Специальное издание Connections

Connections
Ежеквартальный журнал

Консорциум «Партнерство ради мира» военных академий и институтов по изучению вопросов безопасности

Сдерживание в международной безопасности: Теория и современная практика

под. ред. Тодора Тагарева

Зима-весна 2019

Консорциум „Партнерство ради мира" военных академий и институтов по изучению вопросов безопасности

Это издание осуществляется при поддержке Правительства Соединенных Штатов. С изданиями Консорциума можно бесплатно ознакомиться на сайте http://connections-qj.org. Если Вы желаете заказать экземпляр журнала для Вашей библиотеки или если у Вас есть вопросы, связанные с публикациями этой серии, Вы можете обратиться в Оперативный отдел ПРМ по электронной почте: PfPCStratCom@marshallcenter.org.

Д-р Рафаель Перл
Исполнительный директор

Шон С. Костиган
Главный редактор и председатель редакционной коллегии

ISSN 1812-1101, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

Том 18, № 1-2, зима-весна 2019

Консорциум оборонных академий и институтов по изучению безопасности в рамках программы «ПрМ»

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

https://doi.org/10.11610/Connections.rus.18.1-2

Содержание

Том 18, № 1-2, зима-весна 2019

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Тодор Тагарев, *Connections QJ* 18, № 1-2 (2019): 5-11
https://doi.org/10.11610/Connections.rus.18.1-2.00

Редакционная статья

Теория и современная практика сдерживания в международной безопасности

Тодор Тагарев

Центр менеджмента безопасности и обороны, Институт ИКТ Болгарской академии наук, http://www.iict.bas.bg/EN

Резюме: Теория сдерживания возникла с появлением ядерного оружия для решения проблем подготовки и предотвращения полномасштабной ядерной войны между Соединенными Штатами и Советским Союзом. Статьи в этом специальном выпуске вписаны в контекст периода после окончания Холодной войны с возрождающейся и агрессивной Россией. В сборнике статей дается краткое описание теории сдерживания, нынешней практики ее применения для сдерживания и, при необходимости, защиты с помощью обычных сил НАТО и восточного фланга Европы от агрессии, а также критический анализ ее связи с кибер и гибридной войной.

Ключевые слова: сдерживание, НАТО, восточный фланг, передовое присутствие сил на передовых рубежах, конвенциональные силы, киберсфера, кибербезопасность, кибероперации, правовая основа, гибридное влияние.

Сдерживание практиковалось на протяжении веков, чтобы отговорить оппонента от использования курса действий, связанного с принуждением, например, от вооруженного нападения. Эта концепция стала предметом ожесточенных дебатов с появлением ядерного оружия. К 1960-м годам ра-

боты Бернарда Броди,[1] Германа Кана,[2] Гленна Х. Снайдера,[3] Томаса С. Шеллинга[4] и других сформировали совокупность знаний, позволяющих разработать стратегии и политику для ядерного противостояния во время Холодной войны и избежать ядерного конфликта.

Применение теории сдерживания во время Холодной войны привело к равновесию между ядерными арсеналами двух ведущих ядерных держав – Советского Союза и Соединенных Штатов Америки, что гарантировало, что в случае полномасштабной ядерной войны как нападающая, так и обороняющаяся стороны будут уничтожены.[5]

С ядерной разрядкой и окончанием Холодной войны интерес к теории сдерживания утих. На практике сдерживание все еще гарантировалось, хотя и на более низком уровне сил. Например, в то время как в конце Холодной войны Соединенные Штаты поддерживали около 7300 единиц ядерного оружия, развернутых в Европе для обеспечения гарантий безопасности союзникам по НАТО, с тех пор эти силы были сокращены на 90 процентов.[6]

Интерес к сдерживанию возобновился в последние годы. Одной из причин было приостановление действия Договора о ракетах средней и меньшей дальности (РСМД) в начале 2019 года[7] и предстоящее истечение срока действия Нового договора о сокращении стратегических вооружений (новый СНВ),[8] а также необходимость найти новый баланс с учетом ядерных

---

1 Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Company, 1946); Bernard Brodie, *Strategy in the Missile Age* (Santa Monica, CA: RAND, 1969).

2 Herman Kahn, *On Thermonuclear War* (Princeton: Princeton University Press, 1960).

3 Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961).

4 Thomas C. Schelling, *The Strategy of Conflict*, with a new preface by the author (Cambridge, MA: Harvard University Press, 1980); Thomas C. Schelling, *Arms and Influence*, with a new preface and afterword (New Haven: Yale University Press, 2008).

5 James E. Doyle, "Why Eliminate Nuclear Weapons?" *Survival* 55, no. 1 (2013): 7-34, https://doi.org/10.1080/00396338.2013.767402; Tom de Castella, "How Did We Forget about Mutually Assured Destruction?" *BBC News*, February 15, 2012, https://www.bbc.com/news/magazine-17026538.

6 Jessica Cox, "Nuclear Deterrence Today," *NATO Review*, June 8, 2020, www.nato.int/docu/review/articles/2020/06/08/nuclear-deterrence-today/index.html.

7 Simon Lunn and Nicholas Williams, "The Demise of the INF Treaty: What Are the Consequences for NATO," *Policy Brief*, European Leadership Network, February 11, 2019, https://www.europeanleadershipnetwork.org/policy-brief/the-demise-of-the-inf-treaty-what-are-the-consequences-for-nato/.

8 Kingston Reif, "New START at a Glance," *Fact Sheets & Briefs*, Arms Control Association, January 2020, https://www.armscontrol.org/factsheets/NewSTART.

возможностей других игроков, в частности Китая.[9] Другая причина – незаконная аннексия Крымского полуострова Российской Федерацией и ее агрессивные кибер и гибридные действия против членов и партнеров НАТО.

В этом специальном выпуске Connections: The Quarterly Journal основное внимание уделяется вышеупомянутым действиям и использованию обычных, кибер средств и средств дезинформации для сдерживания агрессии.

В первой работе полковник Даррелл Драйвер, директор департамента европейских исследований Военного колледжа армии США, закладывает фундамент, рассматривая теоретические основы сдерживания и две его основные концепции – сдерживание наказанием и сдерживание воспрещением.[10] На этой основе д-р Драйвер критически оценивает позицию НАТО на его восточном фланге и приходит к выводу, что за счет «усиленного передового присутствия» в странах Балтии и Польше, «адаптированного передового присутствия» в Болгарии и Румынии, регулярных учений в Черном море, создания Совместной оперативной группы очень высокой готовности (СОВГ) и создания формирований для интеграции сил НАТО (ФИСН) в семи странах восточного фланга, союзники уже «дали свой вклад», таким образом обеспечивая единый ответ Североатлантического союза на акт агрессии и делая неизбежным ответный удар НАТО. С увеличением оборонных бюджетов в соответствии с обещанием, принятым на саммите в Уэльсе, Европейской инициативой сдерживания Соединенных Штатов, так называемым решением «четырех 30» на саммите НАТО в Брюсселе и развитием «военного Шенгена» в Европе, союзники уже переходят от сдерживания наказанием к сдерживанию воспрещением.

Полковник Драйвер также напоминает нам о требованиях к защите и сдерживанию, сформулированных генерал-лейтенантом (в отставке) Беном Ходжесом, бывшим командующим армией США в Европе, для обеспечения эффективного раннего предупреждения, наличия боеспособных национальных сил, соответствующей инфраструктуры и предварительно размещенных запасов.[11] Велизар Шаламанов, Павел Анастасов и Георги Цветков развивают этот момент дальше, начиная с ангажемента относительно оборонных бюджетов, принятого на саммите в Уэльсе и его реализации на национальном уровне на примере Болгарии.[12] Затем авторы рассматривают

---

[9] Lunn and Williams, “The Demise of the INF Treaty.

[10] Darrell W. Driver, “Deterrence in Eastern Europe in Theory and Practice,” *Connections: The Quarterly Journal* 18, no. 1-2 (2019): 11-24.

[11] Ben Hodges, Janusz Bugajski, and Peter B. Doran, “Securing the Suwałki Corridor: Strategy, Statecraft, Deterrence, and Defense” (Washington, DC: Center for European Policy Analysis, July 2018).

[12] Velizar Shalamanov, Pavel Anastasov, and Georgi Tsvetkov, “Deterrence and Defense at the Eastern Flank of NATO and the EU: Readiness and Interoperability in the Context of Forward Presence, *Connections: The Quarterly Journal* 18, no.1-2 (2019): 25-42.

опыт сотрудничества в сфере обороны в Восточной и Юго-Восточной Европе, подчеркивают преимущества многонационального приобретения необходимых способностей и подробно исследуют потенциальные многонациональные форматы, инициативы и источники финансирования, уделяя особое внимание приобретению информационных и коммуникационных технологий, сенсоров и систем командования и управления или систем C4ISR, а также многонациональному образованию и обучению. Многонациональные формирования на тактическом уровне и проекты по приобретению, реализуемые в формате НАТО и/или ЕС, внесут свой вклад в развитие оперативно совместимых способностей и солидарности, и, таким образом, в более эффективную защиту восточного фланга Европы.

В третьей статье этого номера Рослав Ежевский закладывает основу для обсуждения применимости концепции сдерживания действий, связанных с принуждением, с использованием набора гибридных инструментов.[13] В случае с Латвией автор демонстрирует как Россия пытается влиять на национальный курс в своих интересах, сочетая экономическое и финансовое влияние, коррупцию, эксплуатацию меньшинства граждан русского происхождения, пропагандистские и дезинформационные кампании, организованную преступность в России и широкомасштабные военные учения, проводимые на границах страны. Автор предлагает идеи о том, как защититься, если не сдержать, такую принуждающую деятельность, включая примеры из опыта Финляндии. Тем не менее, заключает он, «междоменное принуждение усилится, и Россия будет проверять сплоченность НАТО».

Кибератаки и кампании дезинформации в сетевых СМИ являются одними из основных инструментов гибридного влияния. Следующие две статьи посвящены применимости концепции сдерживания к киберпространству. Во-первых, Мика Керттунен из Института киберполитики в Тарту, Эстония, излагает критику теории сдерживания в целом и ее применимости к киберпространству, в частности.[14] Среди аргументов в подтверждение последнего положения, автор указывает на изменившийся контекст для кибersдерживания (по сравнению с применением ядерного оружия), соответственно, более высокую степень терпимости к кибератакам, более широкий спектр подходов к сдерживанию и использование более тонких инструментов, в том числе позитивных программ с наградами. В своем заключении г-н Керттунен заявляет, что «сдерживание – это громоздкий и неподходящий инструмент для понимания киберсферы».[15]

---

[13] Rosław Jeżewski, “Cross-domain Coercion as Russia’s Endeavor to Weaken the Eastern Flank of NATO: A Latvian Case Study,” *Connections: The Quarterly Journal* 18, no. 1 (2019): 43-60.

[14] Mika Kerttunen, “Beyond Punishment: Deterrence in the Digital Realm,” *Connections: The Quarterly Journal* 18, no. 1 (2019): 61-68.

[15] Kerttunen, “Beyond Punishment: Deterrence in the Digital Realm,” 67.

С другой стороны, Мануэль Фишер утверждает, что хотя киберсфера требует некоторых особых соображений, сдерживание как «классический инструмент» в международных отношениях может укреплять интересы национальной безопасности.[16] Фишер, выпускник магистерской программы исследований по международной безопасности Европейского центра исследований по вопросам безопасности им. Джорджа К. Маршалла, рассматривает последствия концепции сдерживания для киберпространства по шести направлениям: время, наличные «силы» (ответственные организации с учетом уязвимостей цепочки поставок), выживание, средства защиты и потенциал, а также проблемы атрибуции – с последующим изучением правовых рамок для включения кибер-деятельности в международные отношения. На основе анализа, представленного в этом специальном выпуске, Фишер приходит к выводу, что «[даже] в киберэпохе сдерживание может быть мощным инструментом государственности и способствовать защите интересов государства в области национальной безопасности.[17]

Хотя Мика Керттунен и Мануэль Фишер, кажется, придерживаются противоположных взглядов, их выводы не так уж сильно отличаются. Хотя и в разной степени, оба автора видят ограничения *сдерживания посредством наказания/возмездия* в киберпространстве и отдают предпочтение сдерживанию посредством воспрещения, в том числе посредством соответствующего дизайна сетей, лучшей защиты, повышения устойчивости, государственно-частного партнерства и т.д. Они также указывают на ценность более позитивных подходов, на необходимость усиления международных режимов для обеспечения «сдерживания с помощью нормативных табу» и на построение взаимозависимостей в международной системе, или на так называемого «сдерживания путём обвязывания».[18]

В докладе Тамары Малярчук, Юрия Даника и Чада Бриггса рассматривается использование кибератак против энергетической инфраструктуры в качестве одного из инструментов в наборе средств, используемых Российской Федерацией в ее продолжающемся противостоянии с Украиной.[19] Текущая украинская доктрина рассматривает такие кибератаки (постоянные комплексные угрозы, атаки на системы промышленного контроля) наряду с использованием социальных сетей, атаками на банковскую систему и использованием уязвимостей цепочки поставок. Как и в предыдущих двух статьях этого выпуска, авторы идентифицируют более совершенную защиту, отказоустойчивость и безопасность цепочки поставок в качестве ключевых факторов защиты от кибератак.

---

[16] Manuel Fischer, “The Concept of Deterrence and its Applicability in the Cyber Domain,” *Connections: The Quarterly Journal* 18, no. 1 (2019): 69-92.

[17] Fischer, “The Concept of Deterrence and its Applicability in the Cyber Domain,” 70.

[18] Fischer, “The Concept of Deterrence and its Applicability in the Cyber Domain,” 90.

[19] Tamara Maliarchuk, Yuriy Danyk, and Chad Briggs, “Hybrid Warfare and Cyber Effects in Energy Infrastructure,” *Connections: The Quarterly Journal* 18, no. 1 (2019): 93-110.

Весна Павичич завершает этот выпуск анализом положения Сербии на международной арене.[20] Хотя европейская интеграция кажется очевидным выбором, интересы таких игроков, как Россия и Китай, и инструменты, которые они используют для продвижения своих интересов (в частности, те, которые используются Россией – изощренная пропаганда со ссылками на исторические связи, православное христианство, позиция по вопросу о независимости Косово, зависимость от поставок газа и нефти, сотрудничество в сфере обороны и т.д.), делают будущий путь Сербии неопределенным. Автор видит средства против гибридного влияния в комплексной безопасности, политическом и экономическом диалоге с Европейским союзом, более сильном гражданском обществе, более прозрачной и свободной прессе и сдвигах в политической риторике.

* * *

В этом специальном выпуске представлен обзор теории сдерживания и ее применимости на восточном фланге НАТО и Европы в отношении агрессивной политики и действий Российской Федерации, которые включают использование вооруженных сил против партнеров НАТО, Украины и Грузии, и более изощренные кибератаки и гибридные операции по влиянию как на членов НАТО, так и на партнеров.

Включенные здесь статьи рассматривают вопросы использования обычных вооруженных сил, киберсредств и способов повышения устойчивости вооруженных сил, экономики и общества. Меньше внимания уделялось применению концепции сдерживания к гибридной войне полного спектра,[21] роли ядерного оружия в предотвращении *fait accompli* (ситуации, когда ставят перед свершившимся фактом), обращению вспять или сохранению достижений гибридной операции,[22] а также взаимодействию кибер / гибридных атак и ядерных угроз. Все эти темы заслуживают дальнейшего рассмотрения в будущем специальном выпуске *Connections: The Quarterly Journal*.

---

[20] Vesna Pavičić, "Serbia's Orientation Challenge and Ways to Overcome It," *Connections: The Quarterly Journal* 18, no. 1 (2019): 111-127.

[21] Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs* 92, no.1 (2016): 175-195; Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica, CA: RAND, 2017).

[22] Peter Apps, "Commentary: Putin's Nuclear-tipped Hybrid War on the West," Reuters, March 2, 2018, https://uk.reuters.com/article/us-apps-russia-commentary-idUKKCN1GD6H2; Gustav Gressel, "Protecting Europe against Hybrid Threats," *Policy Brief*, European Council on Foreign Relations, June 25, 2019, https://ecfr.eu/publication/protecting_europe_against_hybrid_threats/.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Тодор Тагарев - профессор Института информационных и коммуникационных технологий Болгарской академии наук и руководитель его Центра менеджмента безопасности и обороны. Инженер по образованию, профессор Тагарев сочетает в себе опыт работы в правительстве с хорошими теоретическими знаниями и опытом в области кибернетики, исследований сложных систем и безопасности – потенциал, который он эффективно реализовал в многочисленных национальных и международных междисциплинарных исследованиях, включая текущие проекты по программе Горизонт 2020 в области кризисного менеджмента и кибербезопасности.
https://orcid.org/0000-0003-4424-0201

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Даррелл Драйвер, *Connections QJ* 18, № 1-2 (2019): 12-28
https://doi.org/10.11610/Connections.rus.18.1-2.01

Рецензированная статья

Сдерживание в Восточной Европе в теории и на практике

Даррелл Драйвер

Военный колледж Сухопутных войск США, Карлайлские казармы, Пенсильвания, https://www.armywarcollege.edu/

Резюме: В этой статье исследуются преемственность и различия между концепциями и подходами сдерживания времен Холодной войны и теми, которые используются сегодня на восточном фланге НАТО. Утверждается, что классические подходы к сдерживанию, основанные на богатых интеллектуальных традициях времен Холодной войны, ясно проявились в ответах НАТО на российскую агрессию и угрозы, и что решения, принимаемые в Брюсселе и столицах Североатлантического союза, можно понять путем рассмотрения таких классических концепций сдерживания, как сдерживание воспрещением и сдерживание наказанием или прямого и расширенного сдерживания. Подобные и другие рассмотренные здесь концепции остаются полезными. Тем не менее необходимо учитывать важные изменения в масштабе и характере угрозы, особенно в том, что касается невоенных аспектов сдерживания и так называемых гибридных угроз или угроз «серой зоны». Это потребует сочетания традиционных концепций сдерживания с более современным акцентом на разработке комплексного подхода к современным вызовам безопасности.

Ключевые слова: сдерживание, воспрещение, НАТО, Восточная Европа, гибридные угрозы.

Большинство людей знакомы с двумя основными символами трансатлантического альянса: аббревиатурой НАТО или l'OTAN и звездой НАТО. Однако есть также такой же старый и почтенный, хотя и неформальный, символ НАТО, который требует внимания при любом обсуждении сдерживания и обороны: еж, впервые упомянутый Дуайтом Эйзенхауэром в 1951 году. Первый Верховный главнокомандующий ОВС НАТО в Европе (SACEUR) призвал

отдельных союзников быть способными превратиться в «ежа обороны», чтобы выиграть время, которое потребуется НАТО для их защиты. После аннексии Крыма Россией в 2014 году этот давно забытый символ сдерживания возродился. Тем не менее, хотя это необходимое переоткрытие концепций сдерживания продолжается, сегодня в сдерживании и коллективной обороне есть много отличий, которые заслуживают рассмотрения. Заимствуя знаменитую метафору Исайи Берлина «лиса и еж»,[1] можно сказать, что изменения в современной среде безопасности означают, что НАТО потребуется большая адаптивность мышления лисы и разнообразие подходов к решению проблем по мере возвращения к тактике ежа, как фокусу сдерживания.

В этой статье исследуются как преемственность, так и изменения, которые требуют рассмотрения при любом обсуждении сдерживания и обороны в сегодняшней Восточной Европе. Я утверждаю, что в ответах союзников на агрессию Москвы проявили себя классические подходы к сдерживанию, и что решения, принимаемые в Брюсселе и столицах Североатлантического союза, можно понять, если рассмотреть эти классические концепции сдерживания. Тем не менее, необходимо учитывать важные изменения в масштабе и характере угрозы, особенно в том, что касается невоенных аспектов сдерживания и так называемых гибридных угроз или угроз «серой зоны».

Концепции сдерживания

Концепция сдерживания, возможно, так же стара, как сами конфликты между людьми, но ее интеллектуальная «золотая эра» процветала в атмосфере Холодной войны примерно с 1946 до конца 1980-х годов. В этот период краеугольные камни были созданы такими фигурами, как Бернард Броди, Герман Кан, Томас Шеллинг и Гленн Снайдер.[2] Хотя движущей силой большей части ранних работ этого периода было появление ядерного ору-

[1] Isaiah Berlin, “The Hedgehog and the Fox: An Essay on Tolstoy’s View of History,” *The Proper Study of Mankind: An Anthology of Essays*, ed. Henry Hardy and Roger Hausheer (New York: Farrar, Straus, and Giroux, 1998). Относительно наиболее недавнего использования метафоры применительно к стратегии см. John Lewis Gaddis, *On Grand Strategy* (New York: Penguin Press, April 2018).

[2] Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Company, 1946); Herman Kahn, *On Thermonuclear War* (Princeton: Princeton University Press, 1960); Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterward* (New Haven: Yale University Press, 2008); Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961).

жия, концепция сдерживания быстро распространилась и на область конвенциональных оружий.[3] Независимо от того, ядерное оно или конвенциональное, суть сдерживания, согласно совместной доктрине США, заключается в «отказе врага от предприятия военных действий из-за наличия реальной угрозы неприемлемого противодействия и/или убеждения в том, что цена действия перевешивает предполагаемые выгоды».[4] Гленн Снайдер охарактеризовал сдерживание просто как «отказ врага от военных действий, создавая для него перспективу затрат и риска, которые перевешивают его предполагаемую выгоду».[5] Сдерживание отличается от понуждения, другой формы принуждения, тем, что оно направлено не на то, чтобы побудить другого участника что-то сделать, а на то, чтобы заставить этого субъекта поддерживать статус-кво, «просто продолжайте делать то, что делаете».[6] Из этого основного положения о цели сдерживания выросла богатая и разнообразная литература, которую невозможно было бы полностью изучить в статье такого объема. Вместо этого я хотел бы сосредоточиться на нескольких центральных концепциях и подходах, на которые стоит обратить внимание при рассмотрении данного комплекса проблем.

Во-первых, в литературе проводится различие между *непосредственным и общим сдерживанием*. «Непосредственное сдерживание, по словам Патрика Моргана, «касается отношений между противостоящими государствами, где по крайней мере одна сторона серьезно рассматривает нападение, а другая создает угрозу возмездия, чтобы предотвратить его».[7] По этой причине Ричард Лебоу и Дженис Стайн прямо называют сдерживание «стратегией управления конфликтом», при этом одна сторона пытается отговорить другую от агрессии.[8] Это можно противопоставить общему сдерживанию, которое Морган описывает как относящееся больше к «противникам, которые поддерживают вооруженные силы для регулирования своих отношений, даже если ни один из них и близко не собирается атаковать».[9] Лоуренс Фридман утверждает, что за некоторыми очень напряженными исключениями, такими как кубинский ракетный кризис 1962 года,

---

[3] Для рассмотрения конвенциональных аспектов см. John J. Mearsheimer, *Conventional Deterrence* (Ithaca, N.Y.: Cornell University Press, 1983).

