнонационализма[6]. Она предполагала достижение традиционных технонационалистических целей через техноглобальные инструменты либеральных торгово-инвестиционных режимов, включая интеграцию в ГСЦ развитых стран.

При наличии коррекции на новые экономические условия и проблематику противостояния сверхдержав концепция неотехнонационализма оказывается наиболее полезной для анализа и концептуализации стратегии США в технологической войне с КНР и самого феномена такой войны, что косвенно подтверждается и ростом апелляций к идеям неотехнонационализма со стороны западных авторов в последние годы[7].

Наблюдаемые процессы действительно могут быть описаны как попытка США обеспечить глобальное экономическое и геополитическое лидерство за

1 Robert Reich, “The Rise of Techno-nationalism.”; Nakayama 2012.
2 Ostry, Nelson 1995; Johnson-Freese, Erickson 2006; Mazzucato 2011; Wade 2014; Andreas Kuehn, and Bruce McConnell, “Weathering TechNationalism.”
3 Во многом это является политической проекцией экономических дискуссий о стратегиях роста развивающихся стран. См., например: Wade 2018.
4 С кратким обзором эволюции термина и его значений можно ознакомиться в: Ostry, Nelson 1995; Montresor 2001; Nakayama 2012; Kennedy 2013; Shim, Shin 2016; Kim et al. 2020.
5 Kennedy 2013; Shim, Shin 2016; Kim et al. 2020; Andreas Kuehn, and Bruce McConnell, “Weathering TechNationalism.”
6 Kennedy 2013; Shim, Shin 2016; Kim et al. 2020.
7 См., например: Robert A. Manning, “Techno-Nationalism vs. the Fourth Industrial Revolution,” Global Asia 14, no 1 (March 2019), accessed November 25, 2020, https://www.globalasia.org/v14no1/cover/techno-nationalism-vs-the-fourth-industrial-revolution_robert-a-manning; Andreas Kuehn, and Bruce McConnell. “Weathering TechNationalism.”; Alex Capri, “Techno-nationalism: The US-China tech innovation race.”

счет усиления национального технологического потенциала и конкурентоспособности с особым акцентом на контроль над глобальными рынками и технологическими процессами. Причем важнейший аспект неотехнонационализма предполагает не только традиционное участие в глобальных экономических процессах и максимизацию технологической ренты, но и преференциальный доступ к глобальным ресурсам цифрового развития: от научно-технологических и кадровых до первичных данных и системы стандартов. В этот широкий концептуальный контекст органично вписываются все наблюдаемые процессы: от санкций до расширенной секьюритизации технологий и данных, выполняющей важную мобилизационную функцию для (нео)технонационалистических усилий.

Рамочные концептуальные установки усиливаются структурирующей ролью цифровых технологий для некоторых международных процессов.

Если опустить вопрос влияния перспективных цифровых технологий на возможности в дипломатической сфере[1], они оказывают существенное, непосредственное влияние на систему отношений и партнерств. Хорошим примером являются технологии 5G, имеющие критическое значение для развертывания так называемых умных инфраструктур (города, электросети, дороги и проч.) и взаимосвязанных решений (цифровое здравоохранение, промышленность – в идеологии «Индустрия 4.0», автономный транспорт и т.д.). Действительно, выбор в пользу того или иного стандарта 5G предполагает рост долгосрочной взаимозависимости экономики-донора и акцептора. Это связано с высокой капиталоемкостью масштабирования телекоммуникационных систем, невозможностью быстрой и полной замены оборудования, особым вниманием к преемственности (по линии производителя) систем разных поколений[2]. С учетом сокращения числа участников рынка, способных выработать ряд перспективных цифровых стандартов и базовых технологий в сфере телекоммуникаций, микроэлектроники и иных отраслях, системы технических стандартов в значительной мере станут также отображением силы связей между различными странами.

Важен и проявившийся в ходе технологической войны феномен контроля над системообразующими ИКТ – от интеллектуальной собственности до поставок оборудования и программных средств – в качестве инструмента системного влияния на партнеров и давления на оппонентов. Наиболее явно это проявилось в сфере микроэлектроники. Хотя ограничения США как страны-держателя ключевых производственных технологий в данной сфере не остановили развитие технологической базы ИКТ КНР, но существенно удорожили и удлинили его, нанесли существенный ущерб крупным китайским корпорациям и обеспечили целый ряд иных негативных долгосрочных последствий, вплоть до потери части рынков[3].

1 См., например, краткий обзор и анализ в: Данилин 2020a.

2 Примечательна ситуация по «большой тройке» операторов мобильной связи в ФРГ (*Deutsche Telekom, Vodafone* и *Telefónica*), которые приняли условия по развертыванию сетей 5G на основе переоборудования инфраструктуры 4G. Значимую роль в этом процессе сыграла *Huawei*, так как от 45–50 до 65% оборудования 4G в ФРГ являются продукцией *Huawei*. См.: Moritz Koch, and Stephan Schueur, "Das bedeutet die Huawei-Entscheidung für die deutschen Netze," Handelsblatt, November 23, 2020, accessed November 25, 2020, http://surl.li/jwbf.

3 См., например: Torsten Riecke, "Resilience and Decoupling in the Era of Great Power Competition," China Monitor, MERICS, August 20, 2020, accessed November 25, 2020, https://merics.org/sites/default/files/2020-08/Merics_ChinaMonitor_PowerCompetition.pdf; Данилин 2020b.

Заключение

Проведенный анализ показывает, что стратегия США по противодействию КНР в цифровой сфере основывается на эволюции концепций неотехнонационализма. Этот процесс развивается под влиянием глобализации экономики, американо-китайского геополитического противостояния и специфики новых цифровых технологий и рынков. Даже безотносительно к объективным условиям, это ведет к изменению воззрений элит на роль рыночно-технологических процессов в цифровой сфере как новой арены глобальной конкуренции сверхдержав. Поэтому в будущем технологические конфликты могут стать системным и самостоятельным феноменом, тем более что значение мировых рынков для цифрового развития, а также связанных с ним категорий экономической (в том числе научно-технической), военной, мягкой силы будет только нарастать, усиливая технонационалистические дискурсы.

В этом смысле политика США 2017–2020 гг. не имела конъюнктурного характера и не была обусловлена личностными установками Д. Трампа, тем более что изменение подходов во взаимодействии с КНР можно отследить как минимум со второй администрации Б. Обамы. Различия курса Б. Обамы (а ныне – Дж. Байдена) и Д. Трампа в этом отношении имеют, скорее, тактический характер. Демократы избирают совокупность односторонних ограничений, акцентируя внимание на значении многосторонних торгово-экономических режимов (например, Трансатлантическое торговое и инвестиционное партнерство, *TTIP*, и Транстихоокеанское партнерство, *TAP*) как средства сдерживания КНР, в том числе в технологической сфере. Д. Трамп же сделал ставку на односторонние санкции и более жесткое давление в логике торговых войн XX в. Причем его жесткий политический курс был частично обусловлен совокупностью накопившихся противоречий и проблем, включая неэффективность предшествующих усилий технологического сдерживания Китая, торговой войной, общим ростом геополитического напряжения между сверхдержавами. Можно предположить, что политика Д. Трампа была необходимым шагом, обеспечившим разрушение старых, не всегда релевантных «правил игры», что открыло возможность для поиска новых решений. Индикатором полезности для США этого «созидательного разрушения» является то, что при всей критике «трампизма» отказываться от его наследия демократы явно не собираются.

Стратегически такая жесткая линия ставит под угрозу рыночные и инновационные процессы в цифровой сфере, что неприемлемо ни для мировой экономики, ни для ключевых государственных и бизнес-участников рынка. Союзники США также не воодушевлены избыточным бесцеремонным давлением Вашингтона.

Соответственно, в период новой администрации ожидаема нормализация инструментария неотехнонационалистической повестки в пользу формирования прежде всего техноэкономических режимов – по аналогии с торгово-экономическими режимами и как их органическая часть. Речь идет о совокупности гармонизированных институтов, технических стандартов и иных формальных и неформальных правил. Если проводить аналогии с междуна-

родными исследованиями, то феномен режимов близок к понятию структурной силы (*structural power*)[1].

Фактически мы уже наблюдаем складывание подобных режимов на примере ЕС, реализующего концепции цифрового / технологического суверенитета[2], и Китая – в рамках концепции «Цифрового Шелкового пути» как органической части мегапроекта «Пояс и путь».

Как следствие, технологическая война сверхдержав переходит в системную стадию, основанную на неотехнонационалистических подходах и воззрениях, а точнее – их дальнейшей эволюции. Эта стадия вряд ли будет столь же богата на яркие события и громкие заявления, но имеет более принципиальное значение для будущего баланса сил в мире и нового формата глобальных технологических процессов.

1 См., например: Culpepper 2015; Gwynn 2019.

2 Mark Scott, "What's driving Europe's new aggressive stance on tech," Politico, October 27, 2019, accessed November 25, 2020, https://www.politico.eu/article/europe-digital-technological-sovereignty-facebook-google-amazon-ursula-von-der-leyen/; "Expanding the EU's digital sovereignty," Official web-site of Germany's Presidency of the Council of the European Union, 2020, October 27, 2019, accessed November 25, 2020, https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828; Tambiama Madiega, "Digital sovereignty for Europe," European Parliamentary Research Service, EPRS Ideas Paper, July 2020, accessed November 25, 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Данилин, И.В. Влияние цифровых технологий на лидерство в глобальных процессах: от платформ к рынкам? // Вестник МГИМО-Университета. – 2020А. – Т.13 (1). – С.100–116. doi:10.24833/2071-8160-2020-1-70-100-116 [Danilin, Ivan V. "The Impact of Digital Technologies on Leadership in Global Processes: from Platforms to Markets?" [Vlijanie cifrovyh tehnologij na liderstvo v global'nyh processah: ot platform k rynkam?] *MGIMO Review of International Relations* 13, no. 1 (2020): 100–116] [In Russian].

Данилин, И.В. Американо-китайская технологическая война: риски и возможности для КНР и глобального технологического сектора // Сравнительная политика. – 2020В. – Т.11 (4). – С.160–176. doi: 10.24411/2221-3279-2020-10056 [Danilin, Ivan V. "The U.S.-China Technology War: Risks and Opportunities for P.R.C. and Global Tech Sector." [Amerikano-kitaiskaia tekhnologicheskaia voina: riski i vozmozhnosti dlia KNR i global'nogo tekhnologicheskogo sektora] *Comparative Politics Russia* 11, no. 4 (2020): 160–176] [In Russian].

Истомин, И.А. Миражи инноваций: «вклад» технологического прогресса в военную нестабильность // Вестник МГИМО-Университета. – 2020. – Т. 13 (6). – С. 7–52. doi: 10.24833/2071-8160-2020-6-75-7-52 [Istomin, Igor A. "Innovation Mirage: The Role of Technological Uncertainty in Military Instability." [Mirazhi innovacij: «vklad» tehnologicheskogo progressa v voennuju nestabil'nost'] *MGIMO Review of International Relations* 13, no. 6 (2020): 7–52] [In Russian].

Лексютина, Я.В. Американо-китайские отношения в 2018–2019 гг.: торговая война и процесс декаплинга // Мировая экономика и международные отношения. – 2020. – Т. 64 (6). – С. 85–93. doi: 10.20542/0131-2227-2020-64-6-85-93. [Leksjutina, Yana V. "US-China Relations 2018-2019: Trade War and Decoupling Process." [Amerikano-kitajskie otnoshenija v 2018–2019 gg.: torgovaja vojna i process dekaplinga] *Mirovaja jekonomika i mezhdunarodnye otnoshenija* 64, no. 6 (2020): 85–93] [In Russian].

Труш, С.М. Торговая война Д. Трампа против КНР: события, мотивации, внутренний контекст // Россия и Америка в XXI веке. – 2018. – Вып. 3. https:/ rusus.jes.su/s207054760000047-8-1 [Trush, Sergey M. "Donald Trump's trade war against China: events, motivations, internal context." [Torgovaja vojna D. Trampa protiv KNR: sobytija, motivacii, vnutrennij kontekst] *Russia and America in the 21st Century* 3 (2018)] [In Russian].

Салицкий, А.И., Семенова, Н.К. США–Китай: анатомия торгового конфликта // Восток. Афро-Азиатские общества: история и современность. – 2019. – Т. 223 (4). – С. 60–72. doi: 10.31857/S086919080005960-3 [Salickij, Alexander I., and Nelly K. Semenova. "USA–China: an anatomy of a trade conflict." [SShA–Kitaj: anatomija torgovogo konflikta] *Vostok. Afro-Aziatskie obshchestva: istoriia i sovremennost* 4, no. 4 (2019): 60–72] [In Russian].

Чеков, А.Д. Проблема влияния передовых военных технологий на стратегическую стабильность // Современный миропорядок и его влияние на национальную безопасность Российской Федерации. Сборник материалов круглого стола. – М.: ФГБОУ ВО «Московский политехнический университет», 2020. – С. 532–539 [Chekov, Alexander D. "The problem of the influence of emerging military technologies on strategic stability" [Problema vlijanija peredovyh voennyh tehnologij na strategicheskuju stabil'nost'] In *Sovremennyj miroporjadok i ego vlijanie na nacional'nuju bezopasnost' Rossijskoj Federacii,* 532–539. Moscow: FGBOU VO "Moskovskij politehnicheskij universitet," 2020] [In Russian].

Эльянов, А.Я. НТП и экономическая политика на периферии мирового хозяйства // Мировая экономика и международные отношения. – 2005. – № 4. – С. 74–85 [Jel'janov, Anatoly Ya. "Science and technology progress and economic policy on the periphery of the world economy." [NTP i jekonomicheskaja politika na periferii mirovogo hozjajstva] *Mirovaja jekonomika i mezhdunarodnye otnoshenija,* no. 4 (2005): 74–85] [In Russian].

Allison, Graham. *Destined for War: Can America and China Escape Thucydides's Trap?* New York: Houghton Mifflin Harcourt, 2017.

Atkinson, Robert D., and Stephen J. Ezell. I*nnovation Economics*. New Hampshire: Yale University Press, 2012.

Chen, Anthony W., Jim Chen, and V. Reddy Dondeti. "The US-China Trade War: Dominance of Trade or Technology?" *Applied Economics Letters* 27, no. 11 (June 24, 2020): 904–9. doi:10.1080/13504851.2019.1646860.

Evans, Paul. "Techno-Nationalism in China–US Relations: Implications for Universities." *East Asian Policy* 12, no. 02 (April 6, 2020): 80–92. doi:10.1142/S1793930520000161.

Evenett, Simon J. "The Smoot–Hawley Fixation: Putting the Sino-US Trade War in Contemporary and Historical Perspective." *Journal of International Economic Law* 22, no. 4 (December 20, 2019a): 535–55. doi:10.1093/jiel/jgz039.

Evenett, Simon J. "Protectionism, State Discrimination, and International Business since the Onset of the Global Financial Crisis." *Journal of International Business Policy* 2, no. 1 (March 26, 2019b): 9–36. doi:10.1057/s42214-019-00021-0.

Fakhari, Hussein. "The Long-Term Impact of Economic Sanctions on the Technological Development of Iran." In *The Development of Science and Technology in Iran*, 243–65. New York: Palgrave Macmillan US, 2017. doi:10.1057/978-1-137-57257-8_14.

Furnell, Stephen M., and M.J. Warren. "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?" *Computers & Security* 18, no. 1 (January 1999): 28–34. doi:10.1016/S0167-4048(99)80006-6.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (2009): 1155–1175.

Hufbauer, Clyde G., Jeffrey Schott, Kimberly A. Elliott, and Barbara Oegg. *Economic Sanctions Reconsidered.* 3rd Edition. Washington, DC: Peterson Institute for International Economics, 2008.

Hufbauer, Gary Clyde, and Euijin Jung. "What's New in Economic Sanctions?" *European Economic Review* 130 (November 2020): 103572. doi:10.1016/j.euroecorev.2020.103572.

Johnson-Freese, Joan, and Andrew S. Erickson. "The Emerging China–EU Space Partnership: A Geotechnological Balancer." *Space Policy* 22, no. 1 (February 2006): 12–22. doi:10.1016/j.spacepol.2005.11.001.

Kaempfer, William H., and Anton D. Lowenberg. "Chapter 27 The Political Economy of Economic Sanctions," 867–911, 2007. doi:10.1016/S1574-0013(06)02027-8.

Kennedy, Andrew B. "China's Search for Renewable Energy." Asian Survey 53, no. 5 (October 1, 2013): 909–30. doi:10.1525/as.2013.53.5.909.

Kim, Mi-jin, Heejin Lee, and Jooyoung Kwak. "The Changing Patterns of China's International Standardization in ICT under Techno-Nationalism: A Reflection through 5G Standardization." *International Journal of Information Managemen*t 54 (October 2020): 102145. doi:10.1016/j.ijinfomgt.2020.102145.

Kshetri, Nir, Prashant Palvia, and Hua Dai. "Chinese Institutions and Standardization: The Case of Government Support to Domestic Third Generation Cellular Standard." *Telecommunications Policy* 35, no. 5 (June 2011): 399–412. doi:10.1016/j.telpol.2011.03.005.

Li, Minghao, Edward J. Balistreri, and Wendong Zhang. "The U.S.–China Trade War: Tariff Data and General Equilibrium Analysis." *Journal of Asian*

Economics 69 (August 2020): 101216. doi:10.1016/j.asieco.2020.101216.

Mascitelli, Bruno, and Mona Chung. "Hue and Cry over Huawei: Cold War Tensions, Security Threats or Anti-Competitive Behaviour?" *Research in Globalization* 1 (December 2019): 100002. doi:10.1016/j.resglo.2019.100002.

Mazzucato, Mariana. *The Entrepreneurial State – Debunking Public vs. Private Sector Myths.* London: Demos, 2011.

Montresor, Sandro. "Techno-Globalism, Techno-Nationalism and Technological Systems: Organizing the Evidence." *Technovation* 21, no. 7 (July 2001): 399–412. doi:10.1016/S0166-4972(00)00061-4.

Nakayama, Shigeru. "Techno-Nationalism versus Techno-Globalism." *East Asian Science, Technology and Society* 6, no. 1 (January 1, 2012): 9–15. doi:10.1215/18752160-1504708.

Qin, Julia Y. "Forced Technology Transfer and the US–China Trade War: Implications for International Economic Law." *Journal of International Economic Law* 22, Issue 4 (December 2019): 743–762. https://doi.org/10.1093/jiel/jgz037.

Shim, Yongwoon, and Dong Hee Shin. "Neo-Techno Nationalism: The Case of China's Handset Industry." *Telecommunications Policy* 40, no. 2–3 (2016): 197–209. doi:10.1016/j.telpol.2015.09.006.

Steinbock, Dan. "U.S.-China Trade War and Its Global Impacts." *China Quarterly of International Strategic Studies* 04, no. 04 (January 11, 2018): 515–42. doi:10.1142/S2377740018500318.

Sun, Haiyong. "U.S.-China Tech War." *China Quarterly of International Strategic Studies* 05, no. 02 (January 8, 2019): 197–212. doi:10.1142/S237774001950012X.

Ostry, Silvia, and Richard R. Nelson. *Techno-nationalism and techno-globalism*. Wash., D.C.: The Brookings Institution, 1995.

Wade, Robert H. "The paradox of US industrial policy: The developmental state in disguise." In: *Transforming Economies: Making industrial policy work for growth, jobs and development,* edited by José M. Salazar-Xirinachs, Irmgard Nübler, Richard Kozul-Wright, 379–400. Geneva: ILO, 2014. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---inst/documents/publication/wcms_315679.pdf.

Wade, Robert H. "The Developmental State: Dead or Alive?" *Development and Change* 49, Issue 2 (March 2018): 518–546. https://doi.org/10.1111/dech.12381.

Сведения об авторе

Иван Владимирович Данилин,

к.пол.н., заведующий Отделом науки и инноваций ИМЭМО РАН,
старший научный сотрудник, Москва, Россия. Ул. Профсоюзная, 23, 117997.
e-mail: danilin.iv@imemo.ru

Дополнительная информация

Поступила в редакцию: 16 декабря 2020. Принята к публикации: 27 января 2021.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Благодарности

Автор выражает благодарность с.н.с., доценту МГИМО МИД России, к.пол.н. И.А. Истомину за консультации по вопросам теоретических аспектов современных международных исследований, а также руководителю Рабочей группы глобализации военно-экономических процессов ИМЭМО РАН, к.пол.н. М.Г. Евтодьевой за ценные комментарии, высказанные в процессе подготовки данной статьи.

Цитирование

Данилин, И.В. Концептуализация стратегии США в технологической войне против КНР: экономика, политика, технонационализм // Международная аналитика. – 2020. – Том 11 (4). – С. 21–38.
https://doi.org/10.46272/2587-8476-2020-11-4-21-38

Conceptualizing American Strategy in the Technology War Against China: Economy, Geopolitics, Techno-Nationalism

ABSTRACT

The paper examines the so-called U.S.-China "tech war" of 2017–2020 in the sphere of cutting-edge digital technologies, its origins, factors, and other aspects, with a focus on the American strategy to limit China's opportunities for technological development. The purpose of this study is to conceptualise the American tech war strategy and to assess the character and prospects of technology conflicts. The article represents the study with the use of comparative, historical approaches, the elements of systematic economic analysis, and some elements of neorealist and constructivist approaches. Based on the examination of key drivers of the tech war (with regard to the U.S. position), as well as the comparative historical analysis of the observed processes and the instruments implemented to fight for technological leadership, it concludes that technology conflict is a new phenomenon, determined, among other things, by the specifics of digital technologies and economic changes of recent decades, which at the same time preserves natural continuity in relation to the past geopolitical and economic conflicts and existing strategies and tools. Taking into account the peculiarities of the new conflict and digital technologies it deduces that it is possible to describe the U.S. policy in the framework of an adjusted concept of neo-techno nationalism (strengthening national technological potential and sovereignty through global economic instruments). It is noted that in the context of the digital revolution and in the analysis of the clash of superpowers this concept implies that goals are achieved through providing preferential access to such specific development resources as global human capital and big primary data, the formation of systems of standards, etc. In the conclusion, it is highlighted that the U.S. strategy under Trump, which led to a tougher American course in the tech war with China, was determined by objective circumstances as well as by personal traits of the president. In particular, such circumstances include the need to break old ineffective practices to design new solutions and approaches. The author draws a conclusion that in the future the United States will focus on building techno-economic regimes as a more systemic strategy for waging a technology conflict considering adjusted neo-techno national logic.

KEYWORDS

emerging digital technologies, sanctions, USA, China, techno-nationalism

Author

Ivan V. Danilin,
PhD in Political Sciences, Head of Department for Science and Innovation, IMEMO RAS,
23 Profsoyuznaya St., Moscow, 117997.
e-mail: danilin.iv@imemo.ru

Additional information

Received: December 16, 2020. Accepted: January 27, 2021.

Disclosure statement

No potential conflict of interests was reported by the author.

Acknowledgements

The author expresses his gratitude to the Research Fellow, Associate Professor at MGIMO Istomin I.A. (PhD), for his insightful comments on theoretical aspects of the study. I also thank the Head of the Working group on Globalization of Military-Economic Processes at IMEMO RAS Evtodieva M.G. (PhD) for her valuable advice made during this paper's preparation.

For citation

Danilin, Ivan V. "Conceptualizing American Strategy in the Technology War Against China: Economy, Geopolitics, Techno-Nationalism."
Journal of International Analytics 11, no. 4 (2020): 21–38.
https://doi.org/10.46272/2587-8476-2020-11-4-21-38

Solving the Strategic Equation: Integrating Missile Defense and Conventional Weapons in U.S.–Russian Arms Control

Andrey A. Baklitskiy

https://doi.org/10.46272/2587-8476-2020-11-4-39-55

ABSTRACT

With the New START treaty extension, Moscow and Washington are on course for new arms control negotiations. The unprecedented breadth of the strategic bilateral agenda issues means that any future talks would entail extensive linkages and trade-offs in various spheres. The article explores two of the domains that would inevitably have to be addressed in future negotiations – missile defense and strategic conventional weapons. Missile defense was an integral part of U.S.–Russian arms control from early on, most prominently reflected in the ABM treaty of 1972. However, a deep look into the current state and trajectory of U.S. missile defense developments suggests that instead of focusing on the "strategic" interceptors in the continental U.S., the aim should be on regulating new mobile systems, which pose a more significant threat to the strategic stability and might be more amenable to limitations. Strategic conventional weapons are less clearly defined, and there is less arms control experience with dealing with them. On occasions where they were subject to arms control regulations, they were either banned or included in the strategic nuclear forces limits. With many types of strategic conventional weapons, it does not seem that a one-size-fits-all approach is feasible. Some of the newer systems might remain too niche to have an impact on strategic stability. With the most ubiquitous strategic conventional weapons – long-range cruise missiles – a framework of asymmetric limits might be considered.

KEYWORDS

arms control, missiles defense, strategic conventional weapons, strategic equation, U.S.–Russian relations

CC BY

When Russia and the United States finally extended New START for another five years in February 2021, it soon became obvious that the hardest part was very much ahead of them. With all but one arms control treaty terminated or suspended, there was a void in place of the complicated architecture that once limited and managed nuclear competition between Moscow and Washington. Well aware of this void, Russia presented the United States with its vision of the "strategic equation" or "security equation," which would account for all the factors impacting strategic stability between the two countries. In the words of Deputy Minister of Foreign Affairs of the Russian Federation S.V. Ryabkov, "it is not limited to nuclear weapons. We consider it very important to embrace the entire spectrum of both nuclear and non-nuclear offensive and defensive arms that are capable of resolving strategic tasks."[1] Such an equation would form a general understanding of U.S.–Russian strategic relations, which could be than implemented in a number of specific agreements and legal arrangements.

Two components of the equation are of particular note. Strategic missile defense has been a problem in bilateral relations for decades, even more so after the United States withdrew from the Anti-Ballistic Missile Treaty (ABM Treaty) in 2002. By contrast, strategic conventional weapons were slowly gaining traction, but became an equally important issue for Moscow. They were almost never regulated by arms control agreements, the most important of which – the Intermediate-Range Nuclear Forces Treaty (INF Treaty) – disappeared in 2019 after yet another withdrawal on the part of the United States. It is hard to imagine any solution to the "strategic equation" without addressing these two issues.

A rich body of research exists on the topic of missile defense in arms control. Among Russian experts, A. Arbatov has noted that current ballistic missile defenses do not change the strategic balance, although defense capabilities aimed at third countries should be considered in the framework of the "interrelationship between strategic offensive and defensive arms."[2] V. Mizin has suggested that Moscow might not be interested in a new ABM agreement since new Russian strategic systems would penetrate any future U.S. missile defense.[3] V. Dvorkin has presented a case for why existing U.S. and Russian missile defense systems do not pose a threat to the strategic nuclear forces of the parties.[4] In an equally well researched piece, V. Yesin agreed that the current U.S. missile defense system does not undermine Russian strategic deterrence and pointed to the open-ended and global nature of the U.S. system, which would require further attention.[5]

American experts generally accept that Russia has an issue with the U.S. missile defense system. P. Vaddi and G. Perkovich have suggested that the United States should explore how its missile defense could be designed to counter missile treats from rogue states, but not Russia or China.[6] However, elsewhere, P. Vaddi and J.M. Acton

1 "Deputy Foreign Minister Sergey Ryabkov's Opening Remarks at a Briefing at the Rossiya Segodnya International Information Agency on Arms Control and Strategic Stability," Russian Ministry of Foreign Affairs, accessed February 11, 2021, https://www.mid.ru/en/main_en/-/asset_publisher/G51iJnfMMNKX/content/id/4570219.
2 *Арбатов, А.Г.* Роль ядерного сдерживания в стратегической стабильности. Гарантия или угроза // Московский центр Карнеги. 28 января 2019. [Электронный ресурс]. URL: https://carnegie.ru/2019/01/28/ru-pub-78209 (дата обращения: 01.03.2021).
3 Мизин 2019.
4 Дворкин 2019.
5 Есин 2017.
6 Perkovich, Vaddi 2021.

have noted that the United States has ruled out the possibility of putting legally binding limits on its missile defense, and Moscow should instead focus on politically binding transparency and confidence-building measures.[1] S. Pifer supported the idea of regular information exchange on U.S. missile defense capabilities, but he believes that this might not be enough for Moscow and has thus suggested limiting the number of U.S. interceptors in Europe.[2] G. Thielmann provided a thorough analysis of how many of the ABM Treaty's provisions could be reenacted in the current setting and reintroduced the idea of joint ceilings for strategic offensive and defensive weapons.[3]

However, few solutions have been offered on the Russian side to Moscow's concerns about the U.S. missile defense system, which undoubtedly will appear in any future negotiations. And the proposals on the American side, while generally well thought through, have not touched on some of the issues of concern and have not been ambitious enough to solve this long-standing problem.

The issue of regulating strategic conventional weapons is less researched, partly because of an ambiguity about what constitutes a strategic conventional weapon, and partly because of the diversity of the systems. On the Russian side, A. Arbatov has suggested that there is probably no single way to cover all existing high precision conventional weapons, but one way to partly address the issue is to control the number of tactical aviation vehicles that carry such weapons (in an agreement similar to the Treaty on Conventional Armed Forces in Europe), and including air-launched strategic conventional weapons in the common warhead ceilings of the next arms control treaty (by returning to the START I counting rules for heavy bombers) alongside strategic nuclear arms.[4] S. Oznobischev and K. Bogdanov propose controlling the numbers of tactical aviation, which carries strategic conventional weapons (in a CFE like agreement).[5] E. Buzhinskiy agrees that limiting air-launched strategic weapons could be straightforward, and that there could be technical solutions for sea- and ground-launched missiles as well.[6]

In the United States, J. Acton, P. Vaddi and T. MacDonald believe that there is no way to realistically limit conventional sea-launched missiles and suggest data exchange.[7] S. Pifer proposes capping the number of U.S. hypersonic boost glide vehicles, although he believes that it would be hard for Washington to limit its conventional sea- and air-launched cruise missiles and thus suggests discussing their implication for the strategic nuclear balance instead.[8]

It is unclear whether Moscow and Washington would even be interested in getting back to the counting rules established by the START I Treaty. In the meantime, transparency measures and discussions would probably not be enough to address the issue from the Russian point of view.

1 Vaddi, Action 2020.
2 Pifer 2016.
3 Thielmann 2020.
4 Arbatov, Alexey, and Ivanov, Igor. "Untangling the Knot of Strategic Arms Control. The Nuclear Threat Initiative," NTI. Building a Safer World, 2020, accessed March 3, 2021, https://www.nti.org/analysis/opinions/untangling-knot-strategic-arms-control/.
5 Ознобищев, Богданов 2020, 46.
6 *Бужинский, Е.* СНВ-3 и перспективы ограничения вооружений в российско-американских отношениях // Международный дискуссионный клуб Валдай. 5 февраля 2021. [Электронный ресурс]. URL: https://ru.valdaiclub.com/a/highlights/snv-3-i-perspektivy-ogranicheniya-vooruzheniy/ (дата обращения 03.03.2021).
7 James M. Acton, Thomas MacDonald, and Pranay Vaddi, "Revamping Nuclear Arms Control: Five Near-Term Proposals," Carnegie Endowment for International Peace, accessed March 3, 2021, https://carnegieendowment.org/2020/12/14/revamping-nuclear-arms-control-five-near-term-proposals-pub-83429.
8 Pifer 2016.

Finally, a number of works look into how arms control itself operates and how specific technologies can be included in it. In 1960, R. Bowie famously described arms control as "any agreement among several powers to regulate some aspect of their military capability or potential. The arrangement may apply to the location, amount, readiness, or types of military forces, weapons, or facilities."[1] In addition to the agreement limiting military capabilities, arms control normally implies the possibility of verifying that the parties are fulfilling their obligations.

Some arms control mechanisms appear to be more successful than others. Counties withdraw from legally binding treaties (for example, the ABM Treaty or theINF Treaty), while informal agreements are sustained even without an ongoing dialogue (such as SALT II). This can be partly explained by domestic politics, but some other general observations can be made. As T. Schelling, one of the first thinkers on arms control, wrote: "Most powerful limitations, the most appealing ones, the ones most likely to be observable in wartime, are those that have a conspicuousness and simplicity, that are qualitative and not a matter of degree, that provide recognizable boundaries."[2] This makes sense from the practical point of view – bans on whole classes of weapons are easier to verify than reducing their numbers or placing limitations on specific parameters.

P. Scharre points out that the success of arms control agreements can also be influenced by the military significance of the weapon in question (the higher the significance, the lower the chance of success) and its distribution (if both parties possess comparable number of the weapon, interest in bilateral limitation increases and the chance of success rises).[3]

In order to understand how to address missile defense and strategic conventional weapons in the U.S.–Russian arms control framework, this paper will explore the technical and political underpinning of both issues in detail, look into past efforts to address them, propose possible solutions, and estimate how realistic they could be.

Strategic Missile Defense

Intercontinental ballistic missiles (ICBMs) are still the main way of delivering nuclear weapons to enemy territory. They form the backbone of nuclear deterrence. The flight trajectory of an ICBM and its reentry vehicle (RV) can be divided into two parts – active (guided flight with an active propulsion) and passive (free flight after the engine shuts down and the RV separates from the missile).[4] The passive stage of the trajectory can also be subdivided into exo-atmospheric and atmospheric parts. Throughout the history, Moscow and Washington have developed missile defense that is aimed at interception at every stage of the trajectory.

Intercepting a missile in the active phase of its flight helps solve the problem of decoys and other countermeasures and destroys several warheads with a single strike

1 Bowie 1960.
2 Schelling 1966, 164.
3 Scharre 2018, Ch. 20.
4 Траектория полёта баллистической ракеты // Министерство обороны РФ. [Электронный ресурс]. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14145@morfDictionary (дата обращения 03.03.2021). In the Western tradition, the trajectory of an ICBM is usually divided in three phases: boost phase, midcourse phase, and terminal phase.

(for missiles with multiple reentry vehicles). A missile with its engines firing provides a highly visible target, even when it has not reached maximum speed. At the same time, trying to intercept a missile at this stage has its disadvantages. The interceptor must "catch up" with the ICBM, which requires considerably high speed and must be launched from a location close to the target. The task is further complicated by existing countermeasures, which include shortening the active part of the trajectory by using more powerful engines.

Atmospheric intercept of RVs is complicated by the high speed and possible change of the missile's trajectory. The atmosphere also limits the use of sensors on the interceptors and their range.[1]

Exo-atmospheric intercept takes place at the most predictable ballistic part of the trajectory. Despite the largest number of possible countermeasures (the lack of atmosphere and orbital motion significantly complicate discrimination between RVs and decoys), exo-atmospheric intercept is currently the most promising and well-developed method, and it is used as the basis for all existing strategic missile defense systems.

U.S. Strategic Missile Defense

As of January 2021, the U.S. missile defense system includes three main components. First, two sites equipped with "heavy" GBI's (Ground-Based Interceptors) in the continental United States. There are total of 44 interceptors: 40 at Fort Greely, Alaska and 4 at Vandenberg Air Force Base, California.[2] Second, 48 U.S. Navy ships equipped with the Aegis Ballistic Missile Defense System and armed with different versions of atmospheric (RIM-156 Standard Block IV (SM-2) and RIM-174 Standard ERAM (SM-6)) and exo-atmospheric (RIM-161 Standard Missile 3 (SM-3)) interceptors.[3] Under the FY2021 budget submission, the number of BMD-capable Navy Aegis ships is projected to increase to 65 by the end of FY2025.[4] Third, land-based Aegis system (Aegis Ashore) in Europe deployed as a part of the European Phased Adaptive Approach, which includes 24 SM-3 interceptors at the Deveselu Facility in Romania. A further 24 are expected to be deployed at a second site in Poland.

In addition, the United States possess mobile THAAD (Terminal High Altitude Area Defense) systems aimed at intercepting intermediate-range ballistic missiles in the atmosphere and at the very end of the exo-atmospheric part of the trajectory.[5]

Ground-based Interceptors consist of a booster and a kinetic kill vehicle. All the GBI's deployed by the United States are currently equipped with an EKV (Exoatmospheric Kill Vehicle). The system has a mixed track record. Since 1999, only 11 of 19 tests were successful.[6] The development of a new kill vehicle – the RKV (Redesigned Kill Vehicle) –

1 Garwin 1999.
2 "Department of Defense Press Briefing on the President's Fiscal Year 2019 Defense Budget for the Missile Defense Agency," The US Dept of Defense, February 13, 2018, accessed March 3, 2021, https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1440326/department-of-defense-press-briefing-on-the-presidents-fiscal-year-2019-defense/.
3 "Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress," Congressional Research Service, December 23, 2020, accessed March 3, 2021, https://fas.org/sgp/crs/weapons/RL33745.pdf.
4 Ibid.
5 "Fact Sheet, Terminal High Altitude Area Defense," The US Dept of Defense, Missile Defense Agency, September 24, 2018, accessed March 3, 2021, https://www.mda.mil/global/documents/pdf/thaad.pdf.
6 "Ballistic Missile Defense Intercept Flight Test Record," Missile Defense Agency, September 2019, accessed March 3, 2021, http://surl.li/mpvo.

led by Boeing was a failure. The deadlines for testing and deployment were constantly postponed, and in August 2019, the Department of Defense terminated the project, stating that "we decided the path we're going down wouldn't be fruitful."[1] On April 24, 2020 the U.S. Missile Defense Agency (MDA) released a request for proposals on the Next Generation Interceptor (NGI).[2]

The cancelation of the RKV put on hold plans for the deployment of 20 additional GBIs in Alaska, which was planned for 2023.[3] As of right now, the Missile Defense Agency is still planning to build 20 silos to be used for NGI deployment. But since the NGI program aims to develop an interceptor from scratch (including a new booster),[4] it is not expected to be deployed until the 2030s, although the director of the Missile Defense Agency has since said it would be possible to field the NGI by 2028.[5]

The U.S. Navy operates the *Aegis Combat System*, which in one of its modifications is capable of intercepting ballistic missiles with an SM-3 interceptor. Aegis is deployed on two types of ships: Ticonderoga-class cruisers (CG-47) and Arleigh Burke-class destroyers (DDG-51). By September 30, 2021, a total of 48 of these ships will be equipped with an Aegis version capable of missile defense, making them BMD-capable Navy Aegis ships. Other ships with Aegis systems can be upgraded to perform a BMD role, which would require changes to be made to the computer systems, new software to be installed, and interceptors to be uploaded.[6] Under the FY2021 budget submission, the number of BMD-capable Navy Aegis ships is projected to increase to 65 by the end of FY2025. However, Congress reduced funding for the future large surface combatant ships in December of 2020, which calls these plans into question.[7]

Ticonderoga-class cruisers are equipped with 122 Mark 41 (Mk-41) Vertical Launching Systems, while Arleigh Burke-class destroyers have 90 or 96 Mk-41 launchers depending on the version. These launchers can fire a broad range of land-attack, anti-ship, anti-submarine, and anti-ballistic missiles. It is impossible to assess the number of launchers equipped with anti- ballistic missiles at any given time, but it is obviously less than the maximum possible.

The most concerning missiles from the point of view of strategic missile defense are the SM-3s, which are capable of performing the exo-atmospheric kinetic intercept of ballistic missiles. There are three consecutive versions of the missile. SM-3 Block IA and Block IB (with an upgraded seeker, processor, and increased maneuverability) are currently deployed on U.S. ships. Estimates put their number at a few hundred.[8]

1 Paul Mcleary, "Pentagon Cancels Multi-Billion $ Boeing Missile Defense Program," Breaking Defense, August 21, 2019, accessed March 3, 2021, https://breakingdefense.com/2019/08/pentagon-cancels-multi-billion-boeing-missile-defense-program/.
2 Aaron Mehta, "Pentagon Releases Request for Proposals on Next Generation Interceptor," Defense News, April 24, 2020, accessed March 3, 2021, https://www.defensenews.com/space/2020/04/24/pentagon-releases-request-for-proposals-on-next-generation-interceptor/.
3 "Missile Defense. Delivery Delays Provide Opportunity for Increased Testing to Better Understand Capability," Government Accountability Office, June 2019, accessed March 3, 2021, https://www.gao.gov/assets/700/699546.pdf.
4 "Hill: NGI Has Flexibility In Development Cycle, Replaces Whole Interceptor," Defense Daily, March 10, 2020, accessed March 3, 2021, https://www.defensedaily.com/hill-ngi-flexibility-development-cycle-replaces-whole-interceptor/missile-defense/.
5 Jen Judson, "Congress Directs DoD to Build Interim Homeland Missile Defense Interceptor," Defense News, December 3, 2020, accessed March 3, 2021, https://www.defensenews.com/land/2020/12/03/congress-directs-dod-to-build-interim-homeland-missile-defense-interceptor/.
6 "Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress," Congressional Research Service, December 23, 2020, accessed March 3, 2021, https://fas.org/sgp/crs/weapons/RL33745.pdf.
7 David B. Larter, "Congress Guts Funding for Cruiser Replacements," Defense News, December 23, 2020, accessed March 3, 2021, https://www.defensenews.com/naval/2020/12/23/congress-guts-funding-for-cruiser-replacements/.
8 "Standard Missile-3 (SM-3)," CSIS Missile Defense Project, September 28, 2018, accessed March 3, 2021, https://missilethreat.csis.org/defsys/sm-3/.

SM-3 Block IIA, developed jointly with the Japan Self-Defense Forces, is purchased by the Pentagon in limited numbers and is still undergoing testing. Block IIA missiles were given a larger fuel tank, which increases its speed and potential flight time, as well as a bigger kinetic warhead.[1] According to expert estimates, the speed of SM-3 Block IIA reaches 4.5km/s compared to 3km/s for Block IB.[2] The United States officially canceled the development of the next generation of SM-3 Block IIB interceptors, which were aimed at intercepting ICBMs, in 2013.[3]

Nevertheless, with the lack of progress of the Ground-Based Midcourse Defense in the continental United States, Washington is investigating the possibility of using SM-3 Block IIA missiles against ICBMs. On November 18, 2020, this anti-ballistic missile successfully intercepted an ICBM-class target.[4] Such developments could potentially threaten Russian strategic forces. Especially with the number of SM-3 Block IIA planned for purchase exceeding 300.[5]

Allies of the United States, including Australia, Spain, Norway, South Korea, and Japan, either have Aegis ships in their fleets, are in the process of building them or plan to build them in the future. Most of the six Japanese Aegis destroyers are BMD-capable. Tokyo plans to upgrade the remaining ships in the upcoming years, with two additional BMD destroyers currently under construction.[6] The Aegis ships of the United States' other allies are not BMD capable.

As a part of the European Phased Adaptive Approach, the Deveselu Facility in Romania hosts *Aegis Ashore* system, with 24 SM-3 Block IB interceptors. The construction of the second U.S. missile defense site in Europe near the Polish village of Redzikowo, which will host another 24 SM-3 missiles, keeps getting delayed. The facility, which was supposed to become operational in 2018, will not be ready before 2022 because of contractor's poor performance.[7] Both sites are expected to host SM-3 Block IIA missiles.

Aegis Ashore is considered as an alternative to both GBIs and Aegis BMD ships. There were proposals to deploy further Aegis Ashore sites in the continental United States,[8] Guam (as a substitute for THAAD battery),[9] and Hawaii (at Pacific Missile Range Facility Barking Sands).[10]

Until recently, Japan was planning to build two Aegis Ashore sites on its territory. According to the Ministry of Defense, the systems could have become initially

1 "Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress," Congressional Research Service, December 23, 2020, accessed March 3, 2021, p. 5, https://fas.org/sgp/crs/weapons/RL33745.pdf.
2 See, for example: Joan Johnson-Freese, and Ralph Savelsberg, "Why Russia Keeps Moving the Football on European Missile Defense: Politics," Breaking Defense, October 17, 2013, accessed March 3, 2021, https://breakingdefense.com/2013/10/why-russia-keeps-moving-the-football-on-european-missile-defense-politics/.
3 "Missile Defense Announcement. As Delivered by Secretary of Defense Chuck Hagel," Legistorm, March 15, 2013, accessed March 3, 2021, https://www.legistorm.com/stormfeed/view_rss/76757/organization/31751.html.
4 "U.S. Successfully Intercepts ICBM with Ship-Launched Missile in Historic Test," ABC News, accessed March 3, 2021, http://surl.li/mpxw.
5 Laura Grego, "The SM-3 Block IIA Interceptor. A New Arms Control Challenge," Union of Concerned Scientists, August 2019, accessed March 3, 2021, https://www.ucsusa.org/sites/default/files/attach/2019/08/SM-3%2520IIA.pdf.
6 "Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress," Congressional Research Service, December 23, 2020, accessed March 3, 2021, p. 5, https://fas.org/sgp/crs/weapons/RL33745.pdf.
7 "MDA, Army Withholding Pay as Aegis Ashore Poland Construction Still Drags," USNI News, March 12, 2020 accessed March 3, 2021, https://news.usni.org/2020/03/12/mda-army-withholding-pay-as-aegis-ashore-poland-construction-still-drags.
8 "Inflection Point: Missile Defense and Defeat in the 2021 Budget," CSIS Missile Defense Project, March 23, 2020, accessed March 3, 2021, https://missilethreat.csis.org/inflection-point-missile-defense-and-defeat-in-the-2021-budget/.
9 "Pentagon Considers Replacing Guam's THAAD Battery with Aegis Ashore," Jane's, February 5, 2020, accessed March 3, 2021, https://www.janes.com/article/94114/pentagon-considers-replacing-guam-s-thaad-battery-with-aegis-ashore.
10 "2019 Missile Defense Review," The US Dept of Defense, accessed March 3, 2021, p. XV, https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF.

operational in the mid-2020s.[1] However, on June 15, 2020, Minister of Defense Taro Kono canceled the program, citing technical issues and the increasing cost.[2] Japan decided to add two more Aegis BMD ships to its fleet instead.

The United States also considers using *THAAD for the atmospheric intercept of ICBMs* and integrating it into a multilayered system together with GBIs and SM-3s. Both the use of the existing interceptors and modification of the seeker and the booster are being considered.[3]

The Donald Trump administration also showed some interest in the *active phase intercept of ballistic missiles*. The 2019 Missile Defense Review stated that, "As rogue state missile arsenals develop, the space-basing of interceptors may provide the opportunity to engage offensive missiles in their most vulnerable initial boost phase of flight, before they can deploy various countermeasures [...] DoD will undertake a new and near-term examination of the concepts and technology for space-based defenses to assess the technological and operational potential of space-basing in the evolving security environment."[4] The same document noted the potential of the F-35 Lightning II for "shooting down adversary ballistic missiles in their boost phase," when equipped with a new or modified interceptor.[5]

At the same time, the required DoD report on space sensors and interceptors, which was supposed to be delivered within six months (by July 2019),[6] was never finished. The National Defense Authorization Acts for 2020 and 2021 show that almost no work is being done on boost phase intercept.[7]

Russian Strategic Missile Defense

Unlike the United States, Russia is not developing and does not plan to develop a country-wide ABM system. Russia maintains *A-135 anti-ballistic missile system*, protecting Moscow and the surrounding industrial region. The system is compliant with the 1972 ABM Treaty. According to open-source information, when the A-135 was completed in 1989, it included a Don-2N battle management radar and two types of interceptors: 68 shorter range 53T6 (Gazelle) missiles for atmospheric interception and 32 longer-range 51T6 (Gordon) missiles for exo-atmospheric interception.[8] The 2019 U.S. Missile Defense Review also states 68 interceptors.[9] The system is currently undergoing modernization with new interceptors that are being developed and tested.

1 "Lockheed Martin Wins Contract Modification for Japan Aegis Ashore Batteries," The Diplomat, March 9, 2020, accessed March 3, 2021, https://thediplomat.com/2020/03/lockheed-martin-wins-contract-modification-for-japan-aegis-ashore-batteries/.
2 "Japan Suspends Aegis Ashore Deployment, Pointing to cost and Technical Issues," Defense News, June 25, 2020, accessed March 3, 2021, https://www.defensenews.com/global/asia-pacific/2020/06/15/japan-suspends-aegis-ashore-deployment-pointing-to-cost-and-technical-issues/.
3 "MDA's FY21 Budget Paves Way for New Homeland Missile Defense Plans," Defense News, February 10, 2020, accessed March 3, 2021, https://www.defensenews.com/smr/federal-budget/2020/02/11/mdas-fy21-budget-paves-way-for-new-homeland-missile-defense-plans/.
4 "2019 Missile Defense Review," The US Dept of Defense, accessed March 3, 2021, p. IX, https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF.
5 Ibid., XII.
6 "Department of Defense Off-Camera Press Briefing on the 2019 Missile Defense Review," The US Dept of Defense, January 17, 2019, accessed March 3, 2021, http://surl.li/mpzz.
7 "Missile Defense. An Assessment of U.S. Military Power," Heritage Foundation, October 30, 2019, accessed March 3, 2021, https://www.heritage.org/military-strength/assessment-us-military-power/missile-defense.
8 Колтунов et al. 2010, 15.
9 "2019 Missile Defense Review," The US Dept of Defense, accessed March 4, 2021, https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF.

The goal is to have the system operational in 2022.[1] There is no indication that the number of the interceptors will be increased as a result.

Russia also employs a wide range of *mobile air and missile defense systems*. The S-500 Prometey "Prometheus" system, which is expected to be initially deployed in 2021 and mass produced in 2025, is designed to intercept intermediate-range ballistic missiles, as well as ICBMs in the terminal phase and under certain conditions in the midcourse phase.[2] Russia widely exports its predecessor, S-400 "Triumph." The system has been delivered to China and Turkey, a contract has been signed with India.

Russia has also been testing its "Nudol" system, which is allegedly capable of intercepting ballistic missiles out of the atmosphere, as well as targeting space objects.[3]

Arms Control Options for Strategic Missile Defense

The most successful arms control initiative in regards to missile defense was the 1972 ABM Treaty. According to the document, the parties agreed:

– to limit their anti-ballistic missile systems to two (later one) missile fields with up to 100 interceptors;

– not to deploy ABM systems or their components for a defense of the territory of its country and not to provide a base for such a defense in other states, and not to deploy ABM systems for defense of an individual region;

– not to develop, test, or and deploy anti-ballistic missile systems or components which are sea-based, air-based, space-based or mobile land-based.

For the most part, the sides still adhere to the first limitation, despite the withdrawal of the United States from the ABM Treaty in 2002. There is no indication that either Moscow or Washington plan to increase the number of silo-based interceptors beyond 100 in the foreseeable future. Considering the current state of the U.S. Ground-Based Midcourse Defense, based on GBIs, it seems realistic to say that, for technical, financial, and organizational reasons it will pose no threat to the Russian strategic forces for at least the next decade. The Ground-Based Midcourse Defense deployed today is also popular with the American people and both political parties in Congress. Trying to limit it through the arms control negotiations is thus doomed to failure. A more promising approach would be to focus the discussion on those systems that are located outside the United States, which, as we have seen, also have a higher destabilizing potential.

The United States is in clear violation of the second limitation, as it deploys or plans to deploy its *de facto* strategic missile defense systems outside its national territory and transfers these systems to its allies. At the same time, with the new Russian BMD systems coming online, the issue of their delivery to Moscow's allies and partners will have to be addressed. It is entirely possible that Beijing and Tehran may not be interested in ICBM defense – Iran would hardly be targeted by strategic nuclear forces, and China

1 *Гаврилов, Ю*. Чтобы муха не пролетела. Как идет модернизация системы ПРО Москвы // Российская Газета. 22 января 2021. [Электронный ресурс]. URL: https://rg.ru/2021/01/22/kak-moderniziruiut-sistemu-pro-moskvy.html (дата обращения: 04.03.2021).

2 Разработчик рассказал о возможностях С-500 // РИА Новости. 10 февраля 2020. [Электронный ресурс]. URL: https://ria.ru/20200210/1564512668.html (дата обращения: 04.03.2021).

3 *Ходаренок,* М. «Нудоль» и «Прометей»: когда армия получит новые системы // Газета.ру. 19 июня 2020. [Электронный ресурс]. URL: https://m.gazeta.ru/army/2020/06/19/13123189.shtml (дата обращения: 04.03.2021).

does not seem to be looking for nuclear invulnerability, aiming at deterrence instead. This could open the door for U.S.–Russian discussions on the export of strategic BMD systems. Moscow and Washington could establish technical limits for the export of ballistic missile systems. The Missile Technology Control Regime (MTCR), which Russia will be chairing in 2021–2022, could serve as a guide for such limitations.

Finally, both Moscow and Washington ignore the third limitation by deploying or developing mobile BMD systems. At the same time, this issue was already present in the 1990s, when the rapid development of mobile missile defense systems at the theater level forced Russia and the United States to look into ways of distinguishing between strategic and non-strategic BMD. At a meeting in New York in 1997, the parties agreed on a memorandum of understanding and two agreed statements, which were later ratified by Russia, but not the United States.