[4] *DOD Dictionary of Military and Associated Terms*, US Joint Chiefs of Staff, Military and Electronic Library, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

[5] Snyder, *Deterrence and Defense*, 35.

[6] Robert J. Art and Kelly M. Greenhill, "Coercion: An Analytic Overview," in *Coercion: The Power to Hurt in International Politics*, ed. Kelly M. Greenhill and Peter Krause (New York: Oxford University Press, 2018), 5.

[7] Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage Publications, 1977), 28.

[8] Richard Ned Lebow and Janice Gross Stein, "Beyond Deterrence," *Journal of Social Issues* 43, no. 4 (Winter 1987): 5-71.

[9] Morgan, *Deterrence: A Conceptual Analysis*, 28.

этот «дальний путь» сдерживания характеризовал баланс сил и стратегию Холодной войны. По словам Фридмана, «общее сдерживание практикуется, чтобы избежать необходимости практического сдерживания».[10]

Вторая известная концепция в литературе связана с различием между *сдерживанием наказанием* и *сдерживанием воспрещением*. Сдерживание посредством наказания требует, чтобы человек убедил противника в том, что любая агрессия, изначально успешная или нет, встретит неприемлемо дорогостоящий ответ. Этот подход включает в себя убеждение противника как в способности наложить такие издержки, так и в своем желании довести дело до конца даже перед лицом дальнейших ответных действий. Наказание отличается от сдерживания воспрещением, которое направлено на демонстрацию реальной способности в первую очередь помешать противнику достичь желаемой цели. Госсекретарь США в начальном периоде Холодной войны Дин Ачесон описал практическую разницу следующим образом: «Мы имеем в виду, что единственным сдерживающим фактором для навязывания российской воли Западной Европе является вера в то, что с самого начала любой такой попытки американская сила будет использована, чтобы остановить это [воспрещение] и, в случае необходимости, для нанесения Советскому Союзу Москву ущерба, который режим не желал бы понести [наказание]».[11] Конечно, оба этих эффекта нацелены на разум противника, причем сдерживание воспрещением, по словам Гленна Снайдера, представляет «для врага угрозу, которую легче подсчитать, чем сдерживание наказанием».[12]

Третье важное различие, описанное в литературе, пожалуй, наиболее очевидное: прямое (или центральное) сдерживание и расширенное сдерживание. Прямое сдерживание относится к способности отговорить противника от нападения на свою родину. Расширенное сдерживание измеряется способностью включать другие государства под тем же зонтиком сдерживания. В последнем случае превалируют проблемы с убедительностью. Одно дело убедить противника в том, что государство ответит, если родина подверглась нападению, независимо от того, существует ли риск возмездия и эскалации в будущем. Совсем другое дело – убедить противника в том, что государство ответит, если его союзник подвергнется нападению, тем самым принимая на себя риск возмездия от имени других. Большая часть усилий США во время Холодной войны заключалась в том, чтобы убедить Советы в достоверность угрозы, что США будут вести борьбу в случае нападения на европейских союзников. Это было сделано благодаря твердым заявлениям о приверженности и намерениях, которые Патрик Морган назвал «залогом

---

[10] Lawrence Freedman, "General Deterrence and the Balance of Power," *Review of International Studies* 15, no. 2 (April 1989): 199-210, цитата на с. 204, https://doi.org/10.1017/S0260210500113002.

[11] Dean Acheson, *Power and Diplomacy* (New York: Atheneum, 1962), 85.

[12] Glenn H. Snyder, *Deterrence by Denial and Punishment*, Woodrow Wilson School Research Monograph (Princeton University, January 1969), 5.

честного слова президента».[13] Это также было сделано путем развертывания войск на передних рубежах в районах, которые могли подвергнуться российской агрессии, и в некоторых случаях, наделения местных командующих полномочиями реагировать на нападение. Цель заключалась в том, чтобы устранить как можно в большей степени сомнения относительно уверенности в том, что нападение на союзника по НАТО вызовет ответ со стороны США, что сделало бы расширенное сдерживание надежным.

Сдерживание в Европе после 2014 года: теория встречается с практикой

Хотя вышеизложенный обзор едва касается поверхности широкого набора литературы по сдерживанию, он на самом деле предлагает отправную точку для размышлений о сдерживании в современной Европе. Хотя был момент, когда казалось, что эту литературу, как и холодную войну, выбросят на свалку истории, российская оккупация Крыма в 2014 году и разжигание нестабильности на востоке Украины снова вернули концепции сдерживания в центр дискуссий о европейской безопасности. Поэтому стоит подумать о том, как с 2014 года формировались усилия НАТО по сдерживанию и как теория сдерживания помогает объяснить эти действия.

В ответ на то, что было названо первым насильственным изменением границ Европы после Второй мировой войны, США быстро отреагировали, продемонстрировав свою готовность отстаивать территориальный суверенитет НАТО. Американская операция «Атлантическая решимость» (OAR) стала проекцией силы путем создания линии небольших подразделений на восточном фланге НАТО как видимого символа решимости США. Визиты президента Обамы и вице-президента Джо Байдена включали в себя демонстрацию «твердой» приверженности безопасности и суверенитету союзников по НАТО, а Конгресс США выделил 1 миллиард долларов из фондов Инициативы по обеспечению безопасности Европы (ERI) на финансирование усиленного присутствия сил США в Европе и начинает посылать дополнительные силы на ротационной основе из США.[14] Словом и делом Вашингтон ответил на обеспокоенность союзников по НАТО тем, что в этот момент нужны немедленные меры сдерживания, сигнализируя о дальнейшей готовности США обеспечивать расширенное сдерживание в Восточной Европе хотя бы небольшими начальными силами.

НАТО также действовало коллективно, чтобы продемонстрировать решимость на Востоке. Был немедленно разработан План действий НАТО по обеспечению готовности для реализации ряда краткосрочных гарантий безопасности для восточных союзников и долгосрочных мер адаптации для

[13] Patrick M. Morgan, *Deterrence Now* (Cambridge, UK: Cambridge University Press, 2003), 15-16.

[14] Congressional Research Service, “The European Deterrence Initiative: A Budgetary Overview,” *In Focus*, August 8, 2018, https://fas.org/sgp/crs/natsec/IF10946.pdf.

улучшения сдерживающего потенциала Североатлантического союза. На саммите глав государств и правительств (HOS/G) в Уэльсе в 2014 году союзники согласились на резкое расширение Сил реагирования НАТО (NRF), включая создание Совместной оперативной группы очень высокой готовности (VJTF), которая могла бы обеспечить развертывание сил на месте в объеме боевой мощи бригады в течение 5-7 дней после активации. Важно отметить, что VJTF будет состоять из подразделений от 10 до 15 союзников, давая сигнал об едином ответе на любую агрессию, которая приведет к ее подразделениям с широким представительством со всего Североатлантического союза при формировании подразделений интеграции сил НАТО (NFIU), также согласованных в Уэльсе. Два года спустя на Варшавском саммите эта логика развертывания подразделений под разными флагами для демонстрации единства НАТО получила дальнейшее развитие с появлением Усиленного передового присутствия (EFP) на северо-востоке Североатлантического союза и Адаптированного передового присутствия (TFP) на юго-востоке.

Таким образом, подобно OAR США, VJTF, EFP и TFP означают, что другие союзники по НАТО также демонстрировали готовность к расширенному сдерживанию на восточном фланге Североатлантического союза и, как и в ответе США, боевая мощь этих формирований была далека от решающей. В исследовании, проведенном корпорацией RAND в 2016 году, прямо говорилось, что «НАТО, в нынешнем положении, не может успешно защищать территорию своих наиболее уязвимых членов».[15] Это было далеко не прозрением. Положение сил в странах Балтии было особенно проблематичным и послужило особым акцентом для того же исследования RAND. По словам авторов исследования Дэвида Шлапака и Майкла Джонсона, «в множестве симуляциях с участием широкого круга экспертов, самое долгое время, которое потребовалось российским войскам, чтобы добраться до окраин Таллина и Риги – 60 часов».[16] RAND оценивал Североатлантический союз с точки зрения его способности сдерживать путем воспрещения в Балтийском море, но усилия союзников можно было бы рассматривать, по крайней мере до 2016 года, как работу, демонстрирующую приверженность к расширенному сдерживанию посредством *наказания*. То есть широкое союзническое «участие в игре» гарантирует, что любой акт агрессии вызовет единый ответ Альянса. Если НАТО не сможет предотвратить первоначальное решение [противника о нападении], развернутые на передовых позициях войска НАТО и быстрое начальное подкрепление сделают конфликт более широким и, следовательно, ответные меры НАТО станут неизбежными.

Между тем, как отдельные союзники, так и Североатлантический союз в целом продолжали работать над долгосрочными мерами адаптации НАТО,

---

[15] David A. Shlapak and Michael W. Johnson, “Reinforcing Deterrence on NATO’s Eastern Flank: Wargaming the Defense of the Baltics” (Arroyo, CA: RAND Corporation, 2016), 1.

[16] Shlapak and Johnson, “Reinforcing Deterrence on NATO’s Eastern Flank.”

которые позволили бы Североатлантическому союзу развить способность для надежного *сдерживания путем воспрещения*. Обязательство HOS/G в Уэльсе обеспечить, чтобы их страны расходовали 2 % валового внутреннего продукта на оборону, и чтобы 20 % оборонного бюджета расходовались на модернизацию и оборудование, стало одним из важных шагов на пути к развитию более надежных военных способностей.[17] Со своей стороны, США отреагировали резким увеличением расходов на оборону, предназначенных для Европы. Расходы на ERI увеличились с 1 млрд долларов в 2015 году до 4,8 млрд долларов в 2018 году, а на 2019 год были затребованы 6,5 млрд долларов.[18] Фактически, в законодательстве за 2017, сама ERI была переименована из Инициативы обеспечения безопасности Европы в Европейскую инициативу сдерживания (EDI). Эти деньги пошли на увеличение присутствия ротационных сил, а также на расширение учений и подготовки, улучшение предварительного расположения оборудования, улучшение инфраструктуры и укрепление потенциала партнеров.

НАТО последовало примеру США, первоначально выделив 200 миллионов долларов на развитие позиций для предварительной дислокации американской техники в Польше,[19] а на саммите в Брюсселе в 2018 году НАТО еще больше заострило внимание на расширение «скамейки запасных» и повышении боевой готовности, чтобы иметь возможность выставить значительные боевые силы в более короткие сроки. План так называемой сети «четыре-30» предусматривает развертывание 30 батальонов, 30 эскадрилий самолетов и 30 боевых кораблей с уведомлением о приведении в готовность за 30 дней.[20] Наряду с развитием боеготовых подразделений, НАТО также работает над улучшением внутриевропейской мобильности. Такие идеи, как создание группы стран ЕС, подобных «Шенгенской зоне», которые взяли бы на себя обязательство по ускорению военной мобильности, начали обретать форму.[21] В настоящее время Альянс начинает решать гораздо более сложную и дорогостоящую задачу улучшения физической инфраструктуры, необходимой для обеспечения мобильности. Все эти усилия предполагают переход от первоначального акцента на утверждение достоверности угроз НАТО для энергичного реагирования на любую агрессию

---

17 North Atlantic Treaty Organization (NATO), “Wales Summit Declaration,” September 5, 2014, para 14, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

18 Congressional Research Service, “The European Deterrence Initiative.”

19 Department of Defense, “Military Construction Program: FY 2019 Budget,” February 2018, 9, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/budget_justification/pdfs/11_NATO_Security_Investment_Program/FY19_NSIP_J-Book_Final.pdf.

20 North Atlantic Treaty Organization (NATO), “Brussels Summit Declaration,” July 11, 2018, para 14, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

21 European Union, External Action Service, “Defence: EU Moves on Military Mobility,” March 28, 2018, https://eeas.europa.eu/headquarters/headquarters-Homepage/42226/defence-eu-moves-military-mobility_en.

против союзников по НАТО, изначально успешных или неудачных (сдерживание наказанием), к более поддающейся расчету способности воспретить агрессору перспективу первоначальной быстрой победы.

Теория сдерживания как руководство к будущей практике

Итак, если мы можем сказать, что текущая работа по обороне в Восточной Европе хорошо согласуется с существующей литературой по сдерживанию, что литература может сказать о необходимой будущей работе? Чтобы ответить на этот вопрос, полезно рассмотреть некоторые из причин, по которым прошлые попытки сдерживания терпели неудачу. Типология Александра Джорджа и Ричарда Смокера 1974 года определяет три модели того, как противник может вызвать провал сдерживания: попытка поставить перед *свершившимся фактом*, ограниченное нападение с целью проверки и контролируемое давление.[22] Различия определяются уровнем риска, на который готов пойти агрессор. Попытка атаки с целью поставить противника перед свершившимся фактом сопряжена с наибольшим риском, но, по словам Джорджа и Смока, она может быть «наиболее рациональным» подходом, если инициатор считает, что противник не в состоянии предотвратить это действие и не ценит спорную территорию в достаточной степени, чтобы гарантировать необходимое жертвование крови и денег, чтобы заставить инициатора отменить первоначальное решение.[23] Наблюдатели указывают на аннексию Крыма в 2014 году как на реализацию политики свершившегося факта.[24] Признавая угрозу, которую представлял такой авантюризм во время Холодной войны, Гленн Снайдер оценил обороноспособность НАТО в Европе и пришел к выводу, что сила сдерживания посредством воспрещения не обязательно должна быть способна сдерживать бесконечно долго или полностью победить захватчика, но ответ действительно должен был быть достаточно сильным, чтобы убедить Советы в готовности союзников к сопротивлению. Таким образом, оперативный вопрос в современной Восточной Европе заключается в том, сколько и какого рода силы необходимы для достижения этой цели.

Недавний доклад Центра анализа европейской политики под руководством бывшего командующего армией США в Европе генерал-лейтенанта (в отставке) Бена Ходжеса предлагает некоторые ответы на этот вопрос, подчеркивая необходимость (1) эффективного раннего предупреждения, (2) дееспособных национальных сил и (3) соответствующей инфраструктуры и

---

[22] Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, October 1974), 534-547.

[23] George and Smoke, *Deterrence in American Foreign Policy*, 537.

[24] Zdzislaw Sliwa, “Poland: NATO’s East Frontline Nation,” in *Deterring Russia in Europe: Defence Strategies for Neighbouring States*, ed. Nora Vanaga and Toms Rostoks (Routledge, 2018), 217-236.

заранее размещенных запасов.[25] Во-первых, согласно отчету, раннее предупреждение на Востоке имеет решающее значение для получения окна возможностей, в рамках которого Североатлантический союз может заявить о своей решимости путем развертывания дополнительных сил, таких как VJTF и более крупные Силы реагирования НАТО численностью в 40 000 человек. Другими словами, чем более заблаговременно будет предупреждено НАТО о переходе от положения общего сдерживания к положению непосредственного сдерживания, тем больше будет возможностей для подачи сигналов, необходимых для устранения любых возможных неправильных представлений или просчетов России в отношении готовности союзников к коллективной обороне. Во-вторых, боеспособные национальные силы необходимы для поддержки восточного фланга и, в первую очередь, для превращения восточных союзников по НАТО в непривлекательную военную цель. Важность сильного национального оборонного потенциала закреплена в учредительном договоре НАТО, в статье 3 которого говорится, что стороны договора будут «по отдельности и совместно, посредством постоянной и эффективной самопомощи и взаимопомощи, […] поддерживать и развивать свою индивидуальную и коллективную способность противостоять вооруженному нападению».[26] Одним из особенно обнадеживающих примеров реализации обоих этих принципов является потенциал укрепления сотрудничества в рамках так называемых договоренностей Б9 + (Бухарестское сотрудничество), в которых девять восточных государств Альянса (Эстония, Латвия, Литва, Польша, Чешская Республика, Словакия, Венгрия, Румыния и Болгария) соглашаются совместно работать над общими проблемами, такими как готовность и совместимость. В-третьих, поскольку нереалистично ожидать, что НАТО сохранит положение с размещением существенных постоянно дислоцированных сил [27] на передовых позициях, как во времена Холодной войны, заранее размещенные резервы и улучшенная транспортная инфраструктура имеют решающее значение для обеспечения быстрой переброски подкреплений. Чтобы стимулировать большие инвестиции в этом направлении, генерал-лейтенант (в отставке) Бен Ходжес и

[25] Ben Hodges, Janusz Bugajski, and Peter B. Doran, “Securing the Suwałki Corridor: Strategy, Statecraft, Deterrence, and Defense” (Washington, DC: Center for European Policy Analysis, July 2018), 4.

[26] “The North Atlantic Treaty,” Article 3 (Washington, DC: NATO, April 4, 1949), https://www.nato.int/cps/ie/natohq/official_texts_17120.htm.

[27] Фактически, Североатлантический союз продолжает придерживаться духа основополагающего акта Совета НАТО-Россия, который обязывает НАТО к коллективной обороне посредством оперативной совместимости и подкреплений, а не «постоянного размещения значительных боевых сил». В Альянсе нет единого мнения об изменении этой позиции. “Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation” (Paris, France: North Atlantic Treaty Organization, May 22, 1997), https://www.nato.int/cps/su/natohq/official_texts_25468.htm.

его соавторы рекомендуют НАТО разработать параметры, с помощью которых союзники могли бы направлять государственные расходы на определенные инфраструктурные проекты двойного назначения (военное и гражданское) в соответствии с согласованным в НАТО показателем расходов на оборону на уровне 2 процентов ВВП.[28] Хотя подобные предложения в настоящее время не имеют необходимой политической поддержки, они демонстрируют растущее осознание критической важности военной мобильности для предотвращения любого рассмотрения Россией подхода *свершившегося факта*. Усилия по демонстрации повышенной мобильности и оперативности проявляются в расширенном режиме учений Североатлантического союза: многонациональные учения Sabre Guardian в 2017 году стали важной проверкой концепций в Юго-Восточной Европе, а учения НАТО Trident Juncture в 2018 году сделали то же самое для Севера.[29]

Тогда как НАТО добивается прогресса в предотвращении потенциальных неудач с применением подхода *свершившегося факта*, ему также следует помнить о том, что Джордж и Смоук называют подходом ограниченного зондирования. В этой угрозе сдерживанию инициатор «создает управляемый кризис, чтобы выяснить решимость и готовность обороняющегося ответить».[30] Вместо тотальной попытки изменить статус-кво и затем бросить вызов обороняющемуся с требованием отменить решение, как в предыдущем примере, инициатор использует управляемое, вычисляемое и обратимое ограниченное нападение с целью зондирования, чтобы проверить решимость защищающегося, пытаясь ограничить риск более широкого конфликта. Такой подход может быть особенно проблематичным для Североатлантического союза, авторитет которого зиждется на договорном обязательстве, согласно которому нападение на одного будет рассматриваться как нападение на всех. Неопределенность, окружающая вопрос о том, каков смысл формулировок договора, например, «вооруженное нападение» или обязательство союзника предпринять «такие действия, которые он сочтет необходимыми»,[31] может превратить ограниченное нападение с целью проверки в отравленную пилюлю, которая разрушит единство Североатлантического союза в отношении того, как бороться с нарушением.

И здесь очень важно обозначать «красные линии». Как утверждают Роберт Арт и Келли Гринхилл, «обороняющийся должен ясно дать понять любому потенциальному нападающему каковы его красные линии, четко заявив о своей решимости, [… и] указать, какие расходы понесет соперник,

---

[28] Hodges, Bugajski, and Doran, “Securing the Suwałki Corridor,” 8.

[29] Осуществляется планирование SABER GUARDIAN 2019, союзного учения в Юго-Восточной Европе такого же или большего масштаба и охвата, чем мероприятие 2017 года.

[30] George and Smoke, *Deterrence in American Foreign Policy*, 540.

[31] “The North Atlantic Treaty,” Article 5.

если он пересечет красные линии».[32] В связи с этим в будущих военных учениях НАТО и учениях по урегулированию кризисов на политическом уровне могут потребоваться творческие способы включения ограниченного пробного реагирования в сценарии учений. Как индивидуально, так и коллективно, союзники могут также разработать более широкий список военных и невоенных мер реагирования на кризисы для различных сценариев ограниченного зондирования. Эти меры работают лучше всего, когда существует широкий консенсус относительно того, какие меры реагирования доступны и как и когда они будут реализованы. По этой причине сотрудничество США, НАТО и Европейского союза (ЕС) в такой работе, особенно в отношении невоенных мер, было бы особенно полезным. Там, где априорный консенсус по мерам реагирования невозможен, стратегическая двусмысленность должна быть ограничена с помощью коллективных заявлений и четких позиций. В такие моменты критичными являются заявления и действия руководства Альянса, особенно президента США.[33]

По словам Джорджа и Смоука, самую большую угрозу сдерживанию можно увидеть в моделях контролируемого давления. Такой подход обеспечивает инициатору наименьший риск и используется в ситуациях, когда инициатор рассматривает решимость обороняющегося как «недвусмысленную», по сравнению с «моделью один, при которой инициатор считает, что никакой решимости нет; во втором варианте он считает, что есть неопределенность или двусмысленность в отношении обязательств защищающегося».[34] Таким образом, третий вариант может быть привлекательным для противника, который считает, что у него есть особое асимметричное преимущество, против которого защищающийся не может предложить адекватную защиту. Джордж и Смок указывают на продолжающееся советское давление на Западный Берлин во время Холодной войны как на попытку использовать советское географическое преимущество (историческая немецкая столица была окружена территорией ГДР). Цель состояла в том, чтобы постепенно подорвать готовность Запада защищать свободный Западный Берлин и обострить напряженность в Североатлантическом союзе из-за уровня решимости НАТО по этому вопросу. Сегодня можно увидеть похожий подход в Грузии, Украине, странах Балтии и Черного моря, хотя и с важными отличиями в тактике в каждом отдельном случае.

Подход с контролируемым давлением, наряду с избранным ограниченным зондированием, также можно увидеть в широком диапазоне действий, совершаемых ниже уровня конфликта. Эти так называемые «серые зоны» или «гибридные» подходы обычно характеризуются «действиями, которые носят направленный на принуждение и агрессивный характер, но

[32] Art and Greenhill, “Coercion: An Analytic Overview,” 12.

[33] Morgan, *Deterrence Now*, 15-16.

[34] George and Smoke, *Deterrence in American Foreign Policy*, 543.

намеренно форматированы для того, чтобы оставаться ниже порога обычного военного конфликта и открытой межгосударственной войны».[35] Это делает данную стратегию идеальной для попыток оказания контролируемого давления с целью преодоления сдерживания. Это может происходить в традиционном географическом контексте через прокси заместителей, как в Восточной Украине, или посредством экономического принуждения, информационной войны, саботажа и, особенно, кибератак. Более того, по мере того, как усиливаются традиционные действия НАТО по сдерживанию, этот подход контролируемого давления, направленный на подрыв сдерживания с помощью действий в «серой зоне», становится все более привлекательным для тех, кто желает изменить статус-кво, избегая при этом открытого конфликта. Это новый фронт в более классическом противостоянии сдерживания, который представляет собой одну из наиболее сложных проблем для современного сдерживания.