The agreement stated that, for the purposes of the ABM Treaty, interceptor missiles with a velocity of up to 3 km/sec over any part of its flight trajectory or whose target missile does not exceed 5 km/sec over any part of its flight trajectory and has a range that does not exceed 3500 kilometers are not counted against ABM Treaty limits.[1] The parties also agreed on transparency measures regarding their non-strategic BMD systems (THAAD and the Navy Theater-Wide Theater Ballistic Missile Defense System, which would later become the Aegis Missile Defense System, for the United States and C-300B for Russia).[2] Additionally, the agreement stipulated an annual exchange of information about the systems, the obligation to notify the other party about the construction of new test sites and interceptor launches. The sides promised that deployed non-strategic BMD systems would not pose a threat to the strategic forces of the other party, which was supposed to be supported by the exchange of information about the numbers of such systems and plans for their use and development.

The 1997 agreements were an interesting experience. Some of their provisions, such as making sure that the configuration of missile defense systems does not threaten the strategic forces of the other side, seem to be quite relevant and promising today. At the same time, other parts need updating. According to the media, SM-3 Block IIA already exceeds the accepted speeds agreed upon in the memorandum. It is safe to assume that this could be the case for some of the newer Russian systems as well. The speed of the interceptors would be an important factor and will have to be addressed, especially for the U.S. anti-ballistic missiles in Europe – both ground- and sea-based. The higher the speed, the bigger the chance that they could be used successfully against Russian ICBMs launched from the European part of the country in the active phase of their trajectory.

At the same time, speed is an important, but not critical factor in successfully intercepting an ICBM in the passive part of its trajectory. The trajectory of the interceptor

1 "First Agreed Statement Relating to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems of May 26, 1972. September 26, 1997. Special Section: New START II and ABM Documents," Arms Control Association, accessed March 3, 2021, https://www.armscontrol.org/act/1997-09/arms-control-today/special-section-new-start-ii-abm-documents.

2 "Agreement on Confidence-Building Measures Related to Systems to Counter Ballistic Missiles other than Strategic Ballistic Missiles," The nuclear information project, September 26, 1997, accessed March 3, 2021, https://fas.org/nuke/control/abmt/text/abm_cbm.htm.

simply needs to cross the trajectory of an ICBM, which is quite easy to calculate.[1] Here the total number of U.S. exo-atmospheric interceptors, primarily SM-3, would make a difference.

Russia and the United States could agree to limit the number of interceptors so that it would be enough to stop a finite number of missiles from third parties, but not enough to threaten the strategic forces of Moscow and Washington. The details of such an agreement could be then re-evaluated every five or ten years. And while the United States is less interested in limiting Russian missile defenses, Moscow's arsenal is growing, and the calculus might change. Additionally, Washington has on multiple occasions raised its concerns about Russian anti-satellite (ASAT) systems. Since exo-atmospheric missile defense and ASAT weapons are essentially based on the same principles, there could be some room for maneuver there.

If Moscow and Washington agree to exchange information on the number of interceptors in their possession, verification and storage would be problematic, as would confirming the presence or absence of SM-3 missiles onboard ships, not least because it would reveal the content of other missile tubes. One idea on how to tackle the issue would be to separate BMD-capable ships, limit their number and provide them with functionally related observable differences (FRODs), which can be observed using national technical means of verification (NTMs). The U.S. Navy might be interested in exploring this option. Its leadership has on several occasions spoken critically about BMD consuming too much of the limited naval resources. For example, in 2018, Chief of Naval Operations Adm. John Richardson said, "Whether that's AEGIS ashore or whatever, I want to get out of the long-term missile defense business and move to dynamic missile defense."[2]

Another critical aspect of missile defense that should be considered in the context of arms control is the non-deployment of BMD systems in outer space and a ban on air-based strategic BMD systems. None of those currently exist, but research and development is being conducted in these areas.

Strategic Conventional Weapons

There is no universally accepted definition of a strategic conventional weapon. However, to have a strategic effect, a conventional weapon must have high precision and be capable of traveling long (though not necessarily intercontinental) ranges, which essentially equates "strategic" with "long-rage high-precision" weapons.

The Handbook of Defence Terminology of the Ministry of Defence of the Russian Federation defines long-rage high-precision weapons as the "weapons of an increased potential threat [...] aimed at the selective assured strike of stationary [...] and in some

1 See, for example, Simon Peterson (@SimonHoejbjerg): "I often see and hear people talking about whether or not a certain interceptor can intercept a specific ballistic missile type, e.g. can an SM-3 intercept an ICBM. And very often people make claims that the interceptor's burn out velocity is critical to that. It's actually not," Tweeter, December 30, 2019, https://twitter.com/SimonHoejbjerg/status/1211582726991691777.

2 "The U.S. Navy is Fed up with Ballistic Missile Defense Patrols," Defense News, June 16, 2018, accessed March 3, 2021, https://www.defensenews.com/naval/2018/06/16/the-us-navy-is-fed-up-with-ballistic-missile-defense-patrols/.

cases quasi-stationary objects [...] at distances exceeding 400 km."[1] The protocol to the New START Treaty defines long-range air-launched cruise missiles (ALCMs) as "an ALCM with a range in excess of 600 kilometers."[2] For air- and sea-launched systems, the genuine range is increased by the range of their platforms. No such criteria have been developed for land-based systems, as they were previously banned under the INF Treaty. Long-range conventional hypersonic missiles should also be included as strategic conventional weapons.

Because of their high precision, strategic conventional weapons are well suited for attacks against enemy infrastructure, including nuclear command and control and dual-use military infrastructure, which can lead to nuclear escalation. Moreover, strategic conventional weapons can be used as a part of a counterforce strike alongside nuclear weapons.

U.S. Strategic Conventional Weapons

The U.S. strategic conventional forces include sea- and ground-launched (after the August 18, 2019 test from a mobile launcher) BGM-109 Tomahawk missiles (conventional only after 2013[3]), air-launched AGM-86C/D cruise missiles (a nuclear version of the missile exists as well), and air-launched AGM-158 JASSM ER cruise missiles (extended range). R&D continues on the new air-launched LRSO (Long-Range Standoff Missile – conventional and nuclear) cruise missile, which is intended to substitute AGM-86 by 2030,[4] the JASSM XR (extreme range) and LRASM (Long Range Anti-Ship Missile) anti-ship cruise missile based on JASSM ER.

In December 2019, a prototype intermediate range ground-launched ballistic missile was tested.[5] According to expert estimates, the prototype was based on the Castor 4A rocket engine. No further tests followed.

The United States has several ongoing R&D projects on hypersonic missiles. Every military service runs its own program. The Army and the Navy design their systems based on a common vehicle developed by the Army.[6] The Navy's project is called Intermediate Range Conventional Prompt Strike Weapon (IR CPS), while the Army's is called Long-Range Hypersonic Weapon (LRHW). The Air Force has canceled a similar program of its own, the Hypersonic Conventional Strike Weapon, (HCSW), to save money and is now focusing on the AGM-183A Air-launched Rapid Response Weapon (ARRW).[7] The Defense Advanced Research Projects Agency (DARPA) is developing at least four hypersonic programs in conjunction with the armed forces: Tactical Boost Glide (TBG), Advanced Full-

1 Высокоточное оружие большой дальности // Справочник по терминологии в оборонной сфере. Министерство обороны России. [Электронный ресурс]. URL: http://dictionary.mil.ru/folder/123102/item/129202/ (дата обращения 03.03.2021).
2 Протокол к Договору между Российской Федерацией и Соединенными Штатами Америки о мерах по дальнейшему сокращению и ограничению стратегических наступательных вооружений // Президент России. [Электронный ресурс]. URL: http://static.kremlin.ru/media/events/files/41d2ef6d0dc8b2e65fc5.pdf (дата обращения 03.03.2021).
3 Hans M. Kristensen, "U.S. Navy Instruction Confirms Retirement of Nuclear Tomahawk Cruise Missile," Federation of American Scientists, March 18, 2013, accessed March 3, 2021, https://fas.org/blogs/security/2013/03/tomahawk/.
4 Kristensen, Korda 2021.
5 "Pentagon Conducts First Test of Non-Nuclear Capable Ballistic Missile Post-INF Treaty," The Drive, December 12, 2019, accessed March 3, 2021, https://www.thedrive.com/the-war-zone/31456/u-s-conducts-first-test-of-non-nuclear-ballistic-missile-following-inf-arms-treaty-collapse.
6 Sydney J. Freedberg Jr., "Army Warhead is Key to Joint Hypersonics," Breaking Defense, August 22, 2019, accessed March 3, 2021, https://breakingdefense.com/2018/08/army-warhead-is-key-to-joint-hypersonics/.
7 "Roper: The ARRW Hypersonic Missile Better Option for USAF," Air Force Magazine, March 2, 2020, accessed March 3, 2021, https://www.airforcemag.com/arrw-beat-hcsw-because-its-smaller-better-for-usaf/.

Range Engine (ARFE), Operational Fires (OpFires) and Hypersonic Air-Breathing Weapon Concept (HAWC).[1]

The U.S. defense budget for FY2021 has earmarked 2.6 billion USD for hypersonic research, including 206 million USD for hypersonic defense.[2] According to the Congressional Research Service, United States is unlikely to field an operational system before 2023.[3]

All the U.S. hypersonic boost glide vehicles under development are conventional only. According to Mike White, the Pentagon's assistant director for hypersonics, because of the differences in ranges and the trajectory of the boost glide vehicles, "any adversary who's got the capability to detect [them] will quickly understand the difference."[4] With this said, the strictly conventional nature of the new weapons increases their requirements, including higher accuracy. Taking the specific conditions in which the hypersonic boost glide vehicles are operating into account – high speed, extreme heating due to air friction – it will be tough to meet these requirements.

Russian Strategic Conventional Weapons

Russian strategic conventional weapons include "Kalibr" sea-launched cruise missiles (a separate nuclear version of the missile also exists), Onyx sea-launched anti-ship cruise missiles (a separate nuclear version of the missile also exist),[5] and Kh-55, Kh-101,[6] and Kh-32[7] air-launched cruise missiles (separate nuclear versions of each of these missiles exist). On December 1, 2017, the "Kinzhal" air-launched ballistic missile (a separate nuclear version exists) mounted on MiG-31K aircraft reached initial operational capability.[8] The "Zircon" hypersonic sea-launched missile is undergoing testing.

The Russian armed forces do not have strategic conventional weapons with intercontinental range. According to open-source information, the "Avangard" hypersonic boost-glide vehicle was developed as a nuclear weapons delivery system.

Arms Control Opportunities for Strategic Conventional Weapons

Russia and the United States have extraordinarily little experience in dealing with strategic conventional weapons in arms control. Whenever Moscow and Washington have touched upon the issue, strategic conventional weapons were either banned or included in the total limits together with the nuclear weapons.

Ground-launched intermediate range conventional missiles were banned alongside their nuclear "cousins" under the INF Treaty, primarily to make the verification easier. START I banned air-launched ballistic missiles, both conventional and nuclear. Finally, New START included conventional ICBMs and SLBMs (in case they would be

1 Kelley M. Sayler, "Hypersonic Weapons: Background and Issues for Congress," Congressional Research Service, accessed March 3, 2021, pp. 4–8, https://www.hsdl.org/?view&did=827149.
2 Sydney J. Freedberg Jr., "Hypersonics Won't Repeat Mistakes of F-35."
3 Kelley M. Sayler, "Hypersonic Weapons: Background and Issues for Congress."
4 Sydney J. Freedberg Jr., "Hypersonics Won't Repeat Mistakes of F-35."
5 Эксперт: бросковые испытания ракеты «Оникс-М» с дальностью 800 км уже проведены // ТАСС. 25 сентября 2019. [Электронный ресурс]. URL: https://tass.ru/armiya-i-opk/6925991 (дата обращения 03.03.2021).
6 Kristensen, Korda 2019.
7 Россия вооружится неуязвимым «убийцей авианосцев» // Лента.ру. 15 мая 2018. [Электронный ресурс]. URL: https://lenta.ru/news/2018/05/15/tu22/ (дата обращения 03.03.2021).
8 Гиперзвуковая ракета «Кинжал». Досье // ТАСС. 19 июля 2018. [Электронный ресурс]. URL: https://tass.ru/info/5387789 (дата обращения 03.03.2021).

produced) in the aggregate strategic offensive arms limit. Neither the United States nor Russia ever built such weapons.

None of this precedent looks especially helpful this time around. It seems clear that neither country is prepared to give up its strategic conventional weapons altogether. And the asymmetry in the Russian and U.S. strategic conventional arsenals just does not stimulate Washington to discuss this issue at all. The United States also needs to take China's substantial missiles arsenal into account.

The situation can change with new Russian systems, such as "Zircon" hypersonic missile, coming online. In the event that Washington becomes interested in discussing sea-, air- and ground-launched strategic conventional missiles, the experience of START I can become relevant. While the original START did not cover sea-launched nuclear cruise missiles, the parties have produced politically binding declarations, limiting the number of long-range nuclear SLCMs (with a range exceeding 600 km) to 880 missiles. Moscow and Washington also pledged to make an annual exchange of plans for the arsenals of such missiles for the next five years. The parties also agreed to exchange the number of nuclear SLCMs with a range of between 300 and 600 km.[1] These limitations were completely lopsided. While the United States was planning to deploy 637 long-range nuclear SLCMs, the USSR only had 100.[2] Similar limitations could be adopted for conventional missiles (including hypersonic) as well.

Washington could be interested in discussing hypersonic systems, an area in which Russia currently has an edge. However, Russian and U.S. hypersonic systems were developed separately and with different goals. In the United States, the Prompt Global Strike was a child of the "capabilities-based" military planning under the G.W. Bush administration, which came to replace the old-fashioned "threat-based approach."[3] For its part, the Russian "Avangard" boost glide vehicle is a continuation of the "Albatros" project started in the 1980s with the aim of defeating the U.S. global BMD and delivering nuclear warhead to the continental United States. Since the Russian and American programs were not created as a reaction to each other, mutual limitation without considering the challenges they were meant to address looks improbable.[4]

Currently the mass production of hypersonic boost glide vehicles is partly limited by New START, which limits the number of deployed ICBMs. The Russian side has agreed to include "Avangard" in the New START limits, as it is mounted on a treaty accountable missile.[5] Hypersonic systems are also rather expensive (more so compared to "classic" warheads), and their missions seem to be quite narrow. One can imagine that hypersonic weapons will remain a niche project, with little impact on strategic stability.

Depending on the pace of development of intermediate-range hypersonic weapons and the threat perceptions of the two sides (especially of sea- and air-

1 "Declaration of the United States of America Regarding its Policy Concerning Nuclear Sea-Launched Cruise Missiles," FAS, July 31, 1991, accessed March 3, 2021, https://fas.org/nuke/control/start1/text/declsts.htm; "Declaration of the Union of Soviet Socialist Republics Regarding its Policy Concerning Nuclear Sea-Launched Cruise Missiles," FAS, July 31, 1991, accessed March 3, 2021, https://fas.org/nuke/control/start1/text/declsts.htm.

2 *The Future of the U.S.-Soviet Nuclear Relationship* 1991.

3 "Special Briefing on the Nuclear Posture Review," The US Dept of Defense, January 9, 2002, accessed March 3, 2021, https://fas.org/sgp/news/2002/01/npr-briefing.html.

4 Borrie et al. 2019, 15–16.

5 В Генштабе заявили, что комплекс «Авангард» не нарушит договоренности по СНВ // Интерфакс. 24 июля 2019. [Электронный ресурс]. URL: https://www.interfax.ru/russia/670264 (дата обращения 03.03.2021).

launched hypersonic weapons), there could be a room for discussing the issue. The sides will have somewhat similar weapons (the Russian "Kinzhal" and the array of the U.S. systems), which could lead to numerical limitations.

Conclusion

None of the possibilities mentioned in this article will be easy to implement. Despite the New START extension, the U.S.–Russia relations remain in poor condition. Views on the strategic stability and the national security of the two countries diverge significantly. Even maintaining the current limitations on strategic offensive arms five years from now is not a given.

Worse still, we should not expect a clean and easy-to-verify solution on missile defense or strategic conventional weapons, and this, experts believe, it increases the chances for an agreement to succeed. In both cases, the capabilities of the two sides are not equal (although Russia is catching up), which leads to an asymmetry of interests. Both missile defense and strategic conventional weapons provide clear military and political benefits (though in a different way) to Moscow and Washington, so limiting them would be a tall order.

However, a case can me made that arms control frameworks could successfully address some of these issues if properly targeted.

In terms of missile defense, instead of focusing on the U.S. Ground-Based Midcourse Defense, which is not the most immediate threat to strategic stability and is an extremely popular program that enjoys bipartisan support in Washington, Russia and the United States should look into the missile defense and mobile systems located outside their territories. Limiting the export of mobile strategic missile defense systems could also be of interest to Moscow and Washington. It will not be easy to put limitations even on mobile U.S. missile defense systems, but some sort of combination of qualitative and quantitative limitations on U.S. interceptors would be beneficial for strategic stability. Such an agreement would need to include robust information exchanges and could be verified by NTMs. Space and air-based missile defense remain as destabilizing as ever and should be avoided.

Moscow and Washington have never had much success in regulating strategic conventional arms. The issue is further complicated by the asymmetry in the U.S. and Russian arsenals. Despite the impressive developments in new technologies, the biggest issue would still be posed by the same old conventional cruise missiles. One possible approach to address this would be to use the experience of SLCM limitations accompanying START I. As for hypersonic boost glide systems, those of the intercontinental range (if produced) will be covered by the existing arms control limitations. Intermediate range hypersonic systems are currently not mass produced. If this changes, and both countries believe that they pose a problem for their security, they can be discussed in the arms control format.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Дворкин, В.З. Влияние систем ПРО на стратегическую стабильность и перспективы ядерного разоружения // Мировая экономика и международные отношения. – 2019. – Т. 63 (8). – С. 5–12. https://doi.org/10.20542/0131-2227-2019-63-8-5-12 [Dvorkin, Vladimir Z. "The impact of missile defense systems on the strategic stability and prospects of nuclear disarmament" [Novie konturi strategicheskoi stabilnosti I perspektivi kontrolia nad strategicheskimi vooruzheniami] *World Economy and International Relation*s 63, no.8. (2019): 5–12] [In Russian].

Есин, В.И. Американская и российская системы противоракетной обороны и стратегическая стабильность // Вестник Московского университета. Серия 25: Международные отношения и мировая политика. – 2017. – Т. 9 (4). – С. 3–41. https://cyberleninka.ru/article/n/amerikanskaya-i-rossiyskaya-sistemy-protivoraketnoy-oborony-i-strategicheskaya-stabilnost [Esin, Victor I. "The U.S. And Russian Missile Defense Systems And Strategic Stability" [Amerikanskaia i rossiyskaya sistemy protivoraketnoi oborony i strategicheskaia stabilnost'] *Moscow University Bulletin of World Politics* 9, no.4 (2017): 3–41] [In Russian].

Колтунов, В., Кубышкин, А., Степанов, В. Противоракетная оборона: история и современность. – М.: Институт стратегической стабильности «Росатом», 2010. – 17 с. http://mil.ru/files/Anti-ballistic/01_Rosatom.pdf. [Koltunov, Victor, Alexander Kubyshkin, and Vladimir Stepanov. *Anti-Missile Defense: History and Current Trends* [Protivoraketnaya oborona: istoriya i sovremennost'], Moscow: Rosatom] [In Russian]

Мизин, В.И. Новые контуры стратегической стабильности и перспективы контроля над стратегическими вооружениями // Пути к миру и безопасности. – 2019. – Т. 56 (1) – С. 96–121. https://doi.org/10.20542/2307-1494-2019-1-96-121 [Mizin, Victor I. "New tenets for strategic stability and prospects for strategic arms control" [Novie konturi strategicheskoi stabilnosti I perspektivi kontrolia nad strategicheskimi vooruzheniami] *Pathways to Peace and Security* 56, no.1 (2019): 96–121] [In Russian].

Ознобищев, С.К., Богданов, К.В. Высокоточные вооружения в Европе // Контроль над вооружениями в новых военно-политических и технологических условиях / отв. ред. А.Г. Арбатов. – М.: ИМЭМО РАН, 2020. – С. 36–47. https://www.imemo.ru/publications/info/kontroly-nad-vooruzheniyami-v-novih-voenno-politicheskih-i-tehnologicheskih-usloviyah [Oznobischev, Sergey K., and Konstantin V. Bogdanov. "High-precision weapons in Europe" [Visokotochnie vooruzhenia v Evrope] in Arms control under the new military-political and technological condition, edited by A.G. Arbatov, 36–47. Moscow: IMEMO RAS, 2020] [In Russian].

Borrie, John, Amy Dowler, and Pavel Podvig. "Hypersonic. A Challenge and Opportunity for Strategic Arms Control Weapons." New York, 2019. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/hypersonic-weapons-study.pdf.

Bowie, Robert R. "Basic Requirements of Arms Control." *Daedalus* 89, no. 4. (Fall 1960): 708–722. https://www.jstor.org/stable/20026612?seq=1.

Garwin, Richard L. "Technical Aspects of Ballistic Missile Defense." *APS Forum on Physics and Society* 28, no. 3 (July 1999). https://fas.org/rlg/garwin-aps.htm.

Kristensen, Hans M., and Matt Korda. "Russian Nuclear Forces, 2019." *Bulletin of the Atomic Scientists* 75, no. 2 (March 4, 2019): 73–84. doi:10.1080/00963402.2019.1580891.

Kristensen, Hans M., and Matt Korda. "United States Nuclear Weapons, 2021." *Bulletin of the Atomic Scientists* 77, no. 1 (January 2, 2021): 43–63. doi:10.1080/00963402.2020.1859865.

Perkovich, George, and Vaddi, Pranay. "Proportionate Deterrence: A Model Nuclear Posture Review." New York: Carnegie Endowment for International Peace, 2021. https://carnegieendowment.org/files/Perkovich_Vaddi_NPR_full1.pdf.

Pifer, Steven. "The future of U.S.–Russia Arms Control." New York: Carnegie Endowment for International Peace, 2016. https://carnegieendowment.org/files/2-17-16_Pifer_US_Russia_Arms_Control_clean.pdf.

Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton, 2018.

Schelling, Thomas C. *Arms and Influence.* Yale University Press, 1966.

The Future of the U.S.-Soviet Nuclear Relationship. Washington, D.C.: National Academies Press, 1991. doi:10.17226/1846.

Thielmann, Greg. "Incorporating Missile Defense in Strategic Arms Control." *The Deep Cuts Issue Brief* 12 (2020): 1–9. https://deepcuts.org/files/pdf/Deep_Cuts_Issue_Brief_12-Missile_Defense_Strategic_Arms_Control_01.pdf.

Vaddi, Pranay, and James M. Acton. "Nuclear Arms Control: Enhancing Security Through Cooperation." New York: Carnegie Endowment for International Peace, 2020. https://carnegieendowment.org/2020/10/02/restart-for-u.s.-russian-nuclear-arms-control-enhancing-security-through-cooperation-pub-82705.

Author

Andrey A. Baklitskiy,

Consultant at PIR Center, 103 4th Dobryninskiy lane, 8, Moscow, 119049.

e-mail: a.baklitskiy@inno.mgimo.ru

Additional information

Received: February 18, 2021. Accepted: March 4, 2021.

Disclosure statement

No potential conflict of interests was reported by the author.

For citation

Baklitskiy, Andrey A. "Solving the Strategic Equation: Integrating Missile Defense and Conventional Weapons in U.S.–Russian Arms Control." *Journal of International Analytics* 11, no. 4 (2020): 39–55. https://doi.org/10.46272/2587-8476-2020-11-4-39-55

Решение стратегического уравнения: интеграция противоракетной обороны и обычных вооружений в российско-американский режим контроля над вооружениями

АННОТАЦИЯ

В связи с продлением срока действия нового договора СНВ Москва и Вашингтон вступили в процесс новых переговоров по контролю над вооружениями. Беспрецедентное количество нерешенных вопросов двусторонней повестки означает, что любые будущие переговоры повлекут за собой компромиссы в различных сферах. В статье исследуются две области, которые неизбежно придется рассматривать на будущих переговорах – противоракетная оборона и стратегические обычные вооружения. Противоракетная оборона была неотъемлемой частью российско-американской архитектуры контроля над вооружениями с самого начала, что наиболее ярко отразилось в договоре по ПРО от 1972 г. Однако изучение текущего состояния и вектора развития противоракетной обороны США позволяет предположить, что вместо того, чтобы сосредоточиться на т. н. «стратегических» перехватчиках, расположенных на континентальной части США, цель переговоров должна заключаться в урегулировании статуса и роли новых мобильных систем, которые представляют существенную угрозу стратегической стабильности и с большей вероятностью могут стать предметом ограничений. Определение стратегических обычных вооружений размыто, и опыт контроля их контроля незначителен. В тех случаях, когда на них распространяются положения о контроле над вооружениями, они либо запрещаются, либо включаются в лимиты, распространяемые на стратегические ядерные силы. Более того, ко многим типам стратегических обычных вооружений невозможно применять универсальный подход контроля. Поэтому применительно к самым распространенным стратегическим обычным вооружениям – крылатым ракетам большой дальности – автор считает, можно было бы рассмотреть рамки т. н. асимметричных лимитов.

КЛЮЧЕВЫЕ СЛОВА

контроль над вооружениями, противоракетная оборона, стратегические обычные вооружения, стратегическое уравнение, российско-американские отношения

Сведения об авторе

Андрей Александрович Баклицкий,
консультант ПИР Центра, 4-й Добрынинский пер., д. 8, 103, Москва, 119049.
e-mail: a.baklitskiy@inno.mgimo.ru

Дополнительная информация

Поступила в редакцию: 18 февраля 2020. Принята к публикации: 4 марта 2021.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Цитирование

Баклицкий, А.А. Решение стратегического уравнения: интеграция противоракетной обороны и обычных вооружений в российско-американский режим контроля над вооружениями // Международная аналитика. – 2020. – Том 11 (4). – С. 39–55.
https://doi.org/10.46272/2587-8476-2020-11-4-39-55

The Threat of Conventional Weapons to Nuclear Security: A New Reality for Deterrence

Peter James Mckenzie Rautenbach

https://doi.org/10.46272/2587-8476-2020-11-4-56-71

ABSTRACT

This paper explores the idea that developments in Conventional Prompt Global Strike (CPGS) systems degrade nuclear security. The United States is developing such weapons for niche conventional use on the surface, but the line between tactical and strategic weapons is becoming blurred. What is more, while there have been discussions in Congress surrounding the problem of missile ambiguity, there is a multitude of other problems, with the largest being that CPGS weapons inherently degrade nuclear security. By looking at the behavior of critical states and actors involved in the emergence of CPGS weapons and combining this with pre-existing literature and insight on similar topics within international relations, we then can conduct a thorough investigation on the impact of these CPGA systems. When compared to nuclear missiles, the increasing usability of these weapons is inherently dangerous, as it increases both the likelihood of their use and the likelihood of a first strike against another state's nuclear deterrent. Traditionally, conducting a first strike has been all but impossible because it entailed using nuclear weapons, which come with ethical and environmental consequences. If nuclear weapons can be replaced or substituted with CPGS weapons, then a first strike becomes an actual possibility. Hence, as a result, the nuclear doctrine is changing to reflect this conventional danger and has led to a lower threshold for nuclear use. This fact then demonstrates clear signs that CPGS technology degrades nuclear security and thus increases the chance of nuclear use.

KEYWORDS

BSU, deterrence, nuclear weapons, first strike, conventional weapons, emerging technologies

CC BY

Introduction

Nuclear weapons hold a unique place in arms control and international relations. In one sense, they viewed are still as one of the greatest threats to humanity – desp ite the fact that 75 have passed since they were last used. On the other hand, they seem to have been largely relegated to the sidelines of the public sphere since the end of the Cold War. A bogyman from a bygone age whose danger is remembered but not truly felt anymore. Recent developments involving North Korea aside,[1] new threats such as terrorism, cyber warfare, and the continuing evolution of conventional weapons have taken the spotlight. The lethality of nuclear weapons remains unchanged, but public and government focus has arguably shifted to face new threats.

However, it is precisely these non-nuclear developments that merit a review of nuclear stability, as they themselves threaten the regimes that were set in place to control nuclear proliferation. In particular, the evolution of conventional capabilities surrounding global strike programs generally referred to as Conventional Prompt Global Strike (CPGS) systems in the United States. These developments threaten to degrade nuclear security and subsequently increase the danger of nuclear use. We are talking primarily here about the increasing accuracy of missiles at the intercontinental level. Increasing the accuracy of a missile means that the yield of the warhead can be lowered and a conventional weapon can theoretically be used instead of a nuclear one in roles traditionally filled by the latter, such as a disarming first strike. While seemingly positive, this development undermines nuclear security by making a first strike a real possibility, which in turn raises the chances of a nuclear response.

Additionally, the increasing viability of conventional weapons with intercontinental range raises a myriad of other questions and concerns. The issue that has drawn perhaps the most attention here is the inherent ambiguity of missiles inflight. After launch, missiles carrying conventional warheads are indistinguishable from those carrying nuclear warheads. This in turn increases the likelihood of one of these weapons being mistaken for an incoming nuclear missile. In Congress, debates surrounding long-range conventional weapons have often focused too narrowly on the issue of miscalculation, and serious concerns have been raided regarding misattribution.[2] To this end, hypersonic weapons systems are being explored as alternate delivery systems because their flight path is distinctly different from that of ballistic nuclear weapons.[3] However, despite the differences in their flightpaths, hypersonic weapons have the same problem as ballistic missiles in that there is nothing preventing nuclear weapons from being loaded onto these systems. Looking deeper into the ramifications of these developments on nuclear deterrence, it becomes clear that not only does the use of hypersonic delivery systems fail to solve the problem of misattribution, but that CPGS weapons, no matter how they are deployed, inherently degrade nuclear security and consequently increase the chances of nuclear use regardless of the launch system used.

1 Choe Sang-Hun, "North Korea Vows to Boost Nuclear Program, Saying U.S. Diplomacy Failed," The New York Times, June 2020, accessed January 29, 2021, https://www.nytimes.com/2020/06/11/world/asia/north-korea-nuclear-trump.html.
2 Acton 2013, 1, 4.
3 Butt 2016, 51.

Background Definitions

The central argument here is that contemporary developments in conventional weapons technology degrade nuclear security, and that this in turn warrants conventional arms control efforts. However, this is not a technical paper and it does not provide technical answers to the problems explored here. The focus is on the wider political and security challenges posed by the development of conventional weapons technologies. This focus on technology posits that, regardless of the state involved, it is technology itself that poses the threat. Consequently, the emphasis here is not on individual states as causal factors behind the danger. Nonetheless, there is a specific focus on the United States due to its consistent and open desire to develop a global strike program using conventional weapons with intercontinental range.[1] We will also discuss the responses of Russia and China to U.S. conventional weapons development, as they are both nuclear states that are arguably adversaries of the United States. It is within these two bilateral relationships that the impact of evolving conventional weapons technologies can be clearly seen. That notwithstanding, it is the strategic impact of these weapons that poses a threat to international stability.

However, as M.C. Horowitz points out, the very fact that this technology is still emerging makes studying its potential impact difficult.[2] This is largely because of the lack of available evidence and the fact that there is real uncertainty surrounding the influence of new technologies.[3] This uncertainly is of course why the topic merits academic exploration and why this paper discusses the danger of CPGS weapons, despite the lack of empirical evidence. Horowitz puts forth that there are research design options available when studying new weapons technologies, as well as a lack of data. One of the more relevant options he presents "involves behavioral research on what influences attitudes toward them within the general public [...] in the military, or among elites."[4] The other relevant approach for this paper involves studying applied theory, which "entails leveraging insights from existing international relations theory – or other fields – and applying them to limited existing evidence to assess how particular weapons systems are likely to shape international politics."[5] Despite the inherent methodological shortcomings of studying the impact of emerging technologies, these two methods allow us to explore existing theories and cross-reference them with the real world actions of military leaders and planners in order to make logical claims about the strategic influence that developments in conventional weapons technology have on international security and stability.

On that note, conventional weapons can be generally understood to be any weapon that derives its destructive power from kinetic energy, or standard explosives. For this discussion, this can be narrowed down to focus on CPGS weapons which are "high-precision conventional weapons capable of striking a target anywhere in the world within one hour's time of the decision to launch."[6] This paper will delve

1 Warren 2011, 446; Butt 2016, 51.
2 Horowitz 2020, 386.
3 Ibid.
4 Ibid., 387.
5 Ibid.
6 Acton 2013, 4.

into the strategic ramifications that inherently come with CPGS weapons; however, it should be noted that many of these weapons also incorporate another emerging technology known as hypersonic launch systems. The inherent instability caused by CPGS weapons is separate from hypersonic technology. However, because the U.S. development of CPGS is increasingly focused on hypersonic variants,[1] this emerging technology warrants an exploration in the context of CPGS weapons. Furthermore, as will be discussed shortly, the U.S. Congress believes that pursing hypersonic variants of CPGS weapons gets around the problem of warhead attribution that comes with the use of conventional missiles.[2]

Hypersonic Weapons and Warhead Ambiguity

At their core, hypersonic weapons are those that "travel faster than Mach 5 (~3,800 mph) and have the capability to maneuver during the entire flight."[3] Both factors theoretically increase the survivability of a hypersonic missile against ballistic missile defense (BMD) systems as "the flight profile of [hypersonic weapons] provides a natural immunity from U.S. ballistic missile defenses."[4] These advantages could allow for maneuverable lightning-fast strikes against adversaries, which is why many states are pursuing this technology. On the surface, developing flexible non-nuclear options appears to be a step in the right direction. In an escalating crisis where some level of nuclear conflict seems inevitable, the option to use CPGS weapons in the place of a nuclear strike appears to be not only desirable, but also the distinctly ethical choice. However, while this flexibility is beneficial to any state, the very existence of these weapons destabilizes nuclear deterrence and international stability, and even increases the odds of nuclear use.

As we stated earlier, the debate surrounding CPGS has been narrowly focused on the issue of warhead ambiguity.[5] However, accurate long-range conventional weapons are inherently dangerous, and this is separate from any ambiguity issues. Despite this danger, it appears that the United States will continue to pursue CPGS weapons, due in part to the belief that hypersonic delivery systems offer an escape from the problem of warhead ambiguity. While it could be argued that a working and unambiguous CPGS system would outweigh the inherent degradation of nuclear deterrence that comes with it, the reality is that hypersonic missiles are not free from the same ambiguity problem. Traditionally, ballistic CPGS systems could easily be misinterpreted as a nuclear attack, "thereby fostering unwanted and strong escalatory incentives."[6] This is because of the "virtually impossibility of knowing the difference between a nuclear and conventionally armed missile" once in flight.[7] This difficulty stems from the fact "that the ballistic trajectory of [conventionally-armed ballistic missiles] makes it undistinguishable from a nuclear-armed ballistic missile."[8] With this difficulty in mind, hypersonic weapons could theoretically act as an unambiguous

1 Butt 2016, 51.
2 Ibid.
3 "Hypersonic Weapons Basics," Missile Defense Advocacy Alliance, accessed January 29, 2021, https://missiledefenseadvocacy.org/missile-threat-and-proliferation/missile-basics/hypersonic-missiles/.
4 Butt 2016, 52.
5 Acton 2013, 4.
6 Gromley 2015, 125.
7 Ibid.
8 Garcia 2017, 359.

global strike system – as the boost-glide trajectory of hypersonic weapons, which differs from a traditional ballistic missile. This would make them less likely to be confused with a nuclear ICBM attack.[1] However, while the United States allegedly intends for hypersonic weapons to remain within the conventional realm, both Russia and China appear to be pursing nuclear variants.[2] Despite assurances by the United States that it will not arm its hypersonic weapons with nuclear warheads, adversarial states have to see incoming hypersonic weapons as a possible nuclear attack. This then puts hypersonic missiles in the same ambiguous category as ballistic missiles. Therefore, regardless of whether we are talking about conventional ballistic or hypersonic missiles, their use could be misinterpreted as an incoming nuclear strike. However, suppose one is to argue that Congress has been focusing too narrowly on the issue of warhead ambiguity. In that case, one must also establish the alternative problem of CPGS weapons that they should be focusing on. By exploring core theories of nuclear deterrence and the strategic impact of CPGS weapons, their degrative effect on the key tenets of nuclear security becomes clear.

Deterrence Theory

One such tenet under threat is Mutually Assured Destruction (MAD). Despite the unquestionable danger of nuclear weapons, many, including the late K. Waltz, argued that they "are a great force for peace."[3] The cold, yet effective logic of this idea is that nuclear states can never afford to go to war with one another because the possible retaliation would be too costly. The key concept here is the absolute certainty nuclear weapons create, as their use would be undeniably catastrophic in every way imaginable. Therefore, states tend to act defensively rather than offensively as "the state that fears attack does not pre-empt – since that would be a wasteful [and dangerous] use of its military resources – but rather prepares to receive an attack. Doing so does not decrease the security of others, and several states can do it simultaneously; the situation will therefore be stable."[4] In theory, nuclear weapons become the ultimate defensive tool. In this way, the theory of MAD has a strong parsimony. However, this is not to say that MAD is an unassailable concept that is destined to remain static. In fact, as stated by B.R. Green and A. Long, MAD is far "more malleable then commonly admitted."[5] While the destructive nature of nuclear weapons is irrefutable, the survivability of a state's second-strike or retaliatory capability is not secure. B.R. Green and A. Long saw that Soviet nuclear policy changed throughout the Cold War as its leadership became increasingly concerned that their deterrent was becoming less effective and thus vulnerable to an American disarming strike.[6] To take this one step further, K.A. Lieber and D.G. Press suggest that developments in ballistic missile accuracy was, and continues to be, a threat to the survivability of fixed targets and thus places doubt on the strength

1 Butt 2016, 51.
2 Ibid.
3 Van Evera 2013, 241.
4 Jervis 1978, 190.
5 Green, Long 2017, 606.
6 Ibid., 608.

of MAD.[1] This paper seeks to build upon these ideas, which, when thoroughly explored, will demonstrate that the stability of MAD eroding due to the continued pursuit of conventional strike weapons, and that new developments in missile accuracy are a large part of this problem.

It can be argued that stability in nuclear security is primarily based on perception and the confidence in one's second-strike capabilities. The perception of a threat can have almost the same effect on states as real threats, especially when it comes to nuclear strategy. Additionally, failing to correctly perceive an adversary's deterrent, or misunderstanding how one's own deterrent is perceived, can cause a complete failure of deterrence efforts.[2] R.K. Betts notes that states could "stumble into [war] out of misperception, miscalculation and fear of losing if they fail to strike first."[3] Furthermore, threat perception guides nuclear doctrine because there would be almost no time to consider real world developments in a situation where nuclear weapons are used. If nuclear weapons are launched, there could be as little as 15–30 minutes before they reach their target.[4] Therefore, states build their nuclear doctrines around what they perceive as threats, rather than around actions directly taken against them.

One core aspect of perception is the idea of an offensive or defensive advantage. The principal idea is whether being aggressive or defensive is advantageous to obtaining security for the state. When offense is said to have the advantage, it is easier to destroy the forces of an adversary and take territory than it is to defend your own. The opposite is true when defense has the advantage. Moving forward and capturing territory becomes less efficient than defending your own.[5] In the defensive world, military buildup by states can be assumed, at least to some degree, to be defensive, as aggression is impractical. Thus, states can increase their own security without threatening the security of others due to the perception of the threat being lowered.

With this in mind, for most of world history, defense has arguably had the advantage.[6] Attacking has been costly, as technology and geography often made it possible to absorb aggression.[7] However, despite this apparent defensive advantage, human history is littered with wars. As mentioned before, perception plays an important role in strategy. Even in a defensive world, if conquest is believed to be easy, or at the very least possible, then states will act accordingly.[8] However, as Betts said, "easy" maybe be too vague an adjective and therefore it should be replaced with "when states believe that conquest of a desired objective is achievable at acceptable cost."[9] Additionally, while the perception of an offensive or defensive advantage is especially pertinent to the potential outbreak of a nuclear conflict, the causes of conflict are undeniably varied. The focus on perception in nuclear deterrence is arguably due to the realist notion of the rational actor.

While the notion of rationality is certainly up for debate, the undeniable destruction of nuclear weapons once again comes into play here and forces states and

1 Lieber, Press 2006, 34.
2 Jervis 1982, 3.
3 Richard K. Betts, "Realism Is an Attitude, not a Doctrine," The National Interest, August 2015, accessed January 29, 2021, https://nationalinterest.org/feature/realism-attitude-not-doctrine-13659.
4 Blair 2020, 18.
5 Jervis 1978, 187.
6 Ibid., 213.
7 Ibid.
8 Van Evera 2013, 117.
9 Betts 1999, 169.

leaders to consider the impact of their use no matter their motivations for aggression. Despite valid critiques of Offense–Defense Theory, when it comes to non-nuclear powers, the theory helps understand how modern great powers act.[1] These weapons force actors to be rational, as defined by R. Keohane, and to consider the consequenc es of aggression. Here, states are: unitary rational actors, carefully calculating costs of alternatives courses of action and seeking to maximize their expected utility, although doing so under the conditions of uncertainty and without necessarily having sufficient information about alternatives or resources to conduct a full review of all possible courses of action.[2]

Even if the factors that drive them to act aggressively fall outside traditional realist thinking, the threat of a second strike cannot be ignored. Planned aggression, in the form a first strike between nuclear armed states, would arguably only occur if one side doubted the resolve of the other to use their nuclear deterrent, or if they believed that they could somehow avoid being hit by a second strike. In either case, it could be said that offensive would have the advantage.

Offense is far more difficult if one's weapons are secure. Nuclear weapons are a powerful deterrent due to their assured level of destruction, but only if they can be relied upon. Therefore, any development that threatens the reliability of nuclear weapons could result in a shift to an offensive focused world and this is precisely what CPGS programs are doing. They have the potential to render the deterrent capability of states such as Russia and China ineffective, thus promoting the possibility of a first strike by the United States. The mutually assured aspects of MAD are removed, and destruction is all that remains.

Given that the perception of whether or not offensive actions have the advantage is a key factor in nuclear decision making, this allows us to put forward a definition of nuclear stability. Nuclear stability is evident when states perceive/believe that adversaries are unlikely to conduct a preemptive strike against their nuclear deterrent. This perception of safety can be created by a multitude of different factors, one being technical limitations on first-strike capabilities. If conducting a first strike is extremely difficult, then states are naturally less likely to perceive such a risk. Stability would thus increase, as the fear of being attacked is reduced. On the other hand, nuclear stability is often influenced by soft power, in the form of arms control agreements. These confidence- and security-building measures often allow for "information exchanges, means for compliance and verification, as well as different forms of military co-operation."[3] Taken together, the concepts that define stability help to provide a framework for exploring the detrimental effects of the development of conventional weapons.

The Dangers of Technological Developments in Weapon Accuracy

Traditionally, the less accurate missiles are, the more powerful they need to be to achieve their objective. A direct hit may not be possible, but this can be accommodated for with a larger payload or by launching more missiles. It is

1 Betts 1999, 168.
2 Keohane1986, 164.
3 "Arms Control," Organization for Security and Co-operation in Europe, accessed January 29, 2021, https://www.osce.org/.

important to remember that first-strike targets are often incredibly far away from launchers and may be hidden or moving. With this in mind, a nuclear silo can withstand at least 10,000 pounds per square inch or more of blast pressure on the ground, so the strike must be able to produce this amount.[1]

However, as accuracy increases, fewer launches and smaller payloads will theoretically be required to achieve a successfully first strike on an adversary. The potential reduction of the payload yield is what turns this into a discussion about developments in conventional weapons technology. A missile targeting a nuclear silo could theoretically be armed with a conventional payload if confidence in the missile's accuracy was great enough. To that end, modern developments in missile accuracy seems to indicate that this level of confidence may be a realistic possibility. One of the more "promising [approaches] to boosting accuracy is the addition of a Global Position System (GPS) receiver."[2] Ballistic missiles within the United States have traditionally relied on inertial navigation, and while this is accurate enough for nuclear weapons with their larger yield, it would not be enough for conventional weapons.[3]

Another development in accuracy is super-fuze technology. The super-fuze increases the effective accuracy of ballistic missiles by giving them a "flexible height-of-burst capability that enables [them] to detonate at any height within the lethal volume over a target."[4] Thus, weapons, warheads and missiles that would have overshot their objective can now be detonated anywhere above their target, close enough to ensure a successful strike. Before the addition of the super-fuze, only half of the U.S. Trident II 100-kt W76-1 ballistic missile warheads would have hit their target with enough force to take out a nuclear silo.[5] While technically not increasing the actual accuracy of the missile, the super-fuze technology increases the ability for weapons to strike their targets with lethal force. Despite its potential, the creation of super-fuze technology should not be viewed as a single moment in time that signifies the advent of useable CPGS weapons. It should instead be seen as part of an overarching push or movement toward the development of long-range conventional weapons that can be used in a counterforce or disarming first strike. Both the addition of GPS systems to conventional weapons and the creation of super-fuze systems effectively increase accuracy, and they indicate that CPGS are becoming increasingly viable tools.

This technological advancement degrades nuclear security because conventional missiles are more useable than nuclear missiles and because this increased viability will further exasperate the pre-existing ambiguity of missile launches. In theory, a state could achieve total victory over another nuclear state by conducting a first strike on its nuclear deterrent. If successful, this preemptive actor would avoid suffering the ramifications of MAD. However, as long as strategic nuclear weapons are used to conduct the first strike, a preemptive nuclear attack has never been a realistic option. This lack of realism is due to the devastation that would be inflicted

1 Han M. Kristensen, Matthew McKinzie, and Theodore A. Postol, "How U.S. Nuclear Force Modernization is Undermining Strategic Stability: the Burst-Height Compensating Super-Fuze," Bulletin of the Atomic Scientists, accessed January 29, 2021, http://thebulletin.org/how-us-nuclear-force-modernization-undermining-strategic-stability-burst-height-compensating-super10578.
2 Acton 2013, 60.
3 Ibid.
4 Han M. Kristensen, Matthew McKinzie, and Theodore A. Postol, "How U.S. Nuclear Force Modernization is Undermining Strategic Stability: the Burst-Height Compensating Super-Fuze."
5 Ibid.

on the global environmental. For example, even a "nuclear war between new nuclear states, say India and Pakistan, using much less than 1% of the current global arsenal, could produce so much smoke that [...] it could produce global environmental change unprecedented in recorded human history."[1] Considering that the three large powers discussed in this paper have approximately 5,800 (in the case of the United States),[2] 6,370 (Russia),[3] and 290 (China)[4] nuclear warheads, respectively, a first strike to eliminate any one of these state's nuclear arsenals, particularly those of the United States or Russia, would have to be large enough that mutually assured destruction would be almost inevitable without a second strike even being launched. It is far more likely that, alongside the potential environmental devastation of a first strike, part of the deterrent would survive and then be used on the aggressor's cities. Bismarck's observation that a preemptive strike was akin to committing suicide out of a fear of death has never held more relevance than with nuclear weapons. This fact alone, barring all others, should be enough to prevent a disarming first strike.

However, this changes as soon as states develop the ability to use nuclear weapons with conventional warheads. These weapons are "useable" in the sense that they lack the well-deserved stigma that comes with strategic nuclear weapons. For example, when considering a first strike on China, even if the targets are too hardened for current conventional capabilities, a combination strike that uses low-yield nuclear warheads alongside conventional weapons could result in a successful first strike and as few as 700 casualties in total.[5] This circumvents the taboo of nuclear genocide and makes for a much more attractive prospect, which again degrades nuclear deterrence.[6] Without both the psychological effect of nuclear weapons and the very real environmental devastation that would occur with nuclear use, a first strike on an adversary becomes an actual possibility.

This should not be taken as the belief that this technology will drastically change the face of war or guarantee the use of nuclear weapons. Some thinkers have rightly pointed out that discussions on emerging technologies often amount to a dangerous form of alarmism.[7] Historically, other technologies, such as chemical weapons, which were predicted to change the nature of warfare failed to live up to these expectations.[8] Other times, "even when technologies do have significant strategic consequences, they often take decades to emerge, as the invention of airplanes and tanks illustrates."[9] The notable exception to this was the advent of nuclear weapons. The undeniability of their sheer destructive power has dominated international security and great power interactions since their conception. CPGS weapons are not nuclear weapons, nor will they come close to reshaping the very nature of war. Where they differ from other once emerging technologies is that while they too will not come close to restricting conflict, they may directly impact how nuclear deterrence and

1 Robock 2010, 419.
2 Kristensen, Korda 2020b, 47.
3 Kristensen, Korda 2020a, 103.
4 Kristensen, Korda 2019, 172.
5 Christensen 2012, 462.
6 Woolf 2013, 7.
7 Sechser 2019, 728.
8 Ibid., 729.
9 Ibid.

nuclear strategy function. The importance of studying these weapons comes from their secondary effects. Their danger lies in the instability they create with regard to nuclear weapons.

Having a useable first-strike weapon increases international instability in a multitude of ways. A state with realistic first-strike capabilities can adopt a much more aggressive foreign policy. Such a policy could lead that state to overconfidently conduct a first strike using CPGS weapons, only to trigger a nuclear response when they almost certainly fail to completely eliminate the adversary's nuclear deterrent. Additionally, a realistic first strike further degrades nuclear stability because other nations tend to lower their own nuclear threshold for nuclear use or adopt more aggressive postures to deter a conventional first strike. Due to the offensive advantage that comes with CPGS programs, other states can be backed into a corner, which could lead them to lash out and fight even if they are at a disadvantage. This offensive domination thus makes war more likely. Instability will occur no matter who has the offensive advantage, as states will struggle to escape this utterly disadvantageous situation – and struggle can hold the seeds of war.[1]

A distinct shift in nuclear doctrine is taking place in both Russia and China that a ppears to reflect the need to respond to CPGS developments.[2] For example, China's Second Artillery Corps has been seriously considering "future scenarios in which China [would] have to consider scrapping the [No First Use] restrictions [...] and threaten nuclear retaliation for purely conventional attacks against the Chinese homeland."[3] They concluded that in a situation where conventional weapons are used in a manner that is similar to weapons of mass destruction, such as an attack on the Three Gorges Dam, then the use of nuclear weapons in response to such attacks would be a "retaliatory strike for de-escalation and possibly even war termination purposes."[4]

Russia too has stressed its concern with the development of CPGS programs.[5] This "growth in capability of the U.S. conventional strike force is another development that Russia has been watching with significant concern [as] many Russian analysts believe that improvements to the accuracy of non-nuclear strike systems and the supporting reconnaissance, communication, and command and control infrastructure could allow the United States to use its conventional forces to augment or even replace nuclear systems in missions that might involve an attack against key elements of Russia's strategic forces."[6] This concern was especially evident when Russian analyst Y. Miasnikov argued that experts in Russia believe that U.S. precision-guided weapons are a greater threat then BMD, as an effective stockpile of these precision-guided weapons continues to grow.[7] Considering that, at one time, American BMD systems were labeled as the single greatest threat to Russia,[8] the concern over CPGS developments cannot be understated.

1 Van Evera 2013, 252.
2 Cimbala 2017, 60; Christensen 2012.
3 Christensen 2012.
4 Medeiros 2006, 64.
5 Elaine M. Grossman, "Russian Experts Question Role of Conventional 'Prompt Global Strike' Weapons," Nuclear Threat Initiative, April 2009, accessed January 29, 2021, https://www.nti.org/gsn/article/russian-experts-question-role-of-conventional-prompt-global-strike-weapons/.
6 Podvig 2011, 45.
7 Miasnikov 2012.
8 Renz, Thornton 2012, 45.

With these concerns in mind, M. Schneider has stated that "military leaders [in Russia] have openly stated that Russia has deliberately lowered the nuclear use threshold and talked about the use of nuclear weapons in regional and local wars."[1] Specifically, in Russian doctrine, this seems to entail the use of nuclear weapons in response to conventional conflicts, as Russian military officials believe that "they are capable of nullifying the combat abilities of all modern conventional systems."[2] More recently, a translation of the "Fundamentals of the State Policy of the Russian Federation in the Field of Naval Operations for the Period until 2030" stated that "during the escalation of military conflict, demonstration of readiness and determination to employ non-strategic nuclear weapons capabilities is an effective deterrent."[3] While somewhat ambiguous, this does seem to indicate that Russia could use nuclear weapons in response to a conventional attack. Considering that the United States can theoretically use CGPS weapons to conduct or supplement a first strike on Russia, and that Russia has clear reservations about CPGS programs, this appears to be, at least in part, a response to this developing U.S. conventional superiority.