Серая зона и парадокс стабильности / нестабильности

С появлением новых технологий, открывающих новые возможности для стратегии контролируемого давления, направленной против усилий Североатлантического союза по сдерживанию, Североатлантический союз стал свидетелем возникновения того, что можно было бы назвать «парадоксом стабильности-нестабильности». Термин был впервые введен в употребление в 1960-х годах для описания того, как ядерное оружие сдерживало войну великих держав, создавая уровень открытой стабильности даже тогда, когда противоборствующие государства вели находящуюся на низком уровне, но неистовую кампанию влияния и прокси войны. Аналогичную динамику можно увидеть в том, как усиленные меры Североатлантического союза с применением обычных вооружений, подкрепленные расширенным ядерным сдерживанием, побудили противников искать все более контролируемые и поддающиеся расчету способы оказания давления на режимы сдерживания. Иными словами, в то время, как усилия НАТО по обычному сдерживанию, похоже, приводят Восточную Европу к состоянию общего сдерживания, зондирования, нападения и кампании в серой зоне попрежнему требуют ответных мер, более подобных кризисному менеджменту, включая действия по усилению непосредственного сдерживания. Хотя эту базовую динамику можно увидеть на примерах из разных гибридных сфер деятельности, кибер и информационная сфера – это области, которые стоит выделить.

Самой большой проблемой в киберпространстве, – по словам бывшего президента Эстонии Тоомаса Ильвеса, – остается сдерживание. «Мы уже много лет говорим о необходимости решать эту проблему в рамках

[35] Hal Brands, “Paradoxes of the Gray Zone,” *Social Science Research Network Electronic Journal* (January 2016), 1, http://dx.doi.org/10.2139/ssrn.2737593.

НАТО».[36] Действительно, Ричард Кларк и Роберт Кнейк заходят так далеко, что утверждают, что теория сдерживания просто не очень хорошо переносится в киберпространство [37] и там, где теория применяется, основное внимание уделялось сдерживанию путем воспрещения с помощью сетевой защиты и более устойчивых систем. Фактически, эту точку зрения высказал и бывший заместитель министра обороны США Уильям Линн, заявив, что «сдерживание обязательно будет больше основываться на отказе в какой-либо выгоде для атакующих, чем на наложении расходов путем возмездия».[38] Это также было основным подходом НАТО, первоначально ориентированного на защиту сетей НАТО и повышение устойчивости посредством обучения, взаимопомощи и групп быстрого реагирования в киберпространстве.[39] Однако, в Варшаве НАТО приняло киберпространство в качестве области своих операций, и Брюссельский саммит 2018 года привел к соглашению о создании Центра операций в киберпространстве и договоренности «продолжать совместную работу по разработке мер, которые позволят нам заставить заплатить тех, кто причиняет нам вред».[40] Таким образом, несмотря на некоторые проблемы, НАТО продолжало адаптировать концепции сдерживания к появляющейся киберсфере операций, переходя от сосредоточения внимания на защите сетей НАТО к оказанию помощи союзникам в обеспечении устойчивости, и в конечном итоге, к признанию необходимости развития способностей для сдерживания путем наказания.

Усилия союзников также начали говорить о более целостном подходе к применению концепций сдерживания в киберпространстве. По словам Здзислава Сливы, публикация Польшей в 2015 году «Доктрины информационной безопасности Республики Польша» была попыткой установить сдерживание путем воспрещения.[41] Опять же, в документе также подчеркивается требование «продолжать активную киберзащиту, включая наступательные действия в киберпространстве, и поддерживать готовность к кибервойне».[42] Благодаря широкой российской кибератаке 2007 года, Эсто-

[36] Цитируется в Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, цитата на с. 44, https://doi.org/10.1162/ISEC_a_00266.

[37] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 189.

[38] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108.

[39] North Atlantic Treaty Organization, "Cyber Defence," July 16, 2018, www.nato.int/cps/en/natohq/topics_78170.htm.

[40] North Atlantic Treaty Organization, "Brussels Summit Declaration," July 12, 2018, para 20, https://www.nato.int/cps/ic/natohq/official_texts_156624.htm.

[41] Sliwa, "Poland: NATO's East Frontline Nation."

[42] National Security Bureau (Biuro Bezpieczenstwa Narodowego), "Cybersecurity Doctrine of the Republic of Poland," January 2015, по состоянию на 4 февраля 2018,

ния, пожалуй, является самым дальновидным союзником в вопросе кибернетической безопасности. В результате план развития обороны на 2017 год обязывает страну создать «национальное киберкомандование для развития как оборонительных, так и наступательных кибер способностей».[43] Наконец, несмотря на предыдущие комментарии заместителя министра обороны Линн, последняя киберстратегия Соединенных Штатов 2018 года предлагает аналогичное признание того, что сдерживание в киберпространстве требует как воспрещение, так и способностей для наказания, утверждая, что «деятельность, которая противоречит ответственному поведению в киберпространстве, должна сдерживаться за счет наложения затрат с помощью кибер и других средств».[44] Этот последний пункт заслуживает особого внимания. Сдерживание посредством наказания в киберпространстве может основываться на симметричном киберответе, но оно также может включать другие асимметричные ответные меры, как например, введение экономических санкций США в отношении России в ответ на вмешательство в выборы в США в 2016 году. Достижение эффективной кибербезопасности потребует от союзников продолжения изучения того, как можно лучше всего использовать как симметричные, так и асимметричные варианты реагирования и сигнализировать о них своевременно.

Будучи особенно уязвимыми, государства Восточной Европы должны продолжить изучение того, как они могут адаптировать свои собственные киберстратегии и углубить сотрудничество с другими союзниками в киберпространстве. И болгарская, и словенская киберстратегии были разработаны в 2016 году, а стратегии Венгрии и Румынии еще в 2013, до принятия Обязательства НАТО по киберзащите в 2016 году. Создание кибер обороны в качестве области операций Североатлантического союза, являющейся подтверждением того, что киберзащита есть часть основной задачи коллективной обороны НАТО, и создание Оперативного центра НАТО в киберпространстве – все это говорит о расширении озабоченности и сотрудничестве в этой области. Идеи, подобные тем, которые выдвинул Атлантический совет Болгарии, о создании центра реагирования на кибер- и гибридные угрозы, следует рассматривать как способы обеспечения постоянной совместимости и координации.

Второй гибридный вызов для НАТО можно увидеть в том, как Москва нацеливается на медиарынки, чтобы повлиять на послания о российских политических и экономических интересах. Результаты недавнего отчета

---

http://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.

[43] Henrik Praks, "Estonia's Approach to Deterrence," in *Deterring Russia in Europe: Defence Strategies for Neighboring States*, ed. Nora Vanaga and Toms Rostoks (New Yourk: Routledge), 217-235.

[44] "National Cyber Strategy of the United States of America," (Washington, DC: The White House, September 2018), 3, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Центра изучения демократии описывают пророссийские олигархические сети, которые осуществляют широкий контроль над черноморскими медиарынками либо посредством прямого владения, либо путем культивирования других форм экономической зависимости.[45] Это привело к более или менее последовательной дезинформации и циркуляции посланий, направляемых Москвой, в пострадавших странах. Случай Болгарии особенно поучителен. Сделав иностранные вложения в средства массовой информации незаконными, на национальных медиа рынках быстро начала доминировать горстка местных игроков, которые служили средством для незаконного внешнего финансирования. Вместо того, чтобы предотвращать влияние извне, эта мера гарантировала, что иностранное влияние будет скрытым и менее прозрачным при незначительной конкуренции на этом рынке.

Поскольку эти и другие гибридные угрозы представляют собой все более серьезную проблему, методы борьбы с ними в основном следовали пути сдерживания воспрещением, включая укрепление политической, экономической и социальной устойчивости. Действительно, Центр изучения демократии призывает к ряду спонсируемых ЕС мер по повышению устойчивости СМИ в Черноморском регионе, таких как программы по повышению журналистских стандартов и предотвращению так называемого захвата СМИ злонамеренными внешними субъектами. По той же причине, в декабре 2018 года в результате растущей обеспокоенности состоянием свободной прессы в регионе в Румынию и Болгарию вернулось Радио Свободная Европа.[46] Хотя эти меры крайне необходимы, можно также рассмотреть и подходы сдерживания с помощью наказания. Такие сдерживающие факторы могут включать агрессивные судебные иски и санкции в отношении отдельных лиц или групп, нарушающих национальные законы. Здесь опять же, центр реагирования на кибер и гибридные угрозы, подобный тому, что предложен Атлантическим советом Болгарии, мог бы внести важный вклад в эти усилия и имел бы преимущество в том, что он включился бы в сообщество заинтересованных сторон, выполняя аналогичную работу по всей Европе.[47]

---

[45] Center for the Study of Democracy (CSD), *Russian Influence in the Media Sectors of the Black Sea Countries: Tools, Narratives, and Policy Options for Building Resilience* (Sofia, Bulgaria: Black Sea Trust for Regional Cooperation and the German Marshall Fund, 2018).

[46] Eugen Tomiuc, Eugen Tomiuc "RFE/RL to Launch News Services in Romania, Bulgaria," *RadioFreeEurope/RadioLiberty*, July 19, 2018, https://www.rferl.org/a/rfe-rl-to-launch-news-services-in-romania-bulgaria/29376248.html.

[47] Гибридный центр передового опыта в Финляндии и Кибер центр передового опыта в Эстонии являются двумя важными примерами того, как многонациональное сотрудничество можно применять на пользу национальным задачам.

Выводы

Хотя теория сдерживания, безусловно, не панацея ни от обычных, ни от гибридных угроз, с которыми сталкивается Восточная Европа, рассмотрение некоторых ключевых принципов теории сдерживания может помочь организовать мышление и выявить дополнительные вопросы, которые стоит рассмотреть. Один из способов понимания усилий Североатлантического союза с 2014 года заключался в том, чтобы в первую очередь надо было противодействовать более непосредственным угрозам сдерживания, предотвращая атаки с целью поставить перед свершившимся фактом и проводя красные линии против ограниченных попыток зондирования. Первоначально это было сделано с расчетом на то, что быстрое подкрепление и передовое развертывание обеспечат ответный удар Североатлантического союза, сдерживая дальнейший авантюризм за счет перспективы наказания. Большой вызов при таком подходе состоял в том, чтобы убедить противника в вероятность наказания и готовность США к расширенному сдерживанию. С тех пор эти усилия были дополнены более устойчивыми усилиями по развертыванию способностей, которые могут противостоять местным, географическим преимуществам российских сил за счет более сильных национальных сил, раннего предупреждения, быстрой мобильности и заранее размещенного оборудования. Этот шаг к сдерживанию путем воспрещения требует большей предкризисной подготовки обороны Восточной Европы, но может быть более надежным, поскольку противнику легче рассчитать риск, который может повлечь за собой агрессия.[48]

Тем не менее, хотя эти усилия продолжают созревать, вызовы контролируемого давления на сдерживание НАТО означают, что единство и решимость Североатлантического союза постоянно подвергаются нападкам. По отдельности союзники осознают опасность, и все вместе в рамках Североатлантического союза приходят к пониманию той роли, которую НАТО может сыграть в противодействии угрозам серой зоны. Какие симметричные и асимметричные возможности, варианты реагирования и меры кризисного реагирования должны быть в наличии? Относятся ли такие способности к процессу оборонного планирования НАТО? Как обеспечить взаимодополняемость между отдельными союзниками, НАТО и ЕС? Какова роль НАТО, включая консультации по статье 4, в привлечении внимания к тактике управляемого давления? Это лишь некоторые из вопросов для будущей работы.

Хотя все это связано с большой идеей иголок ежа – сдерживанием, это также предполагает, что применение сдерживания в современной среде безопасности требует некоторых из более широких и новаторских подходов лисы. Если позаимствовать фразу из другого сценария НАТО, применение сдерживания 21 века потребует *комплексного подхода*. Это включает в себя

[48] Snyder, *Deterrence by Denial and Punishment*, 5.

комплексный подход к обеспечению устойчивости (сдерживание посредством воспрещения) и комплексный подход к наложению пропорциональных затрат на агрессоров (сдерживание посредством наказания).[49] Работоспособная стратегия, дающая возможность сделать и то, и другое, лучше позволит союзникам сдерживать конфликт в обеих концах спектра соперничества. Это потребует как настойчивости, так и способности к адаптации для достижения устойчивых целей с помощью новых инструментов, которые можно использовать против различных угроз. Потребуются инстинкты как ёжика, так и лисы.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Полковник сухопутных войск США **Даррелл Драйвер** является доцентом и директором департамента европейских исследований Военного колледжа армии США. В число его предыдущих должностей входили должность директора Отдела поддержки НАТО Европейского командования США, советника по оборонной политике миссии США при НАТО, старшего научного сотрудника и преподавателя в Европейском центре исследований по вопросам безопасности им. Джорджа Маршалла и доцента политологии в Военной академии США. Он является автором ряда статей и глав в книгах по вопросам, связанным с европейской безопасностью и военно-гражданскими отношениями. Он имеет докторскую степень (2006 г.) в области политических наук Сиракузского университета. *E-mail*: darrell.w.driver.mil@mail.mil.

[49] Фактически, Крис Кремидас Кортни описывает гибридную войну, как «Комплексный подход к наступлению». Подробнее об этом см. Chris Kremidas Courtney, “Hybrid Warfare: The Comprehensive Approach in the Offense,” *Friends of Europe: Europe’s World*, December 2018.

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

В. Шаламанов, П. Анастасов & Г. Цветков
Connections QJ 18, № 1-2 (2019): 29-50
https://doi.org/10.11610/Connections.rus.18.1-2.02

Рецензированная статья

Сдерживание и оборона на восточном фланге НАТО и ЕС: готовность и оперативная совместимость в контексте вынесенного вперед присутствия

Велизар Шаламанов, [1] ***Павел Анастасов,*** [2] ***Георги Цветков*** [3]

[1] *Институт ИКТ, Болгарская академия наук, http://www.iict.bas.bg/EN*

[2] *Отдел по политическим вопросам и политике безопасности, Международный секретариат НАТО*

[3] *Национальная военная академия «Г. С. Раковски», София, https://rndc.bg/en/*

Резюме: В этой статье отражены дискуссии во время конференции в Софии в сентябре 2018 г., организованной Отделом общественной дипломатии НАТО. Основное внимание в ней уделяется политике обороны и сдерживания НАТО и Европейского союза в Восточной Европе. Особое внимание уделяется развитию Бухарестской инициативы (B9) и ее влиянию на Западные Балканы и Черноморский регион. Авторы предлагают программу обеспечения готовности и оперативной совместимости, ориентированную на область C4ISR. Она основана на состоянии обороны и соответствует контексту развития в НАТО и Европейском союзе, направленного на повышение готовности и оперативной совместимости с партнерами. Эта программа вместе с расширенным сотрудничеством в области образования и обучения для данного региона B9+ будут действовать как инструменты для реализации этого сотрудничества и улучшения сдерживания и обороноспособности на восточном фланге НАТО и ЕС, одновременно повышая устойчивость к гибридным угрозам.

Ключевые слова: НАТО, Европейский Союз, оборона, сдерживание, готовность, оперативная совместимость, сотрудничество, Восточный фланг, Балканы, Черноморский регион, устойчивость.

Присутствие НАТО в Восточной Европе после перемен 1989 г.[1]

В этой статье рассматриваются вопросы развития многонациональных формирований в Центральной и Восточной Европе (ЦВЕ)/ Юго-Восточной Европе (ЮВЕ), улучшение их функциональной совместимости и готовности посредством многонациональных проектов, особенно в области коммуникаций и информации (К&И), а также соответствующее образование и обучение, включая учения. Предлагаются дальнейшие исследования в многонациональном формате для определения программ обеспечения готовности и оперативной совместимости многонациональных формирований в ЦВЕ/ ЮВЕ.

После изменений 1989 г. НАТО серьезно начало участвовать в делах Восточной Европы, и в 1995 г. началось заметное присутствие в Восточной Европе военных формирований, несущих ответственность перед Организацией Объединенных Наций (ООН) за выполнение Дейтонских мирных соглашений. Эти соглашения были подписаны 22 ноября 1995 года президентами Боснии, Хорватии и Сербии от имени Сербии и Боснийской Сербской Республики. Фактическое подписание состоялось в Париже 14 декабря 1995 года. Соглашения преследовали три основные цели: прекращение боевых действий, принятие военных и гражданских программ и создание центрального боснийского правительства, исключая при этом участие военных преступников в управлении. Первые многонациональные силы (IFOR) под руководством НАТО были созданы для выполнения военных положений *Общего рамочного соглашения о мире (GFAP) в Боснии и Герцеговине.*

IFOR заменили миротворческие силы ООН (UNPROFOR), которые впервые прибыли в 1992 году, и передача полномочий была согласована в резолюции 1031 Совета Безопасности. В Боснии были развернуты силы НАТО численностью почти в 60 000 солдат, в дополнение к силам из стран, не входящих в НАТО. Операция Решительное усилие (SACEUR OPLAN 40105), начавшаяся 6 декабря 1995 года, была подкомпонентом операции Совместное усилие.

Следующим крупным многонациональным присутствием были силы SFOR, которые были созданы резолюцией 1088 Совета Безопасности от 12 декабря 1996 года, чтобы сменить IFOR. К концу 2002 года численность войск была сокращена примерно до 12 000 человек, а к концу 2004 года – примерно до 7 000 человек, когда на Стамбульском саммите НАТО было объявлено об окончании миссии.

Операция «*Алтея*», официально именуемая «Силы Европейского союза» (EUFOR) в Боснии и Герцеговине, является преемницей SFOR/ IFOR. Переход от SFOR к EUFOR был в значительной степени только сменой названия и командования: 80 % войск остались на своих местах. Официально они заменили SFOR 2 декабря 2004 года.

[1] В этом разделе, в основном, используется информация, опубликованная на вебсайте НАТО, https://www.nato.int, and the English version of Wikipedia.

Следующим крупным многонациональным формированием, развернутым в Восточной Европе после первой реальной боевой операции НАТО в Европе,[2] были силы KFOR. После принятия резолюции 1244 Совета Безопасности ООН, войска вошли в Косово 11 июня 1999 года. В то время Косово столкнулось с серьезным гуманитарным кризисом, когда около миллиона человек были вынуждены покинуть свои дома в качестве беженцев. На пике своей численности военнослужащие KFOR насчитывали 50 000 человек из 39 стран НАТО и стран, не входящих в НАТО.

С течением времени KFOR постепенно передали ответственность Силам безопасности Косово и другим местным властям, и по состоянию на 23 мая 2016 года насчитывали 4600 военнослужащих. Недавно KFOR в Приштине (2018 г.) состояли из: Группы поддержки штаб-квартиры (HSG) в Приштине; Многонационального специализированного подразделения (MSU) в Приштине (полк военной полиции, полностью состоящий из итальянских карабинеров); Многонациональной боевой группы «Восток» (MNBG-E) в лагере Бондстил возле Ферижая (силы армии США, поддерживаемые Венгрией, Польшей, Румынией и Турцией); Многонациональной боевой группы «Запад» (MMBG-W) в лагере Виладжио Италия недалеко от Печа (силы итальянской армии, поддерживаемые Австрией, Молдовой и Словенией); Объединенной группы логистической поддержки (JLSG) в Приштине (материально-техническое обеспечение и инженерное обеспечение); Тактического резервного батальона KFOR (KTRBN) в лагере Ново Село (полностью состоит из войск Венгерской армии); Объединенного регионального отряда – Север (JRD-N) в лагере Ново Село (местная некинетическая связь и мониторинг); Объединенного регионального отряда – Центр (JRD-C) в Приштине (местная некинетическая связь и наблюдение); Совместного регионального отряда – Юг (JRD-S) в Призрене (местная некинетическая связь и мониторинг).

Опыт, накопленный на Балканах, имел важное значение для определения кризисного менеджмента и использования многонациональных формирований вплоть до тактического уровня. Действуя за пределами Европы, ISAF были многонациональными силами, имевшими решающее значение для разработки концепции оперативной совместимости, особенно с введением сети миссий в Афганистане (AMN) в качестве оперативного инструмента.[3]

Следующая крупная операция – Объединенный защитник – была вызовом и в то же время возможностью проверить готовность и оперативную

[2] Gen. Wesley K. Clark, *Waging Modern War: Bosnia, Kosovo and the Future of Combat* (New York: Public Affairs, 2001).

[3] Gen. Stanley McChrystal, *My Share of the Task: A Memoir* (New York: Penguin Publishing Group, 2013).

совместимость в воздушном и морском домене.[4] Задача кризисного менеджмента с оперативной точки зрения решалась с помощью ряда различных инициатив, включая создание Центра управления комплексными операциями в кризисных ситуациях (ССОМС) для обеспечения ситуационной осведомленности и поддержки дальнейшего планирования с помощью имеющихся готовых и оперативно совместимых сил, которые, как правило, являются многонациональными формированиями.[5]

Переход от кризисного менеджмента стал наиболее заметен на саммите в Уэльсе в 2014 году, когда союзники по НАТО согласились реализовать План действий по обеспечению готовности (ПДГ), чтобы быстро отреагировать на фундаментальные изменения в среде безопасности на восточных границах НАТО.

Опираясь на ПДГ, на Варшавском саммите в 2016 году союзники приняли дальнейшие решения по усилению системы сдерживания и обороноспособности НАТО, а также по содействию обеспечения стабильности и укреплению безопасности за пределами территории Североатлантического союза. Вместе эти решения стали самым большим укреплением коллективной защиты Североатлантического союза за последнее поколение. В сочетании с силами и способностями, необходимыми для быстрого подкрепления последующими силами, эти меры повысят безопасность всех союзников и обеспечат защиту территории, населения, воздушного пространства и морских коммуникаций Североатлантического союза, в том числе по ту сторону Атлантического океана, от любых угроз, откуда бы они ни возникали.

Расширенное присутствие НАТО на передовых рубежах носит оборонительный характер, является соразмерным и соответствует международным обязательствам. Оно представляет собой демонстрацию серьезной решимости союзников и является ощутимым напоминанием о том, что нападение на одного – это нападение на всех.

Полностью развернутое в июне 2017 года расширенное передовое присутствие НАТО включает многонациональные силы, предоставленные приграничными государствами и другими участвующими союзниками на добровольной, полностью устойчивой и ротационной основе. Они основаны на четырех сменных боевых группах размером в батальон, которые действуют совместно с национальными силами обороны и постоянно присутствуют в принимающих странах. Канада, Германия, Великобритания и США являются базовыми странами для этого устойчивого многонационального присутствия в Латвии, Литве, Эстонии и Польше, соответственно.

Другие союзники подтвердили свой вклад в эти силы: Албания, Чешская Республика, Италия, Польша, Словакия, Словения и Испания вносят свой вклад в возглавляемую Канадой боевую группу в Латвии; Бельгия, Чешская

[4] Rob Weighill and Florence Caub*, The Cauldron: NATO's Campaign in Libya* (London: Hurst Publishers, 2018).

[5] James Stavridis, *The Accidental Admiral: A Sailor Takes Command at NATO* (Annapolis, Maryland: Naval Institute Press, October 2014).

Республика, Исландия, Люксембург, Нидерланды и Норвегия присоединились к боевой группе под руководством Германии в Литве; Дания и Исландия участвуют в боевой группе под руководством Великобритании в Эстонии; а Хорватия, Румыния и Великобритания присоединились к боевой группе под командованием США в Польше. Эти расширенные силы передового присутствия дополняются необходимой логистикой и инфраструктурой для поддержки предварительного позиционирования и облегчения быстрого подкрепления. Четыре боевые группы находятся под командованием НАТО через штаб многонационального корпуса «Северо-Восток» в Щецине, Польша. Деятельность этих четырех боевых групп по обучению и подготовке координируется и контролируется штабом многонациональной дивизии «Северо-Восток» (MND-NE) в Эльблонге, Польша.

На саммите 2016 года в Варшаве союзники также договорились развивать адаптированное передовое присутствие в юго-восточной части территории Североатлантического союза. На суше это присутствие строится вокруг многонациональной бригады под руководством Румынии в Крайове. В воздухе несколько союзников усилили деятельность Румынии и Болгарии по защите воздушного пространства НАТО. Это означает больше сил НАТО и больше учений и тренировок под руководством штаба многонациональной дивизии «Юго-Восток» (в Румынии), которая начала действовать в полную силу в июне 2017 года. Это адаптированное передовое присутствие способствует усилению сдерживания и обороны Североатлантического союза и его ситуационной осведомленности, оперативной совместимости и готовности к ответной реакции.

Все эти изменения являются ответом на агрессивное поведение России с 2008 года, но поворотным моментом на самом деле стала аннексия Крыма и агрессивные действия на востоке Украины, а также разработка концепции гибридной войны и ее реализация. Это означает, что на Востоке НАТО сталкивается с гибридным вызовом России,[6] но в то же время и вполне реальным вызовом со стороны России в области обычных вооружений.[7]

Стратегия НАТО быстрого подкрепления также гарантирует, что силы передового присутствия в случае необходимости будут усилены Совместной оперативной группой очень высокой готовности НАТО, более широкими Силами реагирования НАТО, дополнительными силами высокой готовности союзников и более существенными последующими силами НАТО. НАТО

---

[6] Franklin D. Kramer and Lauren M. Speranza, “Meeting the Russian Hybrid Challenge: A Comprehensive Strategic Framework” (Washington, DC: Atlantic Council, Brent Scowcroft Center on International Security, May 2017), https://www.atlanticcouncil.org/in-depth-research-reports/report/meeting-the-russian-hybrid-challenge.

[7] Franklin D. Kramer and Hans Binnendijk, “Meeting the Russian Conventional Challenge: Effective Deterrence by Prompt Reinforcement” (Washington, DC: Atlantic Council, Brent Scowcroft Center on International Security, February 2018), www.atlanticcouncil.org/in-depth-research-reports/report/meeting-the-russian-conventional-challenge.

также разрабатывает ряд дополнительных мер по увеличению своего присутствия в Черноморском регионе. Осуществляются конкретные меры по усилению морского и воздушного присутствия НАТО в регионе, при этом несколько союзников предоставляют силы и средства. Хотя передовое присутствие в основном сосредоточено в Северо-Восточной Европе, геостратегическое значение Черного моря растет,[8] особенно для России после аннексии Крыма, и, как следствие, существует видимая конфронтация между Россией и НАТО[9] в этом регионе.

Основываясь на этом кратком обзоре развития многонациональных сил для кризисного менеджмента, а также для сдерживания и обороны, в оставшейся части статьи исследуется потенциал в ЦВЕ после Брюссельского саммита НАТО (2018 г.) с соответствующими возможностями для повышения готовности и оперативной совместимости через многонациональные коммуникационные и информационные проекты и соответствующее обучение.

Потенциал сдерживания Североатлантического союза в его восточной зоне ответственности – путь вперед

Восточная зона ответственности Североатлантического союза и Черноморский регион продолжают оставаться одним из наиболее динамично развивающихся регионов с одними из самых серьезных проблем в области безопасности. Все они проистекают из агрессивной позиции России на Востоке, Юге Европы и Западных Балканах. После Брюссельского саммита на международной конференции в Софии, Болгария, организованной НАТО в 2018 году, специальная группа по сдерживанию и обороноспособности в Восточной Европе согласилась с тем, что из трех основных задач – коллективная оборона, кризисный менеджмент и совместная безопасность, коллективная оборона остается ключевым направлением деятельности, которое постоянно и быстро развивается благодаря саммитам в Уэльсе, Варшаве и Брюсселе. Эта эволюция описывалась как переход от позиции сдерживания посредством наказания к позиции сдерживания путем воспрещения. Новые решения, принятые на Брюссельском саммите, такие как Инициатива готовности НАТО, а также текущая разработка мер передового присутствия вместе с Европейской оборонной инициативой США (EDI) подтвердили непоколебимую приверженность НАТО коллективной обороне и приверженность США защите Европы.

На конференции представители восточного фланга НАТО отдали приоритет дальнейшему развитию сценария сдерживания путем воспрещения с

[8] Bouris Toucas, The Geostrategic Importance of the Black Sea Region: A Brief History, Center for Strategic and International Studies (CSIS), February 2, 2017, www.csis.org/analysis/geostrategic-importance-black-sea-region-brief-history.

[9] Boris Toucas, NATO and Russia in the Black Sea: A New Confrontation? Center for Strategic and International Studies (CSIS), March 6, 2017, https://www.csis.org/analysis/nato-and-russia-black-sea-new-confrontation.

акцентом на роли формата сотрудничества Бухарест-9 (B9), который должен стать голосом ЦВЕ.[10] Альянс должен продолжать концентрировать свои усилия на улучшении расширенных военных возможностей, чтобы продемонстрировать надежную способность противостоять агрессии с первого момента. Основное внимание в рамках основной задачи НАТО должно уделяться перспективному планированию, военной мобильности в Североатлантическом союзе и инициативам по обеспечению готовности с передовым присутствием и улучшенной оперативной совместимостью в многонациональной среде на тактическом уровне. Более подробно, этот потенциал сдерживания требует (1) улучшенных систем раннего предупреждения, чтобы дать Североатлантическому союзу больше времени для реагирования, (2) надежных национальных сил, способных вести начальную оборону, и (3) повышенной мобильности и заранее размещенного оборудования для обеспечения массированного ответа Североатлантического союза.

Одним из важных элементов является твердое понимание того, что адаптация НАТО и развитие Европейского Союза (ЕС) в области обороны должны быть полностью синхронизированы. Преимущества оборонно-промышленного комплекса ЕС и разработка программ оборонных исследований, инструменты, доступные Европейской службе внешних действий, а также разработка проектов PESCO должны согласовываться с разработками НАТО и дополнять друг друга, одновременно обеспечивая и то, и другое и делая НАТО и ЕС сильнее и безопаснее. Европейский Союз должен и впредь наилучшим образом использовать оборонную политику и методологию планирования НАТО. Хорошая координация между НАТО и процессом достижения основных целей ЕС и планом развития потенциала является обязательным условием.

Болгария, Румыния и Турция являются основными заинтересованными сторонами в разработке и реализации текущих мер специально адаптированного передового присутствия НАТО. Эти меры укрепляют сдерживающую и оборонительную позицию Североатлантического союза в Черноморском регионе и должны быть полностью синхронизированы с безопасностью Северо-Восточного / Балтийского региона Восточной Европы (Балтийские государства, Вышеградская группа), связанных с Западными Балканами и Адриатическим морем.

Многонациональная бригада в Крайове с Румынией в качестве базовой нации является основным элементом сухопутного компонента. В воздушной сфере союзники наращивают усилия Румынии и Болгарии по охране воздушного пространства. В морской сфере присутствуют постоянные мор-

[10] Marcin Terlikowski, with Veronika Jóźwiak, Łukasz Ogrodnik, Jakub Pieńkowski, and Kinga Raś, "The Bucharest 9: Delivering on the Promise to Become the Voice of the Eastern Flank," *PISM Policy Paper* no. 4 (164) (Warsaw: Polish Institute of International Affairs, 2018), по состоянию на 29 октября 2018, http://www.pism.pl/Publications/PISM-Policy-Paper-no-164.

ские силы НАТО с большим количеством кораблей и военно-морских учений в регионе. В Морском командовании НАТО создан Черноморский функциональный центр. Новая инициатива по расширенному обучению направлена на повышение согласованности всех учебных мероприятий в регионе. Как правило, все специально адаптированные меры должны обеспечивать готовность и совместимость.

Рассматриваемые как сугубо военно-технические вопросы до саммита в Уэльсе, теперь готовность и оперативная совместимость становятся ключевыми критериями эффективности адаптации НАТО к российскому вызову в области обычных вооружений. И именно здесь союзники должны проявить решимость, поскольку готовность и оперативная совместимость обходятся дорого. Необходимо изучить и развить необходимость новаторства и обдумывания рентабельных вариантов для того, чтобы продемонстрировать убедительное сдерживание. Это включает в себя больше ротаций для учений, трансграничную воздушную подготовку (которая может быть основана на модели NORDEFCO), морское присутствие (как на Балтийском, так и на Черном морях) и расширение постоянно дислоцированных формирований.

Болгария должна работать над обеспечением реального и постоянного присутствия сил союзников на своей территории, размещая наземные, воздушные и военно-морские компоненты передового присутствия НАТО, такие как размещение:

- координационного элемента морского командования союзников в Варне, связанного с подразделениями интеграции сил НАТО (NFIU) в Софии и Бухаресте;
- многонациональной эскадрильи истребителей ВВС на ротационной основе на болгарской военной авиабазе (особенно в период приобретения нового истребителя и потенциального ускорения снятия с вооружения МиГ-29), которая должна осуществлять совместное союзное воздушное патрулирование болгарского воздушного пространства, потенциально для покрытия воздушного пространства и Северной Македонии после завершения процесса присоединения (в сотрудничестве с Грецией и другими союзниками);
- многонациональной механизированной бригады или многонациональной бригады специальных операций, при этом Болгария должна являться базовым государством.

В качестве выражения солидарности и сплоченности на всем восточном фланге, Болгария должна присоединиться к одной из созданных четырех многонациональных боевых групп НАТО в странах Балтии и Польше.

Новая Инициатива готовности, согласованная на саммите в Брюсселе, должна улучшить способность НАТО мобилизовывать и развертывать более крупные силы подкрепления и, следовательно, усилить сдерживание и обороноспособность на восточном фланге Североатлантического союза. Инициатива должна гарантировать, что в распоряжение НАТО можно будет

предоставлять более качественные, боеспособные национальные силы в высокой степени готовности. Из общего пула сил союзники предложат дополнительно 30 основных боевых кораблей военно-морских сил, 30 тяжелых или средних маневренных батальонов и 30 авиационных эскадрилий с обеспечивающими силами в готовности не более 30 дней. Они будут организованы и обучены как элементы более крупных боевых формирований в поддержку общего потенциала сдерживания и обороны НАТО. Как указано в коммюнике саммита, Инициатива готовности еще больше усилит возможности быстрого реагирования Североатлантического союза, либо для усиления союзников в поддержку сдерживания или коллективной обороны, в том числе для ведения боевых действий высокой интенсивности, либо для быстрого военного вмешательства в кризисные ситуации, если это необходимо. Это также повысит важность эффективных общевойсковых и совместных операций. Будучи логическим развитием саммита в Уэльсе, План действий по обеспечению готовности и саммит в Варшаве были сфокусированы на передовом присутствии, новой инициативе, которая какой бы амбициозной и важной она ни была, может столкнуться с множеством проблем при реализации.

Ряд областей потребует особого внимания, поскольку увеличение и поддержание боеготовности сил связано с большими затратами. Задача обеспечения 30-дневной готовности также потребует дальнейшего обсуждения, учитывая региональное превосходство России в сухопутных силах. Для таких стран, как Болгария, помимо проблем с предоставлением обученных и оснащенных подразделений, национальные власти должны срочно рассмотреть возможность предоставления поддержки и мобильности, требуемые от принимающей страны. Принимая во внимание, что приобретение новых оперативно совместимых с НАТО истребителей и кораблей в Болгарии было отложено в 2014 году, наиболее очевидным вкладом будет механизированный батальон. Работая в тесном сотрудничестве с Албанией, Черногорией и вскоре, с Северной Македонией, можно будет внести свой вклад в Инициативу готовности созданием региональных многонациональных батальонов для использования Альянсом, что будет способствовать оперативной совместимости и готовности.

Также важно учитывать усилия как НАТО, так и ЕС по повышению военной мобильности на суше, в воздухе и на море, устранению связанных с этим физических барьеров, таких как недостатки инфраструктуры и ее несовместимость с военными требованиями, а также нехватка транспортных средств. Кроме того, необходимо рассмотреть необходимость устранения процедурных препятствий, таких как время для получения национального разрешения на пересечение границы силами и техникой.

Брюссельский саммит подтвердил приверженность обязательствам по инвестициям в оборону, взятым на саммите в Уэльсе в 2014 году. Справедливое разделение бремени лежит в основе сплоченности, солидарности, авторитета Альянса и его способности выполнять обязательства по статьям

3 и 5. Союзники начали увеличивать суммы, которые они тратят на оборону в реальном выражении, и две трети союзников имеют национальные планы достижения уровня расходов на оборону в объеме 2 % своего валового внутреннего продукта к 2024 году. Более половины из них выделяют более 20 % своих оборонных бюджетов на приобретение основного оборудования, включая соответствующие исследования и разработки и, в соответствии с их национальными планами, 24 союзника к 2024 году выполнят норматив в 20 %.

Болгария должна пересмотреть и адаптировать планы правительства, для того чтобы достичь уровня расходов на оборону в 2 % ВВП в 2020 году, а не в 2024 году. Правительство также должно запланировать достижение уровня расходов на приобретение новых способностей и на исследования не менее 20 % от общих расходов на оборону (и, возможно, для определения варианта увеличения расходов на оборону сверх этих уровней на ранних этапах перевооружения, чтобы ускорить замену старого, несовместимого и часто опасного в эксплуатации советского оборудования). Это должно быть согласовано с достижением договоренности об установлении крайнего срока для прекращения зависимости государств-членов от Российской Федерации в отношении технического обслуживания основных систем вооружений и оборудования, в том числе путем расширения сотрудничества в рамках НАТО и ЕС.

Дополнительной национальной мерой, которую следует здесь рассмотреть, является создание Агентства по закупке вооружений, которое должно быть создано с четко определенными функциями, обязанностями и задачами в соответствии с принципами демократии и надлежащего управления. Создание агентства должно включать механизмы управления проектами и тесную координацию с НАТО и европейскими агентствами по вооружениям и закупкам. В рамках своего мандата оно должно работать над поиском синергии в рамках совместных с союзниками по НАТО / государствами-членами ЕС на Западных Балканах, в Черноморском регионе и за его пределами возможностей приобретения и обслуживания.

Кроме того, как отметила Лаура Брент в недавней статье в журнале «Вестник НАТО», «киберугрозы безопасности Североатлантического союза становятся все более частыми, силовыми, сложными и разрушительными».[11] Киберзащита является частью основной задачи коллективной защиты НАТО. Болгария должна иметь возможность действовать в киберпространстве так же эффективно, как и в воздухе, на суше и на море, чтобы укреплять и поддерживать общую политику сдерживания и обороны Североатлантического союза. Таким образом, Болгария может внести важный вклад в сдерживание и защиту, обеспечивая мощную национальную кибер-

[11] Laura Brent, "NATO's Role in Cyberspace," *NATO Review*, 12 February 2019, https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

защиту за счет полного выполнения Обязательства по киберзащите, которое имеет решающее значение для повышения киберустойчивости и повышения цены наказания за кибератаки.

Предлагаемая мера для Болгарии – создание центра реагирования на кибер и гибридные угрозы при Министерстве обороны с задачами по расследованию, анализу, а затем координации и реализации мер по противодействию кибер и гибридным угрозам. Этот центр должен быть связан со способностями штаб-квартиры НАТО по раннему предупреждению, а также с соответствующими центрами передового опыта в рамках НАТО и ЕС. Разработка новых правил в ЕС по созданию европейской промышленной, технологической и исследовательской компетенции в области кибербезопасности с сетью национальных координационных центров требует тесной координации с разработками в области обороны на национальном уровне и, соответственно, с НАТО.

Вместе с хорошим сотрудничеством в рамках НАТО и ЕС, важнейшим аспектом успеха является региональное сотрудничество. Группа стран, наиболее озабоченных сдерживанием и защитой восточного фланга НАТО, может быть определена как Бухарест 9+ / B9+ (союзники на восточном фланге, которыми являются Польша, три страны Балтии, Венгрия, Чехия, Словакия, Румыния, Болгария, но также Албания, Черногория и Хорватия с Северной Македонией в качестве будущего государства-члена). В этом формате можно было бы активно взаимодействовать с ключевыми партнерами НАТО, такими как Грузия и Украина. Эти два партнера постоянно заявляли, что они приветствуют усилия Североатлантического союза по обеспечению надежной защиты на его восточном фланге и его приверженность поддержанию стабильности в более широком Черноморском регионе. Хороший пример подобных отношений – отношения между Швецией и Финляндией (являющиеся членами ЕС, но не членами НАТО), которые активно участвуют в проецировании стабильности в регионе Балтийского моря.

Следуя передовой практике NORDEFCO и BENELUX, необходимо и дальше развивать проектное сотрудничество в формате B9. Инициирование флагманской программы обеспечения готовности и взаимодействия (PRI) в этом контексте, как показано ниже, могло бы стать первым шагом к изменениям. Существует большой потенциал для интеграции посредством учений и реальных операций для ряда национальных и многонациональных формирований в регионе. Следуя примеру «решения сперва НАТО», использованного для штаб-квартиры структуры сил НАТО, PRI могла бы быть обеспечена полностью за счет поддержки со стороны Агентства связи и информации НАТО (NCIA) и Агентства поддержки и закупок НАТО (NSPA). Региональные проекты по воздушному и морскому наблюдению являются потенциальными пилотными проектами, которые необходимо развивать, а совместный анализ других проектов по осуществлению закупок / логистики в формате B9+ мог бы обеспечить прочную основу для портфеля многонациональных проектов по закупке оборудования или, по крайней мере, для

региональных систем технического обслуживания и ремонта с поддержкой NSPA.

Развитие инициатив оперативной совместимости и готовности в НАТО

Ростки перемен появились на пражском саммите в ноябре 2002 г., когда НАТО признало важность трансформации вооруженных сил на основе принципов информационного века. Затем был продолжен курс на трансформацию в соответствии с концепцией *сетевых способностей НАТО* (NNEC). Все операции на Балканах[12] (Босния и Герцеговина, Косово), а также присутствие в Албании и Македонии дали такой большой опыт, что спровоцировали трансформационные усилия в НАТО с поворотным моментом, основанным на ISAF[13] и OUP.[14] В последнее время реализация ПДГ и новой Инициативы готовности придает дополнительный импульс этим усилиям.

Хорошим примером, в 2003 году, было то, как девять стран НАТО (Канада, Франция, Германия, Италия, Нидерланды, Норвегия, Испания, Великобритания и США) организовали финансирование технико-экономического обоснования NNEC. Это исследование было поручено Агентству НАТО С3 (NC3A), а позже АСТ запустил информационную кампанию по продвижению концепции NNEC на основе результатов исследования. В то же время в NC3A был создан программный офис NNEC для управления всеми проектами, финансируемыми совместно с NNEC. Достижение полного сотрудничества и полной согласованности между различными проектами НАТО и стран НАТО является долгосрочной целью, поэтому в 2009 году Агентство создало новый спонсорский счет «НАТО и нации» для поддержки реализации проектов C4ISR за пределами командной структуры НАТО, связанных с оперативной совместимостью в области К&И.

Программа NNEC, направленная на создание федерации возможностей на всех уровнях, военном (от стратегического до тактического) и гражданском, через информационную инфраструктуру, и в то же время, следуя видению «Делись, чтобы побеждать», начала работу, направленную на изменение культуры участвующих людей. Обмен информацией является предпосылкой для лучшей ситуационной осведомленности и более быстрого принятия решений, что улучшает сотрудничество между странами, что, в конечном итоге, спасает жизни и ресурсы. *Информационная инфраструктура* является опорной базой, которая обеспечивает совместную работу и обмен информацией между пользователями, и сокращает время цикла

[12] Clark, *Waging Modern War*.

[13] McChrystal, *My Share of the Task*.

[14] Weighill and Caub, *The Cauldron*.

принятия решений. Это приводит к *информационному превосходству*,[15] то есть способности доставлять нужную информацию нужным людям в нужное время.

В 2009 году Агентство НАТО по консультациям, командованию и управлению (NC3A) признало растущую потребность в поддержке стран в дополнение к общим программам C4ISR (командование, управление, связь, компьютеры, наблюдение и разведка), финансируемых НАТО по разработке современных, интероперабельных и безопасных возможностей C4ISR. Так, 11 ноября 2009 г. Агентство предложило Совету NC3 для нотации Комплексный подход[16] НАТО к C4ISR.

Домен C4ISR / Cyber в контексте *сети федеративных миссий* (FMN) играет центральную роль в интеграции сил. Для ускорения развития в этой области, особенно для восточноевропейских членов НАТО и партнеров в NC3A (ныне NCIA), в 2010 году было предложено создание Интеграционного фонда[17] C4ISR. Реализация этой модели началась в 2014 году с *трастового фонда C4* для Украины, возглавляемого Канадой, Великобританией и Германией при поддержке NCIA.

В значительной степени инициатива реформирования Агентства в области C4ISR, одобренная на Лиссабонском саммите в 2010 г., продолжала Комплексный подход НАТО к C4ISR. Она оказывала поддержку всему сектору безопасности, выходя за пределы оборонного ведомства и включая других партнеров. Она также охватывала весь жизненный цикл C4ISR способностей от определения требований до развертывания и даже вывода из эксплуатации. Кроме того, она использовала все доступные источники финансирования – от общего финансирования до финансирования на основе многонациональных и целевых фондов и финансирования отдельными странами.

В области C4ISR этот комплексный подход обеспечил основу для «Умной обороны» для развития потенциала и предоставления услуг путем моделирования этой области еще до ее объявления в качестве флагманской инициативы НАТО на встрече на высшем уровне в Чикаго в мае 2012 года. Там лидеры НАТО пришли к согласию принять инициативу «Умная оборона»[18],

---

[15] НАТО определяет информационное превосходство как оперативное преимущество, вытекающее из способности собирать, обрабатывать и распространять непрерывный поток информации, используя или блокируя способность противника делать то же самое.

[16] *NATO C4ISR Comprehensive Approach* (Brussels: NATO C3 Board and NC3A, 11 November 2009).

[17] "Establishment of a C4ISR Integration Fund" (Brussels: NC3A, 2010).

[18] Новый подход к расходам на оборону в трудные экономические времена – Умная оборона – был определен генеральным секретарем г-ном Расмуссеном как «обеспечение большей безопасности за меньшие деньги за счет большей гибкости совместной работы». В рамках этого подхода он призывал страны «объединять и делиться возможностями, устанавливать правильные приоритеты и лучше координировать наши усилия».