Of course, there are thinkers who suggest that the threat of CPGS weapons is overstated for a multitude of reasons. One such critique focuses on the ambiguity surrounding the threat of emerging technology and the fact that other historical examples demonstrate that these "technologies often have countervailing or conditional effects that can temper their negative consequences."[4] Despite having destabilizing effects, the emergence of new technologies can be stabilizing in other areas, and other factors may mediate the potential fallout for the international system.[5] While there certainly are valid points to this critique, the reverse is also true. Even if there are positives to developing CPGS weapons, the negative impact still exists. One does not cancel out the other.

On the other hand, it could simply be argued that deploying this technology will have greater benefits overall. In his paper exploring the deployment of conventional ballistic missiles, B.M. Sugden concludes that the United States ought to deploy CPGS weapons for missions "intended to defeat emerging, time-sensitive, soft targets, such as exposed WMD launchers, terrorist leaders, and sites of state transfers of WMD to terrorists or other states within roughly one hour of a decision to attack."[6] He does not deny that there are serious risks surrounding misperception,[7] or that these weapons could be used for larger-scale counter-nuclear missions.[8] He takes this one step further and argues that CPGS weapons could significantly shape the adversary's military investments and cause them to pump greater resources into supposedly defensive technology such as ballistic missile defense or hardened nuclear capabilities.[9] However, while it is evident that CPGS weapons have an influence on the defense strategies of America's adversaries, this paper has demonstrated that, rather than focusing on simply hardening their existing

1 Schneider 2008, 397.
2 Ibid., 413.
3 "Fundamentals of the State Policy of the Russian Federation in the Field of Naval Operations for the Period Until 2030," U.S. Naval War College, accessed January 29, 2021, https://digital-commons.usnwc.edu/rmsi_research/2.
4 Sechser et al. 2019, 727–735.
5 Ibid., 729.
6 Sugden 2009, 115.
7 Sugden 2009.
8 Ibid., 119.
9 Ibid., 122.

deterrent, states have adopted increasingly aggressive nuclear doctrines. In doing so, they seek to ensure that their deterrent capabilities remain credible in the face of new destabilizing technology. While there may be defendable uses of CPGS weapons in certain scenarios, this again does not negate or balance out the negative effects that this emerging technology has on deterrence.

Finally, there are significant technological difficulties that stand in the way of CPGS weapons becoming reliable tools. This primarily revolves around achieving the functional level of accuracy required for conventional weapons to be reliable at extreme ranges. As we have already stated, one such solution was to attach GPS systems to missiles. While this does appear to significantly increase their accuracy, the missiles "would be vulnerable to losing GPS signals due to vehicle maneuvers, enemy jamming, and plasma formation around the vehicle during the reentry phase."[1] This formation of plasma is particularly prevalent when hypersonic speeds come into play, and combining this speed with the required level of accuracy for CPGS weapons appears to be technically impossible at this time. In this light, discussing the strategic implications of perusing this technology may seem pointless at best, or even alarmist at worst. However, this line of thinking is incorrect and potentially dangerous. Regardless of the technological hurdles, it should not be assumed that they will always be there. Additionally, despite these difficulties, the United States is still actively pursuing a robust CPGS program designed to be delivered with hypersonic boost-glide technology.[2] This speaks to the belief that this combination of speed and accuracy is possible and will deliver tangible benefits. While we cannot be certain of this, the potential impact of this technology and the pursuit of it still merits significant review. Finally, just as with BMD, current technological limitations have not stopped other adversarial nations from reacting to the development of such technologies in the United States. This means that even if the pursuit of these technologies proves fruitless, their impact today remains relevant.

Suggestions

Developing CPGS systems comes with a multitude of risks, most important of which is the inherent degradation of deterrence. If the development of CPGS systems continues – and it appears that it will – then at the very least measures must be taken to limit its negative effects. The first step could involve ensuring that there is clear communication of intent prior to the launch of CPGS weapons. This reduces the possibility of a conventionally armed missile being mistaken for a potential nuclear strike. And this remains true, and is perhaps more relevant than ever, if the target of a CPGS weapon is Russia or China. Even a short amount of notice would likely reduce confusion and lessen the chance of uncontrolled conflict escalation.

Additionally, ensuring that CPGS weapons are land-based only and separate from known land-based nuclear weapons would reduce the ambiguity that comes with the use of CPGS weapons. Even in a dire crisis, it would be clear that a conventionally armed weapon has been launched, as it would be known that the point of origin does not house nuclear weapons. Keeping them geographically separate from nuclear weapons

1 Sugden 2009, 132.
2 Acton 2013, 2.

would reduce the likelihood of the two types of weapons being confused. Conversely, at sea, it would effectively be impossible to make the same sort of distinction between CPGS systems and SSBNs (ballistic missile submarines), as there is no way to tell whether a submarine is housing nuclear weapons when a launch is detected.[1]

Another way to lessen the instability caused by CPGS weapons is to have them be part of the New Strategic Arms Reduction Treaty (New START) or something similar in nature. While conventionally armed ballistic missiles fall under the purview of New START, hypersonic systems do not.[2] While ratifying the treaty, "the [U.S.] Senate made clear that the U.S. interpretation of the treaty precluded 'any prohibition on the deployment of such systems.' "[3] Adding hypersonic weapons to such a treaty would set a limit within which states can work to stabilize the number of CPGS weapons. At this time, the lack of restrictions on hypersonic weapons allows states to pursue strategic superiority over their adversaries. Without regulation, this presents an opportunity to deploy a dangerous number of strategic weapons, which would in turn create massive instability between the United States and its peer-adversaries. This, of course, is true for all states that are developing hypersonic weapons technology. Communication and confidence building must come from both sides.

However, while there are ways to reduce the number of negative issues (for example, missile ambiguity), the inherent degradation of deterrence caused by CPGS weapons and their hypersonic variants is somewhat unavoidable. Weapons will continue to become more and more accurate. But this is not related to nuclear deterrence, and the widespread nature of technological developments in this area means that it cannot be related. Accordingly, the problems pointed out in this and numerous other studies cannot be resolved by simply giving up the pursuit of these technologies. Even if a state were to put such programs on hold, the technology surrounding accuracy will continue to grow, and thus so too will the ability to lower the yield of warheads on missiles. In a sense, the world of deterrence is forever changing, and this new reality must be considered when discussing doctrine and arms control efforts.

With this in mind, even the above mentioned suggestion to include CPGS weapons in arms control regimes may not do enough in terms of combating the degradation of deterrence and CPGS systems. It could be argued that states could simply maintain relatively small numbers of these conventional weapons so that they can act as niche tools and do not pose a serious first-strike threat against states with larger nuclear weapons stockpiles (such as Russia). However, this argument fails to hold up to criticism. Not only would other states armed with a smaller number of nuclear weapons still see these CPGS weapons as existential threats to their nuclear deterrents, but these conventional weapons would also act as a powerful hurdle for meaningful disarmament. As we mentioned earlier, the world could suffer irreversible environmental damage if even less than 1% of the global stockpile of nuclear weapons were to be used.[4] Therefore, meaningful disarmament must, at the very least,

1 Acton 2013, 117.
2 Cameron Tracy, "Fitting Hypersonic Weapons into the Nuclear Arms Control Regime," Union of Concerned Scientists, April 2020, accessed January 29, 2021, https://allthingsnuclear.org/ctracy/fitting-hypersonic-weapons-into-the-nuclear-arms-control-regime.
3 Ibid.
4 Robock 2010, 419.

work to lower the number of nuclear weapons to a level which ensures – intentionally or otherwise – that such global devastation can never happen. However, as we have explored in this paper, CPGS systems create the possibility of a realistic first strike, and thus even a small number could act as a serious roadblock to lowering the number of nuclear weapons to the level previously suggested. Nonetheless, even if the increasing accuracy of CPGS weapons creates this reality for arms control activists, work in this direction must continue with due account of such technological developments. While this paper does not offer a concrete solution to this unavoidable problem, the combination of confidence- and security-building measures, together with clear communication and efforts to signal the lack of nuclear use could develop over time into genuine trust between adversaries. Just as old enemies became close allies in Europe, where the threat of attack is effectively non-existent, perhaps the United States and its peer-adversaries can one day achieve this same trust.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Acton, James M. *Silver Bullet? Asking the Right Questions About Conventional Prompt Global Strike.* Washington: Carnegie Endowment for International Peace, 2013. https://carnegieendowment.org/files/cpgs.pdf.

Betts, Richard K. "Must War Find a Way? A Review Essay." *International Security* 24, no. 2 (1999): 166–98.

Blair, Bruce G. "Loose Cannons: The President and U.S. Nuclear Posture." *Bulletin of the Atomic Scientists* 76, no. 1 (2020): 14–26. DOI: 10.1080/00963402.2019.1701279.

Butt, Yousaf. "A Hypersonic Nuclear War is Coming." *New Perspectives Quarterly* 33 no. 1 (2016): 51–54. https://doi.org/10.1111/npqu.12024.

Christensen, Thomas J. "The Meaning of the Nuclear Evolution: China's Strategic Modernization and U.S.–China Security Relations." *The Journal of Strategic Studies* 35, no. 4 (August 2012): 447–487.

Garcia, Zenel. "Strategic Stability in the Twenty-First Century: The Challenge of the Second Nuclear Age and the Logic of Stability Interdependence." *Comparative Strategy* 36, no. 4 (2017): 354–365. DOI: 10.1080/01495933.2017.1361207.

Green, Brendan R., and Austin Long. "The MAD Who Wasn't There: Soviet Reactions to the Late Cold War Nuclear Balance." *Security Studies* 26, no. 4 (2017): 606–641, DOI: 10.1080/09636412.2017.1331639.

Gromley, Dennis M. "U.S. Advanced Conventional Systems and Conventional Prompt Global Strike Ambitions: Assessing the Risks, Benefits, and Arms Control Implications." the Nonproliferation Review 22, no. 2 (2015): 123–139. DOI: 10.1080/10736700.2015.1117735.

Horowitz, Michael. "Do Emerging Military Technologies Matter for International Politics?" *Annual Review of Political Science* 23, no. 1 (2020): 385–400.

Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30, no. 2 (1978): 167–214.

Jervis, Robert. "Deterrence and Perception." *International Security* 7, no. 3 (1982): 3–30. DOI: 10.2307/2538549.

Keohane, Robert. "Theory of World Politics: Structural Realism and Beyond." In *Neorealism and Its Critics*, edited by Robert Keohane, 332–346. New York: Columbia University Press, 1986.

Kristensen, Hans M., and Matt Korda. "Chinese Nuclear Forces, 2019." *Bulletin of the Atomic Scientists* 75, no. 4 (2019): 171–178. DOI: 10.1080/00963402.2019.1628511.

Kristensen, Hans M., and Matt Korda. "Russian Nuclear Forces, 2020." *Bulletin of the Atomic Scientists* 76, no. 2 (2020A): 102–117. DOI: 10.1080/00963402.2020.1728985.

Kristensen, Hans M., and Matt Korda. "United States Nuclear Forces, 2020." *Bulletin of the Atomic Scientists* 76, no. 1 (2020B): 46–60. DOI: 10.1080/00963402.2019.1701286.

Lieber, Keir A., and Daryl G. Press. "The End of MAD? the Nuclear Dimension of U.S. Primacy." International Security 30, no. 4 (2006): 7–44.

Medeiros, Even S. "Evolving Nuclear Strategy." In *China's Nuclear Future,* edited by Albert S. Willner and Paul J. Bolt, 39–78. Boulder: Lynne Rienner Publishers, 2006.

Miasnikov, Yevgeny. "Precision-Guided Conventional Weapons." In *Nuclear Reset: Arms Reduction and Nonproliferation*, edited by Alexei Arbatov and Vladimir Dvorkin, 432–456. Moscow: Rosspen, 2012.

Podvig, Pavel. "Instrumental Influences." *The Nonproliferation Review* 18, no. 1 (2011): 39–50, DOI: 10.1080/10736700.2011.549170.

Renz, Bettina, and Rod Thornton. "Russian Military Modernization: Cause, Course, and Consequences." *Problems of Post-Communism* 59, no. 1 (2012): 44–54

Robock, Alan. "Nuclear Winter." *WIREs Climate Change* 1, (2010): 418–427, DOI: 10.1002/wcc.45.

Sechser, Todd S., Neil Narang, and Caitlin Talmadge. "Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War." *Journal of Strategic Studies* 42, no. 6 (2019): 727–735. DOI: 10.1080/01402390.2019.1626725.

Cimbala, Stephen J. "Putin and Russia in Retro and Forward: the Nuclear Dimension." *Defense & Security Analysis* 33, no. 1 (2017): 57–67, DOI: 10.1080/14751798.2017.1289636.

Sugden, Bruce M. "Speed Kills: Analyzing the Deployment of Conventional Ballistic Missiles." *International Security* 34, no. 1 (2009): 113–46. http://www.jstor.org/stable/40389187.

Van Evera, Stephen. *Cornell Studies in Security Affairs. Causes of War: Power and the Roots of Conflict.* Ithaca, US: Cornell University Press, 2013.

Warren, Aiden, "The Promises of Prague versus Nuclear Realities: From Bush to Obama." *Contemporary Security Policy* 32, no. 2 (2011): 432–457, DOI: 10.1080/13523260.2011.590364.

Woolf, Amy F. "Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues." Congressional Research Service, 2013. https://fas.org/sgp/crs/nuke/R41464.pdf.

Schneider, Mark. "The Nuclear Forces and Doctrine of the Russian Federation." *Comparative Strategy* 27, no. 5 (2008): 397–425. DOI: 10.1080/01495930802430098.

Author

Peter James Mckenzie Rautenbach,
MSc Candidate in International Relations at the London School of Economics and Political Sciense,
Houghton St, Holborn, London WC2A 2AE.
e-mail: peterjmrautenbach@gmail.com

Additional information

Received: November 11, 2020. Accepted: January 29, 2021.

Disclosure statement

No potential conflict of interests was declared by the author.

For citation

Raurenbach, Peter James M. "The Threat of Conventional Weapons to Nuclear Security: A New Reality for Deterrence." *Journal of International Analytics* 11, no. 4. (2020): 56–71.
https://doi.org/10.46272/2587-8476-2020-11-4-56-71

Угроза применения обычных видов вооружений для ядерной безопасности: новая реальность с точки зрения сдерживания

АННОТАЦИЯ

В данной работе рассматривается тезис о том, что развитие систем «Быстрый глобальный удар» (БГУ) размывает ядерную стабильность. Соединенные Штаты разрабатывают подобный вид обычных вооружений для их применения на театре военных действий, однако вследствие этого грань между тактическим и стратегическим оружием становится размытой. В Конгрессе США ведутся дискуссии по проблемам неопределенности в ракетно-ядерной сфере, самая крупная из которых заключается в том, что системы БГУ по своей сути размывают ядерный паритет. Рассматривая поведение крупнейших государств, ставших главной причиной для создания систем БГУ в США, и сочетая это с ранее существовавшей литературой и пониманием различных аспектов проблематики ядерного нераспространения, автор исследует воздействие БГУ на ядерную стабильность. По сравнению с ракетами-носителями ядерных боеголовок, наличие у США рассматриваемых систем обычных вооружений по своей природе опасно, поскольку оно повышает как вероятность их применения, так и вероятность нанесения первого удара по системам ядерного сдерживания другого государства. Традиционно нанесение первого ядерного удара является практически невозможным, поскольку оно влечет за собой ответный удар. Если ядерное оружие может быть заменено на системы вооружений БГУ, то вероятность первого удара кратно возрастает. Следовательно, в результате изменения ядерной доктрины с учетом систем БГУ, снижается порог применения ядерного оружия. Этот факт демонстрирует явные признаки снижения ядерной безопасности и, как следствие, увеличения вероятности применения ядерного оружия.

КЛЮЧЕВЫЕ СЛОВА

БГУ, сдерживание, ядерное оружие, первый удар, обычные вооружения, возникающие технологии

Сведения об авторе

Питер Раутенбах,

Магистр в области международных отношений в Лондонской школе экономики и политических наук, Houghton St, Holborn, London WC2A 2AE.

Дополнительная информация

Поступила в редакцию: 11 ноября 2020. Принята к публикации: 29 января 2021.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Цитирование

Раутенбах, П. Угроза применения обычных видов вооружений для ядерной безопасности: новая реальность с точки зрения сдерживания // Международная аналитика. – 2020. – Том 11 (4). – С. 56–71. https://doi.org/10.46272/2587-8476-2020-11-4-56-71

The Evolution of Regime Change and Information Warfare in the 21st Century

Greg Simons

https://doi.org/10.46272/2587-8476-2020-11-4-72-90

ABSTRACT

Although information is nothing new to war or conflict, the speed at which it reaches a much wider target audience, and thus its potential impact and consequences, is changing due to the rapid development of information and communications technology. Regime change and information warfare have been around for a very long time in the history of organised human societies. An undertaken review of academic literature demonstrates a great interest today to these concepts in academic, policymaking and practical terms. The present article attempts to track the evolution of the Western conceptual and theoretical thinking on the use of regime change and information warfare, seeking to understand the factors that precipitate it. In the paper I address the following, what is the relationship between information warfare and regime change? The high level of information and communications technology development and persisting leadership globally have allowed the United States to engage in regime change and information warfare more effective, although not without risks. The author considers the most illustrative examples of such engagement and, based on them, concludes that we have seen a shift in motivation from an offensive stance (the desire to spread influence) to a defensive one (the desire to prevent other international actors from gaining influence and power) on the global level. The theoretical method chosen for the analysis is phenomenology, as a means of the reading and analysis of a lived experience as well as a qualitative method will be used to analyse the data, where the goal is to capture the complexity of the object of study.

KEYWORDS

hybrid warfare, information warfare, political warfare, regime change, evolving global order, information operations

CC BY

Introduction

The role of information warfare and regime change has become as topical as it is controversial in the 20th and 21st centuries.[1] The current approach to regime change and information warfare has evolved from its origins in the Cold War.[2] A number of different academic assessments as to the evolution of aspects of regime change and information warfare already exist.[3] However, the focus can be rather narrow for such assessments, meaning that the bigger picture is often missed in terms of the historical and contemporary variables that shape the approach and understanding of information warfare and regime change for various stakeholders, and the evolution of the conceptualisation, practice and perception of information warfare and regime change can thus be overlooked.

This article seeks to track and analyse the contemporary nature of regime change and its relationship to information warfare in the 21st century during the relative decline of the U.S. unipolar global order. As the sole remaining superpower, the United States has far greater opportunity and motivation, as well the capability and capacity, to attempt regime change than other actors. The various examples of individual, as well as cascading regime change are seen in terms of how they function at the theoretical, conceptual, political and practical levels to establish if there is a noticeable evolution. This is done in conjunction with identifying the possible causes of a given evolution.

The article consists of several sections that aim to introduce the reader to the topics and discussions on them. The first two sections deal with a literature review to set the scene as to how to interpret the empirical cases that come later, firstly examining the elements and processes of the information realm. Then the following section examines the most recent reviews on the conceptual and theoretical basis of regime change. The third section provides a review of the methodology used in the paper. This is followed by a number of brief overviews of different attempted and successful regime changes in the 21st century.

Shaping and Influencing the Information Realm

The actor that is able to shape and define information flows in the information realm is better placed to control the content that determines the audience's perception and understanding of reality, and therefore shapes meaning in the physical realm and subsequent assessments in the cognitive realm.[4] Intangible factors within the context of this paper refer to non-physical elements found in the informational and cognitive realms of the human experience (information and communication tools, opinions, perceptions, values, world views, identity and so forth). These aspects can shape and influence the level of effectiveness of the various stakeholders and their tangible elements of power (security, military resources, infrastructure and personnel) for better or worse. This makes understanding the role of information and how it

1 Zollmann 2017; Sakwa 2016.
2 Carne, Barnett 1989.
3 Ofer et al. 2019; Manoylo et al. 2020.
4 Arquilla, Borer 2007.

is communicated crucial to our awareness of the relationship it has with power and influence.

P. Robinson contends that in order to comprehend the contemporary socio-political world around us, we first need to understand how power is exercised through communication.[1] He also suggests that the research agenda should be broadened from its focus on the mass media to include governments, researchers, NGOs, think tanks and popular culture, as these are all additional forms of manipulative and non-consensual modes of persuasive communication. The priming and mobilisation of crowds to support or oppose a planned or proposed regime change depends on the quality and quantity of information received for or against the idea. This requires a deal of coordination and signalling of key stakeholders at the right moment and in the right (resonating) tone, where the role of the manipulation of information to shape the target audience's emotions and consciousness is key.[2] Hence, in the warfare of the 21st century, technology and information play a critical and parallel role to the associated and embedded political considerations and military operations.[3] Information warfare and its influence on conflict does not remain static.

Although information is nothing new to warfare or conflict, the speed with which it reaches a much larger target audience, and thus its potential influence and effects, is changing owing to the rapid development of information and communications technology. Shallcross notes as much: "information used as an element of warfare and national power is as old as civilisation itself; however, the advent of the information age has resulted in an exponential propagation of tactics, technologies, and threats as they relate to the relatively new art and science called Information Operations."[4] Furthermore, the growth and development of new media and digital technologies means that state-based actors have lost their monopoly on globally projecting influence and power (including soft power) via means of mass communication, which is evidenced by the rise of such terrorist groups as Al Qaeda and ISIS (terrorist organization banned in Russia).[5] An understanding of the theoretical and conceptual approach to regime change and its various parts forms the basis of the following section.

Theoretical and Conceptual Underpinnings of Regime Change

In relation to the disastrous Iraq War and current conflict (2003 – present), the social construction of public policy plays a significant role. As noted by R. Burgos, "foreign policy strategies are social choices, embedded in particular discourses about what constitutes a problem and what constitutes a solution."[6] This creates the context of ideational interpretations of problems and solutions that influences the cognitive realm in terms of the perceptions and opinions of policymakers, practitioners and academics. Academic research in such sensitive subject areas as terrorism and

1 Robinson 2019.
2 Edmond 2013
3 Ofer et al. 2019; Karpovich et al. 2020; Manoylo et al. 2020; Walzer 2006.
4 Shallcross 2017, 2.
5 Manoylo 2016.
6 Burgos 2008, 255.

extremism has witnessed collaborations between the academic community and the state, which can create ethical issues and conflicts of interest.

> [...] social scientific research can be compromised: (1) interference with the evidence base (through a lack of transparency on data and conflicts of interest); (2) collaboration on research supporting deception by the state which undermines the ability of citizens to participate in democratic processes; and (3) collaboration on research legitimating human rights abuses, and other coercive state practices.[1]

There are similar risks evident in research on political and information warfare owing to the need for the façade of political legitimacy of actors seeking to subvert a target country or government, for those acts may be legally, ethically or morally flawed. Therefore, contentious politics requires this façade of legitimacy and needs to appear desirable, proper and appropriate within the context of the specific normative, value, definitional and belief framework in which it is situated. The political actor is constrained by the type of legitimacy, network balance and structural dependence.[2] The same can be drawn from contentious policymaking by political actors, such as the act of engaging in warfare.

Waging a war against another actor in the international system can include indirect and covert military operations that are intended to destabilise and target country and its government. This may involve attempting to incite an insurrection through supporting radical politics in a country as a form of political action that supports a foreign policy line of the 'sponsoring' power. This is where insurrection is a destitution of political power seeking to suspend the power of the incumbent authorities and established politics via forms of post-sovereign political activism and mobilisation.[3] Warfare involves the role and influence of relationships and structures on the direction and outcome of a conflict. For example, the dynamics of a proxy war can be visualised through the overlapping dyads between a beneficiary, a proxy and the target by conducting a structural-relational analysis of the interactions among these actors based upon strategic cooperation.[4] These interactions can be direct or indirect, but with a specific policy outcome in mind.

Warfare is a political act, which should involve political goals using coercion and/or force, such as the policy of regime change or an act of revolution. However, the social and political environment needs to be prepared in advance for an act against a target government to increase the likelihood of success by the attacker. L. Beilenson identified three 'traditional' strategic characteristics of subversion: "(1) It was mainly auxiliary to war being waged or expected to come. (2) Decisive external subversion was always geographically spotty. (3) In a particular country to be subverted, decisive external subversion was normally conducted in an opportunist manner."[5]

1 Massoumi et al. 2019, 1.
2 Schoon et al. 2020.
3 Newman 2017, 297.
4 Rauta 2018.
5 Beilenson 1972, 90.

During the latter part of the Cold War (the 1970s–1980s), conservative thinkers in the United States believed that the West was losing the geopolitical contest, mostly due to the supposed effectiveness of Marxist Revolutionary Warfare. They looked to the Soviet model to create an American version (and escalation of the violence inherent in Marxist Revolutionary Warfare) as a way to counter and roll back Soviet influence.[1] The result was the creation and support of the Contras against the governing leftist Sandinistas in the bloody Nicaraguan Revolution. The distinction between war and peace was consequently blurred.

A. Codevilla, for example (in the above context), defined political warfare as "the marshalling of human support, or opposition, in order to achieve victory in war or in unbloody conflicts as serious as war."[2] He understood the need to prepare for success by bringing together a number of environmental circumstances to subvert the target country: the presence of widespread public discontent, for example from a long-term economic recession; the lack of open communication channels between a target government and its population; an iconic event to prime and mobilise a mass public to action, such as projecting a contested election or a government's alleged disproportionate use of force; and a committed foreign power to support (materially and financially) and organise the so-called opposition.[3] These aspects and conditions are seen in the current approach of the United States to vicarious warfare.[4] Once the informational and cognitive environment is prepared, then the operational elements in the physical environment can commence.

The idea and practice of revolution is not new. A basic working understanding and definition of revolution is "the downfall of an old regime through non-legal means and its replacement by a new regime that attempts to establish a new political, and perhaps also socioeconomic, order."[5] As a fundamentally competitive activity, revolutions (seeking regime change) need to be aggressively marketed by the revolutionaries and their backers to various stakeholders to gain publicity and attention so as to create an advantage in social and political capital, together with a perceived sense of legitimacy.[6]

The concept of revolution has gradually developed with physical realm examples and informational realm interpretations in revolutionary theory. One of the strands of this theory involves the categorisation of different generations of revolution that tracks the academic and operational aspects of the act of revolution. G. Lawson understands so-called fourth generation "revolutions as conjunctional amalgams of systematic crisis, structural opening, and collective action, which arise from the intersection of international, economic, political, and symbolic factors."[7] This generational understanding of revolutions considers the increasingly complex number of different factors and circumstances that influence the outbreak of revolution.

1 Beilenson 1972; Carne, Barnett 1989.
2 Codevilla 1989, 77.
3 Ibid.
4 Waldman 2021; Zollmann 2017.
5 Katz 2001, 5.
6 Clifford 2005; Schock 2005.
7 Lawson 2016, 106.

In the wake of recent "revolutionary waves" (such as the Arab Spring) there has been a reassessment of the current fourth generation of revolutionary theory. One of these assessments is that the fourth generation is "imperilled" because it attempts to cover too many variables and move away from pure theorising, becoming stale and being partially displaced by other fields. B. Abrams argues that we need to consider the rise of a fifth generation of revolutionary theory to mitigate these shortcomings.[1] As with the notion and practice of revolution, the idea and practice of regime change has also evolved with time and experience.

One possible definition of regime change exists that has conceptual and operational aspects and consequences. "Regime change is [...] an operation to replace another state's effective political leadership by significantly altering the composition of that state's ruling elite, its administrative apparatus, or its institutional structure."[2] By their very nature, regime changes violate the *de facto* sovereignty of the intended target, but not necessarily its *de jure* sovereignty if the target is not directly occupied or annexed.[3] Regime change has been observed in acts against single targets (such as Bolivia or Venezuela) or in constructed waves of regime change (such as the Colour Revolutions or the Arab Spring).

> Regime change cascades can occur through demonstration effects and active mediation, although common external causes and contemporaneous domestic triggers can cause events outwardly resembling them. Regime change cascades tend to occur where (a) there exists a common frame of political reference, (b) unpopular leaderships are becoming lame ducks; (c) elites lack of other focal points for coordinated defection, and (d) structural conditions supporting a new regime type are in place.[4]

This attempt to define the ideal conditions for regime change cascades includes a number of different variables, but seemingly omits others. There are several embedded ideas or perhaps hopes among the academic community (and also among sections of the policymaker communities) that engage in ideological utopianism, such as regime change spreading democracy and peace.[5] There is a tendency to try and create generic blueprints of different cases of regime change and revolution to make the explanations of the physical realm seemingly clearer and more comprehensible. However, this tendency in social science defies the reality of the physical realm by its interpretations in the information realm. C. Beck observes that an "analysis of the changing structure of comparison over time reveals that comparison precedes the development of an epistemology. The results suggest that conclusions about the possibility, or lack thereof, of generalisation may be an artefact of the comparative

1 Abrams 2019, 383–385.
2 O'Rourke 2020, 95.
3 Ibid., 95–96.
4 Hale 2013, 331.
5 Bermeo 1990; Cederman, Gleditsch 2004; Lawson 1993; Way 2008.

method."[1] This does not discourage the pursuit of knowledge and an evaluation of effectiveness (or lack thereof) in the concept and practice of regime change.

This has prompted research to find and explain the correlation between regime change and regime types.[2] Whenever the United States and its allies complete a successful regime change operation, the target country is typically labelled a 'democracy.'[3] In spite of the relative enthusiasm for employing the strategy of regime change to attain foreign policy goals, some observers nevertheless point out its limitations. R. Haas argues that regime change needs to be a complimentary, rather than a stand-alone tool, especially owing to the unpredictable nature and results of its application.[4] It is for these reasons, in addition to the reputational and financial costs of the aggressor invoking regime change that, according to W. Reisman,[5] make regime change a mostly bad policy idea.[6] Regime change as an operational policy is supported by intangible environmental factors, such as the control of selective and symbolic information to create a convenient perception of events to project a sense of legitimacy.

Methodology

The theoretical method chosen for the analysis is phenomenology, as a means that seeks an "understanding of how appearances affect consciousness prior to the attempt to conceptualise objects and events."[7] In other words, phenomenology is the reading and analysis of a lived experience.[8] As such, a qualitative method will be used to analyse the data, where the goal is to capture the complexity of the object of study.[9] These combined set out the ontology and epistemology of the evolution of the definition and practice of academic concepts with operational implications.

> The theory of science deals with ontology, i.e. the issue of what is real and what exists, and epistemology, issues regarding knowledge and how we know things. [...] According to critical realism it is possible to obtain knowledge about the real domain of social mechanisms by studying the phenomena in the empirical domain.[10]

1 Beck 2018, 134.
2 Björnshov, Rode 2020; Mahoney, Snyder 1999.
3 Sussman 2010.
4 Haas 2005.
5 Reisman 2004.
6 Melissa Willard-Foster, "Three Lessons From the History of Foreign-Imposed Regime Change," Political Violence at a Glance, February 1, 2019, accessed January 22, 2021, https://politicalviolenceataglance.org/2019/02/01/three-lessons-from-the-history-of-foreign-imposed-regime-change/; Henry Butterfield Ryan, "Regime Change: New Name, Dangerous Old Policy," Origins: Current Events in Historical Perspective, October 21, 2002, accessed January 22, 2021, https://origins.osu.edu/history-news/regime-change-new-name-dangerous-old-policy; Benjamin Denison, "Stay Out of the Regime Change Business," War on the Rocks, June 16, 2020, accessed June 18, 2020, https://warontherocks.com/2020/06/stay-out-of-the-regime-change-business/; Benjamin Denison, "The More Things Change, the More They Stay the Same: the Failure of Regime-Change Operations," Policy Analysis no. 883, January 6, 2020, accessed January 22, 2021, https://www.cato.org/publications/policy-analysis/more-things-change-more-they-stay-same; Stephen M. Walt, "Regime Change for Dummies," Foreign Policy, May 14, 2018, accessed January 22, 2021, https://foreignpolicy.com/2018/05/14/regime-change-for-dummies/.
7 Szeman, Kaposy 2011, 535.
8 Simons 2020, 55.
9 Hyett et al. 2014, 2; Simons 2020, 21–23.
10 Boréus, Bergström 2017, 9.

The above-mentioned quote gives a hint at the link that exists between academic concepts and theories and the more pragmatic nature of operational practice that seeks to implement the goals and objectives of policymakers. This link between relevance and importance is expressed by S. Gelman, who notes that "concepts are fundamental to all of human experience. Naming objects, recognizing novel instances, generalizing from the known to the unknown, making inferences, and learning new information all make use of concepts."[1] She also states that concepts should not be treated and analysed in isolation from theories, stating "both are mental representations that give order to experience."[2] This needs to be understood and articulated in order to capture the essence of this academic nature and practical experience, and a literature review is employed to achieve this goal.

Literature reviews play an important role as a foundation for all types of research, where they can serve as the basis for the development of knowledge. As such, they can form the basis of future research and theory.[3] A literature review potentially enables a synthesis of the latest knowledge, which in turn allows the quality and relevance of the current research evidence to be appraised.[4] There are a variety of ways of carrying out a literature review. For example, a structured or a semi-structured literature review or a scoping study. A structured literature review that offers a summary of a number of different studies and may draw some conclusions.[5] Meanwhile, a systematic review is "a specific, carefully defined approach to the literature review," and it is argued that this method should only be applied when they can provide valid means to summarise the literature.[6] The favoured approach of this paper is the semi-structured literature review.[7] The literature review seeks to track the evolving academic definition and operational practice in academic and popular revolutionary and information warfare texts. Theory and practice invariably evolve along with, and because of changes in the society in which it exists and operates through being tested and contested in the arena of academic definition and practical operationalisation.

The research question based upon the literature review and the resulting methodology: What is the relationship between information warfare and regime change? A second follow up question: Has this operational and theoretical relationship changed or remained constant?

Contemporary Developments of the Practice of Regime Change

The end of the Cold War in 1991 saw the collapse of the bipolar world order and the emergence of a unipolar global order with the uncontested supremacy of the U.S. military, whose political and economic might no actor was able to challenge. In practical terms, this meant that the United States could do what it wanted without any checks and balances in the international system, which is precisely what it did. However, the excessive operational (mis)use of regime change and information warfare

1 Gelman 1996, 117.
2 Ibid.
3 Snyder 2019, 339.
4 Gough 2007; Snyder 2019.
5 Armitage, Keeble-Ramsay 2009.
6 Bearman et al. 2012, 638.
7 Mullins, Spence 2003; Pawar, Spence 2003.

has contributed to the relative decline of U.S. power and the gradual emergence of a multipolar global order.[1] Therefore, the following examples of contemporary information warfare and regime change are taking place in a different qualitative environment of international relations.

The Colour Revolutions represent a regime change cascade that occurred in the post-Soviet space from 2000 (in Serbia) until 2005 (in Kyrgyzstan and Uzbekistan). These regime changes had different outcomes and were viewed in different value-normative perspectives. There were debates as to the "real" causes of the Colour Revolutions, such as Lucan Way's argument that structural factors (a single category of casual factors) and not electoral and diffusion dynamics were responsible for the successful regime changes.[2] Meanwhile, V. Bunce and S. Wolchik state that structure, agency and process, such as the effort and role of transnational coalitions of activists, where ideas are diffused to destabilise the incumbent political power, are all important.[3] This idea goes against Way, as it states that electoral breakthroughs come about via practical questions or concerns rather than abstract structural influences. The importance of how stakeholders perceive reality, as opposed to how reality actually is, can be overlooked when over-theorising events and processes in the physical realm.

Therefore, Western scholars and observers tended to see the Colour Revolutions as a political phenomenon, where success depended on a united and organised political opposition and an alternative ideological and political agenda to the targeted government.[4] This is often viewed within the cover narrative of "promoting democracy" in the targeted country and government,[5] where there is often no tangible or meaningful change in the wake of a successful regime change with the exception of a more pro-Western government.[6]

The elites in the target countries also learnt from the successes and failures of regime change in the Colour Revolutions cascade how to counter the subversion tactics employed against their governments.[7] Astute Western observers understood why the Colour Revolutions ultimately failed, as, despite the narrative of promoting democracy, none of the successful regime changes produced a successful consolidated democratic government. The underlying reason for this failure is that "too often, the Colour Revolution governments acted above or with little regard to the democratic standard to which they held their predecessors."[8] In other words, there was no or limited application of the rule of law and no foreign Western government supporting the regime change held them to account.

Other, primarily non-Western interpretations of the goals and purposes of the Colour Revolutions did not see the supposed benevolence of the interfering state. Various Russian observers noted the role and importance of social media and new media (supporting the "opposition") in the political trends and processes involved

1 Simons 2020.
2 Way 2008.
3 Bunce, Wolchik 2009.
4 Lane 2009.
5 Kudlenko 2015; Virkovskiy et al. 2019.
6 Lane 2009.
7 Beacháin, Polese, 2010.
8 Melinda Haring, and Michael Cecire, "Why the Colour Revolutions Failed," Foreign Policy, March 18, 2013, accessed January 22, 2021, https://foreignpolicy.com/2013/03/18/why-the-color-revolutions-failed/.

in the Colour Revolutions, coupled with the diminishing role and influence of traditional media (supporting the government).[1] In contrast to the projected Western view of the Colour Revolutions, China and Russia tended to view and understand them within a geopolitical context. Although domestic factors (such as corruption, poverty and rising levels of inequality) were seen as contributing to the attempts at regime change, the role and actions of Western powers (and the United States in particular), as well as their covert manipulation tactics, were understood and viewed with greater concern, as they posed a potential risk to the foreign and domestic policies of the Chinese and Russian political systems.

In other words, the Colour Revolutions were viewed as an attempt on the part of the United States to preserve its geopolitical hegemony. The tactics were seen as an evolution from the hard power of mass violence and military conquest employed during the Cold War to less violent tactics that employed soft power tactics to try and disarm the target government.[2] Colour Revolutions tended to threaten the leader of the political system, but not the political elites, with the system itself remaining almost exactly the same. In this sense, the Colour Revolutions differed greatly from the next regime change cascade, the Arab Spring.

Even the brand name, Arab Spring, is a symbolic informational mechanism that is intended to manage the expectations of the target audience, where spring is association with a season of growth in temperate climates. The Arab Spring is another example of a regime change cascade that was heavily supported by information and revolutionary warfare to induce regime change across selected countries in the Middle East and North Africa (MENA). It employed soft and hard power, at times in parallel, in to achieve the desired regime change, while maintaining a façade of ethical and moral legitimacy for foreign policy actions that would not be acceptable if placed under critical scrutiny. Some of the general causes for the Arab Spring revolutions included: the protracted stay in power by some of the region's political leaders; the religious factor of an Islamic awakening; poor governance and corruption; human rights abuses; a weak constitutional framework; and foreign interference.[3]

When a targeted government succumbs quickly to regime change, the process is mostly covert and only the public information warfare façade is noticed. However, when a targeted government resists the attempts at subversion, the tactics are rapidly escalated to include a large-scale propaganda campaign through the mainstream media in the information realm to shape the cognitive realm of the audience;[4] or the increased use of covert actions supporting proxy forces, such as arming

1 Voronova, Trushin 2021.
2 Karpovich et al. 2015; Zollmann 2017.
3 Muftau 2016.
4 Robert Fisk, "The Syrian Conflict is Awash With Propaganda – Chemical Warfare Bodies Should not be Caught up in it," The Independent, February 27, 2020, accessed March 1, 2020, https://www.independent.co.uk/voices/syria-war-chemical-weapons-watchdog-opcw-assad-damascus-russia-a9262336.html; Ian Cobain, and Alice Ross, "Revealed: the British Government's Covert Propaganda Campaign in Syria," Middle East Eye, February 19, 2020, accessed February 21, 2020, https://www.middleeasteye.net/news/revealed-british-government-covert-propaganda-campaign-syria; Matthew Alford, Florian Zollman, Alan MacLeod, Jeffrey Klaehn and Daniel Broudy, "How Western Media Support State Terror – Millions Die," Peace News, August 1, 2019, accessed July 25, 2019, https://peacenews.info/node/9433/how-western-media-support-state-terror--while-millions-die; Jeremy Salt, "The End of Truth as We Know it – or Knew it," BS News, March 9, 2019, accessed February 26, 2019, https://bsnews.info/the-end-of-truth-as-we-know-it-or-knew-it/.

the jihadist forces in Syria,[1] in order to shift the balance of power in the physical realm; or direct and overt military intervention, as in the case of Libya (for 'humanitarian' reasons) or Syria (under the pretext of the branded Global War on Terror). Successful regime change during the Arab Spring in terms of international values and norms (human rights, democracy, etc.) would typically be followed by a noticeable drop-off in media coverage and political opinion.

However, the objective result and the projected and interpreted subjective result are two very different things. The case of Libya illustrates this point perfectly. Many thousands in the country have died following their 'liberation' and many tens of thousands more have been displaced. The country is evolving into a geopolitical shatter belt in the form of a protracted civil war after the regime change.[2] As with the Colour Revolutions, the Russian view was that this regime change cascade was aligned more with geopolitical games than human liberation.[3] The results of the Arab Spring have been rebranded the Arab Winter, having ultimately failed to deliver on their promises (according to the Western narrative) of liberation and democracy.

There are also various examples of non-cascade regime changes taking place around the world in the 21st century that are selectively waged in the name of such values and norms as human rights, democracy, freedom of choice and other projected 'universal values' for geopolitical gain. Some of these revolutions and regime changes exhibited similarities with the Colour Revolutions and the Arab Spring. One such example is Euromaidan (also known as the Revolution of Dignity), where new information and communications technologies and social media played a critical role in the rapid priming and mobilisation of mass crowds onto the streets against the targeted government led by President V. Yanukovych, as well as in the internal and external communication, coordination and organisation of the events.[4]

The international dimension of the ensuing competition for influence in determining Ukraine's future among foreign actors did not simply start in 2014. Rather, it was evident much earlier. These aspects of geopolitical self-interest tend to be wrapped in less obtrusive and more appealing value and norm-based narratives.[5] The U.S.-led West was able to control the flows of information in the mainstream Western media in order to give a sense of legitimacy to the regime change agenda and thus de-legitimise the regime defenders. This led to the operational success of the regime change, but has left the country in a protracted state of war ever since.

The events in Belarus starting in early 2020 also hint at an attempt at regime change using the Colour Revolution technologies as a way to oust incumbent President A. Lukashenko and make way for the 'leader of the opposition' S. Tikhanovskaya (in a similar vein to what was attempted in Venezuela). There have been attempts

1 Dilyana Gaytandzhieva, "Islamic State Weapons in Yemen Traced Back to U.S. Government: Serbia Files (part one)," Arms Watch, September 1, 2019, accessed September 14, 2019, www.armswatch.com/islamic-state-weapons-in-yemen-traced-back-to-us-government-serbia-files-part-1/; Dilyana Gaytandzhieva, "U.S. Task Force Smoking Gun Smuggles Weapons to Syria: Serbia Files (part two)," Arms Watch, September 2, 2019, accessed September 14, 2019, https://armswatch.com/us-task-force-smoking-gun-smuggles-weapons-to-syria-serbia-files-part-2/.

2 Doug Bandow, "Ten Years After Regime Change: Libyans are Dying Because of American Arrogance," CATO Institute, May 11, 2020, accessed May 12, 2020, https://www.cato.org/publications/commentary/ten-years-after-regime-change-libyans-are-dying-because-american-arrogance.

3 Karpovich et al. 2015; Korotaev et al. 2012.

4 Bohdanova 2014.

5 Schoon et al. 2020.

to use popular economic grievances, the presumed lack of direct communication between the government and the people, a contested election and foreign support for regime change (notably from Poland and Lithuania) to mobilise the public.[1] Belarus is the target country, but the object appears to be to weaken Russia's military and economic potential by removing its allies and partners. However, the power of this form of subversion is negligible when all of the pieces are not aligned, and the leadership is not instantly cognitively overwhelmed.

In 2019, a series of revolutions and unrest swept through six continents of the globe, affecting various types of political regime across the spectrum in an unprecedented display of public mobilisation.[2] However, some of these events received more attention from the media and politicians than others. Long-term targets of U.S. regime change in Latin America include the governments of Cuba and Venezuela, with numerous and varied attempts having already taken place. Venezuela has been an ongoing regime change project, where the U.S. administrations (across all lines) have always served as a powerful broker that supports anti-government forces (often wealthy and right-wing) to subvert the N. Maduro government. But the tactics used by this group have tended to split the 'opposition' and unite the Chavistas.[3] Several attempts at regime change took place in 2019–2020, such as the U.S.-backed and supported operations in Bolivia and Venezuela.

Once more, the United States used the pretext of an undemocratic election as a means to create a basis for the political subversion of the Venezuelan government by asserting that the 'leader of the opposition' J. Guaidó had 'won' the vote, even though he had boycotted the election. However, as with President of Syria B. al-Assad, the United States decided to meddle in the domestic politics and sovereignty of another country by claiming that the only thing to 'negotiate' was the departure of the sitting (anti-U.S.) president.[4]

Under the D. Trump presidency, and particularly when M. Pompeo was Secretary of State, the regime change agenda was given further priority. The usual political rhetoric was employed, where the narrative of a "free and democratic Venezuela" was projected.[5] A window into the actual reasons and logic for regime change in Venezuela was given when the D. Trump administration publicly stated that it was willing to use overt military force[6] (as in the Cold War with the Noriega Panama-scenario) or other forms of violent subversion.[7] This created concern that the United

1 Simons 2020.
2 Robin Wright, "The Story of 2019: Protests in Every Corner of the Globe," The New Yorker, December 30, 2019, accessed January 3, 2020, https://www.newyorker.com/news/our-columnists/the-story-of-2019-protests-in-every-corner-of-the-globe.
3 Mark Weisbrot, "The Truth About Venezuela: a Revolt of the Well-Off, Not a 'Terror Campaign,'" The Guardian, March 20, 2014, accessed February 8, 2019, https://www.theguardian.com/commentisfree/2014/mar/20/venezuela-revolt-truth-not-terror-campaign.
4 G. Long, "Venezuela Government and Opposition Resume Oslo Talks," Financial Times, May 26, 2019, accessed May 27, 2019, https://www.ft.com/content/f41af220-7fc3-11e9-b592-5fe435b57a3b; G. Long, "Guaido Tries to Build Momentum for Bid to Oust Maduro," Financial Times, May 1, 2019, accessed May 13, 2019, https://www.ft.com/content/3d30a5f4-6c28-11e9-80c7-60ee53e6681d; C. Yilek, "Pompeo Advocates for 'Free and Democratic' Venezuela After U.S. Diplomats Leave," Washington Examiner, March 14, 2019, accessed March 23, 2019, https://www.washingtonexaminer.com/news/pompeo-advocates-for-free-and-democratic-venezuela-after-u-s-diplomats-leave.
5 C. Yilek, "Pompeo Advocates for 'Free and Democratic' Venezuela After U.S. Diplomats Leave."
6 J. Gehrke, "Pompeo: 'Military Force is Available' to Oust Maduro 'If that's What it Takes,'" Washington Examiner, April 30, 2019, accessed May 1, 2019, https://www.washingtonexaminer.com/policy/defense-national-security/pompeo-military-force-is-available-to-oust-maduro-if-thats-what-it-takes.
7 Andrea Lobo, "Leaked Audio of Top Columbian Officials Exposes Failure of U.S. Coup Operation in Venezuela," World Socialist Website, November 23, 2019, accessed November 26, 2019, https://www.wsws.org/en/articles/2019/11/23/colo-n23.html.

States was going to resort once again to military force to effect regime change, this time in Venezuela.[1]

D. Trump ultimately complained about being misled with promises of an easy regime change in the country, which that never happened. The biggest culprit was National Security Adviser J. Bolton, whose advice, the President claimed, could have got the United States embroiled in another war.[2] Deceptive and misleading information has been propagated that is intended to compromise the target government in the eyes of international public opinion, such as the story that claimed N. Maduro was responsible for burning a humanitarian aid convoy attempting to enter the country from Colombia.[3] Proxy forces were also used to (unsuccessfully) kidnap President N. Maduro in a very public debacle that saw former U.S. soldiers and citizens captured after entering Venezuela illegally to carry out the operation.[4]

The mainstream media was condemned for not criticizing the increasingly aggressive stance of the D. Trump administration towards regime change in Venezuela and not holding the abuse of power to account. If anything, the media proved to be complicit in and supportive of war and creating a fog of information around the events.[5] The attempt at regime change was ultimately unsuccessful, although efforts to topple the government there continue. The attempted regime change in Bolivia, on the other hand, was initially successful. However, it highlighted the inherent problems in the attempts at regime changes undertaken by the United States in the 21st century.

In the end, the U.S.-backed coup in Bolivia failed, although the elected leftist leader E. Morales (an irritant to U.S. foreign policy and interests) was violently deposed by a group of right-wing coup leaders backed by the military. The coup and regime change were supported publicly by the United States and its allies. However, they failed to consolidate their power and lost in the democratic election when the people of Bolivia voted overwhelmingly to reject the coup government installed by the United States and re-elected the Movement for Socialism (MAS) party.[6] The United States employed more Cold War-style hard power regime change tactics and through the use of a brutal military crackdown, as demonstrated in Chile. But in the end, the weaknesses and lack of appeal of the U.S. project was exposed and the attempt ultimately failed.

1 Barbara Boland, "Is Trump Using the U.S. Military for Regime Change in Venezuela?" The American Conservative, April 27, 2020, accessed April 30, 2020, https://www.theamericanconservative.com/articles/does-trump-want-regime-change-in-venezuela/; Emma Ashford, and Matthew Kroenig, "Is the U.S. Government Back in the Business of Regime Change?" Foreign Policy, May 15, 2020, accessed May 19, 2020, https://foreignpolicy.com/2020/05/15/is-us-government-back-in-the-business-venezuela-of- regime-change-putin-russia-coronavirus/.

2 A. Gearan, J. Dawsey, J. Hudson, and M. K. Seung, "A Frustrated Trump Questions His Administration's Venezuela Strategy," The Washington Post, May 8, 2019 (accessed May 13, 2019), https://www.washingtonpost.com/politics/a-frustrated-trump-questions-his-administyrations-venezuela-strategy/2019/05/08/ad51561a-71a7-11e9-9f06-5fc2ee80027a_story.html.

3 Nicholas Casey, Christoph Koetti, and Deborah Acosta, "Footage Contradicts US Claim That Nicolas Maduro Burned Aid Convoy," the New York Times, March 10, 2019, accessed March 23, 2019, https://www.nytimes.com/2019/03/10/world/americas/venezuela-aid-fire-video.html.

4 G. Long, and K. Manson, "Venezuela Says Two U.S. Citizens Detained in Failed Plot," Financial Times, May 6, 2020, accessed May 7, 2020, https://www.ft.com/content/bb3e07c6-e928-474d-967f-aed987465915; A. Faiola, K. DeYoung, and A.V. Herrero, "From a Miami Condo to the Venezuelan Coats, How a Plan to 'Capture' Maduro Went Rogue," The Washington Post, May 7, 2020, accessed May 7, 2020, https://www.washingtonpost.com/world/the_americas/from-a-miami-condo-to-the-venezuelan-coast-how-a-plan-to-capture-maduro-went-rogue/.

5 Alan MacLeod, "The 'Venezuelan People' are Whoever Agrees With Donald Trump," FAIR, January 31, 2019, accessed February 8, 2019, https://fair.org/home/the-venezuelan-people-are-whoever-agrees-with-donald-trump/; Gregory Shupak, "U.S. Media Erase Years of Chavismo's Gains," FAIR, February 20, 2019, accessed February 26, 2019, https://fair.org/home/us-media-erase-years-of-chavismos-gains/; Teddy Ostrow, "Zero Percent of Elite Commentators Oppose Regime Change in Venezuela," FAIR, April 30, 2019, accessed May 1, 2019, https://fair.org/home/zero-percent-of-elite-commentators-oppose-regime-change-in-venezuela/.

6 M. Benjamin, and N. J. S. Davies, "Ending Regime Change – in Bolivia and the World," Foreign Policy in Focus, October 28, 2020, accessed December 18, 2020, https://fpif.org/ending-regime-change-in-bloivia-and-th-world/.

China equates the threat of subversion of its political and social system during the Cold War period with the West's current strategy of "peaceful evolution," which is designed and intended to bring about a non-military approach to regime change. The intention is to export the notions of human rights and liberal democracy through the development of trade and economic ties.[1] However, China has observed that the U.S.-led West tends to employ hard power tactics to bring about regime change alongside or instead of the soft power approach, such as witnessed in Libya, Syria and Iraq. in 2019, China experienced a Colour Revolution-type event in Hong Kong that was allegedly triggered by the extradition law and selectively covered in a binary manner of 'good' and 'bad' by the Western mainstream media.