чтобы Североатлантический союз мог разрабатывать, приобретать и поддерживать способности, необходимые для достижения целей программы «Силы НАТО 2020», состоящих из современных тесно связанных сил, которые должным образом оснащены, обучены, натренированы и имеют соответствующее руководство.

В цикле Программы развития руководителей высшего звена НАТО (NEDP) 2013–2014 гг. два основных агентства НАТО попросили молодых лидеров НАТО изучить возможности многонационального сотрудничества[19] при содействии Агентства NCI и NSPA. В цикле NEDP 2015/2016 подразделение оборонных инвестиций использовало тот же механизм для оценки Умной обороны на пять лет вперед.[20]

В качестве элемента «Умной обороны» в агентстве NCI был разработан подход для поддержки стран в повторном использовании решений НАТО с общим финансированием для принятия более быстрых, *совместимых* и безопасных решений в области C4ISR. Эта инициатива была представлена на ежегодной конференции CIO в НАТО как программа «НАТО для наций» в поддержку инициатив Генерального секретаря НАТО «Умная оборона» и «Объединенные силы». Реализация этой программы основана на решении «НАТО прежде всего», предлагаемом нациям через Каталог агентств.[21]

И снова Агентство решило воспользоваться классом NEDP 2015/2016 и инициировало исследование по внедрению решения «НАТО прежде всего»[22] в поддержку инициатив «Умная оборона» и «Связанные силы». Первоначально основной движущей силой разработки решения «НАТО прежде всего» для структуры сил НАТО (NFS)[23] была инициатива сети миссий в Афганистане (AMN) в ответ на просьбу генерала Маккристала создать одну сеть командования и управления (C2) для ISAF в 2009 году.[24]

Решения, принятые на саммите в Уэльсе о разработке Плана действий по обеспечению готовности (ПДГ) и его поддержке с помощью подразделений интеграции сил НАТО (NFIU) в восьми восточноевропейских странах НАТО, резко изменили ситуацию с развитием структуры сил НАТО, созданием многонациональных образований и определением модели присутствия на передовых позициях на ротационной основе с расширенной программой учений типа «Связанных учений».

---

[19] "Smarter Smart Defense: Multinational Cooperation Facilitated," NATO Executive Development Program (NEDP) Project Report (NCI Agency and NSPA, NATO HQ, 2014).

[20] "Smart Defense: Five Years on – Making Smart Defense Even Smarter!" NEDP project report (Brussels: NATO HQ, NCI Agency, 2016).

[21] *Customer Service Catalogue*, *Part I: Customer Handbook* (NCI Agency, 2015).

[22] "NATO First: Sharing Alliance Capabilities with Nations," NEDP project report (NCI Agency, 2016).

[23] "NATO 1st Solution *for NATO Force Structure*" (NCI Agency), accessed October 29, 2018, https://www.ncia.nato.int/Documents/Agency publications/Brochure NATO 1st Solution for NATO Force structure_WEB.pdf.

[24] McChrystal, *My Share of the Task*.

Основываясь на опыте, полученном в рамках инициативы «НАТО прежде всего» в поддержке структуры Сил НАТО, многие партнеры НАТО, такие как Финляндия и Швеция, начали использовать инструменты НАТО в своих процессах для усиленных Сил реагирования НАТО (eNRF) и реализации ПДГ. Эти усилия включали развертывание восьми NFIU за очень короткий период, параллельно и преобразование системы C2 многонационального корпуса «Северо-Восток» в Польше и развертывание новой штаб-квартиры многонациональной дивизии «Юго-Восток» в Румынии. Для решения этой проблемы был подготовлен отчет из проекта NEDP 7-го цикла «НАТО прежде всего, совместное использование возможностей альянса с государствами» для NCIA, программы поддержки этих различных проектов с разными моделями финансирования, но были установлены аналогичные требования.[25]

С решениями Варшавского саммита по вопросам передового присутствия в Восточной Европе и его усовершенствованных и адаптированных моделей, необходимость более формального управления программой стала очевидна для руководства NCIA и, таким образом, была исследована модель партнерства[26] для этого начинания.

Готовность и оперативная совместимость НАТО / ЕС в Восточной Европе – перспектива C4ISR

НАТО приняло Инициативу готовности в 2018[27] году в соответствии с концепцией «*Четырех тридцаток*», согласно которой к 2020 году союзники смогут иметь 30 механизированных батальонов, 30 авиационных эскадрилий и 30 боевых кораблей, готовых быть задействованы в течение 30 дней или меньше. Это большое изменение началось в Уэльсе в 2014 году с инициирования Плана действий по обеспечению готовности, за которым последовало Варшавское соглашение НАТО о передовом присутствии параллельно с более тесной координацией с ЕС в таких областях, как мобильность, киберзащита, реагирование на гибридные войны и устойчивость в целом. НАТО всегда была альянсом оперативной совместимости между членами, но Инициатива оперативной совместимости, принятая на саммите в Уэльсе (2014 г.), стала платформой для повышения оперативной совместимости также с ключевыми партнерами на основе опыта ИСАФ и других операций.

[25] "Initiative for NATO Forces Readiness and Interoperability Partnership (NRIP)," Enclosure 2 to NCIA/DM/2016/02367 (NCI Agency, 2016).

[26] "NATO 1st Solution (N1S) Concept: Partnership with Customers," Enclosure 3 to NCIA/DM/2016/02367, NCI Agency, 2016.

[27] Генеральный секретарь г-н Столтенберг заявил в июне 2018 года: «Речь идет не о создании или развертывании новых сил, а о повышении боеготовности существующих сил».

В этом контексте и на основе опыта, накопленного с 2002 года (более 15 лет развития), предлагается структура для Программы *(Связь и информация) «Готовность и функциональная совместимость (Киберустойчивость)» (PRI)* с первоначальным акцентом на страны Бухарест 9 (Болгария, Чехия, Эстония, Венгрия, Латвия, Литва, Польша, Румыния, Словакия). Это страны, которые перешли из Варшавского договора в НАТО и ЕС за последние 20 лет и образуют потенциальную основу наций для ротационных боевых групп и других формирований в рамках передового присутствия, а также других связанных инициатив. Сюда включаются войска США в рамках инициативы *«Атлантическая решимость / Европейская оборонная инициатива»*, а также дальнейшее развитие многонациональных формирований в Восточной Европе, включая развитие KFOR и миссии Алтея как ключевых элементов многонационального военного присутствия в Юго-Восточной Европе.

Такая программа должна начаться с определения структуры сил в Восточной Европе. Сюда могут входить различные элементы NFS, другие многонациональные формирования в рамках инициатив НАТО или ЕС (например, в Юго-Восточной Европе боевая группа HELBROC в составе Греции, Румынии, Болгарии, Кипра и с участием Украины и даже SEEBRIG, созданная в 1999 г. по региональному сотрудничеству в области обороны в ЮВЕ) и элементы национальных силовых структур принимающих стран, которые должны быть включены в такие крупномасштабные усилия по обеспечению оперативной совместимости и готовности.

Заинтересованными сторонами в PRI будут страны, элементы структуры сил которых охватывают и руководство многонациональных формирований, которых это касается, а также стратегическое командование, соответствующие комитеты НАТО, советы и связанные с ними элементы со стороны европейской обороны. Более того, формат B9 (Бухарестское сотрудничество) можно рассматривать как отличную платформу для преобразования сотрудничества между НАТО и ЕС путем внедрения нового подхода к модернизации сил девяти стран, повышения их готовности к операциям НАТО и ЕС, их оперативной совместимости (включая киберустойчивость) и их интеграции с силами передового базирования других стран НАТО / ЕС на ротационной основе, а также участие в любых экспедиционных силах или силах интервенции НАТО или ЕС.

Польша, Румыния и Болгария потенциально могли бы извлечь наибольшую пользу из эффективного и действенного перевооружения и нового уровня готовности и оперативной совместимости силовых структур в ЦВЕ. Это также было бы в целях как НАТО, так и ЕС, но, прежде всего, для сдерживания и защиты на Востоке и, возможно, на Юго-Востоке через настоящую федерацию с системами НАТО / ЕС. B9 обеспечивает прочную основу для развития PRI в качестве практического аспекта сотрудничества, как в контексте НАТО, так и в контексте ЕС при тесной поддержке Агентства связи

и информации НАТО по развитию возможностей C4ISR и предоставлению услуг.

С 2014 года болгарская сторона прилагает усилия для разработки Национальной программы под названием «Болгария в НАТО и европейской обороне» с упором на перевооружение. Сейчас она движется к реальным проектам, одобренными парламентом. Самая последняя из программ – «Видение 2030» – пользуется поддержкой гражданского населения и представляет собой всеобъемлющий и стратегический подход к перевооружению и тесному сотрудничеству с союзниками B9. С точки зрения Болгарии, включение Албании, Черногории и Северной Македонии имеет решающее значение, и в сотрудничестве с Грецией это изменит состояние обороны в регионе. Следующим шагом будет взаимодействие с Боснией и Герцеговиной, Косово и Сербией.

Будучи членами как НАТО, так и ЕС, страны B9 могут гармонизировать свои требования и использовать все доступные инструменты НАТО, ЕС и многонациональные / региональные инструменты для создания наилучших возможных C4ISR / кибер-способностей для своих вооруженных сил в контексте многонациональных силовых структур НАТО / ЕС. Помимо B9, участие стран Адриатики, таких как Албания, Хорватия, Черногория, Словения и Северная Македония (скоро станет 30-м членом НАТО), а также некоторых черноморских кандидатов на членство в НАТО / ЕС, таких как Украина и Грузия (и даже Молдова), может рассматриваться в рамках договоренностей о партнерстве.

В этом контексте программа «Готовность и оперативная совместимость» для стран *B9+* с участием ведущих боевых групп и / или сменных сил из других стран НАТО в регионе является логичным. Программа может поддерживаться NCIA в контексте решения «НАТО прежде всего» при финансировании со стороны клиентов (включая доступное *общее финансирование* из существующих и будущих *целевых фондов* C4). В прошлом и, безусловно, в будущем, основные усилия в рамках PRI будут включать в себя множество индивидуальных, но неотложных и связанных с операциями действий и запросов на учения, предполагающих быстрое реагирование.

NCIA провела исследование внешней (не финансируемой из общих источников) поддержки клиентов с *Промышленным консорциумом сетецентрических операций* (NCIOC), чтобы определить наиболее адекватную модель, основанную на лучших отраслевых практиках для решения этой проблемы. Это хорошая основа для оказания поддержки внешним клиентам в рамках PRI без вмешательства в общие финансируемые программы.

Очевидно, что область C4ISR / Кибер стимулирует инновации не только в области технологий, но и во всех других аспектах, включая бизнес-модели для сотрудничества и развитие необходимых институтов, чтобы сделать эти усилия успешными для всех. В этом контексте дискуссии о трансформации союзного командования НАТО (NCIOC-ACT) в плане внедрения проверки

оперативной совместимости до приобретения товаров и услуг создают дополнительные стимулы для PRI. В рамках *Инициативы по проверке функциональной совместимости* могут быть начаты новаторские проекты по разработке нового стандарта в практике закупок, который исследует функциональную совместимость на уровне организации для сетевой среды федеративных миссий. Ожидается, что это сэкономит миллиарды евро для НАТО, его членов и партнеров с очевидными преимуществами для стран В9+.

Итак, теперь есть возможность рассмотреть проекты и программы, связанные с C4ISR / Кибер в странах В9+ в контексте реализации ПДГ / ПП и Инициативы обеспечения готовности / Инициативы обеспечения оперативной совместимости, а также консолидировать работу в контексте НАТО / ЕС для экономии денег. Возможно, более важной будет способность достичь высокого уровня оперативной совместимости, безопасности и готовности систем C2 на восточном фланге с включением стран региона в ротацию войск с участием членов и стран-партнеров. Штаб-квартира НАТО, стратегическое командование, NCIA могут сыграть свою роль, но ответственность принадлежит странам В9 с привлечением промышленности и исследовательских институтов для трансформации PRI. Кроме того, PRI принесет пользу европейским оборонным разработкам.

С момента своего создания в 2012 году Агентство NCI, объединив пять различных агентств К&И НАТО, провозгласило инициативу для национальных главных директоров по информационным технологиям (CIO) вместе с представителями ACO, ACT и штаб-квартиры НАТО в NFS, исследовательскими учреждениями и промышленности, чтобы определить наиболее эффективный, действенный и устойчивый к кибер воздействию способ обеспечения взаимодействия и готовности в области К&И. Их, ставшие уже традиционными, ежегодные конференции ИТ-директоров[28] проложили путь к реализации решения «НАТО прежде всего» и достижению оперативной совместимости и готовности в безопасной среде быстрыми, простыми и доступными способами (НАТО R&I SAFE).

Определение PRI как результата обзора требований под руководством НАТО / ЕС с активным внедрением решений, совместимых с FMN в сотрудничестве с промышленностью и NCIA в качестве исполнительного / вспомогательного агентства, выведет практические аспекты оперативной совместимости и готовности на новый уровень в Центральной и Восточной Европе. PRI необходимо полностью синхронизировать со всеми учениями с участием сил в ЦВЕ, с операциями, миссиями, деятельностью и задачами НАТО / ЕС не только для постоянного улучшения оперативной совместимости и готовности, но и для того, чтобы они могли внести реальный вклад в сдерживание и оборону. Параллельно следует рассмотреть возможность

[28] Информацию о каждой из конференций серии «Конференции директоров по информационным технологиям» можно найти на сайте агентства NCI https://www.ncia.nato.int.

распространения PRI на все «новые» страны НАТО в ЦВЕ, а также определить партнеров PRI для поддержки работы с партнерами в ЦВЕ (включая Западные Балканы и регион Черного моря).

Концептуализация охвата и руководства / управления PRI может быть осуществлена в более широкой среде консультаций с представителями промышленности и НПО, но реальные шаги могут быть предприняты только странами или структурами ЕС, связанными с ACO / ACT. Конечно, существующие модели, реализованные для среды AMN / FMN как распределенная сеть боевых лабораторий (DNBL) в качестве инструмента для поддержки программы, также будут использоваться для формирования программы.

Образование и обучение как основные инструменты для достижения оперативной совместимости. Последствия для Западных Балкан и Черноморского региона

Когда речь идет о готовности и совместимости, особенно многонациональных образований, речь идет не только об оборудовании, но и о людях, их образовании и обучении. Это причина рассматривать сеть многонациональных формирований в ЦВЕ как инструмент для развития сотрудничества в области образования и обучения, сертификации и развития персонала. Очевидно, что для многонациональных формирований, в том числе на тактическом уровне (например, батальонные боевые группы, авиаэскадрильи, корабли, включенные в инициативу готовности), рабочим языком будет английский, процедуры будут базироваться на практике НАТО и для систем C2 потребуются решения «НАТО в первую очередь».

По этим причинам синхронизация программ обучения и подготовки офицеров, сержантов и даже солдат должна достигаться в соответствии со стандартами НАТО. Не менее важен опыт ротации в многонациональных подразделениях. Консорциум академий обороны и институтов по изучению вопросов безопасности «Партнерство ради мира» вместе с Программой повышения оборонного образования НАТО уже многое дает благодаря совместной работе над справочными учебными планами в различных областях.[29] Эти учебные программы сближают профессиональное военное образование союзников по НАТО и их партнеров, повышая уровень стандартизации, а также улучшая интеллектуальную совместимость. То же самое можно сказать и об усилиях Европейского колледжа безопасности и обороны, ко-

[29] См. “Generic Officer Professional Military Education – Reference Curriculum,” “Cybersecurity – A Generic Reference Curriculum,” and “Non-Commissioned Officer Professional Military Education – Reference Curriculum,” все доступны на вебсайте НАТО, https://www.nato.int.

торый является частью Европейской службы внешних связей. Он сосредоточил усилия на внедрении единых стандартов в образование и подготовку в рамках профессионального военного образования во всем ЕС.[30]

Хотя часто бывает важно различать образование и обучение, в этой статье высказывается мнение, что они являются взаимовключающими видами деятельности. Для полноценного развития военнослужащих необходимы образование и обучение, а также опыт. Оперативная совместимость как в образовании, так и в обучении – это критически важная дорога, позволяющая вооруженным силам нации соответствовать требованиям национальной безопасности и выполнять их в условиях международной безопасности, где решающее значение имеет тесное сотрудничество с союзниками и партнерами. Отсюда и предложение сконцентрировать дальнейшие усилия НАТО и ЕС на Западных Балканах и в Черноморском регионе для решения текущих проблем безопасности посредством академического диалога и взаимодействия в профессиональном военном образовании и обучении. Это обеспечит прочную основу для сдерживания и обороны и для проецирования стабильности в этих регионах.

Заключение: региональное сотрудничество (SEDM / A5 и B9): Возможна ли консолидация?

Анализ развития присутствия НАТО / ЕС в Центральной и Восточной Европе, особенно через многонациональные формирования – от KFOR до боевых групп eFP в странах Балтии и Польше, боевых групп ЕС (таких как HELBROC в Юго-Восточной Европе) на Первом уровне, за которым следуют штаб-квартиры уровня дивизии / корпуса и вплоть до NCS – обеспечивает исходные данные для определения требований к взаимодействующим системам C2 на тактическом уровне, напрямую связанных с оперативным / стратегическим уровнем и соответствующими требованиями к обучению персонала в этих многонациональных формированиях.

Еще более серьезной является задача определить дорожную карту для развития этих многонациональных формирований в Восточной Европе в рамках НАТО / ЕС с участием западноевропейских и североамериканских членов Атлантического альянса. Важно подчеркнуть, что многонациональность на тактическом уровне – в батальонах, эскадрильях и кораблях – это самое главное. Это потому, что речь идет о реальном использовании процедур НАТО на повседневной основе, системах C2 и демонстрации солидарности. Эти тактические подразделения, будучи многонациональными, будут моделью для национальных подразделений того же типа или размера, но, находясь под многонациональным управлением, системы C2 будет под-

[30] European Security and Defense College (ESDC), “Standard Curricula,” по состоянию на 29 октября 2018, https://eeas.europa.eu/topics/common-security-and-defense-policy-csdp/4369.

держивать готовность и оперативную совместимость, требуемые Инициативой готовности, и поэтому они будут иметь больше шансов быть привлеченными к участию в операциях без каких-либо оговорок.

Основываясь на большом пуле многонациональных тактических формирований, намного проще назначить многонациональные штаб-квартиры более высокого уровня для управления обучением и подготовкой, а также для планирования и C2 в случае активации. Такие организации будут содействовать многонациональным проектам по оперативно совместимым системам C4ISR и другому оборудованию и / или вооружениям. Эти многонациональные проекты могли бы управляться расширенными национальными агентствами, но, возможно, даже лучший вариант – использовать NCIA / NSPA.

И последнее, но не менее важное – это организация образования и обучения, охватывающая все аспекты от индивидуального до коллективного и от полевого обучения до компьютерных учений.

Основной посыл этой статьи заключается в том, что если НАТО хочет достичь зрелости путем консолидации существующих структур многонациональных формирований и разработки дорожной карты для ее дальнейшего развития в ЦВЕ / ЮВЕ с особым акцентом на многонациональные проекты C4ISR и совместное обучение и подготовку, ориентированные на оперативную совместимость и готовность, ландшафт безопасности и обороны может быть резко изменен. В регионе могут произойти настоящие преобразования в сфере обороны, и в результате общая устойчивость будет повышена.

Необходимы дальнейшие исследования для разработки бизнес-обоснования Программы готовности и взаимодействия, для определения модели руководства и управления программой, технологических дорожных карт и конкретных требований к образованию и обучению (включая учения), а также для реализации передового присутствия в ЦВЕ / ЮВЕ, что будет способствовать сотрудничеству между НАТО и ЕС и региональному сотрудничеству.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами авторов и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторах

После 19 лет службы в армии доктор Велизар **Шаламанов** начал научную карьеру в Академии наук, а также несколько раз работал на государственных должностях: заместитель министра обороны (1998-2001 гг.), министр обороны (2014 г.) и директор по менеджменту спроса в Агентстве кибер и информационных технологий НАТО (2009-2017). В настоящее время он занимается консолидацией академического кибер потенциала Болгарии. Параллельно он участвует в политике и в работе неправительственных организаций, стремящихся к улучшению позиции Болгарии в НАТО и в европейской обороне, в информационном обществе и к улучшению управления научными исследованиями. *E-mail*: shalamanov@acad.bg.

Г-н Павел **Анастасов** возглавлял Отдел стратегической политики и анализа Кабинета Президента Республики Болгария в период 2012-2014 гг. В 2014 году он занимал должность заместителя министра обороны. В период с 2014 по 2018 год он работал над вопросами безопасности Черного моря в отделе по политическим вопросам и политике безопасности в штаб-квартире НАТО.

Д-р Георгий **Цветков** – доцент в Национальной военной академии «Г. С. Раковски» в Софии, занимается различными темами в области управления обороной, развития способностей и политики безопасности.

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Рослав Ежевский, *Connections QJ* 18, № 1-2 (2019): 51-71
https://doi.org/10.11610/Connections.rus.18.1-2.03

Рецензированная статья

Междоменное принуждение как попытка России ослабить восточный фланг НАТО: тематическое исследование случая Латвии

Рослав Ежевский

Резюме: Междоменное принуждение ощутимо на восточном фланге НАТО и характеризуется использованием уничижительной пропаганды, фейковых новостей, финансовых активов в латвийской банковской системе, русской организованной преступности и различных военных элементов. Однако это исследование междоменного принуждения направлено на изучение сплоченности латвийского населения, существующих разрывов в обществе и его подверженности использованию со стороны России. Чтобы получить данные для этого исследования, автор провел интервью с представителями стран восточного фланга и сделал обширный обзор литературы. Для определения первопричин вертикального разделения общества был использован метод «5 ПОЧЕМУ». Это исследование доказало, что присутствие русского меньшинства и организованной преступности среди русского меньшинства может быть хорошей базой для создания беспорядков, и что Россия способна влиять на внутреннюю политику страны, когда экономическое воздействие России превышает 12 % ВВП. Демография и сплоченность (включая вертикальное и горизонтальное деление) общества являются факторами, определяющими противодействие Латвии. Триумф популистских партий на парламентских выборах в октябре 2018 года отражает скорее то, что нация устала от коррумпированного и неэффективного правительства, а не то, что население улучшает свое отношение к России. В более общем плане ожидается, что междоменное принуждение усилится, и Россия начнет испытывать сплоченность НАТО.

Ключевые слова: НАТО, Восточный фланг, Латвия, междоменное принуждение, Россия, организованная преступность, экономическое воздействие, противодействие Латвии, коррупция.

Введение

Владимир Путин сказал, что хотел бы, чтобы Советский Союз не распадался; для него и многих россиян это была геополитическая катастрофа, которая оторвала Восточную Европу от российской гегемонии.[1] Тот факт, что страны Балтии и большая часть бывшей советской зоны влияния теперь являются частью НАТО, приводит Россию в ярость. Кремль засыпает их фейковыми новостями и обвинениями в фашизме и нацизме, надеясь найти слабое место в структуре Альянса. Восточный фланг НАТО неоднороден, особенно если речь идет о странах Балтии. Вопрос в том, какая из трех стран Балтии наиболее уязвима?