Furthermore, the Western mainstream media gave far more coverage to the events in Hong Kong (with China portrayed as a competitor) than to protests occurring in states considered to be clients of the Unites States (Chile, Ecuador and Haiti). This illustrates the importance not only of what is covered in the news, but also of what is omitted.[2] It has been noted that supposedly independent Western media outlets often collude with hegemonic powers for mutually beneficial (political and economic) gains.[3]

This has been presented as a contest between 'pro-democracy' ('good') and 'pro-China' ('bad') forces, of freedom against repression.[4] The 'pro-democracy' protesters in Hong Kong wore black clothes to symbolise mourning and sorrow (while counter-protesters wore white clothes to distinguish themselves). This follows a long-standing tradition of sorts to use symbolic colours, as seen in the 2014 Umbrella Revolution in Hong Kong, the Colour Revolutions and the Arab Spring.[5] Although the United States denied official involvement (plausible deniability to avoid possible military responses), the unrest in Hong Kong suited U.S. interests and was spurned on by them. Although there is evidence available in digital sources that would suggest the opposite, beyond the creation and maintenance of obvious props as key influencers such as J. Wong as the 'public face' of the subversion.[6]

Conclusions

Two research questions have been posed in this article: 1) What is the relationship between information warfare and regime change? 2) Has this operational and theoretical relationship changed or remained constant? In short, the answer is that there is a close observable relationship between information warfare and regime change, as the physical, informational and cognitive realms are all connected and influence the perceptions and reactions of stakeholders. An evolution in the conceptualisation, political use and practical application of information warfare

1 Ong 2007.
2 Alan MacLeod, "With People in the Streets Worldwide, Media Focus Uniquely on Hong Kong," FAIR, December 6, 2019, accessed December 16, 2019, https://fair.org/home/with-people-in-the-streets-worldwide-media-focus-uniquely-on-hong-kong/.
3 Shen Yi, "How Western Media Promotes Colour Revolution: a Case Study of Hong Kong," Global Times, September 9, 2019, accessed September 11, 2019, https://www.globaltimes.cn/content/1164100.shtml.
4 E. Bufkin, "Hong Kong Police Threaten Use of Live Ammunition on Pro-Democracy Protesters," Washington Examiner, November 17, 2019, accessed November 21, 2019, https://www.washingtonexaminer.com/news/hong-kong-police-threaten-use-of-live-ammunition-on-pro-democracy-protesters.
5 Heike Mund, "Orange, Green or Black: the Colours of Revolutions," DW, August 16, 2019, accessed January 22, 2021, https://www.dw.com/en/orange-green-or-black-the-colors-of-revolutions/a-50050659.
6 Tony Cartalucci, "U.S. is Behind Hong Kong Protests Says U.S. Policymaker," Land Destroyer Report, September 10, 2019, accessed October 23, 2019, https://landdestroyer.blogspot.com/2019/09/us-is-behind-hong-kong-protests-says-us.html.

and regime change can also be observed, and there are various reasons for his. But there are also some observable constants too.

Western information warfare has played a critical role in regime change in the 21st century. This concerns the ability of the information realm to impose the interpretation and projection of the physical realm and its 'realities' onto the cognitive realm of its target audience. There are two sides to information warfare and its intended effect: 1) to legitimise military/paramilitary attempts to subvert a target government and thereby increase their offensive operational freedom of choice; and 2) to de-legitimise the target government and therefore limit its operational freedom of choice when it comes to self-defence. This creates an Orwellian double speak, where deception is the truth, regime change is freedom, and the U.S.-supported opposition is democracy.

During the Cold War, the narrative was that the United States and its allies were working to prevent the spread of communism in the 'free' world. This notion has evolved in the post-Cold War period of 'universal' values and norms to the narrative that the West is spreading 'democracy' and 'freedom' to the unfree world. This concerns the ability to prime and mobilise (and, in the case of an opponent demobilise) audiences to fulfil the foreign policy agenda and secure the associated national interests. This is done under increasing strain in the 21st century due to the decline in the global power and influence of Western civilisation, and U.S. hegemony in particular, through attempts to stymie the rise of Chinese and Russian influence and thus retain a relative military and political advantage regionally and globally. So, this has moved from the goal of an offensive push towards absolute global hegemony (the 'end of history') to a defensive attempt to slow thwart the rise of competitors and keep hold of its hegemonic position.

As noted by H. Hale, this "leads to a sobering conclusion that the notion of democratising regime change cascade may be a reflection of our hopes more than of hard reality."[1] The difference in here, of course, lies in the space between the emotional hopes of the general public and the more cynical and pragmatic desires of the private plans and intentions of the political elite. Historically, regime change operations have given actors a strong incentive to use covert acts to reduce the potential material, economic and reputational costs of a direct intervention.[2] In this respect, little has changed since the Cold War in the contemporary environment of subversion and regime change in the 21st century.

The contemporary approach to regime change and information warfare adopted by the West is to unleash an all-out attack on the cognitive realm of the target through the informational realm, thus preventing policymakers and practitioners from adequately responding to the impending physical threat. This is coupled with priming and energising those actors and elements that are working for regime change. Information and communications technologies are used to help bring about regime change through methods of information warfare. The speed of information warfare is potentially so great, and its reach so massive that it can cognitively overwhelm a defender. However, the longer a defender manages to survive, the less likely

1 Hale 2013, 349.
2 O'Rourke 2020, 94.

the attempted regime change is to work, as the financial, political and reputational costs increase and the chances of sustaining the façade of legitimacy shrink.

Consequently, regime change and information warfare (employing elements of soft power) may take a step backwards in their evolution to earlier iterations that include the militarised variants of the Cold War (the reliance on hard power), which we have seen in the case of Libya, where NATO helped to eventually bring about a 'successful' regime change, as well as in the ongoing Syrian conflict. Previous examples of regime change and information warfare provide lessons for both attackers and defenders. For example, a government that is communicationally isolated from the population is vulnerable to losing the cognitive contest, as it does not or cannot compete in the informational realm with its attackers for the perceptions and opinions of stakeholders. The motivations and reasoning behind regime change and information warfare essentially remain unchanged, which are to serve national interest and pursue foreign policy objectives.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Abrams, Benjamin. "A Fifth Generation of Revolutionary Theory Is Yet to Come." *Journal of Historical Sociology* 32, no. 3 (September 11, 2019): 378–86. https://doi.org/10.1111/johs.12248.

Armitage, Andrew, and Diane Keeble-Ramsay. "The Rapid Structured Literature Review as a Research Strategy." *US–China Education Review* 6, no. 4 (2009): 27–38.

Arquilla, John, and Douglas A. Borer, eds. I*nformation Strategy and Warfare: a Guide to Theory and Practice*. New York: Routledge, 2007.

Beacháin, Donnacha Ó., and Abel Polese. "What Happened to the Colour Revolutions? Authoritarian Responses From Former Soviet Spaces." *Journal of International and Area Studies* 17, no. 2 (December 2010): 31–51.

Bearman, Margaret, Calvin D. Smith, Angela Carbone, Susan Slade, Chi Baik, Marnie Hughes-Warrington, and David L. Neumann. "Systematic Review Methodology in Higher Education." *Higher Education Research & Development* 31, no. 5 (October 2012): 625–640. https://doi.org/10.1080/07294360.2012.702735.

Beck, Colin J. "The Structure of Comparison in the Study of Revolution." *Sociological Theory* 36, no. 2 (June 21, 2018): 134–61. https://doi.org/10.1177/0735275118777004.

Beilenson, Lawrence. W. *Power Through Subversion*. Washington DC: Public Affairs Press, 1972.

Bermeo, Nancy. "Rethinking Regime Change." *Comparative Politics* 22, no. 3 (1990): 359-77. doi:10.2307/421966.

Bjørnskov, Christian, and Martin Rode. "Regime Types and Regime Change: A New Dataset on Democracy, Coups, and Political Institutions." *The Review of International Organizations* 15, no. 2 (April 4, 2020): 531–51. https://doi.org/10.1007/s11558-019-09345-1.

Bob, Clifford. *The Marketing of Rebellion: Insurgents, Media, and International Activism.* New York: Cambridge University Press, 2005.

Bohdanova, Tetyana. "Unexpected Revolution: The Role of Social Media in Ukraine's Euromaidan Uprising." *European View* 13, no. 1 (June 16, 2014): 133–42. https://doi.org/10.1007/s12290-014-0296-4.

Boréus, Kristina, and Göran Bergström. Analysing *Text and Discourse: Eight Approaches for the Social Sciences.* Thousand Oaks (CA): Sage Publishing, 2017.

Bunce, Valerie, and Sharon Wolchik. "Debating Colour Revolutions: Getting Real About 'Real Causes.'" *Journal of Democracy* 20, no. 1 (January 2009): 69–73.

Burgos, Russell A. "Origins of Regime Change: 'Ideapolitik' on the Long Road to Baghdad, 1993–2000." *Security Studies* 17, no. 2 (May 22, 2008): 221–256. https://doi.org/10.1080/09636410802098693.

Cederman, Lars-Erik, and Kristian Skrede Gleditsch. "Conquest and Regime Change: An Evolutionary Model of the Spread of Democracy and Peace." *International Studies Quarterly* 48, no. 3 (September 1, 2004): 603–29. https://doi.org/10.1111/j.0020-8833.2004.00317.x.

Codevilla, Anthony M. "Political Warfare." In *Political Warfare and Psychological Operations: Rethinking the US Approach,* edited by Carne Lord, and Frank R. Barnett, 77–100. Washington DC: National Defence University Press, 1989.

Edmond, Chris. "Information Manipulation, Coordination, and Regime Change." *The Review of Economic Studies* 80, no. 4 (October 2013): 1422–1458. https://doi.org/10.1093/restud/rdt020.

Gelman, Susan A. "Concepts and Theories." In *Perceptual and Cognitive Development (Handbook of Perception And Cognition)*, 2nd Edition, edited by Rochel Gelman and Terry Kit-Fong Au, 117–150. San Diego: Academic Press Inc, 1996.

Gough, David. "Weight of Evidence: A Framework for the Appraisal of the Quality and Relevance of Evidence." *Research Papers in Education* 22, no. 2 (June 2007): 213–228. https://doi.org/10.1080/02671520701296189.

Haas, Richard N. "Regime Change and its Limits." *Foreign Affairs* 84, no. 4 (July/August 2005): 66–78. https://www.foreignaffairs.com/articles/north-korea/2005-07-01/regime-change-and-its-limits.

Hale, Henry E. "Regime Change Cascades: What We Have Learned from the 1848 Revolutions to the 2011 Arab Uprisings." *Annual Review of Political Science* 16, no. 1 (May 11, 2013): 331–53. https://doi.org/10.1146/annurev-polisci-032211-212204.

Hyett, Nerida, Amanda Kenny, and Virginia Dickson-Swift. "Methodology or Method? A Critical Review of Qualitative Case Study Reports." *International Journal of Qualitative Studies on Health and Well-Being* 9, no. 1 (January 7, 2014). https://doi.org/10.3402/qhw.v9.23606.

Karpovich, Oleg, and Andrey Manoylo. *Colour Revolutions: Techniques in Breaking Down Modern Political Regimes*. Bloomington (IN): Author House, 2015.

Karpovich, Oleg, and Andrey Manoylo. *Politics of Multipolarity: New Challenges and Threats*. Moscow: Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, 2020.

Katz, Mark N., ed. *Revolution: International Dimensions.* Washington DC: CQ Press, 2001.

Korotaev, Andrey V., Yulia V. Zinkina, and Aleksandr S. Khodunov, eds. *System Monitoring of Global and Regional Risks: Arab Spring* 2011. Moscow: URSS, 2012.

Kudlenko, Anastasiia. "From Colour Revolutions to the Arab Spring: The Role of Civil Society in Democracy Building and Transition Processes." *Journal of Contemporary Central and Eastern Europe* 23, no. 2–3 (September 2, 2015): 167–79. https://doi.org/10.1080/0965156X.2015.1116790.

Lane, David. "'Coloured Revolution' as a Political Phenomenon." *Journal of Communist Studies and Transition Politics* 25, no. 2–3 (September 2009): 113–135. https://doi.org/10.1080/13523270902860295.

Lawson, George. "Within and Beyond the 'Fourth Generation' of Revolutionary Theory." *Sociological Theory* 34, no. 2 (June 16, 2016): 106–27. https://doi.org/10.1177/0735275116649221.

Lawson, Stephanie. "Conceptual Issues in the Comparative Study of Regime Change and Democratization." *Comparative Politics* 25, no. 2 (1993): 183-205. doi:10.2307/422351.

Lord, Carne, and Frank R. Barnett. *Political Warfare and Psychological Operations: Rethinking the US Approach.* Washington DC: National Defence University Press, 1989.

Mahoney, James, and Richard Snyder. "Rethinking Agency and Structure in the Study of Regime Change." *Studies in Comparative International Development* 34, no. 2 (June 1999): 3–32. https://doi.org/10.1007/BF02687620.

Manoylo, Andrey V. "Models of 'Soft Power' of the Network Terrorist Organisations (On Examples of the 'Islamic State', Al-Qaida, the Taliban and 'Muslim Brotherhood')." *Geopolitical Journal,* no. 2 (2016): 37–46.

Manoylo, Andrey V., and Konstantin S. Strigunov. *Technologies Non-Classical Wars: Genesis, Evolution, Practice.* Moscow: Goryachaya Liniya – Telekom, 2020.

Massoumi, Narzanin, Tom Mills, and David Miller. "Secrecy, Coercion and Deception in Research on 'Terrorism' and 'Extremism.'" *Contemporary Social Science* 15, no. 2 (April 2, 2020): 134–52. https://doi.org/10.1080/21582041.2019.1616107.

Muftau, Rufai. "Regime Changes and Uprisings in the Middle East and Parts of North Africa: Some Lessons to be Learnt." *Journal of Education and Practice* 7, no. 2 (2016): 107–117.

Mullins, Simon, and Sean A. Spence. "Re-Examining Thought Insertion." *British Journal of Psychiatry* 182, no. 4 (April 2, 2003): 293–298. https://doi.org/10.1192/bjp.182.4.293.

Newman, Saul. "What is an Insurrection? Destituent Power and Ontological Anarchy in Agamben and Stirner." *Political Studies* 65, no. 2 (2017): 284–299. https://doi.org/10.1177/0032321716654498.

O'Rourke, Lindsey A. "The Strategic Logic of Covert Regime Change: U.S.-Backed Regime Change Campaigns during the Cold War." *Security Studies* 29, no. 1 (January 1, 2020): 92–127. https://doi.org/10.1080/09636412.2020.1693620.

Ong, Russell. "'Peaceful Evolution,' 'Regime Chane' and China's Political Security." *Journal of Contemporary China* 16, no. 53 (November 2007): 717–27. https://doi.org/10.1080/10670560701562408.

Pawar, Ajaykumar V., and Sean A. Spence. "Defining Thought Broadcast." *British Journal of Psychiatry* 183, no. 4 (October 2, 2003): 287–291. https://doi.org/10.1192/bjp.183.4.287.

Rauta, Vladimir. "A Structural-Relational Analysis of Party Dynamics in Proxy Wars." *International Relations* 32, no. 4 (December 12, 2018): 449–67. https://doi.org/10.1177/0047117818802436.

Reisman, W. Michael. "The Manley O. Hudson Lecture: Why Regime Change Is (Almost Always) A Bad Idea." *American Journal of International Law* 98, no. 3 (July 27, 2004): 516–25. https://doi.org/10.2307/3181642.

Robinson, Piers. "Expanding the Field of Political Communication: Making the Case for a Fresh Perspective Through 'Propaganda Studies.'" *Frontiers in Communication* 4, no. 26 (July 2, 2019). https://doi.org/10.3389/fcomm.2019.00026.

Sakwa, Richard. *Frontline Ukraine: Crisis in the Borderlands.* London: I.B. Tauris, 2016.

Schock, Kurt. *Unarmed Insurrections: People Power Movements in Non-Democracies.* Minnesota: University of Minnesota Press, 2005.

Schoon, Eric W., Alexandra Pocek Joosse, and H. Brinton Milward. "Networks, Power, and the Effects of Legitimacy in Contentious Politics." *Sociological Perspectives* 63, no.4 (2020): 670–690. https://doi.org/10.1177/0731121419896808.

Shallcross, Nicholas J. "Social Media and Information Operations in the 21st Century." *Journal of Information Warfare* 16, no. 1 (Winter 2017): 1–12.

Silverman, David. *Interpreting Qualitative Data*. London: Sage, 2020.

Simons, G. "The Corona Virus Pandemic and Global Transformations: Making or Breaking International Orders?" *Outlines of Global Transformations: Politics, Economics, Law* 13, no. 5 (November 27, 2020): 20–37. https://doi.org/10.23932/2542-0240-2020-13-5-2.

Snyder, Hannah. "Literature Review as a Research Methodology: an Overview and Guidelines." *Journal of Business Research,* no. 104 (2019): 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039.

Sussman, Gerald. Branding Democracy: *US Regime Change in Post-Soviet Eastern Europe.* New York: Peter Lang, 2010.

Szeman, Imre, and Timothy Kaposy, eds. *Cultural Theory: an Anthology.* Hoboken (NJ): Wiley-Blackwell, 2011.

Fridman, Ofer, Vitaly Kabernik, and James C. Pearce, eds. *Hybrid Conflicts and Information Warfare: New Labels, Old Politics.* Boulder (CO): Lynne Rienner Publishers, 2019.

Virkovskiy, Andrey V., Angelina S. Gorbunova, and Maya I. Davletshina. *Influence of New Media on the Political Processes in Post-Soviet Countries (With the Example of the Colour Revolutions)*. Moscow: Faculty of Journalism at Moscow State University, 2019.

Voronova, Olga E. and Aleksandr S. Trushin, Contemporary Information Warfare: Strategies, Types, Methods, Tricks. Moscow: Aspect Press, 2021.

Waldman, Thomas. *Vicarious Warfare: American Strategy and the Illusion of War on the Cheap.* Oxford: Oxford University Press, 2021.

Walzer, Michael. "Regime Change and Just War." *Dissent* 53, no. 3 (2006): 103–108. https://doi.org/10.1353/dss.2006.0086.

Way, Lucan. "The Real Causes of the Colour Revolutions." *Journal of Democracy* 19, no. 3 (July 2008): 55–69. https://doi.org/10.1353/jod.0.0010.

Zollmann, Florian. *Media, Propaganda and the Politics of Intervention.* New York: Peter Lang, 2017.

Author

Greg Simons,

Associate Professor and Researcher at the Institute for Russian and Eurasian Studies (IRES), Uppsala University, Sweden, P.O. Box 256, SE-751 05 Uppsala.

Leading researcher at the Humanitarian Institute at Ural Federal University in Yekaterinburg, Russia, 620002, Ural Federal District, Sverdlovsk region, Yekaterinburg, Mira str., 19.

ORCID: 0000-0002-6111-5325

e-mail: gregmons@yahoo.com

Additional information

Received: December 18, 2020. Accepted: March 1, 2021.

Disclosure statement

No potential conflict of interest was reported by the author.

To cite the article

Simons, Greg. "The Evolution of Regime Change and Information Warfare in the 21st Century." *Journal of International Analytics* 11, no. 4 (2020): 72–90.

https://doi.org/10.46272/2587-8476-2020-11-4-72-90

Эволюция концепции смены режима и информационные войны XXI века

АННОТАЦИЯ

Хотя информация не является новым явлением, сопровождающим вооруженные конфликты, скорость ее распространения и влияния на широкую аудиторию и, следовательно, ее потенциальная опасность растет в связи с быстрым развитием информационно-коммуникационных технологий. Примеры смены режима и информационных войн существуют в истории организованных человеческих обществ с давних времен. Проведенный обзор научной литературы демонстрирует сегодня большой интерес к этим концепциям в академическом, политическом и практическом планах. В настоящей статье предпринята попытка проследить эволюцию концептуального осмысления смены режима и проблематики информационной войны, а также ставится задача выявить факторы, влияющие на связь информационной политики и смены режимов. Высокий уровень развития информационно-коммуникационных технологий и сохраняющееся глобальное лидерство позволили Соединенным Штатам участвовать в смене неугодных правительств и информационных войнах более эффективно, хотя и не без рисков. Автор рассматривает наиболее показательные примеры такого воздействия и на их основе приходит к выводу о том, что мы наблюдаем сдвиг мотивации от наступательной позиции (стремление распространить влияние) к оборонительной (стремление помешать другим международным акторам добиться сходного влияния в мировой политике) на глобальном уровне.

КЛЮЧЕВЫЕ СЛОВА

гибридная война, информационная война, политическая война, смена режима, эволюционирующий мировой порядок, информационные операции

Сведения об авторе

Грег Саймонс,
доцент и научный сотрудник Института российских и евразийских исследований Уппсальского университета, Швеция, P. O. Box 256, SE-751 05 Уппсала;
ведущий научный сотрудник Гуманитарного института Уральского федерального университета в Екатеринбурге,
Россия, 620002, Уральский федеральный округ, Свердловская область, Екатеринбург, ул. Мира, 19.
ORCID: 0000-0002-6111-5325
e-mail: gregmons@yahoo.com

Дополнительная информация

Поступила в редакцию: 18 декабря 2020. Принята к публикации: 1 марта 2021.

Конфликт интересов

Автор заявляет об отсутствии потенциального конфликта интересов.

Цитирование

Саймонс, Г. Эволюция концепции смены режима и информационные войны XXI века // Международная аналитика. – 2020. – Том 11 (4). – С. 72–90.
https://doi.org/10.46272/2587-8476-2020-11-4-72-90

Hashtagging as an Identifier of Political Transformations in the Digital Age

Aleksandr V. Alekseev

https://doi.org/10.46272/2587-8476-2020-11-4-91-103

ABSTRACT

The article is devoted to the study of the protest movement on social networks. The novelty of the study is in its comparative analysis of protests in different regions of the world. Its relevance is determined by the need to identify the main trends of the protest movement that began a few years ago and continues to play a huge role in the life of society today – particularly during this period of integration and digitalization – which is confirmed by the statistics given in this article. Special attention is paid to autopoietic organizations: loyal to the regime, limitrophe and radical communities. We emphasize that activism in social networks is characterized by cyclicality and orientation towards international recognition. The work presents universal patterns of the formation of lexical units, expressed in the form of hashtags. It provides information on specific political techniques for using social media platforms in the United States, highlighting the most effective ways of constructing social media posts and using slogans and text that attract the attention of the audience. The paper also reveals the vital role of social networks in the political agenda of African countries such as Uganda, Kenya, etc. The paper highlights the protest movements that took place in Muslim countries during the Arab Spring and provides a brief description of the Hong Kong Umbrella Revolution. And it is the totality of lexical units, expressed in the form of hashtags, that fully reveal the nature of protest movements, providing an opportunity to analyse a specific protest not by one word, but by a set of lexemes to view a subject in various ways.

KEYWORDS

protest movements, digitalization, social networks, hashtag activism

CC BY

The modern world is striving to integrate many spheres of today's society: politics and economics, culture and technological progress, sports and art. Interaction seeks to erase boundaries, ensuring the wellbeing of society as a whole, regardless of the region. However, such integration processes often have negative consequences, leading to the interests of some states being catered to, while those of others are ignored.

It is apparent that this trend continues to develop today. In the 21st century, humanity has entered a new era of the information space, where digitalization is becoming the main source of knowledge. The internet, which unites countries and continents, plays a significant role in this process. A separate place in this context should be given to politics.

Indeed, the form of communication both among politicians and in their interactions with society has transformed completely over the past decade. With the advent of social media platforms, the process of providing information has moved to a qualitatively new level. Moreover, the emergence of Twitter has meant that politicians now react to world news in almost real time. In addition, the dissemination of information has acquired a more convenient form through the transmission of messages to the target audience. A phenomenon has thus appeared that in the past only indirectly concerned the media – reader backlash and interactive communication between politicians and their audiences, an understanding of their reaction to specific actions. In this regard, the question of the politician's competent use of his or her image on social networks is an important one.

The second factor that affected the second-generation internet was the protest movement. The process began in 2000–2010 with the flourishing of social media platforms. Some of the first countries to feel the influence of social networks were the Muslim states, where the Arab Spring unfolded with the active participation of users of social networks such as Facebook and Twitter. Subsequently, the experience of these protest movements began to spread throughout the world, affecting Asia, Africa and many other regions. Consequently, the emphasis in this work will be on social networks as an integral means of forming the modern political system.

The second-generation internet has radically transformed the process of virtual communication. High technologies have provided us with a means for engaging in prompt interactive communication both on the internet in general, and on social networks in particular. Transferring and exchanging information has become a two-way process, creating new forms of social interaction. In a relatively short period of time, social networks (Facebook, Instagram, Twitter, etc.) have become one of the main platforms for accessing the internet for millions of users alongside search engines (Google, Baidu, Yahoo, Yandex, etc.). According to O. Dyachenko, in certain situations, groups on social network act as an independent component of converged media in terms of their target content and audience.[1] An increasing number of users employ their social media feeds to monitor the news, a practice that has begun to spread to the field of professional media communication. Today, the number of subscribers to news communities on social networks is gradually overtaking the number of readers of offline versions.

1 Дьяченко 2016, 30

Through the study of individual cases, we test the hypothesis that protest movements in the modern world acquire their scale thanks to hashtags, which, in turn reflect processes in society, and that the most reliable data is not one hashtag, but a combination of lexical units that form a common semantic field. Thus, hashtags represent for material for research, amenable to relatively quick verification due to the transparency of their use on many social networks. Moreover, in our study, we investigate the diachronic aspect of the use of hashtags in the first half of the 2010s (as a stage in the formation of the hashtagging process) using as the example the slogans of the Arab Spring (December 17, 2010 to December 2012), #kony2012 (2012), #BlackLivesMatter (2013) and its 2020 iteration, and the hashtags of Hong Kong demonstrators (#HongKong, #OccupyCentral, and #UmbrellaRevolution) in 2014 and 2019. All the hashtags analysed were processed manually, with no added software.

These hashtags were selected so that we could monitor the chronology of transformations and because they are strong indicators of the largest demonstrations in the world at those specific times. We also pay special attention to the fact that only a combination of various hashtags can give the most complete picture of protest movements, which the above cases confirm.

The Nature of the Hashtag and its Role in the Further Digitalization of Society

One of the important attributes of most large social networks is the hashtag. The first hashtags appeared in the 1990s in the IRC network (Internet Relay Chat). However, they did not start to gain widespread popularity until 2007, when they were used on the Twitter social network to organize messages. C. Messina, a former employee at Google working at Twitter's San Francisco headquarters, suggested using keywords that combine major posts, identified by the hash symbol. The hashtag has enjoyed a widespread currency on social media, simplifying the process of virtual communication. It was S. Boyd, a senior researcher at GigaOM Media, who coined the new term "hashtag." To date, hashtags have already gone through a long evolutionary path, and their main function (text indexing for quick search in the context of a specific topic) has been relegated to the background.[1] The hashtag is gradually becoming an identifier of socio-political transformations, a tool for advertising and image building.

The lexical unit expressed by the hashtag has become an integral part of the media text that is broadcast through the channels of social networks. The form of integrating text or a key lexeme with the pound sign transforms the hashtag into a hyperlink that includes a complex of textual information, audio and video content.

This makes it possible to acquire an extensive layer of information on the target topic. In addition, the interactive nature of the hashtag lies in the fact that communicators on social networks autonomously post a corresponding lexeme, in the form expressed by the hashtag. "Hashtagging" also facilitates operational navigation in the media discourse in order to select the right information. Currently, in connection with the

1 Патрушева 2018, 471

development of graph theory and the analysis of big data, this phenomenon has become the prerogative of users of social networks, and is of key interest to marketing professionals and political strategists.

Within the framework of communication theory, the communication system is differentiated into elements that are defined as "units." This system consists of transmitting devices (or addressers) that encode the text of the communication channel (a translator of information) and receiving devices (or addressees) that receive and decode the text. A complete unit of communication, as defined by the linguist G. Kolshansky, must satisfy two criteria: it must be organized structurally and it must provide complete information.[1]

In this regard, a lexical unit expressed in the form of a hashtag is a unit of media communication, since it reflects a specific segment of speech that independently conveys a message.[2] This study presents four main cases of protest movements and their correlation with hashtag activism. We established that single hashtags are not enough to provide a complete picture on a given topic, and that combinations of hashtags should be investigated. We have thus identified the main slogans on social networks related to specific socio-political processes, which are indicated in Table 1.

Table 1.

SOCIO-POLITICAL PHENOMENA IN HASHTAGS
СОЦИАЛЬНО-ПОЛИТИЧЕСКИЕ ПРОЦЕССЫ, ОТРАЖЕННЫЕ В ХЭШТЕГАХ

Event	Corresponding hashtags
Arab Spring	#Tahrir, #Lulu, #Bahrain, #Egypt, #Libya etc.
Kony 2012	#kony2012, #findkony, #stopkony, #stopatno(thing), #makekonyfamous etc.
Black Lives Matter	#BlueLivesMatter, #BlackLivesMatter, #AllLivesMatter, #WhiteLivesMatter etc.
Hong Kong Revolution	#HongKong, #OccupyCentral, #UmbrellaRevolution etc.

Source: Compiled by the author.

Use of Political Hashtags on Social Media

Before hashtagging and social media became firmly established in society, there were fewer opportunities in politics to create, develop and maintain a person's image, or to strengthen his or her status. In the past, this role belonged to the traditional media. Media communication has expanded the scope of resources for the abovementioned purposes. Social media platforms directly facilitated the establishment of interaction between society and government, and the second-generation internet radically modified the situation in the media sphere. In this regard, special attention should be paid to the political strategies of using these platforms and the search for relevant tactics for both forming and maintaining the positive image of a politician.[3]

Since the emergence of social networks such as Instagram and Twitter, politicians have striven to expand their influence on the internet in order to broadcast their

1 Кольшанский 1984, 176.
2 Филин 1979, 80.
3 Хецелиус 2019, 93.

political views and convey them to audiences by increasing the number of subscribers who are adherents of the politician's ideas and who may vote for them in elections. Thus, the formation of a positive image in modern virtual communication is becoming an integral part of the political programme of modern politicians.

One of the most prominent examples of a world leader using Twitter is the 44th President of the United States, B. Obama, who used the platform extensively during his 2008 campaign. The trend of world leaders using Twitter really caught on among world leaders from 2009 to 2012. In 2015, H. Clinton announced on her Twitter account that she intended to run for presidency, a fact that once again confirms the importance of social media in the political life of society. D. Trump during his term has been the most ardent supporter of Twitter in the political arena. He was an avid user even before he ran for president. Trump's tweets have repeatedly served as information to highlight his position both on radio and television, and in print media. The scandal following the ban of his personal account even raised the profile of this social network.

Currently, around 85% of the state representatives of the 193 member countries of the United Nations have a Twitter account, and approximately 66% of heads of state are personally represented on the platform.[1] In addition, it should be noted that many officials are more actively using Twitter, both as a resource to highlight their point of view, and as a tool for political propaganda. And hashtagging on these social networks acts as a priority source, not only for shaping a politician's image.

Hashtags in modern society are, by their very purpose, multi-tasking lexical units. To a certain extent, they appear as translators of political slogans of the past, modified in the context of the information society into a type of capacious, catchy and informative message. According to S. Fedorchenko, political hashtags in modern virtual communication have a "viral character" and demonstrate hypertextuality, targeting, psychological profiling and coding.

So, hashtags should be viewed as analogues of slogans that dictate the political agenda. This is of particular importance today, when in one capacious phrase on social networks you can instantly outline both your opinion on a certain political topic and influence your subscribers, forming a certain attitude towards the current situation in them. An interesting study on the shaping of the political agenda was carried out by M. Grachev, who, based on the works of M. McCombs and D. Shaw[2] on identifying the first level of the political agenda (which ranks texts in the context of the semantic differential[3]), focused on the second (concentration of the audience's attention on a certain message) and third levels of the political agenda (correlation of the attributive agenda with frames fixed in the minds of recipients).[4]

The thesis of the third level of the political agenda interprets the world of social networks in the best possible way, where lexical units expressed by hashtags act as system-forming components. Social media platforms such as Twitter, Facebook and Instagram have become a kind of experimental platform where politicians compare

1 *Яковенко, Н.* Почему политики полюбили Twitter // ИноСМИ. 16 июля 2015. [Электронный ресурс]. URL: https://inosmi.ru/world/20150716/229132082.html (дата обращения: 8.02.2021).
2 McCombs, Shaw 1972; 1976.
3 Construction of individual or group notional spaces with assessments on a number of rating scales. In this case, the system "main–minor–insignificant" becomes the scale. See: Osgood et al. 1957.
4 Грачев 2018, 146.

newly formed frames with the existing ones, which are actively used in society in the form of political slogans. In this regard, politicians should only correctly establish the current interests of society and, by broadcasting the hashtag (in accordance with their principles), adapt their own point of view to the needs of the audience.

According to German sociologist N. Luhmann, a political message implies accessibility for communication.[1] He distinguishes three autopoietic organizations: loyal to the regime, limitrophe and radical communities.[2] Groups on social media platforms can also be classified under this categorization. Particular attention should be paid to network limitrophe communities, which are in a balancing position between the two remaining binary systems.

Hashtags that take part in the work of self-referential network structures act as political codes. Hashtags can unite communication actors and transform and grow communities on social networks, endowing them with a value-symbolic component that attracts new users.

According to V. Tsymbursky, network limitrophe communities not only smooth out conflicts between pro-government and radical groups, but also provide an opportunity for the regime to appeal to the impartiality, honesty and democratic nature of the current political system without rigidly censoring content.[3] So, we see that in addition to forming a politician's image and serving as a platform for his or her slogans, social networks give the population access to the thoughts and positions of the opposition and actively promote it in the process of media communication.

Thus, an active protest movement can, using hashtags in modern virtual communication in an attempt to rally the support of society, act as a means of socio-political transformations in real life. Contrary to traditional means of expressing political positions, hashtag activism does not force users of social media platforms to take any risky action. The purpose of protest activity is reduced to the simplest actions that they can perform through subscriptions, likes and retweets.

Certain social and political movements have enjoyed popularity and success in many countries around the world over the last decade. In fact, the use of lexical units expressed in the form of hashtags during protest actions has significantly changed the situation in various regions, with governments even turning off the internet during episodes of mass unrest in order to maintain stability in the country. The expansion of the hashtag protest movement is directly related to the increase in the number of social networks and their diversity.

Hashtag activism, despite its short history, has captured the media's attention, engaging a large number of users on issues such as reporting on legal injustices and human rights violations, as well as for the purposes of fundraising and building opposition. The social media protest movement also runs political campaigns that seek to enact regulations and laws aimed at suppressing crimes that are ignored by the courts. Hashtag activism has transformed into a macro-text of defending a specific position, integrating users of social media platforms to participate in the campaign by promoting a capacious, concise and informative message.

1 Луман 2001, 116.
2 Луман 2007, 27.
3 Цымбурский 2011, 45.

J. Ndavula, A. Munuku, and H. Mberia identified[1] how the context in which a hashtag is formulated influences opinions on socio-political issues. Hashtags covering such problems as the political crisis in the country, ministerial scandals, collapsed buildings, terrorist attacks, social unrest and others were studied. The sample included hashtags with more than 100,000 mentions. It was found that most of the hashtags (51%) relate to the political context; 40% to the social context; 6% to security or terrorism; and only 3% to the economic context.

A significant percentage of the use of political hashtags indicates that political life causes more controversy on the internet. The number of tweets under these hashtags indicates that when trouble is brewing, people want to be heard if the nature of the problem is political. Statements, slogans and appeals can reflect both individual and group judgments, at times based on belonging to a particular political party.

Turning to the diachrony of the protest movement on social media, T. Small's work is worthy of note here. Small believes that hashtag activism emerged during the presidential elections in Iran.[2] In 2009, activists from the Democratic movement used the hashtag #iranelection on social media. This technique was used for positioning political statements, organizing mass protests and delegitimizing the political regime in country.[3]

History of the Emergence of Hashtag Activism in the Context of Political Transformations

When studying protest movements in modern virtual communication, we should keep in mind that the Arab Spring was key in the formation and spread of this phenomenon. From December 17, 2010 to December 2012, revolutionary movements took place in such countries of the Arab world as Egypt, Yemen, Tunisia, Libya and others. Social networking platforms (Facebook, Twitter, etc.) have become a means of rallying the population around a common cause in these countries.

The governments of the countries tried to restrict the population's access to the internet, as the coverage of protest actions became wider and the users of social networks became more united. Hashtags in this context have become a macro-text that unites citizens and illuminates relevant data on the results of revolutionary actions. In addition, the coordination of movement processes was entrenched in many hashtags, often bearing the names of the squares where the movement of activists was directed.

It thus established lexical units expressed in the form of hashtags. The most notable were #Tahrir and #Lulu, with the first hashtag marking Cairo's main square (Tahrir) as the venue of mass protests. The second, #Lulu, was used to discuss Pearl Roundabout or Lulu Roundabout – a traffic interchange in Manama (Bahrain).

Regarding the toponymic nature of hashtags, it should also be noted that the coordination function is only one of the factors in the emergence of new lexical units based on a proper name, with the addition of a hash key in front of it. The populations of the countries accorded much greater importance in the lexemes #Bahrain, #Egypt, #Libya, drawing the attention of the global community to the situation in the region,

1 Ndavula et al. 2017.
2 Small 2011, 872.
3 Федорченко 2019, 24.

and the English version of the spelling once again emphasizes the protesters' intention to assert themselves at the international level within the framework of transnational social networks.[1]

Having realized the high level of influence of social networks after the events of the Arab Spring, people and politicians began to gradually use this tool to achieve their socio-political goals. The next surge in protest movements based on hashtag activism was the events in Africa, or rather the coverage of these events in the United States in 2012, which once again underlines the international scope of this phenomenon. In this case, a group of activists from the United States drew the attention of the citizens of their country and the entire world to the oppression of children in Uganda in particular, and in the Central Africa in general. Human rights defenders have accused Ugandan war criminal J. Kony of murdering and mistreating Ugandan children.

The next stage in the deployment of the political campaign was to attract politicians and people who were popular, not only in the United States but all over the world. This is due to the large number of celebrity followers on social media. The campaign attracted a large number of people, which allowed the U.S. authorities to control the situation in Central of Africa moving forward.

Of course, hashtagging was not the only reason for the widespread coverage of this political campaign. In addition, internet platforms such as YouTube played an important role. However, the growing use of video was facilitated by the hypertext component, the main carriers of which were lexical units expressed in the form of hashtags. The difference is that while not all the goals of the Arab Spring were achieved through social media, because the governments of the countries involved opposed the protest actions, in the case of the Kony 2012 political campaign (with the hashtag #Kony2012 and others such as #findkony, #stopkony, #stopatno(thing), #makekonyfamous), the plans were implemented in full.[2]

However, researchers offer an opposite point of view that takes the real effect of protest movements on social networks into account. Thus, according to M.T. Bastos, C. Puschmann and R. Travitzki, a number of media outlets, political institutions and organizations are becoming the subject of widespread deception. The Twitter accounts of political movements in the United States such as Occupy Wall Street and Occupy U.S. spoke only in the role of sock puppeteer. In other words, internet accounts were used to mislead people. In addition, scholars claim that Twitter or media accounts of CNN, The New York Times, Reuters and HuffPost had a fairly large number of retweets without active involvement in a particular information flow.[3]

This fact indicates that well-known and reputable Twitter accounts are being tagged in all sorts of information streams in order to draw the attention of the media to socio-political phenomena and highlight a specific purpose or opinion.

Nevertheless, the situation surrounding the hashtag activism of the Kony 2012 campaign has shown American society what can be achieved using social media platforms. On the other hand, there is also a critical view of this problem. In particular,

1 Steinert-Threlkeld et al. 2015.
2 Joshua S. White, "Final-Retweets-Containing-KONY-Hashtags-for-graphing," Research Gate, accessed October 30, 2020, https://www.researchgate.net/publication/235764178_KONY2012_Retweet_Directed_Graph_Data.
3 Bastos et al. 2013.

M. Chossudovsky expressed the opinion that the struggle for human rights was only a cover for U.S. geopolitical ambitions[1].

The following year (2013), political life in social media was no longer concentrated outside the United States, but within the country. In July 2013, a court decision acquitted G. Zimmerman of the murder of African American teenager T. Martin, an event that provoked outrage from both the black community in the United States and human rights activists. This protest reaction was supported by a significant part of the Democrats, which subsequently resulted in the appearance of the #BlackLivesMatter hashtag, a succinct and laconic protest on social networks. Looking at the history of hashtags in 2020, we can see a repetition of the situation at a higher level. This tells us that the protest movement that originated at a certain point in time and then began to decline also needs research in order to understand its causality and the ability to predict the consequences for society.

The peculiarity of this political campaign in the context of hashtag activism is also expressed in the expansion of the structure of the use of one lexical unit, expressed by a hashtag, with a complex of lexemes focused on opposing the initial one: #BlueLivesMatter, #AllLivesMatter and #WhiteLivesMatter.[2] In this way, part of the U.S. population reacted to the protest movements, speaking out against the discrimination of the majority and the destructive protests, and only in extremely rare cases trying to justify violence. The situation that we currently observe in the United States underlines the fact that the belittling of the role of social networks in the protest movement, and the disparaging name of hashtag activism as slacktivism, has little to do with the state of affairs that arises as a result of virtual protests turning into real ones and vice versa.

In the time between the first mention of the #BlackLivesMatter hashtag and its use in 2020, a flash of LivesMatter movements occurred in July 2016 following police killings in Dallas. This is noted in detail in Figure 1. As we can see, the protest movements can be analysed solely on the basis of all lexical units expressed by hashtags and which form a single semantic field of protest movements in the United States. This trend reflects all cases of protest movement analysis, when only a combination of hashtags can provide a complete picture of demonstrations.

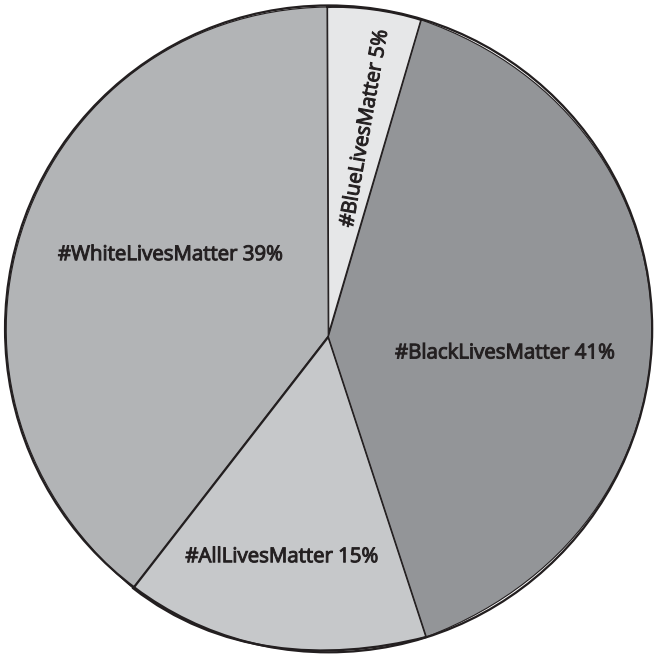
Regarding political events in the United States in 2020, it should be noted that D. Trump was an active user of social networks. He had no rivals among politicians on Twitter in terms of usage. Competition from Joe Biden in this area during the 2020 presidential campaign, even if meticulously coordinated, would be perceived by voters as more than artificial. Thus, a number of political scientists and journalists believe that the Black Lives Matter (BLM) movement on social networks acquired its scale precisely thanks to the work of the Democrats during the presidential campaign to persuade electors who used social networks and who, in turn, contributed to Joe Biden's victory, primarily in the media space of the second-generation internet. On 8 January 2021 the leadership of the American social network Twitter announced that it decided to finally block the account of the U.S. President.

1 "Joseph Kony, America's Pretext to Invade Africa: U.S. Marines Dispatched to Five African Countries," Global research, accessed February 15, 2021, http://surl.li/limn.

2 Emma Madden, "The BTS Army and the transformative power of fandom as activism," The Ringer, July 11, 2020, accessed October 30, 2020, https://www.theringer.com/music/2020/6/11/21287283/bts-army-black-lives-matter-fandom-activism.

Figure 1.

PROTEST MOVEMENTS IN THE U.S. IN JULY 2016 (BASED ON GOOGLE TRENDS)
ПРОТЕСТНЫЕ ДВИЖЕНИЯ В США В ИЮЛЕ 2016 г.
(НА ОСНОВЕ ТЕНДЕНЦИЙ GOOGLE)



Source: Compiled by the author based on Google statistics.

Hashtag activism in the modern world, as we can see from the example above, is cyclical. However, this does not mean that cyclicality manifests itself only in the case of repeating a lexical unit expressed in the form of a hashtag. In a broader sense, this process borrows not only patterns that are characteristic of the protest movement, but also their style, direction and even structure. In addition, the experience of previous protests protects demonstrators from possible actions on the part of politicians against whom the actions were directed in the first place.

A prime example of all of the abovementioned aspects is the hashtag activism that was witnessed during the Hong Kong Umbrella Revolution. In many ways, this revolution repeated the history of the Arab Spring. The main hashtags were #HongKong, #OccupyCentral and #UmbrellaRevolution.[1] In this case, the first two hashtags can be traced back to those used during the Arab Spring: #HongKong and #Egypt (the country of the protest in order to notify the world community) and #OccupyCentral and #Tahrir (the location of the protests and the direction of movement of social media users towards the main square).

The second important point was the level of preparedness on the part of those who took part in the Hong Kong protests. Protestors downloaded the FireChat app, which allows users to distribute messages even without an internet connection thanks to Bluetooth and

1 Griffin Leow, "Analysis of Tweets on the Hong Kong Protest Movement 2019 with Python," Towards Data Science, November 18, 2019, accessed October 30, 2020, https://towardsdatascience.com/analysis-of-tweets-on-the-hong-kong-protest-movement-2019-with-python-a331851f061.

Wi-Fi. The demonstrators of the Arab Spring did not prepare for the protests in this way, since this was the first time such large-scale actions on social networks had been held. It should also be noted that, like the BlackLivesMatter protest movements, the protests in Hong Kong also took place in two stages with a significant break in time: in 2014 and 2019.

Conclusion

Based on all the above examples, it should be noted that political activism is an integral part, not only of social media platforms, but also of real political events taking place in all regions of the world. For a better understanding of the nature of this multifaceted phenomenon, it is necessary to establish the regularities of the functioning of lexical units expressed in the form of hashtags.

Many political phenomena covered in social networks become an important part of media communication, which subsequently also influences the situation in a particular region. Interactivity is a distinctive feature of the second-generation internet; social media platforms allow users to not only to see the information, but also to actively discuss, challenge or support it.

The ambivalence of modern existence (in the framework of constant competition between international and regional social platforms) is an integral part of globalization as a process of strengthening the interconnectedness of different parts of the world, the ever-growing impact on the social reality of individual countries, and various factors of international significance: information and cultural exchange, political and economic ties, art and social movements. A true revolution took place in the information space with the introduction of and connection to the second-generation internet, which made it possible for people to communicate online.

Active use of the internet serves to shape worldviews and facilitate interaction among people. Making adjustments to the value picture of global society, cross-cultural behaviour and behaviour models, the lack of censorship, anonymity, various types of contacts, and the pragmatic orientation of internet interaction all contribute to the development of media communication for the purpose of socio-political protest.

Digitalization has undoubtedly changed the life of modern society, and made communication international. Political transformations in one country instantly become news to the whole world. To date, the function of indexing a message to search for a publication on a given topic is gradually fading into the background. In this work, we emphasize the relevance of hashtag activism. With each new case, this process becomes less and less trivial and, therefore, requires a deeper analysis. Statistical data helps scientists to assess the situation transparently in order to identify the main features of this phenomenon. And it is the totality of lexical units expressed in the form of hashtags that fully reveal the nature of protest movements, providing an opportunity to analyse a specific protest not by one word, but by a set of lexemes to view a subject in various ways.

Based on a number of examples provided in this paper, we see that social media activism is cyclical and internationally recognized. The similarity of the forms of slogans and messages expressed by hashtags, and the algorithm of subsequent actions provide an opportunity to extrapolate new emerging ideas and movements both in the field of modern virtual communication in general, and on social media platforms in particular for the timely adoption of constructive decisions.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Грачев, М.Н. О новой интерпретации соотношении концепций «установления повестки дня» и фрейминга // Политика развития, государство и мировой порядок: Материалы VIII Всероссийского конгресса политологов, Москва, 6–8 декабря 2018 г. / Под общ. Ред. О.В. Гаман-Голутвиной, Л.В. Сморгунова, Л.Н. Тимофеевой. – М.: Издательство «Аспект Пресс, 2018. – 146 с. [Grachev, M.N. "On a new interpretation of the relationship between the concepts of 'agenda setting' and framing." [O novoj interpretacii sootnoshenija koncepcij "ustanovlenija povestki dnja"i frejminga] In *Development policy, state and world order. Materials of the VIII All-Russian Congress of Political Scientists, Moscow, December 6-8, 2018.* Moscow: Aspekt Press, 2018] [In Russian].

Дьяченко, О.В. Российские СМИ в социальных сетях Facebook и в «ВКонтакте»: анализ активности и информционных предпочтений аудитории // Вестник Московского университета. Серия 10. Журналистика. – 2016. – №1. – С. 28–45 [Dyachenko, O.V. "Russian media in social networks Facebook and VKontakte: analysis of audience activity and informational preferences." [Rossijskie SMI v social'nyh setjah Facebook i v «VKontakte»: praktiki vzaimodejstvija] V*estnik Moskovskogo universiteta. Ser. 10. Journalism,* no. 1 (2016): 28–45] [In Russian].

Кольшанский, Г.В. Коммуникативная функция и структура языка. – М.: Наука, 1984. – 176 с. [Kolshansky, G.V. *Communicative function and structure of language* [Kommunikativnaja funkcija i struktura jazyka]. Moscow: Nauka, 1984] [In Russian].

Луман, Н. Власть. – М.: Праксис, 2001. – 256 с. [Luhmann, N. *Power* [Vlast']. Moscow: Praxis, 2001] [In Russian].

Луман, Н. Социальные системы. Очерк общественной истории. – СПб.: Наука, 2007. – 641 с. [Luhmann, N. *Social systems. Essay on the General Theory* [Social'nye sistemy. Ocherk obshhej teorii]. Saint Petersburg: Nauka, 2007] [In Russian].

Патрушева, Л.С. Хештегирование как новый коммуникативный процесс // Вестник Удмуртского университета. Серия «История и филология». – 2018. – Т. 28 (3). – С. 471–475. [Patrusheva, Lidia V. "Hashtagging as a new process of communication." [Heshtegirovanie kak novyj kommunikativnyj process] *Bulletin of the Udmurt University. Series History and Philology* 28, no. 3 (2018): 471–475] [In Russian].

Русский язык: энциклопедия / гл. ред. Ф.П. Филин. – М. : Сов. энцикл., 1979. – 432 с. [*Russian Language: Encyclopedia* [Russkij jazyk: jenciklopedija], edited by F.P. Filin. Moscow: Sov. encycl., 1979] [In Russian].

Федорченко, С. Хештеги: механизм легитимации политического режима или манипулятивная ловушка? // Обозреватель–Observer. – 2019. – №7. – С. 28–41 [Fedorchenko, S. "Hashtags: mechanism of legitimization of the political regime or a manipulative trap?" [Heshtegi: mehanizm legitimacii politicheskogo rezhima ili manipuljativnaja lovushka?] *Obozrevatel–Observer,* no. 7 (2019): 28–45] [In Russian].

Хецелиус, В.Е. Социальные сети как инструмент политической коммуникации // Наука без границ. – 2019. – Т. 33 (5). – С. 93–103. [Khetselius, V.E. "Social networks as a tool of political communication." [Social"nye seti kak instrument politicheskoj kommunikacii] *Nauka bez granic* 33, no. 5 (2019): 93–103] [In Russian].

Цымбурский, В. Конъюнктуры Земли и Времени. Геополитические и хронологические интеллектуальные расследования. – М.: Европа, 2011. – 372 с. [Tsymbursky, V.L. *Conjuncture of the Earth and Time. Geopolitical and Chronopolitical Intelligence Investigations* [Konjunktury zemli i vremeni: geopoliticheskie i hronopoliticheskie intellektual'nye rassledovanija]. Moscow: Evropa, 2011] [In Russian].

Ndavula, John, Anne Manuku, and Hellen Mberia "Influence of the hashtag context on public opinion formation on sociopolitical issues in Kenya." *Journal of Public Policy and Administration* 2, no. 3. (2017): 27–51.

Small, Tamara A. "What the Hashtag?" *Information, Communication & Society* 14, no. 6 (September 2011): 872–95. doi:10.1080/1369118X.2011.554572.