Краткий количественный анализ нескольких показателей помогает найти ответ. В Европейском индексе качества государственного управления за 2017 год Эстония занимает 90-е место (оценка: 54,4 балла), Литва – 114-е место (оценка: 43,6 балла), а Латвия – 142-е место с оценкой 38,2 балла. Другим показателем может быть Индекс человеческого развития, где опять же лучшее место среди стран Балтии занимает Эстония (30-е место с результатом 0,871), затем Литва (35-е место с результатом 0,858) и снова Латвия на последнем месте, занимая 41-е место с результатом 0,847. Такая же последовательность наблюдалась в двух других индексах: Индекс социальной справедливости на 2016 год (Эстония: 6,15, Литва: 5,69 и Латвия: 5,04) и Индекс социальной сплоченности (Эстония: 5,85, затем Литва: 5,69 и, наконец, Латвия: 5,10). Существуют также качественные показатели, которые дают основание присвоить Латвии самый низкий рейтинг, поскольку 26 % населения Латвии составляют этнические русские, есть много неграждан, общество обеспокоено и все еще восстанавливается после финансового кризиса 2008 года. Это делает Латвию особенно уязвимой для войны нового поколения и междоменного принуждения, что является вызовом безопасности стран Балтии.

Россия очень недовольна членством Латвии в НАТО и будет пытаться любыми способами ниже порога войны как подорвать стабильность страны, так и повлиять на сплоченность ее населения, надеясь также ослабить единство НАТО. В Концепции национальной безопасности[2] Министерства обороны Латвии говорится, что в этом стремлении Россия будет действовать во всех доступных доменах, в частности в социальном, экономическом и военном.

---

1 Adam Taylor, “Putin Says He Wishes the Soviet Union Had Not Collapsed. Many Russians Agree,” *The Washington Post*, March 3, 2018, www.washingtonpost.com/news/worldviews/wp/2018/03/03/putin-says-he-wishes-he-could-change-the-collapse-of-the-soviet-union-many-russians-agree.

2 «Концепция национальной безопасности (информационная часть)» была опубликована в 2014. Подробности о возможной российской линии действий можно найти на страницах: 4 (гибридные действия), 15 (угрозы единству общества) и 18 (пропаганда), www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.

Есть несколько примеров российского принуждения в двусторонних отношениях с Латвией[3]: уничижительная активная пропаганда со стороны спонсируемых Россией средств массовой информации, российские учения с боевыми стрельбами в исключительной экономической зоне Латвии в апреле этого года и деятельность русской организованной преступности. Этому трудно противодействовать обычными средствами, поскольку концепция ведения конфликта на низком уровне дает России преимущество перед формализованной системой реагирования, особенно когда речь идет о сценариях, попадающих под статью 5 для стран НАТО.[4]

Применение средств войны нового поколения против Латвии вряд ли приведет к какой-либо форме конвенциональной войны. Россия использует тактику рейдов, которая особенно выгодна и эффективна в противостоянии с более сильным противником.[5] Это дешевая и эффективная форма войны; она охватывает множество областей (кибер, информационную, финансовую), включает инфильтрацию и внезапную атаку, использование маневрирования и помогает достичь желаемого политического результата.[6] Исследование литературы,[7] проведенное для этой статьи, приводит к выводу, что такая тактика может быть успешной в использовании различных уязвимостей, которые существуют или будут существовать в латвийском обществе, подрывая доверие к правительству, и таким образом, ослабляя сплоченность общества.

Во-первых, в Латвии самое большое количество этнических русских в Европе (почти 26 %). Многие из этих людей не являются гражданами, лишены права голоса и не могут владеть землей или имуществом. Это делает их мишенью для российских психологических операций, на первом месте среди которых стоит российская пропаганда, пытающаяся убедить русских экспатриотов в том, что Латвия – такой плохой союзник Запада и не защищает

---

[3] И в Эстонии. Относительно подробностей смотри: Rachel Marie Casselman, "Russia's Hybrid Warfare: The Prowess and Limitations of Putin's (in)Visible Hand in Estonia and Latvia," Master of Arts Thesis (University of Oregon, June 2017), https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/22759/Casselman_oregon_0171N_11972.pdf.

[4] Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," *Proliferation Papers* 54 (French Institute of International Relations, November 2015), 39, https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

[5] Michael Kofman, "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," *War on the Rocks*, June 14, 2018, https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition.

[6] Kofman, "Raiding and International Brigandry."

[7] Тема уязвимостей в качестве мишеней для России отражена в работах: Janis Berzins, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," *Policy Paper* no. 2 (Riga: National Defence Academy of Latvia, April 2014), 12, https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf; "The National Security Concept;" James K. Wither, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87.

их права. Во-вторых, есть свидетельства того, что в латвийском обществе действует организованная преступность из России. Преступные группировки подозреваются в отмывании денег и тесном сотрудничестве с Кремлем во время тайных операций против латвийского общества и правительства (например, участие в разведывательных операциях). Масштабы и охват этого фактора публично не разглашаются, но имеющиеся данные показывают, что несмотря на то, что он почти не попадает в поле зрения, он оказал сильное влияние на латвийскую систему безопасности. В-третьих, у страны есть серьезная социальная проблема, которая представляет собой смесь неравенства доходов, старения населения (из-за низкого уровня рождаемости) и эмиграции.

В этом качественном исследовании будут изучены такие вопросы, как: является ли присутствие русского меньшинства в Латвии угрозой единству страны? Какое влияние оказывает организованная преступность из России на стабильность Латвии? Каков характер враждебных действий России против Латвии? Какие возможные контрмеры можно использовать против этих факторов? Чтобы найти ответы на эти вопросы, необходимо начать с исследования населения Латвии, без которого было бы трудно определить, какие разрывы и уязвимости могут существовать в населении и насколько сплоченным является это население. Следующим шагом будет оценка восприимчивости латвийского населения к эксплуатации со стороны российской пропаганды и отношение русского меньшинства, включая восприятие угрозы латышами и этническими русскими. Автор также намерен выяснить, насколько глубоко организованная преступность из России (ОПР) проникла в русское меньшинство и каковы отношения между ОПР и другими злонамеренными акторами.

Наконец, автор выскажет некоторые предположения, когда и может ли Россия нарушить жизненное пространство Латвии, применяя междоменное принуждение, и подведет итоги исследования. Данные для этого исследования будут взяты из интервью с латвийским (PASS 18-16, персонал SHAPE NMR, члены аналитических центров) и польским (члены аналитического центра) персоналом, сопровождаемые обширным исследованием литературных источников. Подходом к решению этой проблемы будет анализ основных причин (АОП) для выбранного фактора с целью определить его влияние на жизненное пространство Латвии.

Обследование населения Латвии

Население Латвии – одно из самых малочисленных в Европе. В настоящее время оно оценивается примерно в 1 950 000 человек, из которых немногим более одного миллиона являются экономически активными.[8] Из этнических групп в стране 62 % составляют латыши, а крупнейшее меньшинство в Латвии – русские (25,4 %), большинство из которых проживает в Латгальском

[8] *Latvia: Executive Summary* (Englewood, CO: IHS Markit, 2018), 40.

районе на востоке страны. Многие источники упоминают, что у Латвии были давние проблемы, связанные с присутствием русской диаспоры, что является результатом предыдущей советской оккупации. Необходимо отметить, что коренные латыши считают, что в стране есть две основные группы – говорящие на латышском языке и не говорящие на латышском языке. Именно во второй группе можно встретить русскоязычных (в том числе этнических русских, белорусов и др.).[9]

Среди русского меньшинства есть неграждане (примерно 242 000), которые имеют относительно низкий статус в обществе из-за невозможности получить хорошую работу, плохого владения латышским языком и проблемной экономики в Латгальском районе. Большинство доступных им рабочих мест – в транспортном секторе или на строительных площадках. Латвия переживает серьезный демографический спад; прогноз на 2060 год предполагает, что население составит около 1 200 000 человек по сравнению с 1 950 000 в настоящее время. Кроме того, прогнозируется, что к 2030 году половине латвийцев будет больше 50 лет. Еще одной движущей силой спада численности населения, а также старения является эмиграция. Многие мигранты моложе 30 лет,[10] и по оценкам, интенсивная эмиграция будет продолжаться как минимум до 2030 года.[11]

Это серьезная демографическая проблема,[12] которая очень негативно сказывается на системе безопасности. Если эти факторы сложить вместе с небольшой плотностью населения (4 человека/кв. км), весьма вероятно, что некоторые районы страны в конечном итоге станут безлюдными, что создаст условия отсутствия ограничений, в которых могут действовать возможные противники, если они появятся. Веб-страница *www.globalfirepowerindex* определяет это как первостепенную проблему для обороны: «Выходя за рамки общего количества военной техники и предполагаемой боевой мощи – это фактическая численность личного состава делает данную военную силу. Войны, особенно с высоким уровнем потерь, традиционно благоприятствуют тем, у кого больше живой силы».[13] В случае с Латвией, вооруженные формирования отражают внутреннюю структуру этнического разнообразия: Латвийская национальная гвардия в основном говорит по-ла-

---

9 Интервью с латвийским военнослужащим, 8 октября 2018.

10 BMI сообщает, что количество эмигрантов, планирующих вернуться в Латвию в ближайшее время, упадет с 10 % до всего 3 %. В более долгосрочной перспективе демографические проблемы Латвии нанесут серьезный удар по экономике. Дополнительная информация в *Latvia Country Risk Report – Q3 2018* (London, United Kingdom: Business Monitor International, 2018).

11 *Latvia Country Risk Report,* 20.

12 *Latvia: Executive Summary*, 40.

13 "Latvia Military Strength," *GlobalFirepower.com*, https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=latvia.

тышски, армия в основном русскоязычная, полиция – наполовину латышская, наполовину русская, а пограничная охрана в Латгалии в основном русскоговорящая.[14]

Эти выводы относительно сплоченности населения Латвии различаются, особенно при сравнении литературного исследования с частными интервью. Картина населения, представленная во время одного частного интервью в сентябре, заключалась в том, что нация сильна и сплочена, и это не согласуется с уничижительными посланиями ее большого соседа.[15] Другой латвийский чиновник [16] заявил, что народ довольно сплочен и устал от правительственных скандалов и коррупции; сплоченность присутствует в сельской местности, где латыши и русские сосуществуют в компактных сообществах, но общество поляризовано в больших городах, особенно в Риге и Даугавпилсе.

Однако есть и доклад, в котором общество описывается как разделенное, и что люди в латвийском обществе не являются ни социально, ни политически активными,[17] и что население серьезно не доверяет правительству.[18] В этом же документе утверждается, что участие общества в общественных делах низкое.[19] Еще один краткий обзор сплоченности Латвии взят из Индекса социальной справедливости [20] ЕС за 2017 год, в котором говорится, что Латвия достигла 19-го места среди 28 других членов ЕС (последнее среди стран Балтии) с оценкой 5,46 по шкале социальной справедливости. Система образования была особенно хорошо оценена, но было отмечено, что существует разрыв между городом и деревней, в то время как возможности получения образования для людей с особыми потребностями ограничены».[21]

Несмотря на положительные тенденции, экономика имеет значительные уязвимости, в том числе то, что это небольшая и открытая система, зависящая от мировых тенденций. Бизнес и развитие обычно ассоциируются с Ригой, в то время как остальная часть страны не развита. По этой причине около 30 % коренных латышей заявили о своей готовности покинуть страну.

---

[14] Интервью с латвийским государственным служащим, 8 октября 2018 г.

[15] Интервью с латвийским военнослужащим, 12 сентября 2018 г.

[16] Интервью с латвийским государственным служащим, 8 октября 2018 г.

[17] Ieva Bērziņa, Janis Berzins, Martins Hirss, Toms Rostoks, and Nora Vanaga, *The Possibility of Societal Destabilization in Latvia: Potential National Security Threats* (Riga: National Defence Academy, Center for Security and Strategic Research, 2018), 14, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/WP%2004-2016-eng.ashx.

[18] Bērziņa, *et al.*, *The Possibility of Societal Destabilization in Latvia*, 5.

[19] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 14.

[20] Daniel Schraad-Tischler, Christof Schiller, Sascha Matthias Heller, and Nina Siemer, *Social Justice in the EU – Index Report 2017* (Gütersloh: Bertelsmann Stiftung, 2017), 49, https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/Graue Publikationen/NW_EU_Social_Justice_Index_2017.pdf.

[21] Schraad-Tischler, et al., *Social Justice in the EU*, 115.

Существует значительная разница в уровне безработицы: лучшая ситуация в Риге, а худшая – в Латгальском регионе. Структура государственных организаций устарела и не обеспечивает надлежащих услуг для быстро сокращающегося населения. Пенсии настолько низкие, что люди попадают в нищету. В результате, доля старшего поколения, подвергающегося риску социальной изоляции, выросла с 33 % в 2011 году до 43,1 % в 2018.[22] Эти факторы влияют на сплоченность латвийского общества. Но есть и дополнительная внутренняя проблема – отношение русского меньшинства.

Отношение русского меньшинства к Латвии

Первые впечатления от исследования литературы позволяют сделать вывод, что угроза со стороны русского меньшинства невысока,[23] поскольку около 80 % русскоязычных заявляют о своей лояльности к нации.[24] Диаспора достаточно интегрирована в общество, хотя есть некоторое недовольство любым активным участием в систему обороны.[25] Существует также общее мнение, что предстоящая языковая реформа принесет много проблем, и это может вызвать чувство дискриминации.[26] Вероятно, поэтому эти люди не хотят участвовать в публичных протестах. Половина этих неграждан не поддерживает российские счета,[27] а старшее поколение выражает наибольшую лояльность [28] к Латвии; они хотят наслаждаться жизнью в Латвии и предпочитают ее России. Однако большинство из них заявляют, что не планируют получать латвийское гражданство по причинам: проблемы с общением на латышском языке, легкость поездки в Россию (визы не требуются) и, частично, планы на получение русского гражданства.

Другие интервью с представителями Латвии дали более подробную информацию. Один из них выразил довольно негативные чувства по отношению к негражданам, заявив, что их существование является реальной проблемой для его страны. По его словам, эти люди любят Россию, но живут в Латвии; некоторые из них имеют проблемы с алкоголем и наркотиками, особенно молодое поколение (неграждан); старшее поколение обвиняет латвийское население в нацизме. Но в этом разговоре были и положитель-

---

[22] Schraad-Tischler, et al., *Social Justice in the EU*, 12.

[23] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 13.

[24] Aleksandra Kuczyńska-Zonik, “Non-Citizens in Latvia: Is it a Real Problem?” *Sprawy Narodowościowe Seria nowa* (*Nationalities Affairs New series*) 49 (2017), Article 1438, https://doi.org/10.11649/sn.1438.

[25] James K. Wither, “‘Modern Guerrillas’ and the Defense of the Baltic States,” *Small Wars Journal*, January 13, 2018, http://smallwarsjournal.com/jrnl/art/modern-guerrillas-and-defense-baltic-states.

[26] *Latvia: Executive Summary*, 21.

[27] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 10.

[28] Kuczyńska-Zonik, “Non-Citizens in Latvia: Is it a Real Problem?” 8.

ные моменты – говорилось, что многое зависит от родителей молодых неграждан. Есть те, кто пытается выучить латышский язык и интегрироваться в общество. Другой представитель[29] латвийского населения заявил, что те неграждане, которые хотели эмигрировать в Россию, уже эмигрировали, и теперь большинство из них не планирует эмигрировать. У пожилых людей есть какие-то чувства к России, но только из-за их национальности. Они определенно не хотят эмигрировать, особенно в Россию, так как получают информацию от подрастающего поколения о реальных условиях жизни в России и Латвии. Они частично находятся под влиянием российской пропаганды, особенно в восточной части страны, и, имея безвизовый режим, любят ездить в Россию.

Но есть и неграждане, которые действуют против Латвии, и это создает проблемы для национальной безопасности учитывая, что Кремль может использовать их в качестве инструмента. Первый предупреждающий сигнал исходит от Центра передового опыта НАТО, который показывает, что Россия рассматривается как надежный источник информации для меньшинств в странах Балтии.[30] Версии документа, разработанного Латвийской полицией безопасности, рисуют более ясную картину. В этом отчете за 2017 год[31] утверждается, что есть российские соотечественники, которые были вовлечены в российскую кампанию дезинформации, мишенью которой была Латвия, а внутренние проблемы страны были преувеличены.[32] Вероятно, эту часть русского меньшинства можно будет снова использовать, если Россия захочет повлиять на внутреннюю ситуацию в Латвии.[33] До сих пор было несколько случаев, когда некоторые активисты настолько размахнулись в своей уничижительной деятельности, разжигающей ненависть и нетерпимость, что Латвийской полиции безопасности пришлось вмешаться и предупредить их о последствиях любого дальнейшего поведения такого рода.[34] Одним из инструментов подстрекательства может быть организованная преступность (ОПР), проникшая в российскую диаспору. Она напрямую связана с Кремлем, откуда получает поддержку и указания относительно того, как использовать политическое влияние и быть инструментом государственного влияния за рубежом.[35]

---

[29] Интервью с латвийским государственным служащим, 8 октября 2018 г..

[30] Ieva Bērziņa, Māris Cepurītis, Diana Kaljula, and Ivo Jurvee, *Russia's Footprint in the Nordic–Baltic Information Environment*, Report 2016/2017 (Riga: NATO Strategic Communications Centre of Excellence, 2018), 102, www.stratcomcoe.org/russias-footprint-nordic-baltic-information-environment-0.

[31] *Public Report on the Activities of Latvian Security Police in 2017* (Riga: Latvian State Security Service, 2018), 19, URL: https://vdd.gov.lv/en/useful/annual-reports.

[32] "Public report on the activities of Latvian Security Police," 19.

[33] "Public report on the activities of Latvian Security Police," 20.

[34] "Public report on the activities of Latvian Security Police," 15.

[35] Рига считается одним из криминальных центров, специализирующихся на отмывании денег. Смотри Mark Galeotti, "Crimintern: How the Kremlin Uses Russia's

Дальнейшие исследования восприятия угроз безопасности Латвии принесли неожиданные результаты. Для латгальцев Россия – одна из наименьших проблем, что заставляет задуматься, учитывая расположение района. 78 % людей, говорящих на латгальском диалекте, заявляют, что поддерживают Латвию, когда речь идет о российской агрессии. Они заявляют, что готовы бороться за свободу Латвии, если это необходимо.[36] Но для населения Латвии самая большая угроза – это не Россия, а тревожная внутренняя ситуация (низкая заработная плата, плохая демографическая ситуация, неэффективная система здравоохранения, коррупция и преступность).

Что касается опрошенных, то все они считали Россию угрозой.[37] Они также выразили мнение, что Россия может напасть на их страну без предупреждения. Это подтверждается текстами в «Концепции национальной безопасности» Латвии, где Россия признана главной угрозой национальной безопасности Латвии. В других декларациях документа указывается, что Россия реализует свою внешнюю политику, используя комплексные меры, так называемые гибридные угрозы, которые направлены на постепенное ослабление стран, на которые они нацелены.

Основываясь на этих выводах, можно предположить, что русская диаспора в Латвии неоднородна, у нее разные мнения по отношению к правительству и разные взгляды на угрозу со стороны России. Поэтому эта тема определенно требует дальнейших исследований и интервью, поскольку нынешние позиции неграждан и их российских соотечественников плохо отражены в литературе. Это также относится к присутствию организованной преступности, базирующейся в России, которая проникла в русское меньшинство в Латвии.

Влияние организованной преступности в России на Латвию

Происхождение российских структур организованной преступности (ОПР) в Латвии уходит корнями в советские времена, когда многие преступники, которые были освобождены из тюрем, решили переехать в Латвию и начать там новую жизнь.[38] В этом контексте термин «новая» означает преступная, поскольку эти люди сохранили свои наклонности и связи с преступным миром, чтобы использовать их на своей новой родине. По мере роста сотрудничества с Россией в Латвии росла и преступность в сфере незаконного оборота наркотиков, угонов автомобилей, отмывания денег и контрабанды

Criminal Networks in Europe," European Council on Foreign Relations, April 18, 2017), https://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

[36] Интервью с латвийским госслужащим, 8 октября 2018.

[37] Следуя этим заявлениям, Россия и Беларусь должны восприниматься как угроза в паре, в которой Беларусь может выступать в роли прокси-заместителя.

[38] Walter Kegö, et al., *Russian Organized Crime: Recent Trends in the Baltic Sea Region* (Washington, D.C.: Institute for Security and Development Policy, 2012), 69, http://isdp.eu/publication/russian-organized-crime-recent-trends-baltic-sea-region.

топлива. Например, в 2012 году было подсчитано, что 30% потребления топлива в Латвии приходится на контрабандные поставки.

Джон Рюль утверждает, что Россия, несмотря на свою слабость, все же может использовать принуждение в отношениях с многими странами, в том числе с США. В российский инструментарий входит использование меньшинств, кибер и информационных операций, природных ресурсов и ОПР. Такое развитие стало возможным потому что, как указывает автор, между Кремлем и ОПР было достигнуто соглашение о взаимной поддержке, которое привело к созданию мафиозных структур и сетей коррупции в Европе, что позволило России создавать зоны влияния.[39] Это делает ОПР прокси-представителем российских интересов, который может продвигать российскую повестку дня везде, где это возможно.[40] Дальнейшее исследование деятельности ОПР в Латвии показало, что, когда экономический след России в стране превышает 12 % ВВП, это создает условия, позволяющие ОПР использовать экономические каналы.[41] Поскольку между Латвией и Россией существует тесное экономическое сотрудничество, между латвийскими и российскими бизнесменами было налажено множество связей, в основе которых лежат поддерживаемые Россией преступные элементы.[42]

У ОПР также есть второе лицо, связанное с российскими спецслужбами и управляемое ими. Кремль использовал его как канал для разведки и политического влияния,[43] и это становится реальной проблемой, в то время как попытки России подорвать единство Запада продолжаются. Русские преступные группы, которые находятся на территории Латвии, используются российскими службами безопасности для сбора информации о приграничной территории (Латгалия), объектах безопасности и личных данных известных лиц.[44]

Информация о российской организованной преступности в Латвии ограничена. Однако здесь необходимо учитывать несколько аспектов. Краткий обзор ее деятельности в Латвии позволяет сделать вывод, что ОПР проникла в русскую диаспору и хорошо осведомлена о местных криминальных

---

[39] John Ruehl, "How Is Russia so Dangerous with an Economy Smaller than Italy's?" *PoliticsMeansPolitics.com*, April 21, 2018, 6, https://vip.politicsmeanspolitics.com/2018/04/21/how-is-russia-so-dangerous-with-an-economy-smaller-than-italys.

[40] Ruehl, "How Is Russia so Dangerous with an Economy," 6.

[41] Heather A. Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov*, The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Center for Strategic and International Studies, October 13, 2016), 18, https://www.csis.org/analysis/kremlin-playbook.