Steinert-Threlkeld, Zachary C., Delia Mocanu, Alessandro Vespignani, and James Fowler. "Online Social Networks and Offline Protest." *EPJ Data Science* 4, no. 1 (2015). doi:10.1140/epjds/s13688-015-0056-y.

Bastos, Marco Toledo, Cornelius Puschmann, and Rodrigo Travitzki. "Tweeting across Hashtags." In *Proceedings of the 24th ACM Conference on Hypertext and Social Media* – HT '13. New York, New York, USA: ACM Press, 2013. doi:10.1145/2481492.2481510.

Osgood, Charles E., George S. Suci, and Percy Tannenbaum. *The Measurement of Meaning*. Illinois: UIP, 1957.

McCombs, Maxwell E., and Donald L. Shaw. "The Agenda-Setting Function of Mass Media." *Public Opinion Quarterly 36*, no. 2 (1972): 176. doi:10.1086/267990.

McCombs, Maxwell E., and Donald L. Shaw. "Structuring the 'Unseen Environment.' " *Journal of Communication* 26, no. 2 (June 1, 1976): 18–22. doi:10.1111/j.1460-2466.1976.tb01374.x.

Author

Alexander V. Alekseev,

PhD (Linguistics), Associate Professor at English Language Department No. 6

MGIMO University, 76 Vernadsky Ave., Moscow, 119454.

e-mail: alexander1990alekseev@gmail.com

Additional information

Received: October 13, 2020. Accepted: February 15, 2021.

Disclosure statement

No potential conflict of interests was declared by the author.

For citation

Alekseev, Aleksandr V. "Hashtagging as an Identifier of Political Transformations in the Digital Age." *Journal of International Analytics* 11, no. 4 (2020): 91–103.

https://doi.org/10.46272/2587-8476-2020-11-4-91-103

Анализ примеров использования хэштегов как средства координации протестных движений

АННОТАЦИЯ

Статья посвящена исследованию протестного движения в социальных сетях. Актуальность исследования детерминирована необходимостью выявления новых форм протестной активности, сформировавшихся в период цифровизации и глобализации. Исследование построено на эмпирическом анализе конкретных случаев применения хэштегов. Подчеркивается, что активизм в социальных сетях характеризуется цикличностью и ориентацией на международное признание. В работе представлены универсальные паттерны образования лексических единиц, выраженных по форме хэштегами. Исследуется чрезвычайно важная роль социальных сетей в политической повестке таких африканских стран, как Уганда, Кения и др. Также в тексте освещаются протестные движения в мусульманских странах в период Арабской весны. Именно совокупность лексических единиц, выраженных по форме хэштегами, в полной мере раскрывает природу протестных движений, предоставляя возможность анализировать конкретный протест не по одному слову, а по набору лексем для того, чтобы рассмотреть вопрос с разных сторон.

КЛЮЧЕВЫЕ СЛОВА

протестные движения, цифровизация, социальные сети, хэштег-активизм

Сведения об авторе

Александр Владимирович Алексеев,
к.филол.н., доцент кафедры английского языка №6 МГИМО МИД России,
проспект Вернадского 76, 119454.
e-mail: alexander1990alekseev@gmail.com

Дополнительная информация

Поступила в редакцию: 13 октября 2020. Принята к публикации: 15 февраля 2021.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Цитирование

Алексеев, А.В. Анализ примеров использования хэштегов как средства координации протестных движений // Международная аналитика. – 2020. – Том 11 (4). – С. 91–103.
https://doi.org/10.46272/2587-8476-2020-11-4-91-103

Islam and Progress: Between Tradition and Modernity

Julia Roknifard **Orhan Gafarli** **Leslie Terebessy**

https://doi.org/10.46272/2587-8476-2020-11-4-104-121

ABSTRACT

In the course of rethinking how Muslim communities have historically reacted to progress and integrated its achievements into their lives, we tried to revisit the reasons why the Islamic world has preserved a deep rift between tradition and modernity. Looking at the debate in theological and near-theological circles amongst Muslim thinkers and theorists of the past, we conclude that one of the major issues in terms of philosophical grounds is that religion has become associated with tradition more than with the revelation. Religion teaches timeless principles, while tradition adheres to past practices, which are time-bound. When tradition is treated as religion, problems arise, for traditional practices can conflict with modern ones. A large portion of the Muslim world has difficulties in adapting to modernity, and this is related to the fact that religiosity has become associated with feudalism and ritual. While a strong suggestion is to discursively separate religion from politics, this article nevertheless begins by exploring how progress in the Muslim world is affected by the confluence of tradition and revelation, among other factors. The two case studies based on the analysis of the specifics of modernization in Turkey and Iran are highlighted the trends that hinder technological progress in the countries of the Islamic world.

KEYWORDS

Islam, Islamic world, technological progress, ijtihad, innovation, Iran, Turkey

CC BY

Introduction

On the eve of the KL Summit, dubbed as a nascent alternative to the Organisation of Islamic Cooperation (OIC), in Kuala Lumpur in 2019, Prime Minister of Malaysia Mahathir Mohamad lamented that inability of Muslim nations "to progress and become a developed country had resulted in Muslim nations being perceived as weak and Muslims continued to be suppressed, controlled and abused by other countries."[1] Mahathir Mohamad said despite Muslim nations having the ability and capability to compete with other developed nations, they had no desire to do so. The difficulty discussing the causal links between the tenets of Islam and the relative backwardness of Muslim countries in terms of technological, social and economic progress underlies the multiplicity of factors that hinder the development of these countries. Muslim majority countries mostly belong to developing or least developed economies, which by itself can be a consequence of a colonial past, modern neoliberal policies, the oil curse/resource-based economies, corruption, the unequal distribution of wealth, or geopolitical volatility and not of the religious affiliation of their populace and governing authorities.

The lack of innovation and stimulating policies can also be explained by other factors, such as cultural features that do not stem from Islam itself, for example the extreme importance of "face-saving practices," which diminish the appetite for risk and thus discourage innovation. If culture dictates that failure in an endeavor is the height of shame, then people will likely avoid risking their wealth by investing in start-ups. In his *Development as Freedom*, A. Sen defined freedom and development as interconnected notions. To achieve development, he argues, poverty, tyranny, social deprivation, and the machinery of repression need to be removed.[2] In addition, economic opportunities need to be created and public services improved.

Though China's development and technological advances prove that the correlation between freedom and development is not direct or absolute (freedom can be relative and exist as a comprise, for example, in the form of social benefits without political liberties), A. Sen's idea invites the assumption that the configuration of a given political regime and the policies it deploys might be a reason for backwardness, including intellectual backwardness, which, in turn, does not have any relation to the cultural or religious canvas of society. Apologists of Islam, in turn, would suggest that, just as with other world religions, Muslims were called upon to eliminate poverty through charity and the equitable allocation of resources based on the principles of justice. So, development generally is also taken care of by the tenets of Islam, but it says less about how much freedom (and rule of law) is necessary to pursue justice, equity and movement forwards.

The ability to adapt to modernity and thus progress technologically is "path dependent." That is, it depends greatly on what path particular a culture walked through to reach its current point, and culture, in turn, is a substance rigid to change. The nexus of culture, tradition, religion, and the political employment of cultural and

1 Junita Mat Rashid, "Dr M: Muslim nations can become developed and competitive," New Straits Times, November 30, 2019, accessed February 11, 2021, https://www.nst.com.my/news/nation/2019/11/543419/dr-m-muslim-nations-can-become-developed-and-competitive.

2 Sen 2000.

religious sentiments played a great role in how the Islamic world grappled with the idea of modernity and the progress that was supposed to come along. And even though the Islamic world may also have observed a decline of trust in religious institutions, the demand for spirituality has not waned. This demand, along with the cultural baggage that various Muslim communities carry, has an enduring influence on the developmental processes within respective societies.[1] We take this sociological trend, thoroughly researched by R. Inglehart and his colleagues, as a basis for our discussion on the cultural and ideological premises of this barrier to progress in the Muslim world.

In modern global discourse, we find a plethora of figures that support the idea of progress within, and supported by, Islam. One such example is the work of A.H. AbuSulayman, who maintains that there is a "crisis" in the Muslim mind that needs to be overcome. In his opinion this crisis is one of thought and methodology, not one of belief.[2] However, an important problem with A.H. AbuSulayman's recommendation is that he appears unwilling to put the Muslim tradition under the microscope. He simply assumes that tradition is reliable and uncorrupted. Another proponent of renewal is T.J. Alwani, a former colleague of A.H. AbuSulayman. He agrees with A.H. AbuSulayman that the problem is one of thought and thus calls for "sound thinking"[3] Umer Chapra has also highlighted the requirement to welcome science. According to him, decline took place as a result of the influence of tradition.[4]

What all these commentators share is a concern with a revival of rationalism and sound thinking, while either seeking compatibility with the Islamic tradition or completely detaching religious and scientific thinking. When it comes to the former, unfortunately, calls are made but concrete solutions are not offered. In an attempt to re-examine the ability of Muslim civilization to achieve technological progress, we believe that modern discussion on the topic should be highlighted. Ironically, though, this discussion is often underpinned by references to the past, whether it takes place within a close intellectual circle or on a large platform for policy makers.

Discourse on Knowledge and Progress

Religions blossom when they bring knowledge and truth, and they degenerate when they are reduced to rituals and become institutionalized, when their adherents lose sight of the reasons for being religious. Progress makes demands on everybody, but adaptation appears to be a hurdle in stagnant communities. Various resources are required to assist in the transition from tradition to the present, where knowledge matters, but tradition and community culture are also important. Problems adapting to progress arise due to a deficit of knowledge, or when the tradition is rigid.

In some educational traditions, Muslims are brought up to be suspicious of change and reasoning, which are perceived as evil, they are taught to suspect evil in anything unfamiliar, on the grounds that it is bid'ah (innovation), even though it is

1 Inglehart, Baker 2000, 49.
2 AbuSulayman 1993, 28.
3 Ibid., 4.
4 M. Umer Chapra, "Is Rationalism Possible in the Muslim World?" p. 9, accessed August 11, 2017, http://ierc.sbu.ac.ir/File/Article/Is%20Rationalism%20Possible%20in%20the%20Muslim%20World_93498.pdf.

only innovation in religion itself that is proscribed in Islam. Furthermore, embracing "innovation" in tradition was made to appear as a compromise on religious principles, and embracing the present eventually came to be seen as apostasy, the gravest of misdeeds in Islam. That this has taken place is indicated by the paucity of traditions relating to reason or intellect. From this perspective, the traditions appear truncated, and thus it is puzzling that they are presented as "completing" the Quran, the holy book of Islam, which presents itself as "complete" first and foremost.

The Quran says, "We hurl the truth against falsehood ..." (Quran, 21:18), pointing to a way from the morass caused by the traditional denigration of reason that began with the persecution of philosophers at the time of the fourth Abbasid caliph, Musa al-Hadi in 786,[1] and was meant to destroy sciences to the core. The persecution of thinkers betrayed a perception of faith that at the time required believers to prove faith by the sacrifice of reason. That dangerous requirement in itself paved the way for anti-rationalism and in its ultimate form extremism. In order to adjust the entire paradigm to the idea of progress, it would thus need to be freed from the association between religiosity and compliance with the external world and directed more toward inherent values, including the pursuit of knowledge. Let us recall that the prophetic traditions are not the verbatim words of the prophet, but mere paraphrases, hence their reliability differs from that of the Quran.

The problem is epistemological as well as political. And it has been made more controversial by attempts to "Islamize" knowledge, when Palestinian philosopher Ismail al-Faruqi suggested that science be de-Westernized and brought in compliance with Islamic ethos. In other words, he called for paths of reconciliation to be found between the Islamic way of life and modernity when it comes to science. His ideas laid the grounds for further work in that direction by the U.S.-based International Institute of Islamic Thought (IIIT). In Muslim majority Malaysia, whose elites drew the very notion of the Islamization of knowledge from S. Muhammad Naquib Alatas' 1978 work *Islam and Secularism*,[2] this effort was pursued by the International Institute of Islamic Thought (ISTAC) and Civilisation and the International Islamic University, functioning under auspices of the OIC.

Supporters of this kind of campaign think they can bring Muslims into modernity by "re-painting" knowledge with the shades of Islam. The movement is based upon a duality between Islamic and un-Islamic knowledge, while the revelation differentiated only between knowledge and ignorance. Muslims might perceive "progress" as problematic because it is associated with Westernization and abandoning tradition. When properly articulated, religion does not hinder, but rather accommodates and even uses the fruits of progress, for example communications technology.

The aversion to progress is a part of a protective mechanism, where progress is rejected because it is associated with negative experiences or expectations, for example the ruining of social institutions, like the family or encroachment upon dignity. This was the experience of Sayyid Qutb, the leading member of Muslim Brotherhood. During his visit to the United States, he was horrified at couples mingling freely in

1 Sayyid Jamal al-Din al-Afghani 2002, 110.
2 Muhammad Naquib al-Attas 1978.

what he saw as self-indulgence and debauchery. He recoiled it in horror and wrote his books partly in response to this negative experience and his desire to protect the Muslims from a similar fate, should they follow the path of the West. In a move to warn the Egyptian political elite from the curse that comes with modernization, a notion that is sometimes interchangeable with Westernization, he met with President of Egypt G.A. Nasser and asked him to stop the departure from traditional values, for example, by making it compulsory for all Egyptian women to wear a headscarf. Nasser would later mock Sayyid Qutb for this suggestion, pointing to the single most important woman the activist had failed to compel cover her hair – Qutb's own daughter.[1]

When Islamic scholars discuss this issue, many point to the "closure of the gates to *ijtihad*," (independent judgment in juridical matters) and the emergence of *taqlid* (imitation) or the following of tradition even against reason as the main reason why Islamic civilization, after going through a period of bloom in the development of sciences and the cherishing of knowledge, plummeted into this era of darkness, where Muslim societies are only capable of borrowing and not cultivating the fruits of technological progress. Sometimes this closing of the gates to *ijtihad* is presented as the opposite to the Enlightenment in Europe, when thinkers opened wide the doors to reasoning, ushering in the "age of reason." Blame is occasionally placed at the door of Muslim jurists, who around the 10th century proclaimed that all legal issues had been solved and that there was no need for any additional thinking on the subject – that attention should be placed exclusively on practicing the established norms and drawing analogies from existing precedents, where necessary. In the present day, even when it comes to those legal scholars who have been entrusted with spearheading the renewal of Islamic civilization, there is little fresh thinking taking place.

On the other side of the ongoing debate, a few scholars maintain that *ijtihad* among the schools of Islamic jurisprudence continued well beyond the 10th century, while those who believe in the "closure of the gates" became marginalized or extinct.[2] However, the four mainstream schools of jurisprudence remained intact without new ones emerging. This is why it is sometimes believed that the Shia world (where Iran would be the major among the heavyweights) remained faithful to the principles of *ijtihad* because up until now Shia Muslims can choose their own *mujtahids* (those entitled to interpret the existing norms and generate new prescriptions – *fatwas*) and opt for a new one after their demise, instead of relying on the edicts issued by the *mujtahid* they used to follow. Nevertheless, in the present day, the decline in the value of reason leads to calls for a revival of *ijtihad* as a prerequisite for Muslims to progress and adapt to modernity.[3]

The rejection of rationality facilitated the acceptance of the perception, widespread among Sufis, that true piety requires the sacrifice of reasoning on the altar of tradition. This attitude also damaged the spirit of rational enquiry, thereby thwarting the growth of Muslim civilization. A true follower of a Sufi sheikh would practically revere his "master." In a few Muslim countries the reverence for sheiks went to the extent that

1 "(Re)Islamization of Arabia: Nasser on The Muslim Brotherhood and Hijabs (1966 Egypt)-(english) #76," YouTube, accessed February 11, 2021, https://www.youtube.com/watch?v=0fswb4a9jcU.
2 Hallaq 1984.
3 Al-Alwani 2005.

they were referred to as "maulana," or "our protector," a term reserved in revelation for Allah. (Quran, 2:286) This dichotomy was employed in building some education systems, some of which refused to teach mathematics and logic in favor of religious disciplines. Persecution of rationalists was yet another blow to the development of thought within Islamic civilization.

Ethics and the Pursuit of Knowledge

The pursuit of knowledge is also a priority tenet of Islam. According to Islamic philosophy, the search for knowledge is one of the things that is supposed help to bring the believer to paradise. At the same time, the pursuit of knowledge has its own limitations. M. Umer Chapra, for example, reminds us that development based on the welfare of society goes beyond material wellbeing, which is understood as aspects of psychological wellbeing, happiness, justice, human kinship, equal and fair treatment and sharing in the fruits of development.[1]

O. Bakar echoes this perception by asserting that technological development is never value-free but culturally determined.[2] He contrasts the Islamic traditional view of technological development and progress with the contemporary Western approach to the matter. According to the category of scholars represented by O. Bakar and those like him, the Western world has walked the path from medieval times, where religion marginalized science, to the contemporary era, where science has not only marginalized religion but has replaced it altogether. As a result of globalization, Muslims have started to look at science and technology in the same way that people from the West view it, that is, by this detaching it from their religious background. Meanwhile, traditional Islamic culture sees the notion of progress as being closely related to the understanding of its moral boundaries.

O. Bakar states that Western culture is the perfect manifestation of arrogance, most notably in its approach to science and technology, as it has been almost completely desacralized by committing to empiricism and materialism and neglecting ethics and spirituality.[3] The creation of nuclear weapons is something that Muslim scholars would present as an example of exercising freedom of choice without ethical constraints. In other words, not all knowledge is beneficial, and some knowledge should be shunned because of spiritual constraints or to serve a greater public good.

This point of view is a development of the criticism suggested centuries ago by Persian philosopher A.H. al-Ghazali in his *The Incoherence of the Philosophers*, which some instead perceive as an adversary of reason in the Islamic world. According to A.H. al-Ghazali's categorization, "blameworthy" knowledge is that which can be defined as "leading to any harm whether to its practitioner or anybody else; when it is mostly harmful; and when the pursuit of that kind of knowledge does not give the practitioner any real increase in beneficial knowledge."[4]

O. Bakar argues that the classical premises laid out by Abu Hamid al-Ghazali were supposed to lead to the creation of a culture of scientific and technological development that would be in line with Islam. But that did not happen. Instead, Muslims, being

1 Chapra 2008.
2 Kamali et al. 2016, 18.
3 Ibid., 24.
4 Kamali et al. 2016, 31.

mostly borrowers and users of ideas and technology, are no longer in a position to dictate the direction of science and technology.[1] On the other hand, Ghazali is labeled as a delinquent responsible for driving the Muslim world away from science. According to this point of view, al-Ghazali stated that mathematical sciences have no bearing on religion, per se, but pose a greater danger because they fascinate scholars to the extent that they turn their backs on religion.[2] He is also charged with disrupting the notion of causality for future generations of Muslims through the metaphor of fire and a piece of cotton, which argues that it is not fire (cause) that burns a piece of cotton (effect), rather it is Allah who destroys it.[3] This therefore gives humans with limited power to understand and predict the way things work.

Having discussed the discursive, theological and ethical foundations of how knowledge, science and subsequently technological progress were perceived by the Muslim world, the question of how meaningful the link between Islamic philosophy in all its manifestations and technological progress as an area of practice is remains open. To actually achieve technological productivity and progress, Muslims might need to stop searching for the basis in theological and sacred texts and tradition. Vesting a theologian with the authority to adjudicate on scientific matters resulted did not stimulate development, rather it led to restrictions being imposed on it. That is why progressive thinkers sometimes call for a "reformation" of Islam, much like what happened with Christianity. Here, in fact, those who condone Ghazali's texts on science would interpret his ideas that religious discourse should not be mixed with scientific discourse, as both science and religion would be worse for it.[4]

Turkey: Modernism vs. Conservatism?

Among Turkish authors of modern period, N. Berkes,[5] H.Z. Ülken,[6] M. Türköne,[7] İ. Kara,[8] and A.H. Tanpınar[9] examine the same issues starting from the 18th century of Turkish modernization and the processes that led to the establishment of the republic. Particularly interesting are K. Karpat's works on the New Ottomans, where he exposes the role of political movements in the modernization process within Ottoman Empire. İ. Ortaylı deals with the process of cultural modernization,[10] as well as the changes in historical governance and their effects on modernization.[11] F. Sezgin spoke of the backwardness within the Islamic world and amongst the Ottomans and their efforts to internalize technological development from Europe.[12]

With the establishment of the Republic of Turkey and the Academy, research into the causes of the technological lag in the Ottoman and Islamic world and how

1 Kamalı et al. 2016, 32.
2 Peters 1990, p. 46.
3 Al-Ghazali 1963, 185–186.
4 "A grievous crime indeed against religion has been committed by the man who imagines that Islam is defended by the denial of the mathematical sciences, seeing that there is nothing in revealed truth opposed to these sciences by way of either negation or affirmation, and nothing in these sciences opposed to the truth of religion" (quoted as per Watt 1953).
5 Berkez 2019.
6 Ülken 2019.
7 Türköne, 2003.
8 Kara 2020; 2019.
9 Tanpınar 2012.
10 Ortaylı 2007.
11 Ortaylı 1979.
12 Sezgin 2015.

this process affected the modernization of society began. One of the most important historians of the Republic period, H. Inalcık, discussed such issues as the relationship between the state and religion in the Ottoman Empire and the reaction of different religious communities to modernization in his works.[1] H. Inalcık refers to original sources to decipher the kind of relationship that existed between the Sultan and religious communities.

Turkey has gone through its own history of theological-philosophical debates and relevant transformations of the education system. Until the 16th century, the Maturidi interpretation of religious tenets, which places an emphasis on science and philosophy, was dominant in the Ottoman Empire. Later, it largely shifted to the Ashari theology with its dogmatism and questionable relationship with rationalism. At that time, the Ottoman madrasas (schools) underwent a reform under Sultan Suleiman (1520–1556), when disciplines like mathematics and logic lost their value to the curriculum, which arguably led to the Ottoman State falling behind Europe.[2]

The history of modernization in the Ottoman Empire goes back to the 18th century. At the time known as the tulip period (1703–1730), the Grand Vizier Damat Ibrahim Pasha encouraged innovations in the Empire, while studying the European experience closely. With diplomatic missions dispatched to major cities such as Paris, Vienna and London, the imperial establishment started to learn about the Western way of life and think of how to introduce and adopt the best achievements at home. This began with the introduction of technological innovations, such as the printing press by Ibrahim Müteferrika and Said Efendi, the establishment of a paper factory and the introduction of medical innovations, such as the measles vaccine, to Ottoman society.[3] This period also marked the first collision between tradition and innovation within the Ottoman Empire.[4]

Later, the Russo-Turkish War of 1768–1774, which resulted in the Ottoman side making large concessions under the 1774 Treaty of Küçük Kaynarca, including the loss of Muslim-dominated Crimea and the granting to Russia of the extra-territorial right to build a church in Constantinople and protect all the Orthodox Christians under Ottoman rule, forced the imperial leadership to face an unpleasant truth – that the Ottoman Empire was in a state of complete stagnation, uncertainty and technological backwardness compared to its adversary. Radical innovations thus needed to be imposed on society.[5]

In an attempt to reconcile the traditional basis for legitimacy with the ability to introduce new practices, a new "social contract" was signed between the center and imperial vilayets. In order to maintain the communication link between the Ottoman rulers and the provinces, especially Eastern Anatolia, Sultan Mahmut II introduced the Charter of Alliance in 1808. This reconfiguration was supposed to launch a constitutional reform and transform the Empire into the constitutional monarchy.[6] Much has been written about the Charter of Alliance in Turkish-Ottoman historiography. For some,

1 İnalcık 2019.
2 Kalayci 2012; Yıldız 2019.
3 Emecen 2018.
4 Mazanec 2016.
5 Kuzucu 2010.
6 Akyıldız 1998.

the first constitution of the Ottoman Empire represented only a slight adjustment in the continuing relationship between the center and the provinces.[1] However, despite this view – which renders the agreement less significant than it actually was – the constitution was still the first legal text that stipulated power sharing. Nevertheless, Mahmut II (1808–1839) continued with centralist rule despite the Charter of Alliance.

The understanding of the need to modernize, especially in military terms, continued with another period of reform, widely known as Tanzimat (1839–1876), which spurred development of intellectualism and tighter links with the European intellectual tradition. During this period, the Young Ottomans emerged as the first traditionalist intellectual movement as a result of the spread of press and education. The publication of the first Ottoman newspaper *Ceride-i Havadis* (Journal of News) in 1840 and Agah Efendi's *Tercüman-ı Ahval* in 1860 also happened during the Tanzimat period,[2] which advanced the formation of independent public opinion and intellectual circles.

The Young Ottomans themselves represented a conflicting intellectual merger between their openness to technological innovations on the one hand, and the defense of the traditional Ottoman imperial structure on the other. But every single reform initiated by the Ottoman Empire faced backlash, either because they were seen as superficial or introduced at the request of external powers. As a result, these reform initiatives were either delayed or implemented long before society was ready for them, which had a number of consequences.

The second Crimean War of 1854–1856, which took place after the Tanzimat reform, led to the Imperial Reform Edict of 1856, which granted equal rights to minorities in the Empire.[3] This was seen as another attempt at modernization, albeit one that was carried out under external pressure – from France and Great Britain – in exchange for their support with funds and weapons during the war. The first constitutional era 20 years later, in 1876–1878, forced the Ottomans accept the need for profound modernization if they wanted to be embraced by the European family.[4] Acceptance of this constitutional legitimacy led to the emergence of a new political class of governmental bureaucrats, although it was short-lived.

Sultan Abdul Hamid II (1876–1918) was an anti-reformist who abolished the previous constitutional innovations and essentially became a symbol of three decades of staunch conservatism.[5] Nevertheless, the two years of constitutionalism shaped life of Ottoman politics in the long term, and paved the way for the second constitutional era in 1908, with traditional Ottoman life becoming more open to innovations, including the creation of the Republic several years later. We can thus state that in the 19th century, conservatism in the Ottoman Empire was reactive in nature, a movement to preserve the traditional ways of social life, whereas conservatism in the 20th century had started to take on a more developed and ideological form.[6]

1908 marked the beginning of the second constitutional era, during which the Ottoman Empire was on the losing side in the First World War and was ultimately

1 Can 2016.
2 Mardin 2015.
3 Aytekin 2013.
4 Hanioğlu 2010.
5 Ahmad 1991.
6 Ahmad 1986.

destroyed and captured by occupying powers. Resistance against foreign powers, the abolition of the Sultanate and the establishment of the Republic – all this was an extension of the debate on what should and should not have been accepted from the West.

Mustafa Kemal Ataturk, the founding father of the Turkish Republic, believed in modernizing his country, which worried the traditional religious circles of the former empire. For Ataturk, religion was associated with backwardness, hence the most extreme forms of secularization were supported. The Latinization of the Ottoman script in 1928 as part of numerous other reforms eventually led to an increase in literacy levels – from 10% according to the population census in 1927, to 30% 14 years later.[1]

The views of Turkish Islamists and religious conservatives were mainly influenced by the 1979 Iranian Revolution and the literature of the Muslim Brotherhood, although in Turkey itself, no one questioned its own, "special" path. The first anti-Western religious-conservative force, the National Salvation Party (*Milli Selamet*/MSP), came to power in 1973 under the leadership of N. Erbakan. With the assistance of various coalitions in the parliament, they succeeded in determining or significantly influencing Turkish policy for many years. The MSP would never be accused of being liberal – on the contrary, the party always demonstrated a strong anti-Western conservative attitude,[2] and it never advocated for the development of Turkish democratic institutions. However, N. Erbacan's ousting by the military on February 28, 1997 and the closure of his Welfare Party (*Refah Partisi*) propelled him to the forefront of Turkey's modernization effort.

N. Erbakan, who earned his degree in engineering in Germany, pushed for the development of heavy industry, as well as the construction of iron and steel plants and the establishment of the motor, electronics and electromechanics industries in 1976. Driven by the desire to industrialize the country, N. Erbakan also believed that it should be freed from technological dependence on the West. This was why he was so open to cooperation with the Soviet Union as an alternative for the nascent Turkish industry.

Between 1998 and 2001, young politicians such as R.T. Erdogan, A. Gul, B. Arınc, and others formed a splinter group from the supporters of N. Erbakan, which later on became the Justice and Development Party (AKP). As religious conservatives, they were ready to make compromises with the West – to "get engaged" and yield to the forces of liberalism and globalism. In 2001, the conservative AKP came to power on the back of slogans about liberalizing the economy, human rights, and the constitution. Later in the R.T. Erdogan era, the right began to be dominated by religious rhetoric, with some of those right circles being in opposition to modernization as a whole.

The core motive of R.T. Erdogan's tenure (2001–2020) was the need for technology transfer. Having a strained relationship with the West, especially with the United States, and unable to persuade its Western partners to transfer their technologies or engage in joint R&D projects, R.T. Erdogan turned to Russia and China, which became not only

1 Orhan Bursali, "Osmanlı'da okuma yazma bilenlerin sayısı çok muydu? (Were there many literate people in the Ottoman Empire?)," Cumhuriyet, September 14, 2019, accessed February 17, 2021, https://www.cumhuriyet.com.tr/yazarlar/orhan-bursali/osmanlida-okuma-yazma-bilenlerin-sayisi-cok-muydu-1701918.

2 Tezcan et al. 2015, 1.

ideological, as some might claim, but also technological partners, since the West was not open to sharing. In recent years, Turkey's military industry breakthrough and the domestic production of tanks, helicopters, ships, and unmanned aerial vehicles (UAV),[1] as well as the boom in the domestic automobile industry, evidence the country's strategy to revise its relations with the West and reduce technological dependence on it. The purchase of Russian S-400 missile systems, with the promise if technological transfer, and the construction of nuclear power only underline this policy.

Current discourse in Turkey focuses on the nature of conservatism. R.T. Erdogan's statements about the loss of healthy conservatism are scrutinized in the Turkish press, and many arguments about right-wing conservative views are brought up when discussing culture, socio-political life, and even architecture. So far, Turkish conservatism has been unable to "marry" itself to liberalism, and the discussion of Turkey's stance vis-à-vis the West continues.

It should be noted that Turkey stands out in the Islamic world in that it has a healthy economy (albeit with certain flaws) with strong industrial production, including in the military sphere. The Russian scholar N. Ivanov noted that Muslim civilization, especially the Ottomans as the main candidate for global leadership, had a highly developed and professional army and advanced weaponry, on a par with European armies, up until 1571.[2] However, this topic was often imported to Russian discourse from abroad, initially as a response to the attempts to challenge Muslim civilization as a whole, and later in order to support the universal discussion within the global Muslim community about the ability of Muslims to not only adopt the fruits of technological progress, but also to be innovative themselves.

Religious debates were typically restricted to narrow circles, especially in the harshly secularist republican period. Rather, modernization and the understanding of the need for technological progress can be explained by the Ottoman encounter with more powerful adversaries and their further attempts to compel the Empire to modernize politically. In the modern period, the quest for technological development exists side-by-side with the need for technology transfer, as well Turkey's leading efforts in technological advancement as a part of the larger Islamic world.

Iran: from Modernization to Islamization

The example of Iran presents a good opportunity to test how the change in a country's orientation toward Islam in terms of its legislation and societal norms and regulations affected its standing as an emerging technological leader in the Middle East. In the modern era, the founder of the last dynasty that existed before the Islamic Revolution in 1979, Reza Pahlavi, was seen as the driving force behind the country's all-embracing modernization of the 20th century. In order to overcome resistance to modernization, however, he had to eliminate conservative religious opposition, since his modernization plan essentially meant Westernization, which thus triggered a backlash in religious circles.

1 Guc Gonel, "Turkey becoming engine design, manufacturing hub," Anadolu Agency, December 5, 2020, accessed February 17, 2021, https://www.aa.com.tr/en/economy/turkey-becoming-engine-design-manufacturing-hub/2066665#.
2 Рыбаков et al. 1999, 44.

Reza Pahlavi's policy then included both co-option, or buying the friendship of influential *ulama*, and suppressing those who adopted an uncompromising stance toward modernization. The government spent great efforts to demonstrate the compatibility of modernization with Islam and introduced a distinction between "progressive" ulama, who supported modernization and reforms, and "backwards" ulama who did not, into the public discourse.[1]

Earlier, in 1851, the renowned Qajar Chief Minister known as Amir Kabir (Mirza Taghi Khan Farahani), pushing for the same development agenda, established *Dar al-Funun* (polytechnic college), the first institution of higher learning in Iran, which was later incorporated into the university of Tehran. Remarkably, the Western educated elite of Amir Kabir's time paid attention to "human factories" as "the institutions that foster, guide, and manage human activities," practically giving them a higher importance than the factories themselves.[2]

In 1981, amidst the ongoing cultural transformation, the leader of the Iranian Revolution Ayatollah Ruhollah Khomeini declared the need to transform the country's education system, develop different academic programs and formulate the future of universities.[3] Currently, the policies related to science and technology undergo vetting by religious bodies (by the Guardian Council, as well as directly or indirectly by the Supreme Leader), which means that they are at least acknowledged as compliant with the Islamic worldview in terms of its interpretation by the Islamic Republic.[4]

That said, Iran is doing better than other countries in the Muslim world in terms of academic achievement and technological advancement. According to the World Bank, Iran ranked 38th in the number of patents registered in 1970, compared to 7th in 2016.[5] Technological development was named as one of the country's three main national priorities for the period 2016 to 2021.[6] Despite the international sanctions, research and development budgets are set to receive a 400% increase by 2030, reaching 4% of GDP,[7] even though this was expected to take place as a result of the nuclear deal signed in 2015.

There are, however, still a number of drawbacks to Iran's desire to speed up progress in the country. Iran's annual brain drain is estimated at 150,000 specialists,[8] while there are not enough resources to lure these people back to the country. There are also doubts about the quality and effectiveness of Iranian publications in recent decades. According to the Thomson Reuters database, Iranian papers make up just 2.9% of the top 1% of cited papers in 2016.[9]

1 Faghfoory 1993, 280.
2 Semati 2016, 328.
3 Goodarzi 2013, 420.
4 Heshmati 2019.
5 "Iran after the Islamic Revolution: Scientific backtrack or progress? What do the statistics say?" Tehran Times, February 10, 2019, accessed February 11, 2021, https://www.tehrantimes.com/news/432798/Iran-after-the-Islamic-Revolution-Scientific-backtrack-or-progress.
6 "Leader declares outlines of the 6th five-year plan with emphasis on resistance economy, scientific progress," Tehran Times, July 1, 2015, accessed February 11, 2021, https://www.tehrantimes.com/news/247790/Leader-declares-outlines-of-the-6th-five-year-plan-with-emphasis.
7 "S. Leader: Iran's scientific movement to continue non-stop," IRNA, July 3, 2014, accessed February 11, 2021, https://en.irna.ir/news/81223992.
8 "Iran loses $150 billion a year due to brain drain," Mehr News, January 8, 2014, accessed February 11, 2021, https://en.mehrnews.com/news/101558/Iran-loses-150-billion-a-year-due-to-brain-drain.
9 Heshmati 2019, 567.

The actual spending on R&D also remains unclear, and probably does not surpass 1%. UNCTAD also indicates that the share of private investment in R&D is relatively low in Iran (20% of R&D expenditure in 2010). Exports of hi- and medium-tech products accounted for 1% and 30.7%, respectively, of the country's total exports (S&T Vice-Presidency, 2016). According to the high level policy documents, the share of the knowledge-based economy, and thus of hi-tech exports should reach 50% by 2025.

The official rhetoric of the Islamic Republic maintains that Islam is a religion that promotes science and this explains why the country is moving up the rankings of science publications in aerospace, medicine and nuclear technology, despite even deliberate attacks against its nuclear scientists,[1] with the latest being undertaken in November 2020.

One might suggest that the difference in the Iranian discourse, even after the Islamic Revolution of 1979, was pointed out by modernists of the Sayyid Jamal al-Din Asadabadi (better known as al-Afghani) school, who claimed that Muslims could adopt Western science and technology while remaining true to their Muslim traditions and identities.[2] Ali Shariati, another thinker whose works laid grounds for the Islamic Revolution, echoed al-Afghani in the sense that even though one might criticize Western thought, the approach to science and technology must be pragmatic – a quality that the Islamic Republic later proved to have. According to Shariati, in Islam, "science and wisdom" are criteria of "finding truth" and "studying science is a necessary and *vajib* [mandated by religion] duty for all Muslim."[3]

Different pathways of intellectual development backed by a rather liberal attitude to ijtihad and the necessity to constantly apply reason, as well as the configuration of relations between society and the governing elites, brought a set of attitudes to existence in Iran that were different to those in the Arab or Sunni clusters of Islamic civilization. This difference persisted through the R. Pahlavi period into the Islamic Republic. However, the drawn-out war with Iraq and further sanctions against Iran's nuclear program and certain aspects of its foreign policy limit our ability to assess the technological heights it could have risen to, had the political limitations not been put in place.

Conclusion

Speaking of numbers, not a single university in the Muslim world is in the top 100 universities in the world.[4] OIC states contribute to less than 1% of all global academic publications in science, and the quality of that is questionable. Iran and Malaysia were in the top 20 in terms of the number of academic publications in science and technology in 2016, but this achievement is not stable from year to year.[5] According to the latest Coursera report conducted on various sets of skills among the millions of

1 "Iran after the Islamic Revolution: Scientific backtrack or progress? What do the statistics say?" Tehran Times, February 10, 2019, accessed February 17, 2021, https://www.tehrantimes.com/news/432798/Iran-after-the-Islamic-Revolution-Scientific-backtrack-or-progress.
2 Semati et al., 2016.
3 Ibid., 334.
4 "The World University Rankings," The World University Rankings, accessed February 11, 2021, http://surl.li/lbdz.
5 "Scientific and technical journal articles – Country Ranking," Index Mundi, accessed February 11, 2021, https://www.indexmundi.com/facts/indicators/IP.JRN.ARTC.SC/rankings.

learners it attracts, the only Muslim majority country marked as "emerging" in terms of technological skills is Malaysia (in 43rd place). The United Arab Emirates, Saudi Arabia and Turkey are lagging behind in 50th, 54th and 55th, respectively.[1]

Technological progress hinges upon ability of a society to grow human capital. Research conducted by the World Bank has revealed that Muslim countries spend, on average, approximately 0.5% of their GDP on research and development, compared to the global average of 1.78% of GDP and the OECD average of above 2%. Meanwhile, the number of people working in scientific fields in the Muslim world is also well below the global average.[2]

The number of women working in science and technology is not great, as tradition affects the perception of women and their acceptance into the workforce. This raises questions not only about the education system and its methodologies and curricula, but also about the further integration of talent into the workforce. The education systems across the Muslim world have repeatedly been criticized for their lack of "inquiry-based" and "active-learning" approaches, as well as for the need to stimulating critical thinking.

A study conducted by C. Issawi into how the Islamic world was able to at least adopt advanced Western practices, like water and wind mills, in order to optimise the production of energy (and, in turn, production in general) could not offer a concrete answer as to why the technology, while being known, did not spread widely enough in Muslim lands up until the end of 19th century. Comparing 16th century Ottoman Empire, at the height of its prosperity, to 11th century England, he concludes that the former nevertheless had fewer water mills than the latter.[3] Today, a number of Islamic countries have moved to hydrocarbons, and many of the least developed countries (LDCs) have started to import technologies from the developed world, and life has become much easier. However, the Islamic world grapples with the more pressing problem of growing human capital catching up with the ever increasing technological advancement. While the institutionalization of certain disciplines and how they are taught is highly important, the underlying fundamentals stemming from culture and religion facilitated that process in the past and continue to affect the way education and science develop today.

The practical development of knowledge, science and the ability to innovate were tied to the existing traditions in Muslim societies, but the debate outlined above regarding the philosophical grounds was not always a major factor that defined success or failure in that regard. The cases of Iran and Turkey demonstrate that self-awareness about own backwardness came from the outside, especially when an encounter with military adversaries left Muslim armies at loss, because they were not technologically advanced. However, the influence or interference of external powers sometimes fortified the traditional resistance to change, partly because modernization and progress were seen as Westernization and the loss of identity or sovereignty.

1 "Global Skills Index," Coursera, 2020, accessed February 11, 2021, https://www.coursera.org/gsi.
2 Nidhal Guesoum, "Why the Islamic world needs a new 'golden age'," World Economic Forum, January 14, 2016, accessed February 11, 2021, https://www.weforum.org/agenda/2016/01/why-the-islamic-world-needs-a-new-golden-age.
3 Issawi 1991, 284.

When it comes to the discussions about the ability of societies to progress, quantitative indicators are often used as a way to track changes and draw comparisons between developed and less developed states. Meanwhile, even with the emergence of technological marvels and globalization, the ability of innovative practices to travel did not lead to the creative potential of humanity spreading evenly around the globe. We argue that a variety of factors, some of which are related to the way that religious discourse evolved in the Islamic world, affected institutional structures, education, and ultimately the way human capital is cultivated, and predefined the state in which the Muslim *ummah* (community) finds itself at the moment. It must be acknowledged that in some cases, political factors, especially external, shaped the way Islamic communities perceived modernization, which may have been associated with Westernization and thus with a breach of sovereignty, exploitative intentions or the destruction of traditional identity. And the case of Turkey is a good example of this. We also saw that Islamic societies produced bright progressive minds even after the so-called "Golden Age" of Islam, but that effort could be disrupted by other factors, as the case of Iran has shown.

Depending on the cultural path taken by a particular country, the relation between Islam as the religious backbone of society and Islam as the cultural code of society could be conducive to at least adopting innovations. It could also be disruptive to the same process, not to mention the ability of people to innovate themselves. In some intellectual circles across the Islamic world, the debate on the fundamentals – such as the need for Islam to undergo a revival of its own (a "reopening of the gates of ijtihad") and return to the intellectual tradition that was cherished during the "Golden Age" and is still alive and in the minds of religious scholars, some of whom have a strong influence on believers – must serve as the basis of how policies on science and technology are formulated. For some reason, the inability to break out of this essentially theological debate on progress is precisely what prevents the unrestrained cultivation of human potential that is necessary for the Islamic world if it wants to catch up with its advanced civilizational adversaries of the past.

Despite all the research into these matters and our daily engagement with these issues, we have to conclude that practice has not dispelled the seemingly superficial idea that progress and innovation require a secular approach, while calls for revival of reason within Muslim thinking and the Muslim way of life do not yield anything feasible. This justifies our choice to observe the relatively successful examples of Turkey and Iran. Even though the latter is currently governed by a somewhat hybrid theocratic regime, its approaches to science, technology, and academic advancement are rather pragmatic and aimed at cultivating national pride and the nationalist part, rather than the religious part, of the country's identity. This is why the quest for knowledge and discovery is less hindered by the theological debate in these countries.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

История Востока в шести томах. Т. 3. Восток на рубеже Средневековья и Нового времени. XVI—XVIII вв. / Под редакцией Р.Б. Рыбакова. – М.: Издательская фирма «Восточная литература» РАН, 2000. – 696 с. [*The History of the East. Vol. III. The East at the Turn of the Middle Ages and the Modern Age. The 16th–18th centuries* [Istoriya Vostoka v shesti tomah. T. 3. Vostok na rubezhe Srednevekov'ya i Novogo vremeni. XVI—XVIII vv], edited by R.B. Rybakov. Moscow: "Oriental Literature" Publishing Company RAS, 2000] [In Russian].

AbuSulayman, AbdulHamid. *Crisis in the Muslim Mind*, translated by Yusuf Talal DeLorenzo. Herndon: The International Institute of Islamic Thought, 1993. https://iiit.org/wp-content/uploads/Crisis-in-The-Mind-Complete.pdf.

Ahmad, Feroz. "Politics and Islam in modern Turkey." *Middle Eastern Studies* 27, no. 1 (1991): 3–21.

Ahmad, Feroz. *İttihat ve Terakki 1908–1914* [Union and Progress 1908–1914]. Kaynak, 1986 [In Turkish].

Akyıldız, Ali. "Sened-i İttifak'ın ilk tam metni." [First full text of the Sened-i Alliance] *İslam Araştırmaları Dergisi* 2 (1998): 209–222 [In Turkish].

Akyıldız, Ali. "Sened-i İttifak'ın ilk tam metni." [First Full Text of The Sened-i Alliance]. *İslam Araştırmaları Dergisi* 2 (1998): 209–222 [In Turkish].

Al-Alwani, Shaykh Taha Jabir. *Issues in Contemporary Islamic Thought*. London: The International Institute of Islamic Thought, 2005. https://iiit.org/wp-content/uploads/IssuesinContemporarIslamicThought_Combined.pdf.

Al-Ghazali, Abu Khamid. *Tahafut Al-Falasifah* [Incoherence of the Philosophers]. Lahore: Pakistan Philosophical Congress, 1963 [In Turkish].

Aytekin, Attila E. "Tax Revolts during the Tanzimat Period (1839–1876) and before the Young Turk Revolution (1904–1908): Popular Protest and State Formation in the Late Ottoman Empire." *Journal of Policy History* 25, no. 3 (2013): 308–333.

Berkez, Niyazi. *Türkiye'de Çağdaşlaşma* [Modernization in Turkey]. İstanbul: YKY, 2019 [In Turkish].

Can, İslam. "Merkez-çevre düalizmi bağlamında taşranın onto-politik doğası üzerine çıkarımlar." [Inferences on the Onto-political Nature of the Province in the Context of Center-Environmental Dualism] *Selçuk Üniversitesi Edebiyat Fakültesi Dergisi*, no. 36 (December 23, 2016): 531–531. https://doi.org/10.21497/sefad.285501. [In Turkish].

Chapra, Muhammad Umer. *The Islamic Vision of Development in the Light of Maqāsid al-Sharīah.* London: The International Institute of Islamic Thought, 2008. http://surl.li/lbcp.

Emecen, Feridun M. "Matruşka'nın Küçük Parçası: Nevşehirli Damat İbrahim Paşa Dönemi Ve 'Lale Devri' Meselesi Üzerine Bir Değerlendirme." [A Small Part of Matrushka: an Assessment of the Era of Nevşehirli Damat Ibrahim Pasha And the 'Tulip Era' Issue] *Osmanlı Araştırmaları* 52 (2018): 79–98 [In Turkish].

Faghfoory, Mohammad H. "The Impact of Modernization on the Ulama in Iran, 1925–1941." *Iranian Studies* 26, no. 3–4 (September 1993): 277–312. doi:10.1080/00210869308701803.

Goodarzi, Mehdi, and Soroush Ghazinoori. "From Developing a Higher Education System to Moving toward a Knowledge-Based Economy: A Short History of Three Decades of STI Policy in Iran in Science and Innovations." In *Iran: Development, Progress, and Challenges,* edited by Abdol S. Soofi, and Sepehr Ghazinoory. New York: Palgrave Macmillan, 2013.

Gunce, Suheda. "Osmanlı Devleti'nde İlk Daimi Elçilikler ve Diplomasiye Olan Etkileri." [The first permanent embassies in the Ottoman Empire and their influence on diplomacy] *Osmanlı Medeniyeti Araştırmaları Dergis*i 6, no. 10 (April 15, 2020): 101–14. doi:10.21021/osmed.668921 [In Turkish].

Hallaq, Wael B. "Was the Gate of Ijtihad Closed?" *International Journal of Middle East Studies* 16, no. 1 (March 1984): 3–41.

Hanioğlu, Şükrü. *A brief history of the late Ottoman Empire*. Princeton: Princeton University Press, 2010.

Heshmati, Ata, and Seyed Mehran Dibaji. "Science, Technology, and Innovation Status in Iran: Main Challenges." *Science, Technology and Society* 24, no. 3 (November 11, 2019): 545–78. doi:10.1177/0971721819873192.

Hoodbhoy, Pervez. *Islam and Science.* London: Zed Books Ltd., 1991.

Hussein, Taha. *The Days: His Autobiography in Three Parts.* Cairo: American University in Cairo Press, 1997.

İnalcık, Halil. *Osmanlı Tarihinde İslamiyet ve Devlet* [Islam and the State in Ottoman History]. Istambul: Türkiye İş Bankası Yayınları, 2019 [In Turkish].

Inglehart, Ronald, and Baker Wayne E. "Modernization, Cultural Change, and the Persistence of Traditional Values." *American Sociological Review* 65, no. 1 (February 2000): 19–51.

Islamic Perspectives on Science and Technology, edited by Mohammad Kamali, Mohammad Hashim, Osman Bakar, Daud Abdul-Fattah Batchelor, and Rugayah Hashim. Singapore: Springer Singapore, 2016. doi:10.1007/978-981-287-778-9.

Issawi, Charles. "Technology, Energy, and Civilization: Some Historical Observations." *International Journal of Middle East Studies* 23, no. 3 (August 29, 1991): 281–89. doi:10.1017/S0020743800056300.

Kalayci, Murat. "Şeyhülislam Mehmed Esad Efendi ve Eşarîlik-Maturidîlik İhtilafına İlişkin Risalesi." [Şeyhülislam Mehmed Asad Efendi and his treatise on the Asharilik-Maturidilik conflict] *Hitit Üniversitesi İlahiyat Fakültesi Dergisi* 11, no. 21 (2012): 99–134 [In Turkish].

Kara, İsmail. *Cumhuriyet Türkiyesi'nde Bir Mesele Olarak İslam 1* [Islam as a Matter In Republican Turkey 1]. İstanbul: Dergah Yayınları, 2019 [In Turkish].

Kara, İsmail. *Din İle Modernleşme Arasında Çağdaş Türk Düşüncesinin Meseleleri* [Issues of Contemporary Turkish Thought Between Religion and Modernization]. İstanbul: Dergah Yayinlari, 2020 [In Turkish].

Kuzucu, Serhat. "Katerina Donemi Osmanlı-Rus İlişkilerinde Kırım." [Katerina Donemi Crimea in Ottoman-Russian Relations] *Türk Dünyası Araştırmaları* 185, 2010 [In Turkish].

Mardin, Şerif. *Yeni Osmanlı düşüncesinin doğuşu* [Birth of New Ottoman Thought]. İstanbul: İletişim Yayınları, 2015 [In Turkish].

Mardin, Şerif. *Yeni Osmanlı düşüncesinin doğuşu* [Birth of new Ottoman thought] İletişim Yayınları, 2015 [In Turkish].

Mazanec, Jakub. "The Ottoman Empire At The Beginning Of Tanzimat Reforms." *Prague Papers On The History Of International Relations* 2 (2016): 21–45.

Muhammad Naquib al-Attas, Syed. *Islam and Secularism.* Kuala Lumpur: Muslim Youth Movement of Malaysia, 1978.

Ortaylı, İlber. *Mekanlar ve Olaylarıyla Topkapı Sarayı* [Venues and events, Topkapi Palace]. İstanbul: Kaynak Kitapliği, 2007 [In Turkish].

Ortaylı, İlber. *Türkiye İdare Tarihi* [Administrative History of Turkey]. Ankara: Cedit Neşriyatı, 1979 [In Turkish].

Peters, Francis Edward. *Judaism, Christianity, and Islam: The Classical Texts and Their Interpretation, Volume III: The Works of the Spirit*. Princeton: Princeton University Press, 2018.

Sayyid Jamal al-Din al-Afghani. "Response to Renan." In *Modernist Islam,* 1840-1940: *A Sourcebook,* edited by Charles Kurzman. Oxford: Oxford University Press, 2002.

Semati, Mehdi, Mehdi Faraji, and Yalda N. Hamidi. "Elite Discourse on Technology in Iran."

Sociology of Islam 4, no. 4 (October 21, 2016): 323–44. doi:10.1163/22131418-00404002.

Sen, Amartya. *Development as Freedom*. New York: Anchor Publishing, 2000.

Sezgin, Fuat. *İslam'da Bilim ve Teknik* [Science and Technology in Islam]. Ankara: Türkiye Bilim Akademisi, 2015 [In Turkish].

Tanpınar, Ahmet H. *On Dokuzuncu Asır Türk Edebiyatı Tarihi* [History of Nineteenth Century Turkish Literature]. İstanbul: Dergah Yayinlari, 2012 [In Turkish].

Tezcan, Ercüment, and Aras Ilhan. "Adalet Ve Kalkınma Partısı'nde Euroseptısızm: Avrupa Bırlıgı Destegının Elestırıye Dönüsümü." [Euroscepticism in The Justice and Development Party: From Support to Criticism of the European Union] *Uluslararasi Hukuk Ve Politika* 11, no. 41 (2015): 1–35 [In Turkish].

Türköne, Mümtazer. *Türk Modernleşmesi* [Turkish Modernization]. İstanbul: Lotus Yayinevi, 2003 [In Turkish].

Ülken, Hilmi Ziya. *Türkiye'de Çağdaş Düşünce Tarihi* [History Of Contemporary Thought In Turkey]. İstanbul: Türkiye İş Bankası, 2019 [In Turkish].