[42] Conley, et al., *The Kremlin Playbook*, 48.

[43] Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services* (European Council on Foreign Relations, 2016), 4, https://ecfr.eu/publication/putins_hydra_inside_russias_intelligence_services/.

[44] "Public Report on the Activities of Latvian Security Police," 9.

структурах. Между элементами ОПР и российскими спецслужбами существует тесное сотрудничество, в том числе по киберпреступности. И ОПР следует за экономическим участием России. Это означает, что у этого теневого элемента есть значительный потенциал для работы внутри Латвии, вероятно, следуя инструкциям Кремля. В условиях низкой социальной активности в латвийском обществе, это создает благоприятные условия для легкого использования латвийского общества в качестве оружия, например, за счет использования латвийских преступных групп (сотрудничество с ОПР).

Как Россия «использует в качестве оружия» латвийское общество

Использование идентичности в качестве оружия, которое здесь понимается как натравливание русского меньшинства против правительства и государства Латвии, нашло отражение во многих публикациях. На этом этапе неплохо было бы начать с заявления в «Концепции национальной безопасности»[45] (вероятно, в отношении России), в котором говорится о «попытках отдельных стран повлиять на единство латвийского общества». Кроме того, Янис Берзиньш утверждает, что Россия может использовать языковую реформу для создания разногласий между населением Латвии и национальными институтами.[46]

В ходе использования в качестве оружия, Россия использует стратегию рейдерства, которая является недорогим средством ведения войны.[47] Когда возникает ситуация, когда традиционные (обычные) методы слишком дороги, рейдерство является простым и эффективным; в информационной сфере оно дает перспективу для достижения желаемого эффекта – принуждения врага.[48] Как и при любой агрессии, злоумышленник нацелен на центр тяжести противника и, в случае Латвии, это, вероятно, общественное восприятие.

Мириады уничижительных посланий, пронизывающих латвийское информационное пространство, были отправлены, чтобы попытаться создать позитивную картину России в глазах русского меньшинства в Латвии и подорвать доверие к латвийскому правительству. Хотя есть передачи о музыке и культуре, между ними также есть фейковые новости и ложь (например, о том, что Латвия никогда не была оккупирована Россией). Российские СМИ легко использует латвийскую информационную сферу, в которой размещаются средства массовой информации как на русском, так и на латышском языках. Телевидение, радио, фермы троллей, а также троллинг роботы проецируют мягкую силу России в социальных сетях, а также опровергают

---

[45] *The National Security Concept (informative Section)* (Riga: Ministry of Defense, 2018), 1, https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.

[46] Berzins, “Russia’s New Generation Warfare in Ukraine,” 12.

[47] Kofman, “Raiding and International Brigandry,” 1.

[48] Kofman, “Raiding and International Brigandry,” 4.

сообщения других участников конкурентной борьбы. Россия играет на национальных чувствах русского меньшинства, чтобы влиять на внутреннюю политику соседних стран, даже используя этих людей как средство реализации внешней политики. Вероятно, наиболее точное описание этого дается Центром передового опыта в области стратегических коммуникаций (СОЕ) НАТО, в котором говорится, что «нарушение прав человека российских соотечественников за рубежом может использоваться как оправдание для нарушения суверенитета, как было во время войны с Грузией и кризиса на востоке Украины».[49] Можно предположить, что, если Россия решит спроецировать нестабильность, русское меньшинство станет инструментом.

На опасность, связанную с этой деятельностью, указывает Бюро защиты конституции, которое в 2016 году сообщило, что «влияние России на информационную среду Латвии по-прежнему представляет собой одну из самых важных долгосрочных угроз безопасности латвийского государства». Это вещание используется для эксплуатации многих проблем, существующих в обществе, таких как экономическое разнообразие, вертикальное разделение нации и неравенство доходов. Россия будет использовать их всех и использовать любой предлог, соответствующий ее целям. В этом потоке сообщений Россия представляет себя защитником старых привязанностей, критикуя НАТО и политику в отношении латышского языка и повторяя свои предложения о гражданстве и пенсиях для соотечественников. Он нацелен прежде всего на ту часть населения, которая потребляет только русскоязычные СМИ, и в 2015 году опрос СМИ подтвердил, что «46 % русскоязычных не получают никакой информации из латышских языковых СМИ, примерно пятая часть латвийского общества не может быть охвачена средствами массовой информации на государственном языке».[50]

Легкий доступ к латвийскому медиа-пространству не гарантирует России победы в этой информационной войне. Отчет об опросе, проведенном Центром передового опыта НАТО, ясно показывает, что усилия России не так эффективны, как планировалось, поскольку «национальные СМИ в исследуемых странах воспринимаются как более надежный источник информации, чем российские медиа порталы».[51] Например, 54 % респондентов общественного опроса 2017 года полностью не согласны с утверждением: «Русскоязычные люди в Латвии подвергаются дискриминации».[52] В другом примере 45% полностью не согласны с утверждением, что «НАТО является угрозой для России».[53] Это предполагает, что аудитория оценивает российское вещание, сравнивая его с другими источниками.[54]

---

[49] Bērziņa, et al., *Russia's Footprint in the Nordic-Baltic Information Environment*, 32.

[50] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 17.

[51] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 90.

[52] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 98.

[53] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 100.

[54] Bērziņa, et al., *The Possibility of Societal Destabilization in Latvia*, 100.

Вепонизация латвийского общества не ограничивается только информационной сферой. Россия ищет страны или регионы с плохим управлением, чтобы получить возможность оказывать на них влияние с помощью коррупции.[55] Этот процесс находится в авангарде так называемой войны нового поколения, целью которой является влияние на систему путем проникновения в нее и ослабления изнутри.[56] Оказавшись внутри, Россия проникает в страну через налаженные экономические связи и пытается захватить государство и изменить национальные решения.[57] В мае 2018 года Reuters разместила на своем веб-сайте статью о деньгах, предположительно российских, которые хранились в банковской системе Латвии и использовались для вмешательства во внутренние дела европейских стран.[58] Агентство заявило, что эти финансовые активы были доставлены из России и использовались для финансирования гибридной деятельности и подрыва политических систем в других странах. Еще один пример этих попыток со стороны России был дан в июле 2018 года агентством Bloomberg,[59] которое сообщило о предполагаемых финансовых переводов из России в период с 2010 по 2014 год, а также о значительном притоке российских депозитов в Латвию, начиная с 2012 года, для которых подозревается, что используются для организованной преступности и коррупции.

Пример из Финляндии показывает путь финансового принуждения, который приводит к тревожным выводам. В сентябре 2018 года на юго-западе Финляндии прошла массовая операция, когда спецслужбы обнаружили наличие российского заговора. Этнические русские (некоторые с двойным гражданством) покупали или строили дорогие дома в непосредственной близости от жизненно важных путей сообщения и охранных сооружений. Они также покупали списанные военные скоростные катера и хранили огромные суммы денег.[60] По некоторым данным, между Финляндией и Латвией совершались частые полеты на вертолете. В настоящее время в Финляндии ведутся дискуссии о введении сильных финансовых мер противодействия, которые уменьшат возможность покупки иностранцами земли или недвижимости в Финляндии. Аналогичные меры могут быть введены и

---

[55] Conley, et al., *The Kremlin Playbook*, X.

[56] Conley, et al., *The Kremlin Playbook*, X.

[57] Conley, et al., *The Kremlin Playbook*, X.

[58] В настоящее время по этим вопросам проводится расследование. О деталях смотри: John O'Donnell and Gederts Gelzis, "Exclusive: Latvia Probes Whether Russian Money Flows Used to Meddle in Europe," *Reuters*, May 29, 2018, https://fr.reuters.com/article/us-latvia-banks-politics-exclusive-idUSKCN1IU2BM.

[59] Aaron Eglitis and Alessandro Speciale, "Latvia's Corruption Scandal Is Getting Even Weirder," *Bloomberg*, July 13, 2018 https://www.bloomberg.com/news/articles/2018-07-13/latvia-s-corruption-scandal-is-getting-even-weirder-quicktake.

[60] Antoni Rybczyński, "'Zielone ludziki' na Bałtyku? Spektakularna Akcja Fińskich Służb," *TVP Info*, October 1, 2018, https://www.tvp.info/39269003/swiat/zielone-ludziki-na-baltyku-spektakularna-akcja-finskich-sluzb/.

в Латвии, где теперь можно получить 5-летнее постоянное место жительства, выполнив одно из трех условий: покупка недвижимости, инвестирование или открытие банковского счета.[61]

Также необходимо обратить особое внимание на русскую индоктринацию молодежи, которая проходит за пределами Латвии в форме военизированных лагерей.[62] В этих местах молодые умы, как говорят, заражаются фальшивой историей, например, о советской победе во Второй мировой войне. Эти российские инвестиции в молодое поколение могут привести к появлению группы пророссийских лидеров, которые однажды могут попытаться начать формировать внутреннюю политику Латвии. Объявленное 26 июля 2018 года решение президента Путина об ограничении поддержки соотечественников в Латвии может показаться немного спорным и может быть сигналом об отступлении России. Но это может быть только временный и рациональный шаг, возможно, из-за других сфер интересов (Украина, Сирия). Путин может в любой момент активизировать пророссийские настроения. Нападения на табуированные области, такие как язык, история и интеграция, могут создать горизонтальное разделение, которое внутренне ослабит страну.

В ответ Латвия стремится объединить нацию в единое сплоченное общество, которое сможет дать отпор любым враждебным действиям. Официально прозвучал призыв к выполнению «обязанности каждого гражданина защищать свою страну и противостоять агрессии в активной или пассивной манере».[63] Помимо латвийских силовых структур, ядром системы сдерживания является присутствие на территории Латвии подразделений НАТО, которые проводят учения как демонстрацию силы и флага НАТО. На национальном уровне возможности сдерживания основаны на концепции, согласно которой, помимо существования и системы подготовки силовых формирований, существует потенциал «быстрого увеличения численности этих сил до уровня, необходимого для сдерживания или ведения войны».[64] Однако это может означать, что одним из факторов, определяющих устойчивость системы обороны Латвии, является старение населения. Здесь Латвия столкнется с проблемами, потому что «страны Балтии сталкиваются с общей демографической проблемой, поскольку усилиям по увеличению

[61] Больше подробностей можно найти в: “Latvian (EU) Residency Program,” *Elma Global*, www.second-citizenship.org/permanent-residence/latvian-eu-residency-program.

[62] “Saeima Bans Latvian Children’s Participation in Paramilitary Camps in Russia,” *The Baltic Times*, May 4, 2018, https://www.baltictimes.com/saeima_bans_latvian_children_s_participation_in_paramilitary_camps_in_russia/.

[63] Ministry of Defence of the Republic of Latvia, “The National Defence Concept,” approved by the Cabinet of Ministers on May 24, 2016, 7, www.mod.gov.lv/sites/mod/files/document/Valsts_aizsardzibas_koncepcija_EN.pdf.

[64] Ministry of Defence of the Republic of Latvia, “The National Defence Concept,” 9.

размера и потенциала территориальных сил может помешать нехватка молодых, квалифицированных новобранцев, поскольку, вероятно, члены большого русского меньшинства в Эстонии и Латвии не хотят участвовать в этом».[65]

Анализ первопричин: случай вертикального деления

Среди факторов, влияющих на сплоченность населения Латвии и представляющих угрозу национальной безопасности, есть фактор вертикального разделения внутри общества и недоверия к правительству. На первый взгляд, это явление можно объяснить наличием русского меньшинства, коррупцией, плохими экономическими условиями или другими факторами. Поскольку восприятия недостаточно, автор решил, что необходимо найти другие причины этого явления, другими словами – первопричины, и применил один из самых простых, но эффективных методов исследования – 5 ПОЧЕМУ. Идея этого метода такова – итеративно задавая вопросы, начинающиеся с «почему», добраться до сути проблемы. Количество вопросов не обязательно должно быть пять; в зависимости от масштаба и сложности задачи их может быть шесть, семь, даже десять. Исходя из этого, процесс[66] начался с постановки задачи:

В латвийском обществе существует вертикальное разделение.

Затем автор начал задавать вопросы «почему», надеясь найти первопричину.

1. Первый вопрос: почему в латвийском обществе существует вертикальное разделение? Ответ найти было относительно легко: *люди не доверяют политической системе*.
2. Итак, был задан следующий вопрос «Почему»: почему люди не доверяют политической системе? После анализа был предложен ответ: *политики не заботятся о людях должным образом*.
3. Затем последовало следующее «Почему»: почему политики не заботятся о людях должным образом? На тот момент было несколько возможных ответов, которые были отвергнуты: *они недостаточно ква-*

[65] James K. Wither, "'Modern Guerrillas' and the Defense of the Baltic States," 7.

[66] На основе: Una Bergmane, "The Three Little Oligarchs: Latvia's Corruption Scandal," *Foreign Policy Research Institute*, November 22, 2017, https://www.fpri.org/article/2017/11/three-little-oligarchs-latvias-corruption-scandal; Aaron Eglitis, "U.S. Sanctioning Russian Oligarchs Sparks Exodus of Cash From Latvia," *Bloomberg*, April 23, 2018, https://www.bloomberg.com/news/articles/2018-04-23/u-s-sanctioning-russian-oligarchs-spurs-cash-exodus-from-latvia; "Krisjanis Karins & Tambovskaya Mafia," *Lawless Latvia*, March 13, 2019, http://www.lawlesslatvia.com/2019/03/; "How Russian Oligarchs Turned the Country of Latvia into Their Own Personal Money Laundering Machine," *Gangsters Inc.*, August 3, 2016, http://gangstersinc.ning.com/profiles/blogs/how-russian-oligarchs-turned-the-country-of-latvia-into-their-own; "The KNAB Targets Latvia's Oligarchs," *The Economist*, June 8, 2011, http://country.eiu.com/article.aspx?articleid=218189406.

лифицированы, они не общаются с обществом, у них плохие советники и т.д. В конце концов было решено, что лучший ответ был: *политики*[67] *предпочитают заниматься собственным бизнесом*.

Следующие вопросы и ответы, перечисленные ниже, привели к выводу, что основной причиной может быть коррупция:

4. Почему политики предпочитают заниматься собственным бизнесом?
   У них тесные связи.
5. Почему у них тесные связи?
   Они объединяют бизнес с политикой.
6. Почему они объединяют бизнес с политикой?
   Они коррумпированы.

Но автор решил продолжить, поскольку у коррупции также есть первопричина, которую необходимо найти. Автор решил остановиться на этом, так как это могло привести к ошибочным результатам, поэтому на седьмой вопрос нет ответа.

7. *Почему они коррумпированы?*

Будущие последствия

В краткосрочной перспективе правительство Латвии, вероятно, решит, как будет развиваться Латвия следующие несколько лет. Выборы в октябре 2018 г. положили конец существовавшей ранее коалиции правых партий. Пророссийская партия «Гармония» получила почти 20 % голосов, а две другие популистские партии получили соответственно: «КПВ» – 14 % и «Новая консервативная партия» – чуть меньше 14 %.

Вопреки некоторым мнениям, высокий балл «Гармонии» не означает, что Латвия может повернуться в сторону России, поскольку в этой партии также много латышей. Общественная поддержка этой партии снижается: в 2011 г. – 28 % поддержки, в 2014 г. – 23 %, а в 2018 г. – чуть ниже 20 % поддержки. Итак, более высокие результаты популистских партий могут означать, что люди просто устали от многочисленных скандалов, коррупции и отсутствия прогресса. Масштабы изменений значительны, поскольку останется только треть нынешнего парламента, а новые партии, которые, вероятно, сформируют правительство, выдвинут молодых неопытных политиков.[68] Несмотря на многие изменения, оборона и текущая политика безопасности должны остаться неизменными – когда латыши голосовали за усиление передового присутствия НАТО и расходование 2% ВВП на оборону, все партии проголосовали «За». И есть планы потратить больше в случае

[67] Три олигарха по-прежнему активны: один – мэр города, второй – бизнесмен, а третий – правительственный чиновник. Выглядят как один замкнутый круг, отделенный от обычных людей.

[68] Интервью с государственным служащим из Латвии, 8 октября 2018 г.

необходимости.[69] Были некоторые предположения, что Россия может попытаться повлиять на «Гармонию» или будущую коалицию популистских партий против латвийского общества. Если это произойдет, она, вероятно, будет использовать рефлексивный контроль и пытаться использовать такие разрывы, как вертикальное деление (недоверие общества к латвийскому правительству), горизонтальное деление (разногласия между русским меньшинством, которое сталкивается с языковой реформой, и населением Латвии) и экономическое неравенство, когда люди с низкими доходами и пенсиями борются за существование и выживание (например, российские неграждане). С другой стороны, возможный конфликт или кризис в Латвии или другой балтийской стране не может начаться с подстрекательства русского меньшинства. Создание враждебного отношения в диаспоре, а затем попытка дестабилизировать страну изнутри займет слишком много времени и даст достаточно индикаторов для реакции правительства и НАТО; стоит только упомянуть эстонские слова «они могут прийти, но встретят сопротивление на каждом углу» – и, вероятно, то же самое, например, произойдет в Латгалии. Вместо этого вторжение может быть очень быстрым и скрытым с использованием поездов, например.[70]

Но это маловероятно, потому что в октябре 2018 года Верховный командующий силами НАТО в Европе генерал Кертис Скапаротти на заседании Военного комитета в Варшаве обсудил общегосударственный подход как реакцию на любое использование средств гибридной войны Россией. Он также подчеркнул тот факт, что с российским принуждением нужно бороться объединенными усилиями, потому что «сами нации имеют разные сильные, слабые стороны и уязвимые места», и необходимо определить с какими угрозами можно бороться с помощью военных мер, и для которых потребуются другие контрмеры.[71] Похоже, это касается Латвии. Рассматривая активность России, можно предположить, что Латвия действительно испытала российское принуждение, например, в военной сфере – учения ЗАПАД 17, когда российские силы были видны буквально на границе, во внутренней сфере – ОПР и деятельность российских спецслужб, а в экономике – российский след, превышающий 12 % ВВП. Итак, если бреши в латвийском обществе будут закрыты, России будет сложно скрытно проникнуть в страну.

В долгосрочной перспективе, по Латвии сильно ударит демографический спад. Уменьшение численности населения носит катастрофический характер. Малонаселенные сейчас районы будут еще больше обезлюдены, и Латвия может стать страной пожилых людей с огромным экономическим

---

[69] Интервью с государственным служащим из Латвии, 8 октября 2018 г.

[70] Интервью с государственным служащим из Латвии, 8 октября 2018 г.

[71] Samuel Cranny-Evans, “NATO Announces Plans to Counter Russian Hybrid Warfare,” *Jane’s Defence Weekly*, October 2, 2018, https://www.janes.com/article/83503/nato-announces-plans-to-counter-russian-hybrid-warfare.

неравенством. Отсутствие молодежи (утечка мозгов) также будет способствовать этой мрачной картине, которая поднимает такие вопросы, как кто будет работать и кто будет защищать страну в будущем. Это вопросы, которые правительству, независимо от политических убеждений, придется проглотить и переварить. Лекарством от этой тенденции было бы вернуть уровень рождаемости как минимум до 2,2 для поддержания численности населения и попытаться повернуть вспять тенденцию к эмиграции. Что касается нынешнего русского меньшинства, то оно должно быть интегрировано в латвийское общество, потому что альтернативы просто нет. В любом случае диаспора неграждан будет уменьшаться из-за смертности и натурализации молодежи. Это потребует от латвийского правительства жесткой, но открытой позиции по отношению к России, чтобы бороться с уничижительными сообщениями и фейковыми новостями. Независимо от всего, усилия прилагаются. В Латгалии, например, где излучатели латвийского телевидения в настоящее время теряют сигнал из-за более мощных российских станций, устанавливаются передающие станции латвийских телеканалов и транслируются русские программы латвийского производства для связи с восточной частью страны.

Восточный фланг НАТО будет постоянно и агрессивно подвергаться испытаниям со стороны России, которая будет использовать стратегию рейдов, чтобы попытаться ослабить Североатлантический союз. Россия преуспела в принуждении других стран с помощью средств непрямой войны. Однако, поскольку страны Балтии хотя и подвергались прямому воздействию со стороны России, но оказывали сопротивление, Россия может повернуться к другим возможным целям на восточном фланге, таким как Северная Македония, Западные Балканы или даже Венгрия и Болгария.

Но этот процесс также будет зависеть от будущей формы и сплоченности НАТО. Поскольку России нравится иметь дело со странами по отдельности, а не с единой организацией, любая трещина в союзнических отношениях принесет пользу Кремлю. Вот почему требования США к европейским партнерам о необходимости большего вклада в НАТО – это не только призывы к большему участию в разделении бремени. Эта стратегия, вероятно, приведет к более компактной и сплоченной структуре НАТО в Европе – к «возвращению европейской геополитики».[72]

Выводы

Наличие русского меньшинства в Латвии, особенно после выборов в октябре 2018 года, может стать для России хорошей основой для подрыва единства этой страны. Однако не стоит переоценивать данный вопрос, по-

[72] Sten Rynning, “A Europeanized NATO? The Alliance Contemplates the Trump Era and Beyond,” *War on the Rocks*, September 25, 2018, 12, https://warontherocks.com/2018/09/a-europeanized-nato-the-alliance-contemplates-the-trump-era-and-beyond.

скольку эта группа неоднородна. Среди этого меньшинства есть пролатышские и пророссийские граждане. Кроме того, картина, касающаяся потенциальных слабых мест российской диаспоры – соотечественников и неграждан – не черно-белая. Есть латвийские русские, которые имеют разные мнения об условиях жизни в Латвии и в России и не верят российской пропаганде и фейковым новостям. В частности, латгалов не следует воспринимать как полностью пророссийскую группу. Среди них есть как пророссийские граждане, так и патриоты, которые не боятся России и готовы к кровопролитной войне.[73] Однако, хотя русская диаспора *сейчас* не представляет угрозы, если ее подтолкнуть извне, например, принуждением со стороны России, она может отреагировать против латвийского общества. Можно сделать также вывод, что Россия, если она решит вмешаться в Латвию, не будет делать это для защиты диаспоры, а по стратегическим соображениям, и русское меньшинство будет использоваться просто как инструмент.

Организованная преступность из России может стать одним из наиболее эффективных и скрытых средств принуждения в Латвии. Она укоренилась глубоко внутри латвийского общества с советских времен, и стереть ее будет сложно. Ее существование следует анализировать вместе с ее прямой связью с Кремлем, российским экономическим присутствием и проблемами, влияющими на латвийскую банковскую систему. В будущем, если Кремль потребует это, ОПР, вероятно, будет активно участвовать в попытках России разжигать беспорядки, коррумпировать политиков и собирать информацию. Борьба с этим должна вестись как на национальном, так и на международном уровне.