Watt, Montgomery. *The Faith And Practice Of Al-Ghazali*. London: George Allen And Unwin Ltd., 1953.

Yıldız, Hasan. "Osmanlı Medreselerini Islah Çabaları Üzerine Bir Değerlendirme." [An Assessment of Efforts to Reform Ottoman Madrasas] *Vakanüvis-Uluslararası Tarih Araştırmaları Dergisi,* 4(1), 2019: 407–445 [In Turkish].

Authors

Julia Roknifard,

PhD in the History of International Relations, Assistant Professor, School of Politics, History and International Relations (PHIR), University of Nottingham Malaysia (Kuala Lumpur), Jalan Broga, 43500 Semenyih Selangor Darul Ehsan Malaysia.

e-mail: julia.roknifard@nottingham.edu.my

Orhan Gafarli,

PhD in International Relations, Postdoctoral Researcher, Research Center for International Political and Economic Relations (IPER), Ankara University, Siyasal Bilgiler Facultesi, Cemal Gursel Cad., Cebeci, 06590, Ankara, Turkey.

e-mail: orxan.qafarli@gmail.com

Leslie Terebessy,

Academic, former Research Fellow at the International Institute of Advanced Islamic Studies (IAIS), P.O. Box 12303, Pejabat Pos Besar, 50774 Kuala Lumpur, Malaysia.

e-mail: ljterebessy@gmail.com

Additional Information

Received: November 5, 2020. Accepted: November 29, 2020.

Disclosure statement

No potential conflict of interest was reported by the authors.

For citation

Roknifard, Julia, Orhan Gafarli, and Leslie Terebessy. "Islam and Progress: Between Tradition and Modernity." *Journal of International Analytics* 11, no. 4 (2020): 104–121. https://doi.org/10.46272/2587-8476-2020-11-4-104-121

Ислам и прогресс: между традицией и современностью

АННОТАЦИЯ

В ходе переосмысления того, как мусульманские общины исторически реагировали на прогресс и интегрировали его достижения в свою жизнь, авторы статьи попытались вернуться к причинам, по которым исламский мир сохранил глубокий разрыв между традицией и современностью. Анализируя дискуссии мусульманских мыслителей и теоретиков прошлого в богословских и околобогословских кругах, сделан вывод о том, что одним из главных, с философской точки зрения, вопросов для обсуждения является то, что религия стала ассоциироваться больше не с богооткровением, а с традицией. Религия учит непереходящим принципам, в то время как традиции связаны с практиками прошлого, которые привязаны к времени. Значительной части мусульман сложно адаптироваться к новой реальности, и это связано с тем, что религиозность стала ассоциироваться с феодализмом и традиционными ритуалами. Следовательно, мусульмане зачастую связывают сохранение верности своему наследию с внешними признаками, например, с манерой одеваться или совершением ритуалов, при этом не осознавая своей духовной цели или не относясь к ней со всей честностью. Хотя можно было бы дискурсивно отделить религию от области политики, в данной статье тем не менее исследуется, как мусульманский мир переживал застой из-за слияния традиции и богооткровения и как данное слияние парализовало развитие, наряду с другими факторами, такими как конфигурация систем, отвечающих за развитие человеческого капитала, наличие политических интересов и влияние внешних сил. На основе анализа специфики модернизации в Турции и Иране в статье выделяются тенденции, которые препятствуют технологическому прогрессу в странах исламского мира.

КЛЮЧЕВЫЕ СЛОВА

ислам, исламский мир, технический прогресс, иджтихад, инновации, Иран, Турция

Сведения об авторах

Юлия Рокнифард,
доктор философии в области международных отношений,
доцент Школы политики, истории и международных отношений Ноттингемского университета Малайзии (Куала-Лумпур), Джалан Брога, 43500 Семеных Селангор Дарул Эхсан Малайзия.
e-mail: julia.roknifard@nottingham.edu.my

Орхан Гафарлы,
доктор философии в области международных отношений,
преподаватель факультета коммуникаций, Университет Анкары, факультет политологии,
шоссе Джамал Гюрсел, квартал Джебечи, 06590, Анкара, Турция.
e-mail: orxan.qafarli@gmail.com

Лесли Теребесси,
исследователь, бывший научный сотрудник Международного института передовых исламских исследований, 12303, Главное почтовое отделение, 50774 Куала-Лумпур, Малайзия.
e-mail: ljterebessy@gmail.com

Дополнительная информация

Поступила в редакцию: 5 ноября 2020. Принята к публикации: 29 ноября 2020.

Конфликт интересов

Авторы заявляют об отсутствии потенциального конфликта интересов.

Цитирование

Рокнифард, Ю., Гафарлы О., Теребесси, Л. Ислам и прогресс: между традицией и современностью // Международная аналитика. – 2020. – Том 11 (4). – С. 104–121.
https://doi.org/10.46272/2587-8476-2020-11-4-104-121

Стратегическое значение фармацевтической отрасли в условиях пандемии коронавируса

Заур Аязович Мамедьяров

https://doi.org/10.46272/2587-8476-2020-11-4-122-136

АННОТАЦИЯ

Особое значение фармацевтической отрасли для научно-технического и экономического развития стран обусловливает ее включенность в международные процессы. В работе основное внимание уделяется анализу тенденций в фармацевтической сфере и биотехнологиях в условиях пандемии COVID-19. Пандемия обострила такие проблемы отрасли, как эффективность распределения медикаментов между гражданами, зависимость крупных производителей от поставщиков активных субстанций из Китая, ценообразование на медикаменты и роль социальных систем страхования в развитых и развивающихся странах. Автор также выделяет такие области роста конкуренции, как диверсификация поставок активных фармацевтических субстанций, разрешение регуляторами доступа новейших препаратов к рынку, конкуренция фармацевтических компаний за капитал и компетенции. В статье проведен анализ основных проблем отрасли на примере рынка вакцин COVID-19 и представлены возможные траектории дальнейшего развития фармацевтики и биотехнологий в международном контексте.

КЛЮЧЕВЫЕ СЛОВА

фармацевтика, инновации, конкуренция, регулирование, исследования и разработки, технологии, COVID-19

CC BY

Пандемия COVID-19 всё чаще становится предметом анализа исследователей-международников, а центральными темами таких работ, как правило, выступают: международная безопасность[1], влияние пандемии на темпы глобализации[2], международно-политический дискурс[3] и рост национализма[4]. В меньшей степени исследователи изучают влияние пандемии на технологическую конкуренцию стран[5], хотя эта сфера является значимой с точки зрения «пространства» международно-политической конкуренции[6]. Дискуссию о влиянии технологий на межгосударственную конкуренцию в эпоху пандемии представляется актуальным рассмотреть в контексте развития фармацевтической отрасли.

Фармацевтическая промышленность и биотехнологии относятся к наиболее наукоемким и стратегически важным отраслям мировой экономики. За последние десять лет данный сектор демонстрирует ежегодный прирост на 4–7%, и его объём уже превышает 1 трлн долл. США по совокупному объему ежегодно реализуемой продукции[7]. В то же время отрасль сталкивается с постоянно растущей инновационной конкуренцией в первую очередь со стороны производителей из Китая, Индии, Турции и иных развивающихся стран, а также с дисбалансами в ценообразовании и приоритизации исследовательской деятельности. Так, инновационные процессы в отрасли в основном приходятся на несколько десятков крупнейших транснациональных компаний (ТНК) «большой фармы», которые поддерживают исследования в компаниях малого и среднего бизнеса, покупая их разработки и/или поглощая такие компании. При этом наибольшую прибыль приносят препараты с долгим сроком эффективного патентования, и такие препараты направлены, как правило, против редких (и крайне редких – *орфанных*) заболеваний, распространенность которых существенно ниже заболеваний, все еще актуальных для подавляющего числа жителей планеты из развивающихся стран.

Именно успехи фармацевтической отрасли в развитых странах за последние пятьдесят лет, решившие проблему распространенных инфекционных заболеваний, позволили крупнейшим ТНК с конца 1990-х гг. перевести свою деятельность в сферу редких и сложных заболеваний, особенно актуальных при всеобщем повышении средней продолжительности жизни. Таким образом, с одной стороны, возник определенный разрыв между развитыми и развивающимися странами, с другой – распространение влияния ТНК на региональные рынки позволило существенно поднять общий уровень систем здравоохранения в мире. При этом в целях повышения экономической эффективности в ТНК были внедрены такие подходы к работе, как использование офшоринга, аутсорсинга, механизмов нерыночной конкуренции[8], включая инструменты, направленные на удержание рыночной доли[9]. Так, в своих статьях У. Лазоник отмечает финансиа-

1 Drezner 2020; Lipscy 2020.
2 Yaya 2020; Bishop, Payne 2021.
3 Pan, Korolev 2021; McNamara, Newman 2020.
4 Woods et al. 2020; Pevehouse 2020.
5 Boylan et al. 2021; Miller, Smith 2021.
6 Kennedy, Lim 2018.
7 Lindsley 2018.
8 LaMattina 2012.
9 Vogler 2018.

лизацию фармацевтической отрасли – усиление роли финансовых мотивов, финансовых рынков и финансовых институтов в деятельности компаний[1]. По мнению Т. Клинге и Р. Фернандеса, финансиализация фармацевтических компаний характеризуется несбалансированной структурой рынка, при которой ряд крупных фармацевтических компаний доминирует в цепочках создания стоимости[2].

Тем не менее, как показывают исследования[3], рыночная концентрация в фармацевтической отрасли остается относительно низкой, конкуренция растет, а доля мирового лидера – США – постепенно сокращается. Более того, крупнейшие ТНК зависят от поставок активных фармацевтических субстанций (АФС) из узкой группы стран (преимущественно, Китая), что стало особо заметно в условиях пандемии COVID-19, когда пострадала даже Индия[4], поставляющая на мировой рынок АФС. Как следствие, в США и странах ЕС уже принимаются программы повышения конкуренции в сегменте поставок АФС. В целом же в отрасли обострение инновационной конкуренции наблюдается в течение последних двадцати лет. Место и роль России в этом процессе изучались такими исследователями, как А.В. Евстратов[5], Е.В. Нежникова, М.В. Максимчук[6], роль транснационального капитала и корпораций отрасли рассматривается А.В. Березным[7] и А.В. Кузнецовым[8].

Последствия пандемии COVID-19 для мировой фармацевтической отрасли включают в себя, с одной стороны, такие тенденции, как смещение спроса, пересмотр портфолио крупнейших исследовательских подразделений, изменение принципов проведения исследований и разработок, обострение конкуренции регуляторов разных стран, с другой – повышение роли открытой науки и цифровых технологий в исследованиях и производстве. Именно открытая наука и кооперация ученых из разных стран позволили[9] оперативно прояснить природу вируса SARS-CoV-2 и возможные пути борьбы с ним. При этом, как отмечается в работе Э. Торреэле, массовое производство вакцин, ставшее необходимостью в условиях пандемии, не укладывается в существующие бизнес-модели большинства фармацевтических ТНК[10]. Представляется, что в будущем в отрасли повысится значение регионализации и диверсификации поставок. Можно также ожидать замедления темпов роста фармацевтической промышленности, задержек с допуском к рынку препаратов из других стран, перехода к самообеспечению в цепочке поставок продукции.

Невозможность производителей лекарств в первые месяцы пандемии получать АФС с китайских фабрик стала для ведущих регуляторов крайне серьезной проблемой, хотя разговоры об этом велись много лет, и ранее поставки из Китая

1 Lazonick et al. 2019; Tulum, Lazonick 2018.
2 Klinge et al. 2020.
3 Richman et al. 2017.
4 Chatterjee 2020.
5 Евстратов 2018.
6 Нежникова, Максимчук 2019.
7 Березной 2018.
8 Кузнецов 2020.
9 Matt Apuzzo, and David D. Kirkpatrick, “Covid-19 Changed How the World Does Science, Together,” The New York Times, April 1, 2020, accessed February 15, 2021, https://www.nytimes.com/2020/04/01/world/europe/coronavirus-science-research-cooperation.html.
10 Torreele 2020.

нередко рассматривались как признак эффективности ТНК ЕС и США[1]. Учитывая рост конкуренции в отрасли, можно утверждать, что Китаю удалось фактически монополизировать мировое производство АФС (до 60% производства в стране). Аутсорсинг низкомаржинального бизнеса по производству АФС начался более тридцати лет назад, когда европейские и американские ТНК уступили эту нишу контрактным организациям по производству и разработке, некоторые из которых занимают позицию единственного поставщика целого ряда АФС на мировой рынок.

Фармацевтические компании США сталкивались с недостатком поставок АФС еще до пандемии, что приводило к дефициту препаратов первой необходимости. Пандемия актуализировала проблему децентрализации цепочек создания стоимости и повышения конкуренции за каналы поставок, так как кризис напрямую отразился на поставках медицинских товаров и на удорожании некоторых препаратов в связи с закрытием заводов, особенно в Китае. Те компании, которые имели запасы АФС в условиях пандемии, начали поставлять их по завышенным ценам. Проблема наблюдалась и в Индии, компании которой закупают больше всего АФС в Китае. По этой причине в стране было решено запустить программу повышения объемов, производимых в стране АФС. В России самообеспеченность АФС составляет менее 10%.

Не имея других надежных поставщиков АФС, ТНК полагаются на Индию в производстве непатентованных медикаментов, которые затем продаются под различными брендами, в том числе в США. Таким образом, в США признают, что точно не могут оценить объем ввозимых в страну из третьих стран АФС и реальную степень зависимости местных ТНК от китайских поставщиков, несмотря на продолжающееся торговое противостояние между США и Китаем. Ситуацию не спасло и заключение первой фазы торговой сделки в начале 2020 г., ключевое место в которой заняли вопросы интеллектуальной собственности применительно к фармацевтической отрасли. Именно эта сфера останется ключевым чувствительным элементом торговых и политических отношений США и Китая, так как именно биотехнологии и фармацевтика сохраняют первенство в инновационной активности и интенсивности исследований и разработок в мировой экономике.

Конкуренция в фармацевтической отрасли

К настоящему моменту в мировой фармацевтической отрасли сложилась система, в которой вывод новейших медикаментов на мировой рынок фактически определяется двумя регуляторами: Американским федеральным агентством по санитарному надзору за качеством пищевых продуктов и медикаментов (*Food and Drug Administration,* FDA) и Европейским агентством лекарственных средств (*European Medicines Agency,* EMA). Так как на ЕС и США вместе приходится почти 75% мирового рынка фармацевтической продукции, определяющим для работы глобальных фармацевтических компаний является получение доступа к рынку

1 Dierks 2013.

от обоих регуляторов. Это касается как инновационных (новейших) медикаментов, так и рынка препаратов-аналогов (дженериков), который стремительно растет в развитых и развивающихся странах благодаря успешной ценовой конкуренции. Однако, так как большую часть прибыли фармакологические компании извлекают из запатентованных медикаментов, именно в сегменте препаратов-брендов наблюдается наиболее острая технологическая и политическая конкуренция.

Так, уже многие годы ведется конкурентная борьба между регуляторами FDA и EMA за первенство в выводе препаратов на рынок с целью максимизации прибыли местных фармацевтических компаний. Более быстрые механизмы доступа новейших препаратов к рынку и выделение биотех-препаратов в отдельную категорию позволили американскому регулятору обеспечить лидерство США в большинстве фармацевтических инноваций (с точки зрения их коммерциализации). Таким образом, значение регуляторного фактора в работе отраслевых компаний ставит фармацевтику и биотех-сектор экономики в особое положение, связанное с широким контекстом международных процессов: от торговых войн и протекционизма до мягких нетарифных ограничений конкуренции. При этом фармацевтическая отрасль последние несколько десятилетий демонстрировала особое значение глобализации не только в сфере расширения рынков сбыта продукции, но и для рынков по привлечению компетенций: в отрасли высока активность слияний и поглощений, а появление все новых компаний обеспечивает привлечение квалифицированной рабочей силы, технологических ноу-хау и интеллектуальной собственности в крупнейшие фармацевтические транснациональные компании, что способствует инновационному процессу. Особо эффективно в связи с этим показал себя американский венчурный рынок и система электронных торгов *NASDAQ*, которые обеспечивают приток капитала в фармацевтическую отрасль и позволяют занимать биотех-компаниям лидирующие позиции в индексе.

Одним из значимых последствий пандемии стало ускоренное внедрение цифровых технологий в фармацевтику и здравоохранение, в частности в распределение лекарственных средств среди населения. Это является продолжением начавшегося в 1990-х гг. процесса, когда стимулом к внедрению цифровых технологий в отрасли стал ее естественный переход на новую технологическую парадигму (от химических – к биотех-препаратам и персонализированным/таргетированным медикаментам). Тогда стало ясно, что традиционные химические медикаменты со временем уступят по эффективности биотех-препаратам, в основе которых лежат достижения клеточной и молекулярной биологии. В то же время цифровизация отрасли и системы здравоохранения в целом подразумевает использование огромных объемов чувствительных персональных данных, а в этой сфере регулирование и политический дискурс в ЕС и США различаются весьма значительно. Если в ЕС регуляторы пытаются задать общемировые стандарты защиты пользовательских данных и решительно противопоставляют себя крупнейшим ТНК-монополистам в цифровой сфере, то в США корпоративные права существенно шире. Внедрение телемедицины в единый рынок ЕС–США будет требовать серьезных встречных шагов от конкурирующих регуляторов. Неготовность ряда сил в ЕС делать такие шаги быстро может быть заметна и по

темпам внедрения американских вакцин – в лидерах оказался Израиль и покинувшая ЕС Великобритания, тогда как в ЕС-27 регуляторные механизмы оказались для американской продукции более сложными.

Разработка современных медикаментов все чаще связана с генетическими особенностями того или иного организма и/или возбудителя заболевания, позволяющих найти наиболее эффективный ответ на болезнь. Но именно в силу вычислительной сложности моделирования живых систем новые механизмы создания лекарств все больше зависят от специальных алгоритмов, часто исполняемых с использованием суперкомпьютеров. Таким образом, фармацевтическая промышленность становится, во-первых, все более математизированной, а, во-вторых, все больше направленной на индивидуализацию лечения заболеваний. С одной стороны, фармацевтика все больше сращивается с ИКТ-компаниями, с другой – в перспективе возможен резкий рост конкуренции между ними за медицину будущего. Первенство США в построении таких цифровых компаний дает долгосрочное стратегическое преимущество фармацевтической отрасли страны. Не исключено, что в среднесрочной перспективе многие лекарства от рака и других тяжелых заболеваний будут создаваться под конкретного пациента, что потребует определенной перестройки бизнес-моделей компаний фармацевтической отрасли.

Фармацевтическая отрасль – основная цель для киберпреступников, охотящихся за интеллектуальной собственностью. В 2020 г. киберпреступность нанесла фармацевтической отрасли ущерб в размере 18 млрд долл.[1] Так, в Таблице 1 продемонстрированы итоги проведенного анализа проблем и путей их решения с помощью цифровых технологий в глобальную фармотрасль на основе отчетов за 2020 г. топ-10 крупнейших фармацевтических ТНК.

Таблица 1.

ПРОБЛЕМЫ И РЕШЕНИЯ В ФАРМАЦЕВТИЧЕСКОЙ И БИОТЕХ-ПРОМЫШЛЕННОСТИ
PROBLEMS AND SOLUTIONS IN THE PHARMACEUTICAL AND BIOTECH INDUSTRIES

Проблема	Сопутствующие проблемы	Решения
Низкая доступность ряда инновационных медикаментов	Старение населения, недостаточная автоматизация производственных площадок	Внедрение цифровой аналитики на производстве, развитие новой производственной инфраструктуры
Ужесточение регулирования на рынках сбыта продукции	Недостаток автоматизации документооборота, медленный уход от бумажных документов	Использование цифровых технологий отслеживания поставок, внедрение блокчейн-технологий
Необходимость персонализации здравоохранения	Вовлечение медиков и пациентов в процессы выработки приоритетов отрасли, отслеживание цифровых данных об эффективности препаратов в каждом терапевтическом случае	Технологии отслеживания поставок, цифровизация регулирования отрасли

1 "Cyber & Insider Risk at a Glance: The Pharmaceutical Industry," Deloitte, accessed February 15, 2021, https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/life-sciences-health-care/ls/jp-ls-cyber-insider-risk-en.pdf.

Проблема	Сопутствующие проблемы	Решения
Повышение качества продукции	Низкое качество дженериков, возможные негативные юридические последствия, репутация	Внедрение программного обеспечения по контролю за качеством
Снижение стоимости производства	Рост конкуренции на мировых рынках, дисбалансы в поставках, усиленная конкуренция для ТНК со стороны производителей дженериков	Внедрение технологий непрерывного производства, использований облачных технологий для хранения и обработки данных, внедрение робототехники на производстве

Источник: составлено автором.

Таким образом, учитывая сложившуюся высокую конкуренцию в фармацевтической отрасли как среди компаний, так и между регуляторами, можно ожидать, что в ближайшее время конкурентная борьба сместится в сторону цифровых технологий. В будущем возможна активизация сделок по поглощению фармацевтическими ТНК различных ИТ-стартапов, а также заключение новых соглашений о сотрудничестве между фармацевтическими компаниями и компаниями, разрабатывающими цифровые продукты. Кроме того, усилится противостояние между европейским и американским фармацевтическими рынками, так как цифровизация отрасли актуализирует вопросы использования и хранения персональных данных, подходы к которым различаются в США и ЕС.

Гонка вакцин как аспект противостояния стран

По данным организации *Regulatory Affairs Professional Society* (RAPS) на конец февраля 54 вакцины от вируса SARS CoV-2 находятся на различных стадиях клинических и доклинических испытаний[1]. В наибольшем числе стран получила одобрение вакцина *Pfizer-BioNTech*, которую разрешили к использованию в 61 государстве (включая США, Великобританию и все страны ЕС-27). Вакцина *AstraZeneca* получила одобрение в 51 стране (в том числе в ЕС-27 и Великобритании), а вакцина *Moderna* – в 39 странах (в том числе в США, Великобритании и ЕС-27). Российская вакцина «Спутник-V» одобрена в 30 странах.

Во многих странах разработка вакцины была объявлена национальным приоритетом; в работу над вакцинами были вовлечены не только фармацевтический сектор и академические круги, но и военная промышленность. Например, при участии американского Министерства обороны в США была запущена инициатива *Warp Speed Operation,* направленная на ускорение разработки и производства вакцин[2]. Так называемая гонка вакцин является отражением геополитического противостояния стран. В то же время, несмотря на то что западные страны конкурировали друг с другом за первенство в разработке вакцины,

1 Jeff Craven, "COVID-19 vaccine tracker," RAPS, accessed February 20, 2021, https://www.raps.org/news-and-articles/news-articles/2020/3/covid-19-vaccine-tracker.

2 "Trump Administration Announces Framework and Leadership for 'Operation Warp Speed'," HHS, May 15, 2020, accessed February 15, 2021, https://www.hhs.gov/about/news/2020/05/15/trump-administration-announces-framework-and-leadership-for-operation-warp-speed.html.

они оказались готовы к взаимному сотрудничеству, о чем свидетельствует то, что американский регулятор одобрил международную вакцину *Pfizer-BioNTech,* а европейский и британский регулятор, в свою очередь, – американскую *Moderna*. При этом российские и китайские вакцины не одобрены ни в одной из стран западного мира: учитывая экономические и дипломатические возможности, которые открывает разработка вакцины, успехи России и Китая в этой области воспринимаются США как потенциальная угроза[1].

Этим противостоянием объясняется, в частности, первоначальный скептицизм западных стран относительно российской вакцины «Спутник-V»: когда Россия заявила, что национальный регулятор одобрил вакцину, западные эксперты указывали на незавершенность 3-й фазы клинических испытаний[2]. В свою очередь, в российских СМИ велась информационная кампания против западных вакцин, направленная в первую очередь на аудиторию стран Латинской Америки и Восточной Европы. В рамках кампании, как отмечает *The New York Times,* российские медиа указывали на недостатки вакцин *Pfizer и Moderna*[3]. Кроме того, первоначально аналогичная кампания велась и против вакцины *AstraZeneca*, однако после того, как *AstraZeneca* заключила соглашение о сотрудничестве с Национальным исследовательским центром эпидемиологии и микробиологии им. Н.Ф. Гамалеи, разработавшим российскую вакцину «Спутник-V», российские государственные СМИ, напротив, начали писать о препарате *AstraZeneca* в позитивном ключе.

В условиях пандемии стала заметна неготовность многих стран к кооперации, в том числе в сфере разработки и распределения между населением вакцин против вируса SARS CoV-2. Всё чаще отмечается такое явление, как «вакцинный национализм», при котором страны в одностороннем порядке ведут исследования по разработке вакцин, пытаясь «переманить» к себе исследователей из других государств и в рамках информационных кампаний указывают на преимущества собственной вакцины[4]. Так, еще в мае 2020 г., когда разработка вакцин находилась на начальном этапе, глава французской фармацевтической ТНК *Sanofi* вызвал критику в свой адрес, заявив, что США будут иметь приоритетный доступ к вакцине, разработанной в компании, – вскоре после этого в официальном заявлении *Sanofi* сообщила, что ни у одной из стран не будет приоритетного доступа к разрабатываемой вакцине. Как отмечают ученые, «борьба между странами за ограниченные поставки вакцины от COVID-19 привлекла внимание к давно существующему неравенству в здравоохранении»[5].

По мнению исследователей, вакцинный национализм впервые возник не в связи с пандемией COVID-19: подобное явление наблюдалось и в 2009 г. во время распространения вируса H1N1[6]. Опыт пандемии H1N1 показывает, что более

1 Daoudi 2020.
2 Stepan Kravchenko, Ilya Arkhipov, and Yulia Fedorinova, “How Russia Shortened the Covid Vaccine Race to Declare Victory,” Bloomberg, October 2, 2020, accessed February 15, 2021, https://www.bloomberg.com/news/features/2020-10-01/russia-covid-19-vaccine-sputnik-v-has-scientist-doubters-in-the-west.
3 Sheera Frenkel, Maria Abi-Habib, and Julian E. Barnes, “Russian Campign Promotes Homegrown Vaccine and Undercuts Rivals,” The New York Times, February 5, 2021, accessed February 15, 2021, https://www.nytimes.com/2021/02/05/technology/russia-covid-vaccine-disinformation.html.
4 Santos Rutschman 2020.
5 Ibid.
6 Hafner et al. 2020.

богатые страны стремятся первыми получить доступ к вакцинам, заключая сделки непосредственно с фармацевтическими компаниями[1]. Согласно модели, построенной аналитиками *RAND Corporation*, подобное неравенство в распределении поставок вакцин имеет негативные последствия для глобальной экономики. По подсчетам исследователей, в случае если страны, разрабатывающие вакцину (США, Россия, ЕС, Великобритания, Китай и Индия), вакцинируют большую часть своего населения, потери для мирового ВВП сократятся на 2,4 п. п. в год, однако отсутствие доступа к вакцинам для остального мира все же приведет к потерям для глобального ВВП в размере около 1,2 трлн долл. ежегодно[2].

По данным группы НКО *People's Vaccine Alliance*, в декабре 2020 г. 53% всех доз вакцин были закуплены богатыми странами, в которых проживает всего 14% мирового населения[3]. Согласно исследованию, проведенному *Duke Global Health Innovation Center*, к середине февраля 2021 г. страны с высоким уровнем доходов населения зарезервировали для себя 4,6 млрд доз вакцин, страны с уровнем доходов выше среднего – 1,2 млрд доз, страны со средним уровнем доходов – 599 млн доз, а страны с низким уровнем доходов – 670 млн[4].

Чтобы обеспечить населению более бедных стран доступ к вакцинам от вируса SARS CoV-2, Всемирная организация здравоохранения (ВОЗ) совместно с Глобальным альянсом по вакцинам и иммунизации (ГАВИ) и Коалицией по инновациям в области готовности к эпидемиям создала платформу распределения вакцин *Covax*, в рамках которой будут поддерживаться исследования и разработки вакцин, их производство, а также будут вестись переговоры о цене и закупках вакцин[5]. Предполагается, что к концу 2021 г. в распоряжении платформы будет 2 млрд доз вакцин для распределения среди людей из групп риска и медицинских работников, специализирующихся на борьбе с COVID-19. Поставки вакцин в рамках программы в наиболее бедные страны начались в конце февраля 2021 г. К середине февраля 2021 г. для платформы *Covax* было зарезервировано 1,1 млрд доз вакцин против вируса SARS CoV-2[6].

Подводя итог, можно отметить, что гонка вакцин, развернувшаяся на фоне борьбы с пандемией COVID-19, стала еще одним проявлением политизации конкуренции в фармацевтической отрасли. Однако здесь противостояние наблюдается между западными странами (в лице США и ЕС), Россией и Китаем. Информационные кампании против тех или иных вакцин, которые инициировались как одной, так и другой стороной, стали свидетельством неготовности стран к сотрудничеству, которая, в свою очередь, и привела к возникновению дисбалансов в распределении вакцин между жителями стран с низким уровнем доходов населения.

1 Fidler 2020.
2 Hafner et al. 2020.
3 "Campaigners warn that 9 out of 10 people in poor countries are set to miss out on COVID-19 vaccine next year," Oxfam, December 9, 2020, accessed February 15, 2020, https://www.oxfam.org/en/press-releases/campaigners-warn-9-out-10-people-poor-countries-are-set-miss-out-covid-19-vaccine.
4 "Launch & Scale Spedometer," Duke Global Health Innovation Center, accessed February 20, 2021, https://launchandscalefaster.org/COVID-19.
5 Seth Berkeley, "COVAX Explained," Gavi, September 3, 2020, accessed February 15, 2021, https://www.gavi.org/vaccineswork/covax-explained.
6 "Launch & Scale Spedometer," Duke Global Health Innovation Center, accessed February 20, 2021, https://launchandscalefaster.org/COVID-19.

Взаимодействие ТНК и регуляторов в условиях COVID-19

Пандемия COVID-19 в некоторой степени упростила взаимодействие фармацевтических ТНК и государственных регуляторов. В условиях пандемии регуляторы проявили высокую гибкость как в области снижения угрозы распространения самого COVID-19, так и в области обеспечения непрерывности процесса одобрения лекарственных препаратов, не связанных с коронавирусом. Ряд новых мер позволил регулирующим органам переориентировать свою работу и перераспределить внутренние ресурсы, однако кардинальные решения, принятые в условиях пандемии, должны внедряться только в схожих чрезвычайных ситуациях, поскольку в долгосрочной перспективе они могут оказаться неустойчивыми[1].

В то же время цифровизация процессов стала актуальна не только для фармацевтических компаний, но и для самих регуляторов. Регулирующие органы многих стран во время пандемии разрешили компаниям, к примеру, осуществлять дистанционный мониторинг за состоянием пациентов во время проведения клинических испытаний – это нововведение использовалось, например, при пострегистрационных испытаниях российской вакцины «Спутник-V», когда вакцинированные волонтеры сообщали о побочных эффектах и своем самочувствии через мобильное приложение[2]. Более широкое внедрение телемедицины в дальнейшем может открыть возможности для масштабного реформирования системы клинических испытаний, в результате которого в цифровой режим будут переведены такие сферы, как скрининг пациентов, получение информированного согласия, посещение пациентом врачей. Снятие регуляторных барьеров в этих сферах уже началось: Международный совет по гармонизации технических требований к фармацевтическим препаратам для применения человеком (*International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use*, ICH) уже пересматривает стандарты в области клинической практики[3].

Еще одна сфера работы регуляторов, ставшая объектом цифровизации во время пандемии COVID-19, – это проведение дистанционных регуляторных инспекций, при которых представители регуляторов инспектируют производство фармацевтической продукции. По мнению представителей Европейской федерации фармацевтической промышленности и ассоциаций (*European Federation of Pharmaceutical Industries and Associations*, EFPIA), дистанционные инспекции продемонстрировали эффективность и могут использоваться и в дальнейшем. Как отмечают в организации, инспекции на местах могут оказаться ненужными или же будут требоваться только в исключительных случаях[4].

Кроме того, пандемия повысила спрос на добровольный открытый обмен данными фармпроизводителей и регуляторов в целях ускорения борьбы

1 Stewart 2020.
2 *Шубина, Д.* Побочные эффекты Спутника V будут мониторить через мобильное приложение // Vademecum. 9 сентября 2020. [Электронный ресурс]. URL: https://vademec.ru/news/2020/09/09/pobochnye-effekty-sputnika-v-budut-monitorit-cherez-mobilnoe-prilozhenie/ (дата обращения: 15.02.2021).
3 Stewart 2020.
4 Milmo 2020.

с COVID-19. Учитывая высокую конкуренцию в фармацевтической отрасли маловероятно, что и после завершения пандемии продолжится процесс активного обмена данными, однако облачные технологии совместного хранения и обмена данными могут использоваться для отображения актуальной информации о регуляторных решениях[1]. Не приходится ожидать значительных изменений в средне- и долгосрочном планировании в крупнейших транснациональных фармацевтических компаниях: приоритетом, вероятнее всего, так и останется разработка и реализация препаратов против онкологических, а также редких (орфанных) заболеваний. Именно на них приходится основная выручка компаний отрасли, и их динамичное развитие поддерживает инновационную активность. По итогам 2019 г. из более чем 2500 активных препаратов в разработке лишь около 20% были связаны с вирусными заболеваниями. С точки зрения бизнеса, пандемии и их специфика так и останутся труднопрогнозируемы, тогда как рост спроса на препараты со стороны онкологических и сердечно-сосудистых заболеваний стабилен и обеспечивает долгосрочную финансовую устойчивость корпораций.

* * *

Пандемия привела не столько к масштабной трансформации отрасли, сколько к появлению дополнительных приоритетов в работе фармацевтических компаний. Во-первых, это повышение конкуренции в сфере поставщиков АФС, в первую очередь связанное со стремлением снизить зависимость от Китая. Согласно докладу Комитета Европейского парламента по окружающей среде, общественному здравоохранению и безопасности продуктов питания, дефицит фармацевтической продукции в ЕС вырос в 20 раз с 2000 по 2018 г., в 12 раз – с 2008 г. Однако возврат производств полного цикла на территорию ЕС остается спорным, так как рентабельность производства в ЕС по многим важнейшим продуктам ограничена, реорганизация должна быть поддержана промышленной политикой, например, субсидированием, чтобы компенсировать издержки ТНК. В новой стратегии по фармацевтической отрасли ЕС (конец 2020) напрямую о возвращении производств не говорится, акцент сделан на повышении устойчивости цепочек поставок.

Во-вторых, происходят регуляторные изменения, направленные как на повышение конкуренции в отрасли, так и способствующие сокращению сроков вывода на рынок новейших препаратов (*fast track*). Данная тенденция уже проявила себя в США за последние пять лет (после многочисленных жалоб крупнейших ТНК на финансовые риски, связанные с массовым истечением сроков патентов на наиболее прибыльные медикаменты в 2010-х).

В-третьих, наблюдается всплеск инновационной активности в отрасли по ряду научных направлений, в первую очередь, в сфере создания вакцин на основе РНК и ДНК и т. н. субъединичных вакцин. В будущем данные исследования способны привести к распространению новых механизмов создания вакцин и ухода традиционных (все еще доминирующих в мире) живых вакцин в про-

1 Robertson et al. 2020.

шлое. Появление вакцин от нового коронавируса и иммунных паспортов ставят новые этические вопросы, связанные в том числе с правами человека и свободой перемещения. Данные регуляторные аспекты способны стать еще одним измерением технологического противостояния как США с Китаем, так и широкого круга заинтересованных стран.

За последние два десятилетия драйвером роста отрасли был сегмент биотех-препаратов (к ним можно отнести и разработки описанных выше перспективных вакцин). Мощная конкуренция, особенно в сфере науки, сложилась именно в сегменте биотех-компаний, многие из которых традиционно привлекают средства через венчурные механизмы и биржу *NASDAQ*. Представляется, в-четвертых, что этот процесс только усилится в ближайшие годы, в первую очередь из-за избытка оптимизма инвесторов относительно потенциала данного направления и высокой инвестиционной активности в этой сфере. Таким образом, биотехнологии будут получать все большую поддержку как со стороны инвестиционных компаний, так и с помощью дополнительных регуляторных механизмов. Наконец, еще одним приоритетом отрасли становится дальнейшая цифровизация производственных мощностей, включая новые стимулы к непрерывному производству (*continuous manufacturing*) медикаментов.

Правительства и государственные регуляторы будут активно участвовать в процессе восстановления фармацевтической отрасли после кризиса. В США примером такого участия является программа *Coronavirus Treatment Acceleration Program* (CTAP), учрежденная FDA. Цель программы – поддержка компаний и ученых, желающих провести испытания средств для борьбы с коронавирусом, а также содействие в скорейшей регистрации новых лекарственных средств. Государственный контроль за фармацевтическими препаратами может проявляться не только в оказании поддержки производителям, но и в более пристальном внимании к важным лекарственным препаратам. Так, регуляторы могут повысить требования к минимальным запасам тех или иных лекарственных средств и применять более жесткие санкции к поставщикам в случае их дефицита. Регулирующие органы могут также начать требовать от компаний диверсификации поставщиков активных компонентов, а также более внимательно относиться к качеству жизненно важных препаратов. В России, например, может появиться реестр требований к качеству лекарственных средств. Учитывая глобальную цифровую трансформацию фармацевтической промышленности, можно ожидать смягчения барьеров в сфере регистрации лекарственных препаратов, в том числе и в ЕАЭС. Так, если фармацевтическое производство осуществляется стабильно и без каких-либо отклонений в контрольных точках, от синтеза первичных субстанций до создания готового продукта, то производители и регуляторы могут скоро отказаться от контроля промежуточных продуктов, что позволит более рационально распределять ресурсы как производителей, так и регуляторов.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Березной, А.В. Транснациональный бизнес в эпоху глобальной цифровой революции // Мировая экономика и международные отношения. – 2018. – Т. 62 (9). – С. 5–17. [Bereznoi, Aleksei V. "Transnational Business in the Era of the Global Digital Revolution." [Transnatsional'nyi biznes v epokhu global'noi tsifrovoi revolyutsii] *World Economy and International Relations* 62, no.9 (2018): 5–17] [In Russian].

Евстратов, А.В. Основные тенденции и перспективы развития фармацевтического рынка в Российской Федерации. – Волгоград: Федеральное государственное бюджетное образовательное учреждение высшего образования Волгоградский государственный технический университет, 2018. – 192 с. [Evstratov, Aleksandr. V. *The Main Trends and Prospects for the Development of the Pharmaceutical Market in the Russian Federation*. [Osnovnye tendentsii i perspektivy razvitiya farmatsevticheskogo rynka v Rossiiskoi Federatsii]. Volgograd: Volgograd State Technical University, 2018] [In Russian].

Кузнецов, А.В. Цифровизация как логика глобальных корпораций // Философия хозяйства. – 2020. – №. 5. – С. 124–139. [Kuznetsov, Aleksei V. "Digitalization as the Logic of Global Corporations." [Tsifrovizatsiya kak logika global'nykh korporatsii] *Philosophy of Economy*, no. 5 (2020): 124–139] [In Russian].

Нежникова, Е.В., Максимчук, М.В. Фармацевтическая отрасль в РФ: проблемы и перспективы развития // Вестник Российского университета дружбы народов. Серия: Экономика. – 2019. – Т. 27 (1). – С. 102–112. [Nezhnikova, Ekaterina V., and Maksim V. Maksimchuk. "Pharmaceutical Industry in the Russian Federation: Problems and Prospects for Development." [Farmatsevticheskaya otrasl' v RF: problemy i perspektivy razvitiya] *Bulletin of the Peoples' Friendship University of Russia. Series: Economics* 27, no. 1 (2019): 102–112] [In Russian].

Bishop, Matthew Louis, and Anthony Payne. "Steering towards Reglobalization: Can a Reformed G20 Rise to the Occasion?" *Globalizations* 18, no. 1 (2021). doi:10.1080/14747731.2020.1779964.

Boylan, Brandon M., Jerry McBeath, and Bo Wang. "US–China Relations: Nationalism, the Trade War, and COVID-19." *Fudan Journal of the Humanities and Social Sciences* 14, no. 1 (2021). doi:10.1007/s40647-020-00302-6.

Chatterjee, Patralekha. "Indian pharma threatened by COVID-19 shutdowns in China." *The Lancet* 395, no. 10225 (2020): 675. doi: 10.1016/S0140-6736(20)30459-1

Daoudi, Salma. *Vaccine Nationalism in the Context of COVID-19: An Obstacle to the Containment of the Pandemic.* Policy Center for the New South, 2020.

Dierks, Alexander, Kuklinski, Christian Paul Jian Wei, and Roger Moser. "How Institutional Change Reconfigures Successful Value Chains: The Case of Western Pharma Corporations in China." *Thunderbird International Business Review* 55, no. 2 (2013): 153–171. https://doi.org/10.1002/tie.21533.

Drezner, Daniel W. "The Song Remains the Same: International Relations After COVID-19." International Organization 74, no. S1 (December 19, 2020): E18–E35. https://doi.org/10.1017/S0020818320000351.

Fidler, David P. "Vaccine Nationalism's Politics." Science 369, no. 6505 (2020): 749. https://doi.org/10.1126/science.abe2275.

Hafner, Marco, Yerushalmi, Erez, Fays, Clement, Dufresne, Eliane, and Christian Van Stolk. Christian. *COVID-19 and the Cost of Vaccine Nationalism.* RAND Corporation, 2020.

Kennedy, Andrew B., and Darren J. Lim. "The Innovation Imperative: Technology and US-China Rivalry in the Twenty-First Century." *International Affairs* 94, no. 3 (2018). doi:10.1093/ia/iiy044.

Klinge, Tobias J., Fernandez, Roberto, and Aalbers, Manuel B. "The Financialization of Big Pharma." *Revista Internacional de Sociología* 78, no. 4 (2020): 1–15. https://doi.org/10.3989/ris.2020.78.4.m20.006

LaMattina, John L. *Devalued and distrusted: can the pharmaceutical industry restore its broken image*? John Wiley & Sons, 2012.

Lazonick, William. et al. *Financialization of the US Pharmaceutical Industry.* Institute for New Economic Thinking, 2019.

Lindsley, Craig W. "New 2017 Data and Statistics for Pharmaceutical Products." *ACS Chemical Neuroscience* 9, no. 7 (2018): 1518–1519. https://doi.org/10.1021/acschemneuro.8b00320.

Lipscy, Phillip Y. "COVID-19 and the Politics of Crisis." *International Organization* 74, no. S1 (December 12, 2020): E98–E127. https://doi.org/10.1017/S0020818320000375.

McNamara, Kathleen R., and Abraham L. Newman. "The Big Reveal: COVID-19 and Globalization's Great Transformations." *International Organization* 74, no. S1 (December 14, 2020): E59–E77. https://doi.org/10.1017/S0020818320000387.

Miller, Seumas, and Marcus Smith. "Ethics, Public Health and Technology Responses to COVID-19." *Bioethics*, February 17, 2021. https://doi.org/10.1111/bioe.12856.

Milmo, Sean. "Inspecting GMP at a Distance." *Pharmaceutical Technology* 44, no. 12 (2020): 6–8.

Pan, Guangyi, and Alexander Korolev. "The Struggle for Certainty: Ontological Security, the Rise of Nationalism, and Australia-China Tensions after COVID-19." *Journal of Chinese Political Science* 26, no. 1 (March 5, 2021): 115–38. https://doi.org/10.1007/s11366-020-09710-7.

Pevehouse, Jon C.W. "The COVID-19 Pandemic, International Cooperation, and Populism." *International Organization* 74, no. S1 (December 11, 2020): E191–212. https://doi.org/10.1017/S0020818320000399.

Richman, Barack, Will Mitchell, Elena Vidal, and Kevin Schulman. "Pharmaceutical M&A Activity: Effects on Prices, Innovation, and Competition." *Loyola Univercity Chicago Law Journal* 48 (2017): 787–819.

Robertson, Andrew S., Hilary Malone, Fabio Bisordi, Helen Fitton, Carlos Garner, Stacy Holdsworth, Peter Honig, et al. "Cloud-Based Data Systems in Drug Regulation: An Industry Perspective." *Nature Reviews Drug Discovery* 19, no. 6 (June 11, 2020): 365–366. https://doi.org/10.1038/d41573-019-00193-7.

Santos Rutschman, Ana. "The Reemergence of Vaccine Nationalism." *SSRN Electronic Journal*, 2020. https://doi.org/10.2139/ssrn.3642858.

Stewart, Jerry, Peter Honig, Lina AlJuburi, Deborah Autor, Susan Berger, Patrick Brady, Helen Fitton, et al. "COVID-19: A Catalyst to Accelerate Global Regulatory Transformation." *Clinical Pharmacology & Therapeutics,* September 29, 2020. https://doi.org/10.1002/cpt.2046.

Torreele, Els. "Business-as-Usual Will Not Deliver the COVID-19 Vaccines We Need." *Development* 63, no. 2–4 (December 9, 2020): 191–199. https://doi.org/10.1057/s41301-020-00261-1.

Tulum, Öner, and Lazonick, William. "Financialized Corporations in a National Innovation System: the US Pharmaceutical Industry." *International Journal of Political Economy* 47, no. 3–4 (2018): 281–316. https://doi.org/10.1080/08911916.2018.1549842

Vogler, Sabine, ed. *Medicine Price Surveys, Analyses and Comparisons: Evidence and Methodology Guidance*. Academic Press, 2018.

Woods, Eric Taylor, Robert Schertzer, Liah Greenfeld, Chris Hughes, and Cynthia Miller-Idriss. "COVID-19, Nationalism, and the Politics of Crisis: A Scholarly Exchange." *Nations and Nationalism* 26, no. 4 (2020). doi:10.1111/nana.12644.

Yaya, Sanni, Sanni Yaya, Akaninyene Otu, Akaninyene Otu, and Ronald Labonté. "Globalisation in the Time of COVID-19: Repositioning Africa to Meet the Immediate and Remote Challenges." *Globalization and Health* 16, no. 1 (2020). doi:10.1186/s12992-020-00581-4.

Сведения об авторе

Заур Аязович Мамедьяров,
заведующий сектором экономики науки и инноваций, к.э.н.,
Национальный исследовательский институт мировой экономики и международных отношений имени Е.М. Примакова РАН
Российская Федерация, 117997, Москва, Профсоюзная ул., 23.
ORCID: 0000-0002-4336-1020
e-mail: mamedyarov@imemo.ru

Дополнительная информация

Поступила в редакцию: 25 февраля 2021. Принята к публикации: 14 марта 2021.

Конфликт интересов

Автор заявляет об отсутствии потенциального конфликта интересов.

Цитирование

Мамедьяров, З.А. Стратегическое значение фармацевтической отрасли в условиях пандемии коронавируса. // Международная аналитика. – 2020. – Том 11 (4). – С. 122–136.
https://doi.org/10.46272/2587-8476-2020-11-4-122-136

Strategic Role of the Pharmaceutical Industry in the Context of the Global Pandemic

ABSTRACT

The strategic importance of the pharmaceutical industry for the scientific, technological and economic development of countries determines its impact on international processes. The paper traces the current trends in the growth of innovative competition in pharmaceuticals and biotechnology, taking into account the factor of the COVID-19 pandemic. The following areas of increased competition are highlighted: diversification of supply of active pharmaceutical substances, regulators' permission of the newest drugs to access the market, competition of pharmaceutical companies for capital and competence. The pandemic has also exacerbated long-standing problems: the efficiency of drug distribution to citizens, the dependence of large manufacturers on active substance suppliers from China, drug pricing, and the role of social insurance systems in developed and developing countries. The article analyzes the main problems of the industry and presents possible trajectories of further development of international relations in the context of pharmaceuticals and biotechnology, analyzing the progress of creation and market admission of COVID-19 vaccines. For all the high-tech trends, the pharmaceutical industry is a rather conservative industry in which regulatory issues play a significant role. Therefore, legal, ethical and practical issues related to the collection of sensitive patient health data may slow down the digitalization of the pharmaceutical industry. Much will also depend on the decisions of major regulators – in the U.S. and the EU – regarding telemedicine and digital health in general. A serious barrier for the pharmaceutical industry is also the lack of pharmaceutical companies' own experience in developing software solutions, which makes them dependent on external suppliers of IT solutions, complicates the problem of sharing clinical patient data and particularly raises the issue of cybersecurity.

KEYWORDS

pharmaceuticals, innovation, competition, regulation, research and development, technology, COVID-19

Author

Zaur A. Mamedyarov,
Head of the Sector of Economics of Science and Innovation, PhD in Economics,
Primakov National Research Institute of World Economy and International Relations
of the Russian Academy of Sciences,
23, Profsoyuznaya Street, Moscow, 117997, Russian Federation.
ORCID: 0000-0002-4336-1020
e-mail: mamedyarov@imemo.ru

Additional Information

Received: February 25, 2021. Accepted: March 14, 2021.

Disclosure statement

No potential conflict of interest was reported by the author.

For citation

Mamedyarov, Zaur A. "Strategic Role of the Pharmaceutical Industry in the Context of the Global Pandemic." *Journal of International Analytics* 11, no. 4 (2020): 122 –136.
https://doi.org/10.46272/2587-8476-2020-11-4-122-136

LAWS with AI: How to aBANdon the Superiority

Natalya A. Samoylovskaya

https://doi.org/10.46272/2587-8476-2020-11-4-137-146

ABSTRACT

Taking the relative novelty of issues relating to the military use of AI and its influence on international relations into account, the author of this paper relies on the latest reports of international research centres, organizations and national programs on the issue. The paper considers the political consequences of the military use of AI, as well as the national and international approaches to mitigate its challenges. With great attention to the AI policies of two technological leaders in the field, the author concludes that a balanced U.S. policy will determine whether China and the United States will be able to create, despite the presence of competition, common rules for legalizing the use of AI systems in the military sphere and form common standards that include a high level of security in the use of these systems, including the proliferation of such weapons. The author points out that Europe's concentration on the conflict with Russia and its exclusion from the environment created by the technical and ethical legal tools for using AI will increase unpredictability in relations. This is why it is in Europe's interests to involve Russia in the development of a common platform and standards for AI. The development and establishment of common safety standards will help avoid problems with perception and introduce an element of predictability in international relations.

KEYWORDS

AI, LAWS, responsibility, U.S., China, EU, Russia

CC BY

The rapid development of dual-use technologies alongside the distinct lack of progress in the traditional arms control architecture feed uncertainty in international relations, which is more dangerous in the digital age, as our world is interconnected and more vulnerable to these global challenges. A group of researchers at the Stockholm International Peace Research Institute (SIPRI) point out that there is a rapidly expanding body of literature on the impact that the military use of AI could have on international peace and security, most of which focus on two approaches to risk assessment – humanitarian and strategic.[1]

An analysis of national artificial intelligence (AI) strategies reveals that AI has become a crucial technology with military implications in terms of the possible creation of fully autonomous weapons. This, in turn, has legal and ethical ramifications for humanity. It is for this reason that the Nobel Peace Laureates and Peace Laureate Organisations in their Final Declaration of the XVII Summit of Nobel Peace Laureates in 2019 addressed seven topics affecting the peace wellbeing and sustainability of humankind, calling on states to pre-emptively ban the use of fully autonomous weapons or "Killer Robots,"[2] or, to use UN terminology, lethal autonomous weapons (LAWS).

The problem of LAWS has been debated on various international platforms since the beginning of the 2000s. Some dominant approaches to the issue have appeared during this time. The most noticeable examples of international collaboration on the problem of LAWS are the efforts of the International Committee of the Red Cross (ICRC)[3] and the Campaign to Stop Killer Robots,[4] both of which have been involved, alongside a range of other non-governmental organizations and institutions, in UN discussions on LAWS that have raised ethical issues, including those relating to responsibility and humanitarianism, in addition to a number of legal and strategic questions.

The interaction of the two last points – legal and strategic approaches – is rooted in an understanding of what autonomy means. Autonomy is the most difficult and debatable concept within the framework of the Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE) established in 2016 by the Fifth Review Conference of the High Contracting Parties to the Convention on Certain Conventional Weapons (CCW) to specifically address this issue area of emerging technologies. Despite the annual meetings of the GGE with state officials, NGOs and invited experts, there are still many difficulties in understanding the concept, which creates a big obstacle for the international community when it comes to developing a common stance on LAWS.

This paper examines the political and psychological aspects of the influence of AI technologies on international security and peace. It summarizes the emerging

1 Boulanin et al. 2020, 3.
2 "Make Your Mark for Peace," Final Declaration of the 17th Nobel Peace Summit, September 2019, accessed February 4, 2021, http://www.nobelpeacesummit.com/make-your-mark-for-peace-final-declaration-of-the-17th-nobel-peace-summit/.
3 The official position of the ICRC, which is actively involved in creating an international legal framework for new types of weapons, is not to join calls for a moratorium or ban the development, production and use of LAWS. For more information, see "Autonomous Weapon Systems – Q&A," The International Committee of the Red Cross, November 2014, accessed February 4, 2021, https://www.icrc.org/en/document/autonomous-weapon-systems-challenge-human-control-over-use-force.
4 The Campaign to Stop Killer Robots, which calls for a ban on the development, production and use of LAWS, is a coalition of non-governmental organizations, the original coordinator of which is the Human Rights Watch (HRW). Its Steering Committee also includes Nobel laureates: The Nobel Women's Initiative and the Pugwash Conferences on Science and World Affairs. For more information, see "Steering Committee Members as of October 2018," "The Campaign to Stop Killer Robots," accessed February 4, 2021, https://www.stopkillerrobots.org/wp-content/uploads/2018/10/KRC_SCmembers_Oct2018rev.pdf.

approaches in the international community to the risks posed by the military use of AI. Taking the most problematic areas for international collaboration in this field into account, the author focuses on existing efforts to avoid the worst-case scenario of an uncontrolled arms race and the polarization of the world in the face of rising distrust. The main finding is that cooperation in AI technologies in the sensitive military sector is indeed possible. Emerging international approaches open up various opportunities for such cooperation. In addition, advances in this field depend on how responsibly the leading powers tackle the issue, as well as on how willing they are to develop cooperative approaches in order to build confidence and eliminate the risks of misunderstandings taking place.

Human–Machine Interface

One of the key elements in understanding autonomy is the level of human involvement. Thus, in all conclusions, the GGE paid key attention to aspects of human–machine interaction. There is a common notion that maintaining human control is crucial in the context of the use of force and compliance with International Humanitarian Law (IHL). However, as pointed out in the GGE's 2018 Report, states have different conceptual and terminological understandings of human control: "One was the importance of maintaining human control over the critical functions of autonomous weapons systems. Another was the human element in the different phases of the lifecycle of a weapons system and the level and quality of human control that can be applied at each stage."[1]

Human–machine interaction of highly automated systems is a long-standing, yet straightforward dilemma. It is our understanding of the concepts of autonomy and lethality that is lacking today, despite the confidence in the ability of humankind to answer these questions. Without a doubt, human control in maintaining responsibility and the ability to intervene in critical cases are important elements of the human–machine interface. However, two under-studied trends have emerged on this front, particularly since the emergence of drones (or UAVs): the routinization and gamification of warfare for operators.

In the case of routinization, humans may play just a minor part in a machine's decisions. This concept is connected to the problem of placing a high level of trust in a machine or being indifferent to the real situation because physical distance from the events lends a sense of safety and is psychologically no different from regular training exercises.[2] In the case of gamification, humans may glean excitement or satisfaction from violence. Both trends have a big impact on the role of humans within the human–machine decision-making process and on the humanitarian aspect of military operations in general. As K. Payne points out, "the danger in AI, whether employed for a tactical weapons system or a strategic-scenario planner, lies primarily

1 "Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems," UNDOCS, 2018, p. 13, accessed February 4, 2021, https://undocs.org/en/CCW/GGE.1/2018/3.

2 In this context, I would like to point out one of the main findings of the "Millennials on War" study commissioned by the ICRS, for which it interviewed over 16,000 millennials in 16 countries, and that was that "the experience of war makes people hate war." "News Release: Majority of Millennials See Catastrophic War as Real Possibility, and Believe There Should Be Limits," ICRC, January 2020, accessed February 4, 2021, https://www.icrc.org/en/document/majority-millennials-see-catastrophic-war-real-possibility.

in the gap between how the AI solves a problem framed by humans, and how those humans would solve it if they possessed the AI's speed, precision and brainpower."[1]

The strong interconnection between the approaches to training and selecting individuals for the human–machine interface has a direct influence on the use and termination of highly automated intelligent military systems. Despite the limitations of international regulation in this area, focusing on training standards is crucial to maintaining high-quality human control in the area of lethal autonomous weapons systems and formulating an agenda for a human-centric approach among states.

An (Un)controlled World

Experts at the World Economic Forum see the ambiguous role of AI technologies and advances in autonomy as a potential future shock that could fundamentally destabilize the world by creating new forms of strong social control that may verge upon a new type of authoritarianism.[2] It is not difficult to extend this argument further and within a context where the creation of LAWS with AI may become a monopolized global process. Experts at the Institute of World Economy and International Relations of the Russian Academy of Sciences (IMEMO) have pointed out that the process of transferring decision-making from man to autonomous systems in the military sphere will not be launched within the next five years, although technological arms control is moving in this direction, and the potential of transparency without traditional inspections is growing too.[3]

The technological dynamics of nuclear arms control is one of the main issues facing international decision-makers today. The most important factor here is how nuclear-armed states will implement such technologies for military purposes and how this will affect strategic stability. The SIPRI project, which aims to present regional perspectives on how AI technologies impact nuclear weapons, has worked hard to try to understand the interconnection between autonomy, AI advances and nuclear risks.[4] It is interesting that some SIPRI researchers also note positive technological trends, especially in the implementation of machine learning, that will give human military command better situational awareness, allowing more time to make decisions.[5] But there is still a great deal of concern about the implementation of AI technologies in conventional warfare. Strengthening the role of nuclear arms, alongside measures to lower confidence among nuclear states, provoking fear, misperceptions and accidents, will carry far-reaching consequences.

The GGE's 2019 review of potential military applications and related technologies highlights the following existing weapons:[6] air defence weapon systems with autonomous modes or functions; missiles with autonomous modes or functions; active protection weapon systems with autonomous modes or functions; loitering

1 Payne 2018.
2 "The Global Risk Report 2019. 14th Edition," World Economic Forum, Geneva 2019, p. 39, accessed February 4, 2021, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.
3 Dynkin et al. 2019, 19.
4 Boulanin 2019; Saalman 2019; Topychkanov 2020.
5 Boulanin 2019, 54.
6 "Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems," UNDOCS 2019, p. 13, accessed February 4, 2021, https://undocs.org/en/CCW/GGE.1/2019/3.

weapons with autonomous modes or functions; naval or land mines with autonomous modes or functions; and "sentry" weapons with autonomous modes or functions. Further research and discussion regarding these weapons systems will be valuable in understanding and possibly developing a moratorium within the framework of the CCW on technological implementation to reduce the command time in the context of nuclear strike decision-making. This is the key sphere where a race for technological superiority may have catastrophic consequences for everyone involved. Moreover, such consequences for humanity are not justified by national security interests.

Back to the Future

M.C. Horowitz, P. Scharre, A. Velez-Green have studied the influence of autonomous systems and artificial intelligence on nuclear stability in great depth, concluding that psychology plays a key role in autonomous systems and nuclear security.[1] The unwillingness to comply with old agreements, tabling of new ones, and emphasis on military superiority that could return countries to an arms race has sped up warfare development and reduced the time that states have to stop and to think about whether we really need these technologies. Developing such emerging technological autonomous systems will light a 'powder keg,' making nuclear arms escalation inevitable and ambitions of military technological superiority more attractive. But genuine progress will first require a wide range of existing problems to be solved, including strengthening confidence-building measures and arms control transparency.

Possessing one of the deadliest weapons requires a high level of responsibility and consciousness, most notably self-restraint. If at the dawn of the nuclear age the acquisition of strategic knowledge was largely spontaneous, now, after the accumulated experience, we recognize the potential of bringing the current situation to a critical point and creating conditions for a nuclear disaster through the introduction of AI technologies and automation, which can only be mitigated through the urgent need to develop human intelligence. The wisdom of the Russell–Einstein Manifesto, which marked the beginnings of the Pugwash movement, is more relevant for contemporary issues than ever before.

The famous speech of R. McNamara in San Francisco 1967 and his thesis that real freedom is "in facing the matter rationally and realistically and discussing actions to minimize the danger" is crucial for understanding our possibilities and responsibilities in using dual technologies with revolutionary nature today.[2] We have made many mistakes since the dawn of the nuclear era, being unprepared to use such a breakthrough technology. About 50 years were needed to create measures to avoid the worst scenarios for humanity. Current international crises in arms control have proved that neither 50 years of effective working measures, nor restrictions and bans will help if the influential countries do not want to bear responsibility for it and if national strategic interests are the only priority in international communication.

1 Horowitz et al. 2019, 34.
2 "Mutual Deterrence," Speech by Sec. of Defense Robert McNamara, San Francisco, September 18, 1967, accessed February 5, 2021, https://www.atomicarchive.com/resources/documents/deterrence/mcnamara-deterrence.html.

This is why a superficial ban of LAWS may not work, as the only way to bring about the desired result is if the main international players actually want it and if AI technology holders follow the restrictions. Instead, we will see the same process as with the current arms control regimes. While main international players are not ready to restrict the potential strategic superiority that military AI givens them, this does not mean that using military AI should be left unchecked. The most advanced countries in arms will develop such technologies. Moreover, existing advanced military systems use some characteristics of highly autonomous weapons, and this is why the debates in the UN on definitions seem endless.

Despite these significant obstacles, international society is nevertheless searching for responsible approaches to the use of military AI in all cycles, from research to deployment. The AI principles developed by the EU in its 'human-centric' approach, which run parallel with national initiatives of several member states on ethics and AI, are particularly interesting here. As pointed out in the European Union's Guidelines on Ethics in Artificial Intelligence, "this approach will unfold in the context of the global race on AI."[1] The most ethical EU principles of AI are harmonized with the OECD Principles on AI adopted in May 2019 and based on the understanding of trustworthy AI, which includes inclusive growth, sustainable development and well-being; human-centred values and fairness; transparency and explainability; robustness, security and safety; and accountability.[2]

In the SIPRI Report, the authors point out that the EU members would benefit from the responsible military use of AI, but there is a huge risk that the military policies of the United States, China and Russia could affect EU values in this field.[3] Despite the fact that Russia occupies a weak position in AI R&D in the world rankings, it is thought to be a leader in terms of the military applications of AI.[4] This is why there is a clear need when establishing the legal mechanisms for the responsible military use of AI to develop common understandable and shared standards. The OECD Artificial Intelligence Policy Observatory may hold potential in this respect for the European Union and Russia. Of course, transparent military cooperation between European Union and Russia is unlikely; however, launching cooperation in different public policy areas may lead to progress in the development of trustworthy AI standards between the two sides. The International Organization for Standardization (ISO) is a good example of such cooperation. The authors of the SIPRI Report note an important aspect here: the safety of AI is a key for the military use of these technologies and high technical standards could provide the legal and ethical norms for the military sector.[5]

At the global level, the tension between China and the United States is more complex.[6] As mentioned in the Brookings Report, the United States should be ready for a technological competition between the superpowers. However, this does not

1 "EU Guidelines on Ethics in Artificial Intelligence: Context and Implementation," European Parliamentary Research Service, September 2019, p. 3, accessed January 23, 2021, https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.
2 "Recommendation of the Council on Artificial Intelligence," OECD/LEGAL/0449, May 22, 2019, accessed January 23, 2021, https://oecd.ai/assets/files/OECD-LEGAL-0449-en.pdf.
3 Boulanin et al. 2020, 2.
4 Nikolai Markotkin, and Elena Chernenko, "Developing Artificial Intelligence in Russia: Objectives and Reality," Carnegie Moscow Center, August 5, 2020, accessed February 2, 2021, https://carnegie.ru/commentary/82422.
5 Boulanin et al. 2020, 16–17.
6 *The Digital Great Game* 2020.

mean war with an enemy: "we must reject the notion that the competition with China is a 'clash of civilizations' and that conflict is inevitable. Our concerns are with the CCP and not the Chinese people. We can collaborate where possible but compete aggressively to protect our national interest and the international order that has kept us safe since 1945."[1]

As Chair of the Center for International Security and Strategy at Tsinghua University F. Ying points out, Chinese leaders are open to international cooperation in this field, especially with the United States: "The U.S. is trying to make high-tech a platform for strategic rivalry, which is not how China sees it. The reality in the field is a kind of constructive and strategic mutual dependency, although no one can deny that competition in science and industry is not abnormal."[2]

Obviously, the technological competition between the United States and China will always be accompanied by secrecy surrounding sensitive technologies and economic protection, but the military component plays a crucial role in exploring the limits of the struggle for superiority, as was the case during the Cold War. This experience tells us that compromise is possible, that unlimited military competition is dangerous and harmful, and that the powers involved need to start the long but inevitable process of bringing their positions closer together. This is why responsibility means the awareness of these limits and the discipline to not go beyond them.

Launching special U.S.–China working groups on LAWS may go a long way towards achieving stability and controlling the proliferation of arms, especially nuclear arms, as the United States and China are the two leading countries in AI research and development. In the context of nuclear application, this process will need to include Russia. Substantial progress in negotiations on the mutually accepted definition of LAWS and its applications in the nuclear field between the United States, China and Russia could be a good signal for the international community. This process also has to be multilateral, involving all nuclear states, in order to make progress in autonomous systems for effective monitoring and verification activities in arms control and disarmament.

Furthermore, it may be worthwhile for the United States, a country with a democratic culture of checks and balances, where civil society, including the STEM community and leading private companies in AI research and development, plays a significant role in formulating the country's ethical standards on the military use of AI and the possible constraints of using such systems as LAWS, to support and develop the Chinese position in UN to ban LAWS because China does not have such internal restrictions. By bringing their positions closer together and preserving a degree of interdependence in spite of the national safeguards that are in place, the two countries will help maintain the order that has been "keeping us safe since 1945."

Towards Responsible AI

The responsible military use of AI is an indicator of human progress that is marked by a decline of violence around the world, and includes the rise of rationality during

1 Brown et al. 2020, 13.
2 Fu Ying, "Understanding the AI Challenge to Humanity," China–US Focus, December 17, 2019, accessed January 31, 2021, https://www.chinausfocus.com/foreign-policy/understanding-the-ai-challenge-to-humanity.

communication and cooperation, according to Steven Pinker.[1] But now the current crises in the arms control and disarmament process demonstrate a lack of desire for active cooperation in this field. Annual meetings of the GGE on LAWS are undoubtedly important in terms of providing guiding principles for states, but they are not enough to mitigate the risks of new arms race. That is why we see a great deal of activity among the STEM community, private AI companies and international non-governmental organizations when it comes to warning about the dangers of the uncontrolled use of autonomous technologies with AI.

The fundamental question arises: How can we, as humans, control those machines that are already outperforming us in terms of data collection and processing? Of course, it is too early to take strong AI and its challenges into account, but the Russian neuropsychologist T. Chernigovskaya suggested that we approach the issue from a different angle: Is it possible for humanity to verify the possible birth of consciousness in a machine that is capable of learning? Another ambiguous question is pertinent today: What do we teach these machines, or do they learn independently of a "human teacher"?

Trends in AI development show that this technology has a fundamental impact on human society. While the complexity of AI and the interconnection between its civil and military applications create difficulties when it comes to finding a single solution for the international community, this also opens up opportunities for a common approach. An analysis of national strategies and initiatives shows that states are aware of the risks and challenges and want to engage in dialogue in this field, but geopolitical competition and distrust impose certain restrictions on this process. The responsible use of AI involves, first of all, developing constructive collaboration to mitigate the challenges stemming from the military use of AI, which is for the most part based on strategic calculations rather than on ethical standards.

Effective cooperation on sensitive issues such as the military use of AI may become an optional platform for developing integration among like-minded states; however, there are still risks of it being politicized if all states are involved, or polarized if the decision is made to follow national standards or standards developed by a separate regional group of countries. This is why the international community needs inclusiveness and harmonization, despite the geopolitical competition and distrust.

According to a group of researchers from SIPRI and IISS, strategy and ethics may be reconciled not only by sharing best practices in safety standards, but also through track 1.5 and track 2 diplomacy in the multi-stakeholder activity.[2] This reflects the links between science, industry and the military sector and allows for greater flexibility and creativity even in sensitive security matters. UNESCO's educational initiative under the "Beijing Consensus on Artificial Intelligence and Education" has the most integrative potential in this respect.[3]

The history of conflicts and world wars shows that technological superiority does not always help to win the battle, and this once again reminds us of how important

1 Pinker 2012.
2 "Capturing Technology. Rethinking Arms Control. 2020," Conference Reader, November 5–6, accessed February 10, 2021, https://rethinkingarmscontrol.de/wp-content/uploads/2020/10/20-AA-RAC-Reader-2020-10-28-final-korr-kompr.pdf.
3 "Beijing Consensus on Artificial Intelligence and Education," UNESCO, 2019, accessed February 14, 2021, https://unesdoc.unesco.org/ark:/48223/pf0000368303.

the problem of perception among states is. In this case, multilevel cooperation in AI field and a deliberate ban of LAWS with AI may become an indicator of the strength of powers that can take responsibility for stability and security to the international community.

СПИСОК ЛИТЕРАТРУРЫ / REFERENCES

Boulanin, Vincent, ed. the *Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Euro-Atlantic Perspectives. Vol. I.* SIPRI, May 2019. https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf.

Boulanin, Vincent, Netta Goussac, Laura Bruun, and Luke Richards. *Responsible Military Use of Artificial Intelligence: Can the European Union Lead the Way in Developing Best Practice?* SIPRI, November 2020. https://www.sipri.org/sites/default/files/2020-11/sipri_report_responsible_artificial_intelligence_research_and_innovation_for_international_peace_and_security_2011.pdf.

Brown, Michael, Eric Chewning, and Pavneet Singh. *Preparing the United States for the Superpower Marathon with China*. The Brookings Report, April 2020. https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_superpower_marathon_brown_chewning_singh.pdf.

Dynkin, Alexander and Vladimir Baranovsky, eds. *Russia and the World: 2024. Economy and Foreign Policy*. Primakov National Research Institute of World Economy and International Relations, Russian Academy of Sciences (IMEMO), 2019. https://doi.org/10.20542/978-5-9535-0563-5.

Horowitz, Michael C., Paul Scharre, and Alexander Velez-Green. *A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence.* Conference Paper, December 2019. https://arxiv.org/ftp/arxiv/papers/1912/1912.05291.pdf.

Payne, Kenneth. "Artificial Intelligence: a Revolution in Strategic Affairs?" *Survival* 60, no. 5 (September 3, 2018): 7–32. https://doi.org/10.1080/00396338.2018.1518374.

Pinker, Steven. *The Better Angels of Our Nature.* Penguin Books Ltd., 2012.

Saalman, Lora, ed. *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. East Asian Perspectives. Vol. II*. SIPRI, October 2019. https://sipri.org/sites/default/files/2019-10/the_impact_of_artificial_intelligence_on_strategic_stability_and_nuclear_risk_volume_ii.pdf

"The Digital Great Game." *Strategic Comments* 26, no. 7 (August 8, 2020): iv–vi. https://doi.org/10.1080/13567888.2020.1846453.

Topychkanov, Petr, ed. T*he Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. South Asian Perspectives. Vol. III.* SIPRI, April 2020. https://sipri.org/sites/default/files/2020-04/impact_of_ai_on_strategic_stability_and_nuclear_risk_vol_iii_topychkanov_1.pdf.

Author

Natalya A. Samoylovskaya,

Chair, Russian Student/Young Pugwash Group of the Russian Pugwash Committee under the Presidium of the Russian Academy of Sciences,

Russia, Moscow, 32A Leninskiy Prospect, 119991.

e-mail: natalya.samoylovskaya@gmail.com

ResearcherID: C-6267-2015

Additional information

Received: January 30, 2021. Accepted: February 15, 2021.

Acknowledgments

The author would like to thank reviewers and editors for their valuable and accurate comments that have benefited the research.

Disclosure statement

No potential conflict of interest was reported by the author.

For citation

Samoylovskaya, Natalya. "LAWS with AI: How to aBANdon the Superiority." *Journal of International Analytics* 11, no. 4 (2020): 137–146. https://doi.org/10.46272/2587-8476-2020-11-4-137-146

Смертоносные автономные системы с искусственным интеллектом: как избежать превосходства

АННОТАЦИЯ

Учитывая относительную новизну вопросов военного применения искусственного интеллекта (ИИ), автор изучает его влияние на международные отношения, опираясь на последние доклады международных исследовательских центров, организаций и национальные стратегии и программы. Автор в данной статье рассматривает политические последствия военного применения ИИ, национальные и международные подходы к смягчению его вызовов. Уделяя большое внимание политике двух технологических лидеров в этой области, автор приходит к выводу, что сбалансированная политика США определит, смогут ли Китай и США создать, несмотря на наличие конкуренции, единые правила легализации использования систем ИИ в военной сфере и сформировать единые стандарты, включающие высокий уровень безопасности при использовании этих систем, в том числе в вопросах нераспространения данного вида вооружения. Автор также обращает внимание, что сосредоточенность Европы на конфликте с Россией и ее исключение из среды, создаваемой техническими и этико-правовыми инструментами использования ИИ, усугубит элемент непредсказуемости в двусторонних отношениях. Именно поэтому в интересах Европы привлечь Россию к разработке общей платформы и стандартов для применения ИИ. Разработка и установление единых стандартов безопасности поможет избежать проблем с искаженным восприятием применения ИИ и привнесет элемент предсказуемости в международные отношения.

КЛЮЧЕВЫЕ СЛОВА

ИИ, смертоносные автономные системы, ответственность, США, Китай, ЕС, Россия

Сведения об авторе

Наталья Александровна Самойловская,
председатель молодежного отделения Российского Пагуошского комитета при Президиуме РАН,
Ленинский проспект 32А, 119991.
e-mail: natalya.samoylovskaya@gmail.com
ResearcherID: C-6267-2015

Дополнительная информация

Поступила в редакцию: 30 января 2021. Принята к публикации: 15 февраля 2021.

Благодарности

Автор благодарит рецензентов и редакторов за их ценные и точные комментарии, которые пошли на пользу исследованию.

Конфликт интересов

Автор заявляет об отсутствии потенциального конфликта интересов.

Цитирование

Самойловская, Н.А. Смертоносные автономные системы с искусственным интеллектом: как избежать превосходства // Международная аналитика. – 2020. – Том 11 (4). – С. 137–146. https://doi.org/10.46272/2587-8476-2020-11-4-137-146

Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве

Олег Игоревич Шакиров

https://doi.org/10.46272/2587-8476-2020-11-4-147-170

АННОТАЦИЯ

Сложившееся в последние десятилетия понимание киберпространства как среды, в которой государство может сталкиваться с серьёзными угрозами своей безопасности, способствовало поиску путей предотвращения таких угроз в военно-политической сфере. Одним из решений этой задачи стало обращение к концепции сдерживания, которая в период холодной войны заняла центральное место в стратегии держав. Однако прямой перенос привычных подходов в цифровое пространство оказывается проблематичным. С одной стороны, это накладывает ряд концептуальных ограничений, связанных с применением этой концепции. С другой стороны, способствует дискуссии о том, каким образом можно добиться сдерживания в киберпространстве с помощью традиционных и новых механизмов. Несмотря на неопределённости, возникающие при экстраполяции, на практике ведущие государства используют концепцию сдерживания в контексте их деятельности в киберпространстве, хотя и делают это по-разному. В этой связи в статье автор рассматривает не столько проблемы применения концепции сдерживания в киберпространстве, сколько ее интерпретации государствами при формулировании и реализации политики в этой сфере. Такой конструктивистский подход позволяет выявить специфику восприятия, точки пересечения и расхождения взглядов. На примере России и Соединённых Штатов автор на основе анализа официальных документов и практических кейсов показывает, какие расхождения существуют в интерпретации концепции сдерживания в киберпространстве, как это влияет на позиции России и США по данной проблематике.

КЛЮЧЕВЫЕ СЛОВА

Россия, США, киберпространство, сдерживание, информационная безопасность, кибербезопасность

CC BY

Сдерживание и киберсдерживание

В самом общем виде концепция сдерживания строится на идее о том, что с помощью угрозы одна сторона может убедить другую сторону воздержаться от определённых действий. Угроза заставляет оппонента заново оценить перспективы успеха своих планов и возможные издержки. При этом в англоязычной литературе сдерживание (*deterrence*) отличают от принуждения (*compellence*), подразумевающего использование силы, чтобы заставить другую сторону совершить или не совершить определённые действия.

Необходимо также различать два английских термина, которые часто переводятся на русский как «сдерживание»: *deterrence* и *containment*. Если под первым понимается предотвращение конфликта посредством угрозы, то второй связан с ограничением, удержанием противника в определённых рамках, прежде всего, географических. Понятие *containment* тесно ассоциируется с политикой США во время холодной войны, заключавшейся в ограничении политического влияния социалистического блока в разных регионах мира. В данной статье сдерживание будет рассматриваться в первом значении (*deterrence*).

Сдерживание может пониматься в широком смысле как концепция, применимая в любых конфликтных ситуациях. Но в контексте международной безопасности речь чаще всего идёт о сдерживании от применения военной силы и о военно-политических конфликтах. Энциклопедия РВСН РФ определяет военно-политическое сдерживание как «[систему] мер военно-политического характера, предпринимаемых государством (их коалицией) с целью предотвращения угрозы агрессии или ее эскалации, а также угрозы жизненно важным интересам на основе косвенного, опосредованного использования военной силы в качестве политического средства убеждения противника отказаться от агрессии под угрозой неприемлемых для него последствий в ответных действиях, приводящих к срыву планируемых военно-политических целей»[1].

Идея использования угрозы для предотвращения конфликта имеет долгую историю и, например, отражена в крылатом выражении *Si vis pacem*, *para bellum*. Ю.А. Печатнов выделяет три исторических этапа становления теории сдерживания и соответствующих им парадигм – общепризнанного понимания проблематики сдерживания[2]:

1. Парадигма «стратагемного» сдерживания в неядерном мире (древние времена – начало 1940-х). Сдерживание неотделимо от военного искусства, его политическое значение не рассматривается и больше связывается с приемами, используемыми древними полководцами.

2. Парадигма ядерного сдерживания (1945 г. – конец 1980-х). Основанием этой парадигмы служат концепции и доктрины использования ядерного оружия. По мнению Ю.А. Печатнова, это относится только к США, а в СССР, как он отмечает, формально понятие сдерживания отсутствовало. Однако с такой точкой зрения сложно согласиться. Очевидно, что начиная с ускоренного созда-

1 Сдерживание военно-политическое // Энциклопедия РВСН. Министерство обороны Российской Федерации. [Электронный ресурс]. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14205@morfDictionary (дата обращения: 24.02.2021).

2 Печатнов 2016, 26–27.

ния собственной атомной бомбы, руководство СССР осознавало необходимость иметь возможность нанести ответный удар США и тем самым сдержать их от использования ядерного оружия. В дальнейшем взаимное сдерживание играло определяющую роль во взаимоотношениях между двумя великими державами, приводя как к кризисам, так и к периодам снижения напряжённости. Учитывая исключительную роль ядерного оружия, на этом этапе парадигма сдерживания становится основополагающей для формирования военного и внешнеполитического курса всех ядерных держав.

3. Парадигма стратегического сдерживания (начало 1990-х– настоящее время). Согласно Ю.А. Печатнову, после холодной войны парадигма сдерживания меняется под влиянием новых инструментов силового и несилового давления, а также в связи с геополитическими изменениями. Следуя данному подходу, в рамках такой расширенной парадигмы можно рассматривать и проблематику сдерживания в киберпространстве.

Во время холодной войны (второй этап, согласно Ю.А. Печатнову) возрастает академический интерес к проблеме сдерживания[1]. Г. Снайдер предлагает классическую типологию стратегий сдерживания: «сдерживание посредством недопущения» (*deterrence by denial*) и «сдерживание посредством наказания» (*deterrence by punishment*)[2]. Он иллюстрирует это на военных примерах: в первом случае сдерживание достигается за счёт обладания военной силой, которая может не допустить захвата территории противником; во втором – военная сила увеличивает издержки для противника при нападении настолько, что они превышают возможные выгоды. Г. Снайдер пишет, что сдерживание, как и политическая сила в целом, не должно основываться только на военных возможностях, но может обеспечиваться и невоенными средствами, такими как торговые ограничения. Т. Шеллинг рассматривал концепцию ядерного сдерживания как инструмент торга, уделяя внимание проблемам восприятия и убедительности сдерживания[3].

К основным типологиям сдерживания также относятся[4]:

– Прямое сдерживание, если оно направлено на предотвращение нападений на саму защищающуюся сторону, либо расширенное – в этом случае страна предотвращает нападения на третьи страны, прежде всего на своих союзников.

– Общее сдерживание, рассчитанное на предотвращение нежелательных действий в нормальных условиях на протяжении продолжительного времени, и непосредственное, то есть сдерживание в конкретных кризисных ситуациях.

– Сдерживание в узкой трактовке (когда речь идёт исключительно о военных инструментах) и в широком понимании (в эту концепцию могут включаться невоенные вызовы и средства реагирования на них).

Имея в виду периодизацию развития парадигм сдерживания, описанную выше, можно сказать, что на текущем этапе сдерживание чаще понимается в широком смысле. Однако в конечном счёте определение зависит от контек-

1 Huth 1999.
2 Snyder 1960, 163.
3 Schelling 2008, 23.
4 Mazarr 2018.

ста (например, в военном конфликте достаточным может быть узкая концепция сдерживания).

Распространение концепции сдерживания на киберпространство было обусловлено ее популярностью, прежде всего в ядерных странах, где она стала одной из основ стратегического мышления. Также этому способствовало расширение возможностей использования информационно-коммуникационных технологий (ИКТ) в военных целях. В США, в частности, киберпространство ещё с 1990-х гг. начало восприниматься как самостоятельный театр военных действий, которое описывалось с помощью привычных терминов. Продолжающаяся милитаризация киберпространства и всё более широкий спектр связанной с ним военно-политической деятельности государств сделал сдерживание в этой сфере востребованной задачей.

С одной стороны, перенос концепции сдерживания в киберпространство стимулировал попытки переосмыслить сдерживание применительно к новой практике. Так, исследователи выделяют не только классические, но и дополнительные стратегии сдерживания, которые могут предотвратить конфликт с учётом специфики среды. Дж. Най[1] выделяет четыре основных механизма сдерживания в киберпространстве: помимо классического сдерживания посредством наказания и посредством недопущения, было также выделено сдерживание посредством взаимозависимости (*entanglement*) и посредством формирования норм и табу.

Сдерживание посредством взаимозависимости достигается за счёт того, что ущерб в результате возможной атаки будет нанесён не только жертве, но и самому нападающему. Сдерживание посредством норм и табу должно обеспечиваться выработкой общепринятых правил того, какая деятельность считается приемлемой для государств. Так же как человечество постепенно пришло к недопустимости применения некоторых видов оружия, оно, вероятно, сможет прийти к недопустимости некоторых видов кибератак. Н. Райан добавляет к этому перечню ещё одну стратегию: сдерживание посредством ассоциации – установление виновных в кибератаках и публичная атрибуция к ним, что, как предполагается, должно в дальнейшем изменить их поведение[2].

С другой стороны, прямой перенос этой концепции на киберпространство проблематичен. М. Либики, автор одной из первых книг о киберсдерживании, в 2009 г. обозначил некоторые проблемные вопросы, отличающие сдерживание в киберпространстве от ядерного[3]:

– Можно ли знать, кто стоит за атакой (проблема атрибуции)?

– Может ли быть установлен порог для ответных действий?

– Можно ли избежать эскалации?

– Будут ли третьи стороны (в т.ч. негосударственные акторы) воздерживаться от вмешательства в межгосударственный киберконфликт?

В академической литературе был выделен ряд ограничений, возникающих при переносе концепции сдерживания в киберпространство. Так, М. Таддео рассматри-

1 Nye 2017, 54–62.
2 Ryan 2018, 35–36.
3 Libicki 2009, xvi–xvii.

вает процесс сдерживания на основе абстрактной модели из трёх ключевых элементов: атрибуция, сигнализирование и стратегия[1]. Он показывает, что каждый из этих элементов работает при переносе в киберпространство лишь частично. Проблема атрибуции, с одной стороны, делает кибератаки привлекательными для нападающего, с другой стороны, повышает риск ошибок при возмездии. Из-за сложности быстрой и надёжной атрибуции сдерживание сталкивается с большими неопределённостями, что подрывает его эффективность. Ограничения есть и со стратегиями сдерживания: обороной и наказанием. По мнению М. Таддео, оборона в киберпространстве сводится к обеспечению устойчивости системы в случае атак, но не к их отражению, что принципиально отличается от оборонительных стратегий в традиционном сдерживании. Что касается угрозы возмездия, то автор обращает внимание на отличие сдерживания в киберпространстве от ядерного сдерживания, которое часто используется в качестве аналогии. Так, в частности, киберсдерживание является несимметричным, потенциально повторимым, а угрозы не носят экзистенциальный характер. Проблемы сигнализирования связаны со сложностью убедительной демонстрации своих возможностей для обороны или возмездия, что снижает шансы на эффективное сдерживание.

Несмотря на это Россия и США используют концепцию сдерживания в своих подходах к киберпространству, что позволяет проследить, как на практике учитываются ограничения и неопределённости концепции сдерживания в контексте информационного пространства. Выбор России и США как пары для анализа обусловлен, во-первых, их лидирующими ролями в международных дискуссиях о регулировании государственного поведения в киберпространстве и их влиянием на подходы других стран к этой проблеме. Так, усиление конкуренции в подходах США и России усиливает поляризацию позиций других стран, и напротив, когда им удаётся договориться, это благоприятно сказывается на общей атмосфере переговорных процессов на различных международных площадках. Во-вторых, хотя возможности определить баланс сил в киберпространстве ограничены, Россия и США, очевидно, относятся к ведущим державам в этой сфере, имеющим наиболее развитые стратегические взгляды на киберпространство и связанные с ним вопросы сдерживания.

Наконец, выделение этой пары обусловлено давними традициями двустороннего стратегического взаимодействия между Москвой и Вашингтоном, которое оказывало влияние на их взгляды на сдерживание. Как показано в этой статье, и сегодня изменения в подходах к сдерживанию в киберпространстве в обеих странах нередко происходят под влиянием друг друга.

Конструктивитский взгляд на сдерживание

В качестве теоретической основы для рассмотрения интерпретаций сдерживания в киберпространстве в России и США был выбран подход, предложенный А. Луповичи[2]. Основная идея подхода заключается в том, что сложность обеспечения сдерживания в киберпространстве обусловлена не самими техническими

1 Taddeo 2018.
2 Lupovici 2016.

особенностями этой среды, а интерпретацией в социальном контексте. А. Луповичи отмечает, что понимание того, как киберпространство влияет на поведение, является продуктом социального взаимодействия. Ссылаясь на М. Либики, он пишет, что в этой связи правила в киберпространстве являются социально сконструированными: «Эти правила определяют, что осуществимо, уместно и полезно, и это влияет на то, как защищающаяся сторона демонстрирует угрозу и, что более важно, как эти угрозы интерпретируются предполагаемыми соперниками. Именно поэтому конструктивистский подход к киберсдерживанию, акцентирующий внимание на интерсубъективных понятиях, становится весьма актуальным»[1].

Конструктивистский подход, предлагаемый А. Луповичи, позволяет перевести фокус с проблем переноса концепции сдерживания в киберпространство на особенности *интерпретации* этой концепции государствами, что позволяет в ходе их сравнения выявить общие положения, которые могут послужить опорой для дальнейшего развития взглядов на сдерживание в этой сфере.

Дискуссии о терминологии

Одной из проблем международных дискуссий об информационно-коммуникационных технологиях в контексте международной безопасности является отсутствие общепринятой терминологии. Различая в понятийных аппаратах, используемых государствами, отражают особенности их понимания этой сферы и подходов к обеспечению безопасности в ней. Так, между Россией и США на протяжении многих лет сохраняется расхождение в концептуальных подходах к данной теме. В США и других странах Запада предпочтение отдаётся термину «кибербезопасность», под которым понимается защита компьютерных систем, сетей и данных.

В России на официальном уровне используется термин «информационная безопасность»[2]. Информационная безопасность рассматривается в более широком контексте и подразумевает защищённость как от угроз инфраструктуре и информации (аналогично с кибербезопасностью), так и от потенциального воздействия информации на общественное сознание, политическую и социальную ситуацию[3]. Применительно к состоянию глобального информационного пространства используется термин «международная информационная безопасность»[4] (МИБ), прямого аналога которого в западном дискурсе нет.

1 Lupovici 2016, 328.

2 Информационная безопасность Российской Федерации – «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Подробнее см. Доктрина информационной безопасности Российской Федерации (2016) // Российская газета. 2016. [Электронный ресурс]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 24.02.2021).

3 Remington et al. 2016, 1; *Шариков, П.А.* Российско-американские отношения в сфере информационной безопасности // Московский центр Карнеги. 2013. [Электронный ресурс]. URL: https://carnegieendowment.org/files/Article_Sharikov_Russian.pdf.

4 Международная информационная безопасность – «такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры». Подробнее см. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (2013) // Совет Безопасности Российской Федерации. 2013. [Электронный ресурс]. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 02.03.2021).

Помимо различий в подходах между государствами свои терминологии существуют и на уровне профессиональных сообществ, где предпочтение может отдаваться использованию тех или иных понятий, либо же понятия кибербезопасность и информационная безопасность могут использоваться взаимозаменяемо.

Приставка «кибер-» широко используется политиками, журналистами, авторами популярной литературы для образования названий явлений, связанных с цифровой эпохой: «киберпандемия», «кибер- Перл-Харбор», «кибергигиена». С одной стороны, использование этой приставки вызывает узнаваемую ассоциацию с компьютерами и интернетом и может служить удобной отсылкой для смежных областей. С другой стороны, смысл приставки в результате делается все менее конкретным. Некоторые исследователи, например Э. Фаттер, выступают за отказ от повсеместного использования термина «кибер» и за замену соответствующих слов и словосочетаний более точными терминами[1].

В международных организациях для преодоления разногласий вырабатываются громоздкие консенсусные формулировки. Так, в ООН обсуждения правил поведения государств в киберпространстве на протяжении более чем двух десятилетий проводятся в рамках повестки «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в том числе в форматах Групп правительственных экспертов (ГПЭ) и с 2018 г. – Рабочей группы открытого состава. В ОБСЕ разработка мер доверия для государств в киберпространстве рассматривается в контексте «обеспечения безопасности при всеобъемлющем и многомерном использовании информационных и коммуникационных технологий»[2]. При этом и в рамках ГПЭ, и в ОБСЕ были предприняты шаги по выработке общей терминологии. ГПЭ в докладе 2010 г. рекомендовала найти возможности «для выработки общей терминологии и определений»[3] в связи с обсуждаемыми ей вопросами. В ОБСЕ в аналогичных целях участники договорились в качестве первого шага обменяться перечнями используемых ими терминов[4]. На неправительственном уровне работа ОБСЕ была продолжена, например, фондом «Новая Америка», который при поддержке швейцарского председательства в ОБСЕ запустил проект «Глобальная база данных киберопределений»[5]. Несмотря на все усилия, существенные различия в используемой странами терминологии по-прежнему сохраняются.

В предложенной статье автор опирается на глоссарий «Основы критически важной терминологии» (2-е издание)[6] – российско-американский проект Института проблем информационной безопасности МГУ и Института «Восток-Запад». В глоссарий включены 40 консенсусных определений, выработанных экспертами из Рос-

1 Futter 2018.
2 Решение № 1039 Разработка мер укрепления доверия с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий // ОБСЕ. 2012. [Электронный ресурс]. URL: https://www.osce.org/files/f/documents/6/4/90634.pdf (дата обращения: 24.02.2021).
3 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/70/174 // ООН, Генеральная Ассамблея. 2010. [Электронный ресурс]. URL: https://undocs.org/ru/A/70/174 (дата обращения: 02.03.2021).
4 Решение № 1106 Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий // ОБСЕ. 2013. [Электронный ресурс]. URL: https://www.osce.org/files/f/documents/0/a/109648.pdf (дата обращения: 02.03.2021).
5 "Global Cyber Definitions Database," New America, accessed March 2, 2021, http://cyberdefinitions.newamerica.org/.
6 Godwin et al. 2014.

сии и США. В нём, в частности, даны определения «информационного пространства» («любая среда, в которой информация создается, через которую передается, принимается, в которой хранится, обрабатывается и уничтожается») и «киберпространства» («электронная (включая фотоэлектронные и пр.) среда, в (посредством) которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается») – следовательно, они соотносятся как общее и частное. Также дано определение «кибербезопасности» (свойство киберпространства (киберсистемы) противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз) и аналогичное определение «информационной безопасности» как свойства информационного пространства. Наконец, в глоссарии определены «средства киберсдерживания» (*cyber deterrent*) (признанный механизм, который считается действенным для препятствования киберконфликту, или угрожающей деятельности в киберпространстве). В качестве средств киберсдерживания могут использоваться, в частности, оборонительные и наступательные возможности в киберпространстве.

Логика, которой придерживались авторы глоссария, полезна для рассмотрения вопросов сдерживания в киберпространстве. В случаях, когда киберпространство не упоминается (например, в российских официальных документах), можно исходить из того, что государственная политика в информационном пространстве распространяется и на киберпространство, оставаясь при этом более широкой по смыслу. В тех же случаях, когда речь идёт прежде всего о киберпространстве, кибербезопасности, логика глоссария позволяет держать в уме их тесную взаимосвязь с информационным пространством, возможное воздействие на неэлектронную среду. Фокус на киберпространстве позволяет сузить рамки исследования и охватить сферу, характеризующуюся новизной и неопределённостью с точки зрения применения концепции сдерживания.

Вопросы сдерживания в киберпространстве в российских стратегических документах

В российских официальных документах киберпространство напрямую не упоминается. Речь идёт об информационном пространстве и, соответственно, (международной) информационной безопасности, информационной сфере. Но, как уже было отмечено, киберпространство относится к информационному как частное к общему, и поэтому изложенные подходы релевантны и для киберпространства.

Сдерживание в контексте информационной безопасности, использования ИКТ, занимает важную роль в российских официальных документах. Формально упоминание сдерживания в данном контексте появилось в Военной доктрине 2014 г.[1] По сравнению с редакцией 2010 г.[2] пункт «Основные задачи Российской Федерации по сдерживанию и предотвращению военных конфликтов» в разделе «Деятельность Российской Федерации по сдерживанию и предотвраще-

1 Военная доктрина Российской Федерации (2014) // Российская газета – Федеральный выпуск № 298(6570). 2014. [Электронный ресурс]. URL: https://rg.ru/2014/12/30/doktrina-dok.html (дата обращения: 24.02.2021).
2 Военная доктрина Российской Федерации (2010) // Сайт Президента России. 2010. [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/461 (дата обращения: 24.02.2021).

нию военных конфликтов» был дополнен семью задачами. Одна из них непосредственно касается сдерживания в киберпространстве: «создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности».

Ещё одно важное нововведение Военной доктрины 2014 г. – понятие «система неядерного сдерживания», под которым понимается «комплекс внешнеполитических, военных и военно-технических мер, направленных на предотвращение агрессии против Российской Федерации неядерными средствами». В тексте Доктрины оно не конкретизировано, но, согласно комментариям составителей документа, неядерное сдерживание должно послужить ответом на разнообразные угрозы и вызовы, которые не могут сдерживаться ядерным оружием[1]. Как отмечает А.А. Кокошин, в контексте развития неядерного сдерживания необходимо учитывать и угрозы в киберпространстве[2].

В более раннем документе, Концептуальных взглядах на деятельность Вооруженных Сил Российской Федерации в информационном пространстве 2011 г.[3] (на основе Доктрины информационной безопасности 2000 г. и Военной доктрины 2010 г.), приведён список из 10 правил «сдерживания и предотвращения военных конфликтов в информационном пространстве», включающих как международные усилия по снижению риска возникновения конфликтов в этой области, так и меры военного характера по выявлению угроз, предотвращению конфликтов и противодействию их развития по пути эскалации.

Наконец, в Доктрине информационной безопасности Российской Федерации 2016 г.[4], «стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий» названо первым в списке направлений обеспечения информационной безопасности в соответствии с российской военной политикой (другие направления: обеспечение информационной безопасности Вооружённых сил; прогнозирование и обнаружение угроз; содействие в защите союзников России; нейтрализация информационно-психологического воздействия).

В предыдущей версии Доктрины от 2000 г.[5] термин «сдерживание» не упоминается. Но среди функций государства по обеспечению информационной безопасности названы меры, направленные на «предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации», источники которых могут лежать за пределами России.

1 *Набережнов, Г.* В военную доктрину России внесли положение о неядерном сдерживании // РБК. 2014. [Электронный ресурс]. URL: https://www.rbc.ru/politics/13/12/2014/548bf2c22ae59653833655c9 (дата обращения: 24.02.2021).
2 Кокошин 2014, 203.
3 Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве // Министерство обороны Российской Федерации. 2011. [Электронный ресурс]. URL: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (дата обращения: 24.02.2021).
4 Доктрина информационной безопасности Российской Федерации (2016) // Российская газета. 2016. [Электронный ресурс]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 24.02.2021).
5 Доктрина информационной безопасности Российской Федерации (2000) // Гарант. 2000. [Электронный ресурс]. URL: http://base.garant.ru/182535/. (дата обращения: 24.02.2021).

Хотя в этих документах подробно не рассматриваются средства и способы сдерживания в киберпространстве, сдерживание в них описывается, скорее, в оборонительном ключе, то есть в логике «сдерживания посредством недопущения». Прямых указаний на возможность «сдерживания посредством наказания» в документах нет. Это очевидно при сравнении с ядерным сдерживанием: в Военной доктрине чётко оговаривается, в ответ на какие действия Россия может применить ядерное оружие. Однако в целом описание сдерживания в киберпространстве носит в российских официальных документах общий характер.

Концепция сдерживания в киберпространстве (и шире – информационном пространстве) может получить развитие в российских стратегических документах с принятием новой редакции Стратегии национальной безопасности, ожидаемой в 2021 г.[1], и последующим обновлением Военной доктрины. Также изменения могут быть внесены в Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.[2], которые нуждаются в актуализации. В первоначальной редакции документа упоминание сдерживания отсутствовало, но учитывая описанные в этой статье тенденции, появление этой концепции представляется вероятным.

Практическая реализация подходов России к сдерживанию в киберпространстве

Россия избирательно обнародует информацию о развитии военных возможностей для сдерживания в киберпространстве. Так, информация о создании мультисервисной транспортной сети связи – «военного интернета» – освещается достаточно подробно[3]. Планируется, что эта система будет использоваться для военных задач, данные будут храниться на серверах Минобороны, за счёт чего будет обеспечиваться безопасность и защищённость от внешних угроз. С другой стороны, официально почти не публикуется информация о развитии наступательных и других возможностей российских военных в киберпространстве, особенностях сдерживания угроз в этой среде. Большая часть информации в открытом доступе, в частности об операциях, атрибутируемых российским военным или спецслужбам, базируется на журналистских расследованиях, научных публикациях, отчётах компаний по кибербезопасности или специализированных ведомств западных стран[4]. Таким образом, с точки зрения презентации Россией своих усилий в сфере создания возможностей для сдерживания в киберпространстве, акцент делается на усилении обороны, то есть на создание условий для недопущения нанесения ущерба с помощью ИКТ.

«Сдерживание посредством недопущения», очевидно, служит руководящим принципом и для государственной политики в более широком плане.

1 Совбез заявил о готовности новой редакции Стратегии национальной безопасности // ТАСС. 2021. [Электронный ресурс]. URL: https://tass.ru/politika/10676717 (дата обращения: 02.03.2021).

2 Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (2013) // Совет Безопасности Российской Федерации. 2013. [Электронный ресурс]. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 02.03.2021).

3 *Рамм, А., Козаченко, А., Степовой, Б.* Военный, красивый, суверенный: армия РФ создает закрытый интернет // Известия. 2019. [Электронный ресурс]. URL: https://iz.ru/854961/aleksei-ramm-aleksei-kozachenko-bogdan-stepovoi/voennyi-krasivyi-suverennyi-armiia-rf-sozdaet-zakrytyi-internet (дата обращения: 24.02.2021).

4 См., например, Lilly 2020.

Показательный пример – «Закон о суверенном Рунете/интернете»[1]. При внесении соответствующего законопроекта его авторы, сенаторы А.А. Клишас, Л.Н. Бокова и депутат Госдумы А.К. Луговой, пояснили, что он «подготовлен с учетом агрессивного характера принятой в сентябре 2018 года Стратегии национальной кибербезопасности США» (имеется в виду Национальная киберстратегия, *National Cyber Strategy* 2018), в которой «Россия впрямую и бездоказательно обвиняется в совершении хакерских атак»[2], что требует дополнительных мер по защите работы интернета в России. Закон, принятый и вступивший в силу в ноябре 2019 г., в частности предписывает операторам связи установку фильтрационного оборудования на точках обмена трафиком, Роскомнадзору – создание системы централизованного управления Рунетом. По закону в России должны регулярно проводиться учения по обеспечению стабильности работы интернета, а также должна быть создана национальная система доменных имён, дублирующая глобальную, на случай отключения России от глобального интернета.

Внешними угрозами обосновывается и импортозамещение иностранного программного обеспечения (ПО). По оценкам Совета Безопасности России, использование на российских объектах критической инфраструктуры зарубежного ПО сопряжено с рисками кибербезопасности, поскольку это может содержать недекларированные уязвимости[3].

Обеспечение суверенитета над национальным сегментом интернета[4] может преследовать разные задачи, а их эффективность – оставаться предметом споров, но с точки зрения сдерживания в киберпространстве они могут быть интерпретированы как шаги по снижению уязвимости России от внешних воздействий в киберпространстве и тем самым обеспечивать «сдерживание посредством недопущения» нежелательного ущерба.

Официальные заявления, касающиеся вопросов информационной безопасности и её международного измерения, также могут интерпретироваться для понимания российских подходов к сдерживанию в киберпространстве. На международном уровне основной посыл представителей России чаще всего заключается в необходимости выработки общих правил и использования дипломатии для предотвращения конфликтов. Главным адресатом таких посланий являются США; так, в сентябре 2020 г. российская позиция была высказана на высшем уровне в предложении президента В.В. Путина восстановить двустороннее сотрудничество в области международной информационной безопасности. Согласно его заявлению: «Одним из основных стратегических вызовов современности является риск возникновения масштабной конфронтации в цифровой сфере. Особая ответственность за её предотвращение ле-

1 Федеральный закон от 1 мая 2019 г. N 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Российская газета. 2019. [Электронный ресурс]. URL: https://rg.ru/2019/05/07/fz90-dok.html (дата обращения: 24.02.2021).

2 *Корченкова, Н., Тишина, Ю., Шестоперов, Д.* «Интернет не абонент» // Коммерсантъ. 2018. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3833069 (дата обращения: 24.02.2021).

3 *Петлевой, В., Кантышев, П., Топорков, А.* Зарубежное программное обеспечение – это угроза // Ведомости. 2019. [Электронный ресурс]. URL: https://www.vedomosti.ru/business/articles/2019/01/23/792289-zarubezhnoe-programmnoe-obespechenie (дата обращения: 24.02.2021).

4 Ilona Stadnik, "Sovereign RUnet: What Does it Mean?" Internet Governance Project, Georgia Institute of Technology, 2019, accessed February 24, 2021, https://www.internetgovernance.org/wp-content/uploads/IGPWhitePaper_STADNIK_RUNET-1.pdf.

жит на ключевых игроках в сфере международной информационной безопасности (МИБ)»[1].

Россия не прибегает к практике публичной атрибуции кибератак, в чём проявляется существенное отличие от американского подхода. Более того, российские официальные лица критически оценивают обвинения Вашингтона в адрес конкретных стран в кибератаках и рассматривают такие обвинения как возможный предлог для агрессивных действий. Заместитель секретаря Совета безопасности О.В. Храмов заявил, что участники разведывательного объединения «Пять глаз» (Австралия, Великобритания, Канада, Новая Зеландия, США) «сходятся на том, что виновником компьютерного инцидента можно объявить любое государство и, ссылаясь на закрепленное Уставом ООН право на самооборону, агитируют за возможность предпринимать любые ответные действия»[2]. По его словам, цель обвинения: в одностороннем порядке «легализовать возможность проведения не только информационных, но и военных операций против «неудобных» государств, вплоть до применения ядерных арсеналов»[3].

Если российские представители называют источники тех или иных кибератак, то говорится, как правило, о государстве, с территории которого предположительно осуществлялась вредоносная деятельность. Например, спецпредставитель президента по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских, говоря о нападении на инфраструктуру ЦИК и других российских госорганов в период проведения голосования по поправкам в Конституцию летом 2020 г., заявил: «Источники DDoS-атак мощностью до 240 тыс. запросов в секунду фиксировались с территории США, Великобритании, Украины и ряда стран СНГ»[4].

В российских заявлениях содержатся и намёки на «сдерживание посредством наказания». Так, А.В. Крутских, в 2018 г. комментируя слова Дж. Болтона, на тот момент советника президента США по национальной безопасности, о возможном использовании киберсредств против России, отметил: «А он уверен, что Россия не ответит на подобную провокацию?»[5]. При этом спецпредставитель назвал попытки применить логику сдерживания к киберпространству чудовищной. В июне 2019 г. после публикации *New York Times* о размещении США зловредного ПО (закладок) в российских электросетях, А.В. Крутских процитировал по этому поводу высказывание «кто к нам с кибермечом придет, тот от кибермеча и погибнет»[6]. По его словам, «все политические деятели должны понимать, что за каждым действием будет противодействие. [...] Поэтому желательно этим мечем не размахивать и нас не запугивать»[7].

1 Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности // Сайт Президента России. 2020. [Электронный ресурс]. URL: http://kremlin.ru/events/president/news/64086 (дата обращения: 24.02.2021).

2 *Егоров, И.* Войны виртуальные и реальные // Российская газета. 2019. [Электронный ресурс]. URL: https://rg.ru/2019/08/14/chislo-opasnyh-kiberatak-na-obekty-v-rf-vyroslo-v-11-raz-za-tri-goda.html (дата обращения: 02.03.2021).

3 Там же.

4 При голосовании по конституции в РФ фиксировали DDoS-атаки из США, Великобритании, Украины // ТАСС. 2020. [Электронный ресурс]. URL: https://tass.ru/politika/9391631 (дата обращения: 02.03.2021).

5 *Черненко, Е.В.* Нам не надо бороться за репутацию. Мундир наш и так чист // Коммерсантъ. 2018. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3611689 (дата обращения: 24.02.2021).

6 Крутских: Москву удивляет, что Трамп назвал статью о кибератаках против РФ госизменой // ТАСС. 2019. [Электронный ресурс]. URL: https://tass.ru/politika/6566204 (дата обращения: 24.02.2021).

7 Крутских о киберугрозах и способах противодействия им // Международная жизнь. 2019. [Электронный ресурс]. URL: https://interaffairs.ru/news/show/22314 (дата обращения: 24.02.2021).

Можно предположить, что противодействием от закладок в российских критических системах могли бы по аналогии быть закладки в критических системах другой стороны, например, США. Действительно, Агентство по кибербезопасности и безопасности инфраструктуры США сообщало о российской правительственной киберактивности, мишенью которой, по их сообщению, были различные организации, относящиеся к критической инфраструктуре[1]. Однако необходимо уточнить, что из этих и подобных сведений сложно выделить мотивацию актора, стоящего за такими действиями (являются ли они действительно инструментом сдерживания или решают иные задачи). Кроме того, российские официальные представители последовательно отрицают причастность России к тем или иным приписываемым ей кибератакам, ссылаясь на отсутствие достаточных доказательств.

Вопросы сдерживания в киберпространстве в американских стратегических документах

В США вопросы безопасности киберпространства появляются в официальных документах с 1990-х гг.[2] Первый полноценный стратегический документ в этой сфере – Национальная стратегия для защиты киберпространства[3] – была принята в 2003 г. администрацией Дж. Буша-мл. Хотя в этой стратегии не содержится самого термина «сдерживание», в ней неоднократно упоминается необходимость сдерживать киберугрозы и злонамеренных акторов, способных нанести ущерб критической инфраструктуре США.

Международная стратегия для киберпространства 2011 г.[4], принятая во время президентства Б. Обамы, включила сдерживание в число основных направлений деятельности США по снижению кибер-рисков наряду с правоохранительными мерами, согласованием норм и правил ответственного поведения государств, мерами укрепления доверия и повышения транспарентности и дипломатией. Сдерживание рассматривается в качестве основы оборонительной части стратегии, причём в документе проводится различие между двумя компонентами такого подхода: убеждением отказаться от атак (*dissuasion*) и угрозой возмездия (*deterrence*). Эти два компонента примерно соответствуют «сдерживанию посредством недопущения» и «сдерживанию посредством наказания». Отмечается, что в рамках сдерживания США оставляют «за собой право использовать все необходимые средства – дипломатические, информационные, военные и экономические – по мере необходимости и в соответствии с применимым международным правом»[5]. Использование военной силы рассматривается как крайний вариант.

Несмотря на то что в документе не прописаны конкретные параметры сдерживания в киберпространстве, в нём отмечены такие особенности, как необхо-

1 "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," CISA, 2018, accessed February 24, 2021, https://us-cert.cisa.gov/ncas/alerts/TA18-074A.
2 Стадник 2018, 159.
3 "National Strategy to Secure Cyberspace (2003)," White House, accessed February 24, 2021, https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.
4 "International Strategy for Cyberspace (2011)," White House, accessed February 24, 2021, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
5 Ibid.

димость вовлечения в оборонительные мероприятия всего правительства, частных компаний и граждан, угрозы со стороны преступности и негосударственных акторов, взаимосвязанность безопасности одной страны в киберпространстве с остальным миром. Наконец, в стратегии говорится и о необходимости развития коллективных средств сдерживания в киберпространстве США совместно с партнёрами и союзниками.

При администрации Д. Трампа киберсдерживание ещё более прочно закрепилось в официальных документах по национальной безопасности. Их общей характеристикой стал сдвиг в сторону более решительной и активной политики в киберпространстве на фоне растущих опасений по поводу кибератак и, с другой стороны, желания обеспечить доминирование США в этой среде[1]. В Стратегии национальной безопасности 2017 г.[2] обеспечение безопасности Америки в киберэпоху было выделено в одно из приоритетных направлений в рамках защиты американского народа, страны и образа жизни и включало сдерживание и пресечение деятельности злонамеренных киберакторов. В рамках другого столпа стратегии – «Сохранение мира с помощью силы» – сдерживанию в целом, не только в киберпространстве, отводилась важная роль в возобновившемся «соперничестве великих держав» (стратегическое видение, предложенное администрацией Д. Трампа, предстоящей эпохи как соперничества США с Китаем и Россией). Согласно документу, «сегодня обеспечить сдерживание значительно сложнее, чем во времена холодной войны. Противники изучили американский способ ведения войны и начали развивать возможности, которые нацелены на наши сильные стороны и стремятся использовать наши предполагаемые слабости». К таким возможностям отнесены в том числе киберинструменты. Авторы стратегии делают вывод: «Необходимо распространить сдерживание на все эти области и направить его на все возможные стратегические атаки»[3].

Положения Стратегии национальной безопасности 2017 г. в отношении киберпространства развивались в более специализированных документах: Национальной киберстратегии и Киберстратегии Министерства обороны, принятых в сентябре 2018 г. В первом упомянутом документе сдерживание в киберпространстве вновь рассматривается в контексте сохранения мира с помощью силы. США, с одной стороны, будут продвигать нормы ответственного поведения государств в киберпространстве, а с другой – заниматься атрибуцией и сдерживанием неприемлемого поведения. Это будет обеспечиваться путём идентификации конкретных акторов ответных действий на кибератаки, выстраивания международной коалиции единомышленников для сдерживания в киберпространстве, а также противодействия враждебным информационным операциям[4]. Это отражает меняющееся восприятие угроз в США.

На протяжении многих лет американские представители настаивали на узком понимании кибербезопасности, но в последние годы на фоне скандалов вокруг

1 См. Alexander 2018.
2 "National Security Strategy of the United States of America (2017)," White House, accessed February 24, 2021, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
3 Ibid.
4 "National Cyber Strategy of the United States of America (2018)," White House, accessed February 24, 2021. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

российского вмешательства в президентские выборы 2016 г. и различных примеров злонамеренного использования соцсетей на уровне риторики и в отдельных документах киберугрозы все чаще рассматриваются вместе с другими информационными угрозами в более широком контексте.

Наконец, Киберстратегия Пентагона проецирует «соперничество великих держав» на киберпространство: «мы должны обеспечить способность американских вооружённых сил сражаться и побеждать в войнах в любой сфере, включая киберпространство. Это основополагающее требование национальной безопасности США и залог к обеспечению того, чтобы сдерживать агрессию, включая кибератаки, представляющие собой применение силы, против США, наших союзников и наших партнеров»[1]. Непосредственно о сдерживании в стратегии говорится, что США «стремятся использовать все инструменты национальной силы для сдерживания противников от ведения злонамеренной деятельности в киберпространстве, которая угрожала бы национальным интересам США, нашим союзникам или партнёрам». Для Пентагона это в первую очередь предполагает защиту собственных сетей, но также и готовность при необходимости ответить с использованием военной силы. В этом документе вводятся ещё две концепции, которые также должны способствовать сдерживанию: «передовая оборона» (*defend forward*) в киберпространстве, что предполагает пресечение угроз их источника, а также идея «непрерывного» *(persistent*) соперничества, то есть действий против противников в каждодневном режиме, не только в случае конкретных атак.

Важная особенность всех ключевых официальных документов администрации Д. Трампа, касающихся кибербезопасности, заключается в том, что в них обозначены основные противники, которые воспринимаются в США главным объектом сдерживания в киберпространстве: Китай и Россия как два равных соперника *(peer competitors*) и участника «соперничества великих держав». Также это Иран и КНДР, которые проводят враждебную по отношению к США политику и в том числе могут нанести ущерб национальной безопасности с помощью кибератак. Дополнительно к этим странам (которые некоторые американские чиновники окрестили «большой четвёркой»[2]) в числе противников называются негосударственные акторы: террористы и киберпреступники.

Приход Дж. Байдена в Белый дом в 2021 г. открывает новый этап эволюции взглядов на сдерживание в киберпространстве в американских официальных документах. Можно ожидать, что в этой сфере во многом сохранится преемственность: так, ключевые позиции, связанные с кибербезопасностью, в команде нового президента занимают эксперты с большим опытом службы в предыдущих администрациях, в том числе при Д. Трампе[3]. При этом обновлённые стратегические документы будут приниматься под влиянием как последних событий (в том числе таких широко обсуждаемых взломов, как проникновение хакеров в систе-

1 "Department of Defense Cyber Strategy Summary (2018)," U.S. Department of Defense, accessed February 24, 2021, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
2 "Full Transcript of 'Face the Nation' on December 6, 2020," accessed February 24, 2021, https://www.cbsnews.com/news/full-transcript-of-face-the-nation-on-december-6-2020/.
3 Christopher Bing, and Joseph Menn, "After Big Hack of U.S. Government, Biden Enlists 'world Class' Cybersecurity Team," Reuters, January 22, 2021, accessed February 15, 2021, https://www.reuters.com/article/us-usa-biden-cyber-idUSKBN29R18I.

мы федеральных ведомств в США, раскрытое в конце 2020[1]), так и инициатив различных групп влияния внутри США.

Особого внимания заслуживает работа Комиссии по киберпространству (*Cyberspace Solarium Commission*), которая была учреждена Конгрессом в 2019 г. и названа по аналогии с проектом «Солярий», созданным президентом Д. Эйзенхауэром в 1953 г. для определения согласованной стратегии военно-политического сообщества США по противодействию Советскому Союзу. Целью Комиссии по киберпространству было «выработать консенсус в отношении стратегического подхода к защите Соединенных Штатов в киберпространстве от кибератак, чреватых значительными последствиями»[2], а её мандат включал рассмотрение вопросов сдерживания как одного из вариантов защиты США – наряду с продвижением нормативных режимов и срывом враждебных атак. В состав Комиссии вошли члены палаты представителей и сенаторы от обеих партий, высокопоставленные представители Минобороны, ФБР, Министерства внутренней безопасности и других органов. В её основном докладе в марте 2020 г. в качестве нового стратегического подхода к киберпространству было предложено многоуровневое киберсдерживание (*layered cyber deterrence*)[3]. Предполагается, что США будут сдерживать угрозы на трёх уровнях: формирование (ответственного) поведения в киберпространстве (*shape behavior*); недопущение получения противниками выгод с помощью кибератак (*deny benefits*); повышение издержек за счёт поддержания угрозы возмездия (*impose costs*). Эти компоненты уже составляют основу американского подхода к киберсдерживанию, и доклад Комиссии по киберпространству переосмысляет их как часть цельной стратегии.

Доклад Комиссии сам по себе не носил характер стратегического документа, но он содержал более 80 рекомендаций по имплементации предложенного подхода, и 25 из них были включены в закон об ассигнованиях на оборону на 2021 финансовый год[4]. В преддверии инаугурации Дж. Байдена Комиссия, работа которой была продлена до декабря 2021 г., опубликовала «Белую книгу» для новой администрации с предложениями по дальнейшему внедрению основных в области кибербезопасности в политику, в том числе их закрепление в новой редакции Национальной киберстратегии[5].

Практическая реализация подходов США к сдерживанию в киберпространстве

Демонстрация возможностей в киберпространстве является одной из отличительных черт американского подхода к сдерживанию. Несмотря на то что деятельность военных и спецслужб США в этой сфере далеко не является про-

1 Ellen Nakashima, "Biden Administration Preparing to Sanction Russia for SolarWinds Hacks and the Poisoning of an Opposition Leader," Washington Post, February 23, 2021, accessed March 2, 2021, https://www.washingtonpost.com/national-security/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fa-e0ccb3660358_story.html.

2 "H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019," § 1652, U.S. Congress, 2018, accessed March 2, 2021, https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

3 "Cyberspace Solarium Commission Report," Cyberspace Solarium Commission, March 2020, accessed March 2, 2021, https://www.solarium.gov/report.

4 "Cyberspace Solarium Commission – NDAA Override Press Release," January 2, 2021, accessed March 2, 2021, https://www.solarium.gov/press-and-news/ndaa-override-press-release.

5 "Transition Book for the Incoming Biden Administration. CSC White Paper #5," Cyberspace Solarium Commission, March 2020, accessed March 2, 2021, https://www.solarium.gov/public-communications/transition-book.

зрачной, о ней известно гораздо больше в сравнении с другими государствами. Официальное и полуофициальное (через санкционированные утечки в СМИ) раскрытие информации может рассматриваться в контексте сдерживания в том смысле, что США повышают таким образом убедительность угрозы ответных действий в ответ на кибератаки. При этом сдерживание вряд ли можно считать единственным поводом для открытости, во многом она мотивирована внутриполитическими соображениями, например, необходимостью показать Конгрессу или налогоплательщикам, что действующая администрация решительно противодействует тем или иным угрозам.

В 2020 г. своё десятилетие отметило Киберкомандование США – главный военный инструмент сдерживания в киберпространстве. По мнению М. Уорнера, с момента своего создания командование выполняло три основные миссии: «(1) защита информационных систем Минобороны, (2) поддержка командующих объединёнными силами с помощью кибероперацией, (3) защита нации от значительных кибератак»[1]. Акцент на сдерживании обозначился в повестке Киберкомандования во второй президентский срок Б. Обамы. Необходимость пересмотра подходов к сдерживанию обсуждалась в контексте растущего внимания к кибератакам против США и ограниченным возможностям военных по их предотвращению.

К 2018 г. Киберкомандование достигло запланированного показателя по численности киберсил (военнослужащих, задействованных в проведении кибероперацией), доведя количество военных хакеров из разных родов сил до 6200, объединённых в 133 команды[2]. В том же году статус Киберкомандования был повышен до самостоятельного объединённого боевого командования – до этого киберсилы были подчинены стратегическому командованию. При этом руководство Киберкомандованием с момента создания по настоящий момент осуществляет глава Агентства национальной безопасности. Изначальным мотивом сдвоенной должности являлось то, что молодое командование, физически базирующееся вместе с Агентством в Форт-Миде, сможет использовать экспертизу и возможности наиболее опытной разведслужбы по радиоэлектронной и технической разведке[3]. Однако на протяжении большей части истории Киберкомандования обсуждается целесообразность разделения роли командующего и главы АНБ.

Помимо создания и развития отдельного командования, специализирующегося на противоборстве в киберпространстве, США демонстрируют свои возможности на примере конкретных операций. Наиболее открыто Киберкомандование делится информацией об операции «Сияющая симфония» против ИГИЛ (запрещенная в России организация)[4], в ходе которой американским военным удалось подорвать работу информационных ресурсов террористической группировки. По мнению исследователя Р. Дебера, раскрытие информации о данной опера-

1 Warner 2020.
2 “Cyber Mission Force Achieves Full Operational Capability,” U.S. Department of Defense, accessed February 24, 2021, https://www.defense.gov/Explore/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/.
3 Andrew Schoka, “Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat,” War on the Rocks, April 3, 2019, accessed February 24, 2021, https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.
4 Dina Temple-Raston, “How the U.S. Hacked ISIS,” NPR, September 26, 2019, accessed February 24, 2021, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

ции было обосновано соображениями сдерживания: «Ваши кибероперации не смогут реально сдерживать ваших противников, если те не знают, что у вас есть такие возможности»[1]. Официальные лица, включая главу Киберкомандования П. Накасоне, называли операцию «Сияющая симфония» предшественником усилий «по сдерживанию российского вмешательства в выборы 2018 и 2020 гг.»[2].

В 2018 г. во время промежуточных выборов в Конгресс Киберкомандование, согласно репортажам СМИ на основе анонимных источников, нарушило работу Агентства интернет-исследований в Санкт-Петербурге – организации, которую в США рассматривают как один из инструментов российского вмешательства в американскую политику. В статье *Washington Post* ситуация рассматривается в логике сдерживания: «Некоторые американские чиновники утверждали, что “широкомасштабное стратегическое сдерживание” не всегда является целью. [По словам одного военного чиновника], “Мы показали, что возможно в этой сфере. Это больше не старый подход”. Эта операция была признана успешной сотрудниками Пентагона, а некоторые сенаторы записали в заслуги Киберкомандованию предотвращение вмешательства России в промежуточные выборы»[3].

В 2019 г. *New York Times* со ссылкой на анонимных чиновников сообщила о размещении США закладок в российских электросистемах. В статье не уточняется, кто за этим стоит, но при описании контекста авторы сообщают, что Киберкомандование, отрабатывая сценарии выборов 2020 г., рассматривало возможность избирательного отключения Россией электроэнергии в ключевых штатах. На этот случай Киберкомандованию необходимо было средство сдерживания[4].

Киберкомандование также реализует расширенное сдерживание, направляя специалистов для проведения совместных операций с союзниками или партнёрами на их территории – например, с сентября до ноября 2020 г. американские военные хакеры посещали Эстонию[5]. Эти так называемые «передовые поисковые операции» (*hunt forward operations*) направлены на поддержку местных киберсил, а также на сбор информации, которая будет полезна для сдерживания угроз.

Подход Киберкомандования администрации Д. Трампа суммирован в статье главы командования и директора АНБ П. Накасоне и старшего советника командования М. Салмейера[6] (впоследствии получившего должность старшего директора по кибербезопасности в Совете национальной безопасности Дж. Байдена[7]). Авторы рассказывают о практической реализации концепций «передовой обо-

1 Dina Temple-Raston, “How the U.S. Hacked ISIS.”
2 Dustin Volz, “How a Military Cyber Operation to Disrupt Islamic State Spurred a Debate,” Wall Street Journal, January 21, 2020, accessed February 24, 2021, https://www.wsj.com/articles/how-a-military-cyber-operation-to-disrupt-islamic-state-spurred-a-debate-11579604400.
3 Ellen Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms,” Washington Post, 2019, accessed February 24, 2021, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
4 David E. Sanger, and Nicole Perlroth, “U.S. Escalates Online Attacks on Russia’s Power Grid,” The New York Times, June 15, 2019, accessed February 24, 2021, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.
5 “Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation,” U.S. Cyber Command, December 3, 2020, accessed February 24, 2021, https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/.
6 Paul M. Nakasone, and Michael Sulmeyer, “How to Compete in Cyberspace,” Foreign Affairs, January 20, 2021, accessed February 15, 2021, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.
7 Christopher Bing, and Joseph Menn, “After Big Hack of U.S. Government, Biden Enlists ‘world Class’ Cybersecurity Team,” Reuters, January 22, 2021, accessed February 15, 2021, https://www.reuters.com/article/us-usa-biden-cyber-idUSKBN29R18I. Ellen Nakashima, “Biden Administration Preparing to Sanction Russia for SolarWinds Hacks and the Poisoning of an Opposition Leader.”

роны» и «непрерывного воздействия» в киберпространстве: проведении «передовых поисковых операций» в Черногории и других странах, создании специализированной «малой группы» по противодействию российскому вмешательству, онлайн-борьбе с ИГИЛ (запрещенная в России организация) и пр. Резюмируя, они приходят к следующему выводу: консенсус между разными предложениями по защите США в киберпространстве (включая доклад Комиссии по киберпространству) заключается в том, «что для соперничества в этой среде американские киберсилы должны и далее выступать более активно и реализовывать стратегию по борьбе с вредоносной деятельностью противников онлайн»[1]. Уточняется, что действия США при этом должны соответствовать международному праву. Примечательно, что в статье П. Накасоне и М. Салмейера не используется термин «сдерживание», хотя меры, о которых они пишут, в других контекстах представляются именно так.

В качестве инструмента сдерживания в США также рассматривается публичная атрибуция кибератак, также получившая название стратегии «обвинения и пристыжения» (*blaming and shaming*). Так, в 2014 г. первой страной, против граждан которой США выдвинули обвинение за государственное хакерство, был Китай[2]. Публичная атрибуция со стороны американского правительства может осуществляться в нескольких формах: преимущественно технических отчётах Агентства по кибербезопасности и безопасности инфраструктуры, обвинительных заключениях Министерства юстиции, заявлениях спецслужб, политических заявлениях Госдепартамента и других высокопоставленных чиновников.

Публичная атрибуция позволяет сигнализировать противникам, стоящим за кибератаками, что их действия не остаются скрытыми, и за счёт «пристыжения» создаёт стимул для них воздерживаться от аналогичных действий в будущем, чтобы избежать репутационных и иных издержек. Несмотря на критику эффективности такого подхода, американская практика публичной атрибуции кибератак распространяется и на некоторых их союзников, прежде всего участников объединения «Пять глаз» и Нидерланды.

Публичная атрибуция может сопровождаться введением санкций против лиц и организаций, причастных к кибератакам. Так, в октябре 2020 г. Министерство финансов США ввело санкции по закону *CAATSA* против российской научно-исследовательской организации ЦНИИХМ, которая, по оценке Минфина, участвовала в кибератаке против нефтехимического завода на Ближнем Востоке[3].

Уникальным для киберпространства инструментом сдерживания в США стала так же загрузка образцов зловредного программного обеспечения, используемого противниками, на сайт *VirusTotal*. *VirusTotal* даёт возможность специалистам по кибербезопасности делиться вредоносным кодом, что позволят быстрее проводить анализ подозрительных файлов. Но США, загружая на сайт инструменты, используемые враждебными хакерами или другими странами для кибератак, помогает

1 Paul M. Nakasone, and Michael Sulmeyer, "How to Compete in Cyberspace."
2 "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Justice Department, May 19, 2014, accessed February 24, 2021, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
3 "Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware," U.S. Department of the Treasury, 2020, accessed February 24, 2021, https://home.treasury.gov/news/press-releases/sm1162.

компаниям по кибербезопасности учитывать их при разработке своих решений и при проведении расследований.

Таким образом, Киберкомандование подрывает наступательные возможности оппонентов, выводя из строя их киберорружие. На *VirusTotal* благодаря американским военным попали образцы кода, предположительно используемого северокорейскими[1], иранскими[2] и российскими хакерами[3].

Защита собственной инфраструктуры также интерпретируется в США как часть сдерживания в широком понимании. Это стало особенно заметно в контексте обеспечения безопасности электоральных процессов, что можно рассматривать как «сдерживание посредством недопущения». Так, после президентских выборов 2020 г. руководитель Агентства по кибербезопасности и безопасности инфраструктуры США заявил об отсутствии свидетельств о внешнем вмешательстве, причиной чего стала хорошая подготовка властей на разных уровнях и привлечение к защите выборов частного сектора.

Дипломатия также рассматривается в США как средство сдерживания угроз в киберпространстве. Вашингтон вместе с союзниками активно продвигает необходимость выработки и соблюдения правил ответственного поведения государств в киберпространстве. Во время президентства Б. Обамы США заключили двусторонние договорённости по безопасности в киберпространстве с Россией в 2013 г.[4] и Китаем в 2015 г.[5] Однако сегодня опыт этих соглашений для предотвращения киберугроз в США оценивается неоднозначно. Так называемая «горячая линия» по вопросам, связанным с киберугрозами, между Россией и США сохраняется, но в Вашингтоне считают, что созданные механизмы не предотвратили вмешательство в выборы 2016 г.[6] Американо-китайское соглашение о том, что стороны не будут проводить друг против друга кибероперации с целью кражи интеллектуальной собственности, согласно оценкам американских фирм по кибербезопасности, в течение первого года после заключения привело к резкому снижению китайских кибератак против американских компаний. Однако к началу президентства Д. Трампа атаки возобновились[7]. Представитель АНБ Р. Джойс в 2018 г. заявлял, что, по мнению США, Китай не соблюдал договорённости[8].

1 Shannon Vavra, "Cyber Command's Biggest VirusTotal Upload Looks to Expose North Korean-Linked Malware," CyberScoop, September 8, 2019, accessed February 24, 2021, https://www.cyberscoop.com/cyber-command-virus-total-north-korean-malware/.
2 Shanon Vavra, "Why Cyber Command's Latest Warning Is a Win for the Government's Information Sharing Efforts," CyberScoop, July 10, 2019, accessed February 24, 2021, https://www.cyberscoop.com/cyber-command-information-sharing-virustotal-iran-russia/.
3 Catalin Cimpanu, "US Cyber Command Exposes New Russian Malware," ZDNet, November 1, 2020, accessed February 24, 2021, https://www.zdnet.com/article/us-cyber-command-exposes-new-russian-malware/.
4 Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия // Сайт Президента России. 2013. [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/1479 (дата обращения: 24.02.2021).
5 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," White House, September 25, 2015, accessed February 24, 2021, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.
6 Erin Banco, and Kevin Poulsen, "This Hotline Could Keep the U.S. and Russia From Cyberwar," The Daily Beast, February 23, 2019, accessed February 24, 2021, https://www.thedailybeast.com/this-hotline-could-keep-the-us-and-russia-from-cyber-war.
7 Laskai et al. 2018.
8 "U.S. Accuses China of Violating Bilateral Anti-Hacking Deal," Reuters, November 9, 2018, accessed February 24, 2021, https://www.reuters.com/article/us-usa-china-cyber-idUSKCN1NE02E.

Выводы

Теоретические подходы к сдерживанию в киберпространстве развиваются в тесной связке с их практическим использованием для обеспечения странами своих интересов в этой сфере. Как показано в статье, классические и новые способы сдерживания находят применение в арсенале России и США. Однако, учитывая ограниченность эмпирических знаний, говорить об эффективности тех или иных подходов преждевременно.

Важно учитывать процесс конструирования странами практики сдерживания в киберпространстве. Попытка интерпретации российских и американских взглядов на сдерживание в киберпространстве, предпринятая в этой статье, позволяет сопоставить их и обратить внимание на характерные для каждой страны особенности. Как в США, так и в России, сдерживание в киберпространстве закреплено в официальных документах. В России эта концепция понимается в более широком контексте обеспечения информационной безопасности. При этом параметры сдерживания представлены в стратегических документах в общих чертах и не конкретизированы. В США развитие концепции киберсдерживания в официальных документах имеет более долгую историю, а её описание более детализировано. И в России, и в США сдерживание в киберпространстве понимается прежде всего в военно-политическом смысле, но не исключительно. Американский подход предполагает использование для сдерживания разных инструментов; в России подчеркивается роль дипломатии и международных договорённостей как средства предотвращения конфликтов.

Наиболее заметное различие во взглядах, вероятно, заключается в том, что и на уровне документов, и на практике США делают ставку на «сдерживание посредством возмездия». Это проявляется, в частности, в готовности демонстрировать возможности по сдерживанию в киберпространстве. США за счёт относительно открытого строительства Киберкомандования, раскрытия деталей некоторых кибероперaций стремятся сделать угрозу возмездия в киберпространстве более убедительной. Российская демонстрация возможностей «сдерживания посредством возмездия» на официальном уровне отсутствует. Но принимая во внимание высказывания российских официальных представителей, а также сообщения о приписываемых России атаках, справедливо полагать, что и в Москве рассматривают «сдерживание посредством возмездия» как возможную стратегию.

Россия, в свою очередь, на практике делает акцент на оборонительных мерах, что можно трактовать как предпочтение «сдерживанию посредством недопущения». Несмотря на различие используемых мер, у России и США схожее понимание необходимости защиты критической инфраструктуры как части сдерживания в более широкой трактовке, однако в США практика «возмездия» превалирует над практикой «недопущения».

Две страны придерживаются противоположных взглядов на проблему публичной атрибуции кибератак. В Вашингтоне публичную атрибуцию считают одним из способов сдерживания киберугроз. И хотя её эффективность остаётся дискуссионным вопросом, США продолжают использовать этот инструмент и призывают к коллективной атрибуции союзников. В Москве же обвинение

в адрес конкретных государств считают не только нелегитимными из-за недостаточной доказанности, но и потенциально опасными, поскольку они могут использоваться для оправдания агрессивных действий против предполагаемых виновников. Соответственно, Россия не рассматривает атрибуцию как средство сдерживания.

Подходы к сдерживанию в киберпространстве в обеих странах эволюционируют, причём некоторые изменения связаны с поведением другой стороны. Так, в России обоснованием «Закона о суверенном Рунете/интернете» стало принятие новой Национальной киберстратегии США, в которой Россия обозначалась в качестве угрозы. В этом документе сдерживание не только распространяется на киберпространство, но и захватывает информационные угрозы – то, против чего США многие годы выступали на международных площадках.

Это наблюдение подводит к выводу о том, что подходы к сдерживанию в двух странах формируются по мере взаимных попыток истолковать намерения и поведение друг друга. Этот процесс носит долгосрочный характер и тесно связан с проблемой выработки общих глобальных подходов к киберпространству.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Кокошин, А.А. Стратегическое ядерное и неядерное сдерживание: приоритеты современной эпохи // Вестник Российской академии наук. – 2014– Т. 84 (3). – С. 195–205. https://doi.org/10.7868/S0869587314030086. [Kokoshin, A. A. "Strategic Nuclear and Non-nuclear Deterrence: Priorities of the Modern Era." [Strategicheskoe yadernoe i neyadernoe sderzhivanie: prioritety sovremennoi ehpokhi] *Bulletin of the Russian Academy of Sciences* 84, no. 3 (2014): 195–205] [In Russian].

Печатнов, Ю.А. Теория сдерживания: генезис // Вооружение и экономика. – 2016. – №2 (35). – С. 26–27. [Pechatnov, Yu. A. "Theory of Deterrence: Genesis." [Teoriya sderzhivaniya: genezis] *Armament and Economics*, no. 2 (2016): 26–27] [In Russian].

Стадник, И.Т., Цветкова, Н.А. Политика кибербезопасности США эволюция восприятия угроз // Международные процессы. – 2018. – Т. 16 (3). – С. 157–169. https://doi.org/10.17994/IT.2018.16.3.54.9. [Stadnik, Ilona, and Natalia Tsvetkova. "United States Cybersecurity Policy." [Politika kiberbezopasnosti SSHA ehvolyutsiya vospriyatiya ugroz] *International Trends / Mezhdunarodnye Protsessy* 16, no. 3 (February 1, 2019): 157–169] [In Russian].

Alexander, Keith B., and Jamil N. Jaffer. "Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition." *Georgetown Journal of International Affairs* 19 (2018): 51–66.

Futter, Andrew. "'Cyber' Semantics: Why We Should Retire the Latest Buzzword in Security Studies." *Journal of Cyber Policy* 3, no. 2 (May 4, 2018): 201–16. https://doi.org/10.1080/23738871.2018.1514417.

Godwin III, J. B., Andrey Kulpin, Karl F. Rauscher, and Valery Yaschenko. *Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity.* East-West Institute, Policy Report 2, 2014. http://www.ipib.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%202.pdf.

Huth, Paul K. "Deterrence and International Conflict: Empirical Findings and Theoretical Debates." *Annual Review of Political Science* 2, no. 1 (June 1999): 25–48. https://doi.org/10.1146/annurev.polisci.2.1.25.

Laskai, Lorand, and Segal, Adam. *A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage*. Council on Foreign Relations, 2018. https://www.cfr.org/report/threat-chinese-espionage.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. RAND Corporation, 2009. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Lilly, Bilyana, and Joe Cheravitch. "The Past, Present, and Future of Russia's Cyber Strategy and Forces." In *2020 12th International Conference on Cyber Conflict (CyCon),* 129–55. Estonia: IEEE, 2020. https://doi.org/10.23919/CyCon49761.2020.9131723.

Lupovici, Amir. "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward." *International Studies Perspectives* 17, no. 3 (August 1, 2016): 322–42. https://doi.org/10.1111/insp.12082.

Mazarr, Michael J. *Understanding Deterrence.* RAND Corporation, 2018. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (January 2017): 44–71.

Remington, T., Chris Spirito, Elena Chernenko, Oleg Demidov, and Vitaly Kabernik. *Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity*. Working Group on the Future of U.S.-Russia Relations Paper 7, 2016. https://us-russiafuture.org/publications/working-group-papers/toward-u-s-russia-bilateral-cooperation-in-the-sphere-of-cybersecurity/.

Ryan, N. J. "Five Kinds of Cyber Deterrence." *Philosophy & Technology* 31, no. 3 (September 27, 2018): 331–38. https://doi.org/10.1007/s13347-016-0251-1.

Schelling, Thomas C. *Arms and Influence.* Yale University Press, 2008.

Snyder, Glenn H. "Deterrence and Power." *The Journal of Conflict Resolution* 4, no. 2 (June 1960): 163–78.

Taddeo, Mariarosaria. "The Limits of Deterrence Theory in Cyberspace." *Philosophy & Technology* 31, no. 3 (September 16, 2018): 339–55. https://doi.org/10.1007/s13347-017-0290-2.

Warner, Michael. "US Cyber Command's First Decade." *A Hoover Institution Essay. Aegis Series Paper,* no. 2008 (2020). https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf.

Сведения об авторе

Шакиров Олег Игоревич,
консультант ПИР-Центра, Россия, 119019, Москва, а/я 147.
e-mail: shakirov@pircenter.org

Дополнительная информация

Поступила в редакцию: 1 декабря 2020. Принята к публикации: 31 января 2021.

Конфликт интересов

Автор заявляет об отсутствии потенциального конфликта интересов.

Цитирование

Шакиров, О.И. Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве // Международная аналитика. – 2020. – Том 11 (4). – С. 147–170. https://doi.org/10.46272/2587-8476-2020-11-4-147-170

Whoever Comes to Us With a Cyber Sword: Russian and U.S. Approaches to Deterrence in Cyberspace

ABSTRACT

Developed in recent decades, the understanding of cyberspace as an environment in which a state can face serious threats to its security has contributed to a search for ways to prevent such threats. In the military and political spheres, the concept of deterrence has become one of the ways to solve this problem. During the Cold war, the policy of deterrence became central to the strategic thought in the leading countries, but the direct transfer of conventional approaches to a new reality turns out to be problematic. On the one hand, this opens up a debate about the ways to attain deterrence in cyberspace via traditional and new mechanisms. However, theoretical discussions on cyberspace deterrence highlight the limitations of this concept. At the same time, despite some uncertainties that stem from such a transfer, in practice, the leading states use the concept of deterrence in the context of their activities related to cyberspace, although they implement it differently. In this regard, the article suggests focusing on states' interpretation of deterrence when designing and implementing their policies in this area, rather than on the problems of applying the concept of deterrence. Such a constructivist approach allows to reveal the peculiarities of the understanding of deterrence without considering them predetermined and identify common aspects of views. Using Russia and the United States as examples, we studied specific features of the application of the deterrence concept in respect to cyberspace in official documents and in the course of the practical implementation of their provisions. The analysis shows that countries interpret the concept of cyberspace deterrence in different ways, with an emphasis on specific deterrence strategies. At the same time, Russia and the United States influenced each other while developing views on deterrence.

KEYWORDS

Russia, United States, cyberspace, deterrence, information security, cyber security

Author

Oleg I. Shakirov,
Consultant of the PIR Center, Russia, 119019, Moscow, po / po 147.
e-mail: shakirov@pircenter.org

Additional Information

Received: December 1, 2020. Accepted: January 31, 2021.

Disclosure statement

No potential conflict of interest was reported by the author.

For citation

Shakirov, Oleg I. "Whoever Comes to Us With a Cyber Sword: Russian and U.S. Approaches to Deterrence in Cyberspace." *Journal of International Analytics* 11, no. 4 (2020): 147–170. https://doi.org/10.46272/2587-8476-2020-11-4-147-170

О теории космической мощи

Bowen, Bleddyn E. War in Space: Strategy, Spacepower, Geopolitics. Edinburgh: Edinburgh University Press, 2020.

Дмитрий Викторович Стефанович

https://doi.org/10.46272/2587-8476-2020-11-4-171-176

В настоящее время стремительно растет роль космического пространства как новой сферы международного противоборства. При этом, как представляется, практически отсутствуют попытки найти теоретические основы такого противоборства, равно как и его анализа. В книге «Война в космосе» доктор Б. Боуэн сделал смелую попытку по формированию такой теоретической основы в целях изучения проблематики «космической мощи»[1].

В самом словосочетании «космическая мощь» заключена отсылка к классическим работам А.Т. Мэхэна (о морской мощи) и Д. Дуэ (о господстве в воздухе). Б. Боуэн активно использует наследие видных военных теоретиков прошлого и настоящего (от К. фон Клаузевица до Э. Долмана; внимание также уделяется и наследию адмирала С.Г. Горшкова), творчески его перерабатывает и справедливо отмечает, что за многие десятилетия освоения космического пространства до настоящего времени так и не появилось полноценной теории космической мощи, или господства в космосе.

В целях создания такой теории автор выдвигает семь утверждений, или принципов, а именно:

– космическая война ведется ради господства в космосе;

– космическая мощь уникальна в инфраструктурном смысле и связана с Землей;

– господство в космосе не означает господства на Земле;

– господство в космосе позволяет управлять небесными линиями связи;

– земная орбита – это космическая береговая линия, подходящая для стратегических маневров;

1 Из этого краткого обзора очень важной книги сознательно исключены, что называется «заклепки», то есть сугубо технические вопросы, связанные с космическими и противокосмическими вооружениями, небесной механикой, орбитальной инфраструктурой разведки и целеуказания, связи и проч., осознание которых весьма способствует более глубокому пониманию проблематики противоборства в космосе – равно как нежелание разбираться в «железе» и «физике» значительно снижает уровень любой дискуссии по данному вопросу. Отметим, что Б. Боуэн в полной мере продемонстрировал обладание необходимыми знаниями для профессионального исследования заданной темы.

CC BY

– космическая мощь существует в рамках геоцентрического мышления;

– космическая мощь рассредоточена и способствует рассредоточению на Земле.

В первой части книги доктор Б. Боуэн сводит первые четыре принципа к условным «имперским традициям», привязывая их к концепции доминирования в космосе (что в определённой мере находит отражение в актуальных документах военного планирования в сфере космической деятельности, например, в США[1]). Во второй части два последующих утверждения позволяют сформулировать «новый образ» космической мощи через введение понятия «небесного побережья». Третья и заключительная часть увязывает космическую мощь и боевые действия на поверхности Земли путем подробного изложения седьмого принципа. В ней также иллюстрируется его «реализация» на примере сценария американо-китайского конфликта вокруг Тайваня.

Следует подчеркнуть, что автор неоднократно отмечает исключительно научное значение своего подхода. Цель работы – формирование понятийного инструментария в рамках теории международных отношений, адаптированного для исследования противоборства в космическом пространстве. Иными словами, Б. Боуэн не ставит себе задачу сформулировать оптимальную «космическую стратегию» для того или иного государства, но предлагает подход, который позволяет анализировать такие стратегии, а также реальные шаги государства в космосе.

Остановимся подробнее на семи базовых принципах, или утверждениях, которые предлагается использовать в качестве основы для анализа космического противоборства с точки зрения теории международных отношений.

Первый принцип определяет, что боевые действия в космосе должны быть направлены на достижение господства в космосе, которое может заключаться в контроле космической инфраструктуры и/или недопущении ее использования противоборствующей стороной. При этом такое господство должно быть увязано с политическими целями государства на Земле.

Второй принцип подчеркивает необходимость осознания уникальных свойств околоземной орбиты, что обуславливает характер космической мощи как пространства, в первую очередь, для инфраструктуры, а не для боевых платформ. Одновременно космическая мощь не может быть в изоляции от потенциала государства на Земле.

Третий принцип сформулирован как аргумент против общепринятого мнения о том, что господство в космосе автоматически ведет к господству на Земле, т. н. концепции *Ultimate High Ground*[2], т. е. «абсолютной высоты» (в военном смысле этого слова). Данный принцип является своего рода предостережением от чрезмерного сосредоточения на стратегии государства по уничтожению вражеских космических систем, что зачастую является аксиомой для военных, ищущих «центр тяжести» противника для нанесения сокрушительного удара.

В четвертом принципе изложено то, как «небесные линии коммуникаций» соединяют воедино компоненты космической инфраструктуры, а также то, как возможно достижение господства в космосе путем сосредоточения на узких ме-

1 "Defense Space Strategy Summary," June 2020, accessed March 3, 2021, http://surl.li/mvqe.
2 Benjamin S. Lambeth, "Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space," Santa Monica, CA: RAND Corporation, 2003, accessed March 5, 2021, https://www.rand.org/pubs/monograph_reports/MR1649.html.

стах противника и его ключевых позиций как на околоземной орбите, так и на земной поверхности.

Как уже упоминалось, первые четыре принципа фактически перерабатывали существующие элементы теории космической мощи, заимствующие отдельные постулаты теории морской мощи. На этой основе и формируются следующие утверждения/принципы.

Пятый принцип обосновывает взгляд на орбиту Земли как на «космическую береговую линию»: околоземная орбита и поверхность Земли являются своего рода прибрежными зонами, в которых необходимы стратегические маневры. Автор отмечает, что идеи «континентальной» теории морской мощи (с использованием отдельных постулатов теории С.Г. Горшкова, а также в соответствии с подходами французского военно-морского теоретика Р. Кастекса) позволяют взглянуть на ряд таких аспектов космической мощи, которыми часто пренебрегают: подобно прибрежной зоне, подходящей для стратегических маневров, космическая мощь на околоземной орбите напоминает использование морской мощи именно континентальными государствами (Россия, Франция), а не морскими державами (Великобритания, США).

Шестой принцип развивает эту континентальную аналогию; в нем обосновывается следующий тезис: все, что происходит в космосе, имеет значение только тогда, когда оно влияет на Землю, то есть «земные» угрозы при прочих равных воспринимаются как приоритетные относительно «космических» пространств.

Седьмой принцип является, пожалуй, наиболее важным и сложным, переводящим теорию космической мощи от абстрактных, высоких «стратегических» вопросов к непосредственно современным боевым действиям. Этот принцип обосновывает влияние космической мощи как способствующей рассредоточению военного потенциала государства и увеличению интеграции и координации боевых элементов армии на общем театре военных действий. Также подчеркивается, что в условиях «враждебного небесного побережья» сохраняют актуальность концепции концентрации и рассредоточения сил и средств как на Земле, так и в околоземном пространстве.

Стоит отметить весьма творческий подход автора к анализу упомянутого ранее сценария американо-китайского конфликта вокруг Тайваня. Он позволяет продемонстрировать, что «космическая» война никак не может быть отделена от войны «земной», что ведет к, казалось бы, очевидному, но все же зачастую ускользающему выводу: в современных военно-политических условиях нельзя изолировать космическую стратегию.

Военные и политические процессы на Земле определяют то, как космическое пространство используется. В свою очередь, космическая инфраструктура стала неотъемлемой частью военной и экономической мощи и, соответственно, потенциальной целью в военное время. Подобно тому, как самолеты дальнего радиолокационного обнаружения и управления открыто заявляются как приоритетные цели для зенитно-ракетных комплексов большой дальности[1], нет

1 С-400 «Триумф» // Рособоронэкспорт. [Электронный ресурс]. URL: http://roe.ru/catalog/protivovozdushnaya-oborona/zenitnye-raketnye-kompleksy-i-ustanovki/s-400-triumf/ (дата обращения: 03.03.2021).

ни малейших сомнений, что и разведывательные спутники в случае реального конфликта станут столь же приоритетными целями для всех возможных средств поражения (кинетического и некинетического). Другой вопрос в том, как не допустить такого конфликта.

Б. Боуэн подчеркивает, что раз космическая война является продолжением земной политики, то «старые теории и концепции относительно человеческого политического опыта приобретают новую жизнь в новейшей среде, и именно системные и не поддающиеся количественной оценке политические соображения должны сопровождать анализ боевых действий в космосе». По мнению автора, это не только повышает «канон» стратегической теории, который необходимо перенести в «астрополитику», но может также повысить применимость других инструментов из арсенала теории международных отношений для исследования космического пространства.

В отечественной военно-теоретической традиции, как представляется, доминирует взгляд на космическое пространство как продолжение пространства воздушного, отсюда и приоритет единой воздушно-космической обороны, формирование Воздушно-космических сил Российской Федерации[1], а также шаги в направлении создания объединенной системы воздушно-космической обороны государств-участников СНГ[2]. Вероятно, космическое пространство в данном случае воспринимается в целом в рамках предложенной Б. Боуэном концепции «космической береговой линии», но не как «космический океан».

При этом определенное число научных работ посвящено анализу изменений в части использования космического пространства в военных целях, и, как правило, подчеркивается постепенное смещение от «обеспечивающего» к «ударному» функционалу[3]. Вместе с тем сохраняется понимание тесной взаимосвязи происходящего в космосе и на земле (и в других средах)[4], а также необходимости интеграции соответствующих мер противодействия[5].

Возможно, на сегодняшний день актуальной задачей для отечественных специалистов в области теории международных отношений, международной безопасности, космических технологий становится формирование собственных общетеоретических междисциплинарных подходов к анализу противоборства в космосе, либо адаптации наработок иностранных коллег в данной области к российским подходам.

1 Служить здесь почётно и интересно // Красная звезда. 31 июля 2020. [Электронный ресурс]. URL: http://redstar.ru/sluzhit-zdes-pochyotno-i-interesno/ (дата обращения: 03.03.2021).
2 Объединенной системе противовоздушной обороны государств – участников СНГ исполнилось 26 лет // Исполнительный комитет СНГ. 11 февраля 2021. [Электронный ресурс]. URL: https://cis.minsk.by/news/17934/obedinennoj_sisteme_protivovozdushnoj_oborony_gosudarstv_%E2%80%93_uchastnikov_sng_ispolnilos_26_let (дата обращения: 03.03.2021).
3 Макаренко 2016.
4 Стучинский, Корольков 2020.
5 Хряпин, Евсюков 2020.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Макаренко, С.И. Использование космического пространства в военных целях: современное состояние и перспективы развития систем информационно-космического обеспечения и средств вооружения // Системы управления, связи и безопасности. – 2016. – №4. – С. 161–213. [Makarenko, Sergey I. "Use of Outer Space for Military Purposes: Current State and Prospects for the Development of Information and Space Support Systems and Weapons." [Ispol'zovanie kosmicheskogo prostranstva v voennyh celyah: sovremennoe sostoyanie i perspektivy razvitiya sistem informacionno-kosmicheskogo obespecheniya i sredstv vooruzheniya] *Control, Communication and Security Systems*, no. 4 (2016): 161–213] [In Russian].

Стучинский, В.И., Корольков, М.В. Обоснование боевого применения авиации для срыва интегрированного массированного воздушного удара в многосферной операции противника // Воздушно-космические силы. Теория и практика. – 2020. – №. 16. – С. 29–36. [Stuchinsky, V.I., and M.V. Korolkov. "The Rationale for the Combat Application of Aviation to Disrupt an Integrated Massive Air Strike in a Multispectral Enemy Operation." [Obosnovanie boevogo primeneniya aviacii dlya sryva integrirovannogo massirovannogo vozdushnogo udara v mnogosfernoj operacii protivnika] *Air and Space Forces. Theory and Practice,* no. 16 (2020): 29–36] [In Russian].

Хряпин, А.Л., Евсюков, А.В. Роль новых систем стратегических вооружений в обеспечении стратегического сдерживания // Военная мысль. – 2020. – №. 12. – С. 26–30. [Hryapin, Alexandr L., and A.V. Evsykov. "The Role of Emerging Strategic Weapon Systems in Strategic Deterrence." [Rol' novyh sistem strategicheskih vooruzhenij v obespechenii strategicheskogo sderzhivaniya] *Military Thought,* no. 12 (2020): 26–30] [In Russian].

Сведения об авторе

Стефанович Дмитрий Викторович,

научный сотрудник Центра международной безопасности, Национальный исследовательский институт мировой экономики и международных отношений им. Е.М. Примакова РАН (ИМЭМО РАН), Москва, Россия. Ул. Профсоюзная, 23. 117997.

e-mail: stefanovich@imemo.ru

Дополнительная информация

Поступила в редакцию: 30 декабря 2020. Принята к публикации: 3 января 2021.

Конфликт интересов

Автор заявляет об отсутствии потенциального конфликта интересов.

Цитирование

Стефанович, Д.В. О теории космической мощи // Международная аналитика. – 2020. – Том 11 (4). – С. 171–176.
https://doi.org/10.46272/2587-8476-2020-11-4-171-176

Author

Dmitry V. Stefanovich,
Research fellow, Center for International Security, IMEMO RAS,
Moscow, Russia. Profsouznaya str. 23, 117997.
e-mail: stefanovich@imemo.ru

Additional information

Received: December 30, 2020. Accepted: January 3, 2021.

Disclosure statement

No potential conflict of interest was reported by the author.

For citation

Stefanovich, Dmitry V. "On Theory of Space Power."
Journal of International Analytics 11, no. 4 (2020): 171–176.
https://doi.org/10.46272/2587-8476-2020-11-4-171-176

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

Представление рукописей на рассмотрение редакционной коллегией осуществляется через сайт журнала www.interanalytics.org в разделе «Отправить статью» или по электронной почте: submissions@interanalytics.org

Подача статьи осуществляется в формате двух файлов: текст статьи без указания сведений об авторе и текст с информацией об авторе. Такое разделение мотивировано правилами двойного слепого рецензирования.
Во втором файле мы приветствуем указание идентификатора автора: ORCID, SPIN-код, Researcher ID, Scopus Author ID, РИНЦ Author ID.

Журнал выпускает аналитические материалы по трём направлениям: исследовательская статья, обзорная статья, рецензия.

Исследовательская статья содержит результаты самостоятельных исследований автора и несет добавочное научное знание. Обзорная статья даёт другим исследователям представление о текущем состоянии и направлении развития некоторой области знаний, теории или методов. Рецензия является критическим очерком о прочитанном научном исследовании.

Объем научной литературы, рассматриваемый автором, должен содержать как минимум 20 работ, в том числе и наиболее свежие по теме исследования. В список литературы не включаются ссылки на авторефераты, диссертации, учебники, учебные пособия, ГОСТы, распоряжения.

К публикации принимаются статьи объемом от 35 000 до 45 000 знаков с пробелами без метаданных. Материалы для рецензий принимаются в виде краткой (до 25 000 знаков с пробелами) аналитической рецензии на недавно вышедшую книгу по тематике журнала. Работа должна быть оригинальной. Неоригинальные материалы не принимаются к рассмотрению.

Аннотация объемом 250–300 слов должна содержать характеристику темы исследования и основные выводы. Аннотация должна быть представлена на русском и английском языках.
После аннотации следуют ключевые слова (до 7 слов) также на двух языках.

При оформлении списка литературы, полные требования по которому указаны на сайте журнала www.interanalytics.org в разделе «Правила для авторов», не забудьте указать имеющийся DOI всех цитируемых работ. Указание DOI осуществляется путем добавления рабочей гиперссылки в конце библиографического описания работы. Проверить наличие DOI можно на сайте www.crossref.org, в разделе Simple Text Query.

За разрешением на перепечатку или перевод опубликованных в нашем журнале материалов обращаться в Редакцию.

Содержание статей не обязательно отражает точку зрения Учредителя и Редакции.

Адрес редакции:
Проспект Вернадского, 76Б. Москва, 119454.

Оформить подписку на журнал «Международная аналитика» можно:
в почтовом отделении по каталогу «Пресса России», подписной индекс 38777;
по интернет-каталогу ООО «Агентство «Книга-Сервис», а также по каталогам стран СНГ www.akc.ru

Международная аналитика. – 2020. – 11(4). – С. 1-176.
Подписано к печати: 20.03.21.
Формат: 108x70/16. Печать офсетная. Цена свободная.
Уч.-изд. л. 11. Тираж 200 экземпляров. Заказ
Отпечатано в отделе оперативной полиграфии и множительной техники МГИМО МИД России.
119454, Москва, просп. Вернадского, 76.