Россия осуществляет обширное враждебное междоменное принуждение в жизненном пространстве Латвии, надеясь ослабить сплоченность на восточном фланге НАТО. Наиболее яркими проявлениями были учения ЗАПАД 17, кибератаки, уничижительная пропаганда государственных телеканалов и радикализация молодежи (лагеря для радикализации).[74] Эти усилия могут перерасти в более агрессивные меры, и даже использование прямых военных действий нельзя списывать со счетов.[75] Более того, Россия способна использовать Беларусь в качестве прокси против стран Балтии. Хорошая новость заключается в том, что самооценка населения Латвии растет, поскольку люди сравнивают информацию из разных источников и ставят под сомнение фейковые новости. Это также может привести к еще одному выводу о том, что российская пропаганда становится устаревшим инструментом, и поэтому Россия попытается использовать другие области, возможно, киберпространство, что и относительно дешево, и очень эффективно, и не имеет границ.

---

[73] Интервью с латвийским военнослужащим, 8 октября 2018 г.

[74] Об этой проблеме говорила и Латвийская полиция безопасности. Смотри “Public Report on the Activities of Latvian Security Police,” 8, 9,15.

[75] Дело Скрипаля показывает истинные намерения России – для Кремля нет границ, которые могли бы остановить его влияние.

Восточный фланг НАТО подвергается испытаниям давно, и этот процесс будет усиливаться. Усилия России могут быть сосредоточены, помимо стран Балтии, на других «многообещающих» целях, таких как Северная Македония, Западные Балканы или даже Болгария, где российский экономический след делает захват государства вполне реалистичным. Это исследование показало, что вертикальное и горизонтальное разделение латвийского общества опасно для национальной безопасности. Социальное неравенство также является серьезным препятствием для латвийского общества и национального единства. К сожалению, недоверие к правительству оправдано из-за наличия коррупции и политического сговора, наряду с отмыванием денег и социальным неравенством, которое особенно распространено в сельской местности. Это широко распространенное явление носит очень опасный характер, поскольку его существование в условиях низкого социального капитала и демографического спада создает благоприятные условия, влияющие на латвийское общество во многих сферах. Эту брешь следует устранить как можно скорее, поскольку она подрывает сплоченность и устойчивость Латвии.

Есть области, в которых это исследование не нашло данных, и на первом месте, это характер российской организованной преступности в Латвии. На самом деле информации об этом не так много, может быть, из-за того, что большинство данных засекречены. Но предполагаемая способность ОПР воздействовать на российскую диаспору путем физического принуждения и запугивания, и ее прямая связь с Кремлем могут иметь катастрофические последствия, если они когда-либо будут приведены в действие. Есть свидетельства того, что помимо отмывания денег, в настоящее время она занимается сбором разведданных для России, а также сотрудничает с преступными группировками на границе. Это означает, что несмотря на удивительно позитивную стойкость русской диаспоры в Латвии, у России есть канал и потенциал для тайного проникновения в страну и применения междоменного принуждения изнутри. Другие области, которые следует изучить дополнительно, включают текущее состояние латвийского населения, сотрудничество между странами Балтии в отношении их русских меньшинств и распад русского меньшинства в Латвии.

Это исследование затронуло лишь некоторые аспекты непрямого ведения войны Россией. Есть и другие многообещающие области для исследований, такие как кибервойна, экономика или сфера законодательства. Безусловно, исследование любой из них может дать обширные результаты и некоторые интересные выводы для будущего НАТО. Но даже на этом этапе данная работа представляет собой очень четкое послание о том, что сплоченность и единство нации имеют первостепенное значение при противодействии междоменному принуждению.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Рослав Ежевский служит в Национальном военном представительстве Польши при Верховном штабе союзных операций НАТО в Европе в Бельгии. Он имеет опыт работы в ВМС Польши и в отделах текущих операций и планирования Польского оперативного командования. Он был направлен в Эфиопию в качестве военного наблюдателя Организации Объединенных Наций и в Афганистан в качестве советника афганской армии. Его опыт включает демографические тенденции, миграцию, региональную безопасность и прогнозирование стабильности. Он выпускник программы прикладных исследований в области безопасности Центра им. Маршалла.
E-mail: r.jezewski@ron.mil.pl.

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Мика Керттунен, *Connections QJ* 18, № 1-2 (2019): 72-80
https://doi.org/10.11610/Connections.rus.18.1-2.04

Рецензированная статья

Помимо наказания: сдерживание в цифровой сфере

Мика Керттунен

Институт киберполитики, Тарту, Эстония, https://cpi.ee/

Резюме: Теория сдерживания с момента своего появления оправдывала наращивание и поддержание арсеналов оружия, предположительно гарантируя наше выживание. Однако мы не знаем, работает ли теория сдерживания на практике: крупных войн, возможно, удалось избежать по многим другим причинам, кроме страха наказания или (другие) высоких затрат. Скептицизм в отношении киберсдерживания используется для оправдания односторонних, карательных, даже превентивных, упреждающих или постоянных действий против предполагаемых противников. Сдерживание, ориентированное на ядерное оружие, с упором на недопущение безрассудного поведения государства, могло бы быть улучшено, чтобы противостоять современным, пронизанным технологиями реалиям, где абсолютная нетерпимость к допущению ошибок или инцидентов, критически важная в сфере ядерного сдерживания, нереальна. В результате мы пришли к принятию кибероперации или отказу от них в зависимости от их целей и последствий. В качестве вклада в достижение ответственного поведения государства в киберпространстве, автор предлагает в полной мере использовать расчет затрат, лежащих в основе теории сдерживания, и включить обещание вознаграждений в наши варианты политики.

Ключевые слова: кибербезопасность, сдерживание, кибердомен, соответствие, толерантность, атрибуция.

Комфортабельная леность теории сдерживания

Можно ли сказать что-нибудь новое и значимое о сдерживании? Не обязательно начиная с Гермократа Сиракузского, любой анализ сдерживания должен, по крайней мере, отметить, что сдерживание в узком понимании

касается угрозы наказания.[1] В то же время следует отметить, что более широкое прочтение признает два аспекта сдерживания: наказание и воспрещение. Более того, уместно представить последнюю интерпретацию, специально разработанную для кибер проблем, которая добавляет аспекты связанности и нормативных табу.[2]

Интеллектуальный анализ начинается со ссылки на логику сдерживания. Во-первых, в основе лежит чисто предполагаемая логика, или закон, экономики. Рациональный актор – это расчетливое создание, которое знает, что выбрать: более низкую стоимость (Формула 1).

Стоимость соблюдения < Стоимость несоблюдения

Формула 1. Чисто экономическая логика сдерживания. (авторская компиляция)

Независимо от того, что, как предполагается, вызывает сдерживающий эффект – воздержание от мыслимого поведения: боль, неудачи, вознаграждения, накопление затрат или стыд – теория или теории предполагают, что противник агрессивен, но, несмотря на это, действует рационально, основывая свое решение на расчетах, взвешивая весь потенциал, учитывая при этом вероятные затраты и выгоды.[3] Во-вторых, не помешает упомянуть фундаментальный тезис Шеллинга о силе выбора между *ущербом и отсутствием ущерба*:

> Но для страдания нужна жертва, которая может чувствовать боль или ей есть что терять. Причинение страдания ничего не приносит и ничего не спасает напрямую; оно может только заставить людей вести себя так, чтобы избегать этого. Единственная цель ... должна заключаться в том, чтобы повлиять на чье-то поведение, заставить его принять решение или сделать выбор. Чтобы осуществлять принуждение нужно, чтобы было предчувствие насилия. И чтобы этого можно было избежать за счет подчинения. Сила причинять боль – это сила торговаться. Использовать ее – это дипломатия – зловещая дипломатия, но дипломатия.[4]

---

1 Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960/1980); also Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966/2008); and Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyber War," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. For Hermocrates of Syracuse, see Thucydides, trans. Martin Hammond, *The Peloponnesian War* (Oxford: Oxford University Press, 2009).

2 Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.

3 Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961).

4 Schelling, *Arms and Influence*, 2.

Наконец, необходимо признать ограниченность сдерживания. Теория сдерживания – и что наиболее важно, доверие к ней – предполагает сходство между навязываемыми угрозами, ценностями противника и ожидаемым рациональным поведением. Сдерживание, как основное политическое обязательство, является абсолютным, но реальный выбор и практическое применение сдерживания требует непростого выбора ценностей.[5] Сколько, например, ущерба, затрат или боли необходимо, и что представляют собой затраты, боль или стыд?

И как Другой узнает о наших возможностях и о расчетах, которые мы провели от его/ее имени? Коммуникация несовершенна, и совершенное понимание невозможно. Более того, существует асимметрия информации. Например, хотя можно с уверенностью предположить, что нападающий достаточно хорошо осведомлен о целевой киберсистеме и связанных с ней ценностях, обороняющийся не обязательно знает идентичность, стратегию или выгоды нападающего. Более того, кибер обороняющийся может быть вынужден действовать только в определенные моменты времени, в то время как кибер нападающий может активизироваться в любое время. Это демонстрирует дилемму между *дискретным временем* для одного игрока и *непрерывным временем* для другого.[6]

Что касается киберпространства, уместно отметить, что сдерживание в киберпространстве является сложной задачей или вообще не работает. Сам факт проведения злонамеренных кибероперациий установить сложно. Дополнительным фактором является скрытый, быстрый или непредсказуемый характер кибер-деятельности, которая часто осуществляется негосударственными субъектами, или отсутствие соответствующих средств или политико-правовых рамок для наказания киберпреступников.

Фактически, само утверждение о том, что сдерживание работает, не может быть проверено или опровергнуто. Сам сдерживающий эффект имеет когнитивный характер. Теория сдерживания, хотя и часто обременена расчетами, не может объяснить или предсказать какое-либо поведение; в лучшем случае, это *идеальный или гипотетический набор фактов, принципов*

---

[5] Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica, CA: RAND, 2017), 21–22, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf; Andrew Higgins, "Two Border Cities Share Russian History – and a Sharp European Divide," *The New York Times*, November 9, 2017, https://www.nytimes.com/2017/11/09/world/europe/narva-estonia-ivangorod-russia.html.

[6] Kien C. Nguyen, Tansu Alpcan, and Tamer Basar, "Security Games with Incomplete Information," in *Proceedings of the 2009 IEEE International Conference on Communications*, 14-18 June 2009, Dresden, Germany, https://doi.org/10.1109/ICC.2009.5199443 (studying the game theory of security games and discrete time); Stefan Rass, Sandra König, and Stefan Schauer, "Defending Against Advanced Persistent Threats Using Game-Theory," *PLoS ONE* 12, no. 1 (2017), https://doi.org/10.1371/journal.pone.0168675.

или обстоятельств, или просто абстрактная мысль.[7]

Соответственно, изучение сдерживания превратилось в изучение определенных элементов, которые считаются важными в установленном каноне сдерживания. Более того, скептицизм по отношению к киберсдерживанию используется для оправдания односторонних, карательных, даже превентивных, упреждающих или постоянных действий: поскольку сдерживание не работает в киберпространстве, оно несет ответственность за принятие мер и причинение дорогостоящих последствий для предполагаемого Другого, особенно в том случае, если нет угрозы уничтожения в результате возмездия. Это убеждение основано на ограниченном понимании киберсдерживания. Несмотря на свою узкую формальную правильность, оно опасно неверно.[8]

Мы просто не знаем, действительно ли сдерживание работает или нет. Эта неопределенность вместе с фактом, утверждением или предположением о том, что с киберпространством мы вошли, по крайней мере, частично, в новую операционную среду, требует нового описания сдерживания.

Новый нарратив сдерживания: четыре утверждения

Измененный контекст

Хотя логика сдерживания может быть прослежена до общего и древнего человеческого поведения, генеалогия теории сдерживания обусловлена биполярной Холодной войной. В те годы можно было сказать, что обоюдное намерение двух сверхдержав состояло в том, чтобы обладать достаточной силой, чтобы уничтожить другую, обеспечивая при этом выживание человечества на планете. Концепция сдерживания позволяла оправдывать первое и гарантировать второе.

Ядерное оружие и способность сверхдержав уничтожить планету никуда не делись. Тем не менее, условия и контекст киберсдерживания различны. В то время как ранее сдерживание подчеркивало необходимость избегать безрассудного поведения государства, в современном кибер-дискурсе основное внимание уделяется ответственному поведению государства. Сдерживание, как мы его знаем, не кажется уместным и заслуживающим доверия.

---

[7] *Merriam-Webster English Dictionary.*

[8] Точно так же неправильно было бы некритически предполагать, что кибер-деятельность невидима, быстра и не подлежит атрибуции. Любой анализ, выходящий за рамки дорожной литературы, может выявить ощутимые последствия, месяцы и годы подготовки кибератак, а также официальную аттрибуцию государственным и негосударственным субъектам. Скорость света, а также скорость пули или истребителя – очень плохие индикаторы для определения скорости атаки, операции или кампании.

Более широкая терпимость

Кроме того, будь то в ядерной обстановке, во времена Холодной войны или сейчас, всегда преобладала культура нулевой терпимости. Неудачи в сдерживании, по крайней мере в чистом смысле, были бы неприемлемы. Ядерная или любая крупная военная атака была бы встречена ответными ударами, даже возмездием, когда все уже было бы потеряно.

В кибер-делах никто не может жить с нулевой терпимостью. Информационные и коммуникационные системы по своей природе уязвимы, подвержены техническим инцидентам или человеческим ошибкам, не говоря уже о преднамеренных атаках. Фактически, если во время Холодной войны военная конфронтация сверхдержав была допустима на глобальной периферии – в Азии, Африке и Латинской Америке, – то теперь мы имеем три уровня фактического принятия кибероперациий.

С готовностью принимаются операции, проводимые спецслужбами, органами безопасности, правоохранительными органами и вооруженными силами против общепризнанных экстремистских, террористических или преступных организаций, поскольку, например, Резолюция 1373 (2001) Совета Безопасности Организации Объединенных Наций (СБ ООН) определяет все формы терроризма как представляющие угрозу международному миру и безопасности. Поэтому международному сообществу относительно легко принять, даже приветствовать наступательные военные кибероперации США против «Исламского государства». С другой стороны, государственные кибероперации в рамках существующих бинарных конфликтов или против менее значимых целей, лицемерно или нет, условно принимаются. Например, израильские кибероперации против сирийского правительства или «Хезболлы» не вызывают международных возражений сверх обычного – в отличие от американских операций против тех же целей. Предполагаемая операция голландской разведслужбы, проникшей в системы Московского Государственного Университета,[9] не произвела никакого шума, возможно потому, что государства не хотят проблематизировать разведывательную деятельность, которую они все проводят, а может быть потому, что мишенью операции была (как утверждается) кибер-преступная группировка российского происхождения. Действия, которые воспринимаются как неприемлемые, представляют собой те операции, которые каким-нибудь образом ставят под угрозу международный порядок или национальную безопасность. Поэтому такие операции, как проникновение на серверы Национального конгресса Демократической партии в 2016 году и кража данных или попытка взлома серверов Организации по запрещению химического

[9] Rick Noack, “The Dutch Were a Secret U.S. Ally in War against Russian Hackers, Local Media Reveal,” *The Washington Post*, January 26, 2018, www.washingtonpost.com/news/worldviews/wp/2018/01/26/dutch-media-reveal-country-to-be-secret-u-s-ally-in-war-against-russian-hackers/.

оружия в 2017 году, считаются опасными и безответственными, и подверглись широкому международному осуждению.

Очевидно, такая фактическая терпимость к кибероперациям бросает вызов устоявшейся логике сдерживания: они несовместимы. Само отсутствие каких-либо серьезных кибероперациий свидетельствует скорее либо о неспособности государств, либо об их осторожности проводить такие действенные и глубокие операции в мирное время, чем о сдерживании. Тем не менее, практика кибероперациий, подвергающих проверке пороговые значения применения силы и вооруженного нападения, бросает вызов международному праву и, что самое серьезное, верховенству права, которые многие из активных операций на словах поддерживают.

Другие подходы

С концептуальной точки зрения и заимствуя из древнекитайского мышления, сдерживание наказанием является негативным подходом, а сдерживание лишением – нейтральным. Как нам говорят, первый активно стремится уменьшить ценности плохого субъекта, а второй отрицает какое-либо увеличение этих ценностей. Если расчетная логика рационального человека верна, как предполагается, то предложение вознаграждения также должно удерживать игрока от действий, которые он в противном случае предпринял бы – позитивное сдерживание: сдерживание с помощью выгод.

Такие выгоды можно создать несколькими способами. Отражая зеркально концепцию сдерживания с помощью наказания, сдерживание с помощью выгод может вознаграждать определенное поведение государств. Принимая во внимание концепцию сдерживания путем лишения, оно может включать развитие инфраструктуры, моделей сотрудничества, обмен ноу-хау или постановку плюрилатеральных, субрегиональных или других общих целей, которые используют экономические и социальные преимущества информационных и коммуникационных технологий. Выгоды также могут быть получены в контексте взаимной связанности в результате сокращения расходов и оптимизации затрат путем совместного снижения киберрисков. Кроме того, ожидаемыми выгодами могут быть улучшение репутации, рейтинг в соответствующих международных организациях или оценках, или признанное лидерство в международных процессах. В отличие от нормативных табу и инструментов нулевой терпимости, сдерживание выгодой подчеркивает максимизацию общих выгод и, следовательно, полную поддержку и всеобщее принятие/одобрение определенного поведения.

Далее выдвигается гипотеза, что классическая теория сдерживания больше не удовлетворяет в достаточной мере политические амбиции государств. Особенно в Европе существует сильная нерешительность в отношении жестких средств сдерживания, включая санкции и контрмеры, вводимые в соответствии с международным правом и особенно на его периферии. Вместо этого государства все больше интересуются экономическими и социальными стимулами, лежащими в основе поведения их контрагентов.

Ключевой критикой сдерживания наказанием является тот факт, что всякий раз, когда наказание применяется, сдерживание по определению потерпело неудачу. Соответственно, в случае получения выгод упреждающий и превентивный характер сдерживания максимизируется. Можно также утверждать, что сдерживание выгодами максимизирует взаимность и, следовательно, обещает создание максимально широкой платформы общих интересов и всеобщее принятие определенных поведенческих модальностей. Расширяя исследования по изменению вычисления злонамеренных или враждебных действий, государства могут увеличить отдачу от инвестиций в безопасность. Предполагается, что уменьшение военно-политического риска также снижает вынужденные оборонные и военные расходы, одновременно увеличивая социальный и экономический бюджет, что создает устойчивость и укрепляет информационное общество.

В свою очередь, инвестиции в обеспечение устойчивости и надлежащие методы обеспечения безопасности могут значительно увеличить стоимость плохого поведения, тем самым создав дополнительные пороги лишения. В этом контексте особое внимание уделяется устойчивости как нейтральной к действующим лицам мере.

Тонкие инструменты

Таким образом, государства или группы государств должны смотреть за рамки санкций или негативных аспектов в целом. В самом деле, мы должны признать, насколько хорошо работает устойчивость как неявное сдерживание путем лишения: количество создающих эффект кибероперациий очень мало, особенно по сравнению с киберпреступностью и расхожими разговорами о ведении кибервойны.[10] На самом деле, сам масштаб киберпреступности свидетельствует о недостаточных государственных и организационных инвестициях в потенциал, необходимый для того, чтобы помешать киберпреступникам в достижении их целей. Более того, национальная и международная политика кибербезопасности должна включать позитивные программы с вознаграждением.

Заключение

Как мы узнали, сдерживание – это громоздкий и неподходящий инструмент для понимания киберсферы. Условия киберпространства и новая генеалогия сдерживания отличаются от условий и сдерживания ядерным оружием и имеют гораздо больше нюансов.

[10] Eneken Tikk, Kristine Hovhannisyan, Mika Kerttunen, and Mirva Salminen, *Cyber Conflict Fact Book: Effect-Creating State-on-State Cyber Operations* (Jyväskylä: Cyber Policy Institute, 2019). Этот анализ основан на публично известных государственных кибероперациях, собранных Советом по международным отношениям «Cyber Operations Tracker» и другими базами данных.

Поскольку технологические, политические и социальные параметры и предпосылки различны, то и вывод тоже. Киберсдерживание, чтобы функционировать как кибернетический механизм управления поведением государства, парадоксальным образом требует принятия ошибок и инцидентов, а также атак низкой интенсивности. Это признание проводит границу между терпимым и неприемлемым. Мы, Запад, должны сделать так, чтобы стандарты ответственного поведения государств стали настолько высокими, насколько это возможно. Наше стремление использовать наше технологическое превосходство и проводить кибероперации не должно подрывать верховенство закона и более высокие моральные принципы. Поскольку сдерживание субъекта как теоретически сомнительно, так и практически невозможно в киберсфере, санкции всех видов призваны создать государственную практику и установить границы ответственного / безответственного поведения государств.

Менеджмент новой обстановки неопределенности, размытых линий ответственности, множества пороговых значений и множества действующих лиц не может полагаться исключительно на черно-белую логику негатива, то есть наказания. Устойчивость должна заменить в нашем стратегическом лексиконе балансирование на грани наказания и предостережения. Надежная (национальная) устойчивость, как нейтральная к угрозам и приводящая к деэскалации, также лучше подходит для условий непредсказуемости, качество, которое более актуально для кибер-контекста, чем сдерживание или постоянное взаимодействие в этом отношении. Успех подходов, основанных на доминирующем риске и угрозе (со стороны субъекта), или одновременном сдерживании и постоянном взаимодействии, обусловленных точностью (предварительных) оценок, сам по себе слишком рискован.[11] Запад должен стимулировать ответственное поведение в киберпространстве. Устойчивость и вознаграждение вместе создают мощный и мирный вариант политики, который не может предложить ни одно другое государство или группа государств.

Таким образом, в новой формуле сдерживания (формула 2 ниже) по-прежнему действует закон экономики, но затраты заменяются вознаграждением.

---

[11] Gerard de Vries, Imrat Verhoeven, and Martin Boeckhout, “Governing a Vulnerable Society: Toward a Precaution-Based Approach,” in *Vulnerability in Technological Cultures: New Directions in Research and Governance*, ed. Anique Hommels, Jessica Mesman, and Wiebe E. Bijker (Cambridge, MA: MIT Press, 2014), 225. Упомянутая глава основана на докладе «Ненадежная безопасность», который Голландский научный совет по правительственной политике (WRR) принял в качестве официальной рекомендации голландскому правительству. Управление рисками, принятое или по крайней мере упомянутое во многих национальных стратегиях кибербезопасности, направлено на выявление и оценку рисков с точки зрения вероятности и степени ущерба и проектирования, а также принятие мер по ограничению или контролю тех рисков, которые считаются неприемлемыми.

Награды за соблюдение требований > Награды за несоблюдение

Формула 2. Новая экономическая логика сдерживания.
(компиляция автора)

Этот поворот не предполагает почти автоматической воинственности Другого. Таким образом, мы избегаем иллюзии сдерживания Другого в ситуации, когда считается, что такая воинственность не обязательно имеет место. Вместо этого мы сосредотачиваемся на более вероятной мотивации и амбициях правительств – положительном вознаграждении. Очевидно, что лидер, решившийся пойти на войну, не будет разубежден угрозой наказания, ожидаемыми трудностями или благосклонным вознаграждением.

Такой поворот мышления не будет оценен по достоинству оборонным киберпромышленным комплексом, который оправдывает свое существование угрозой и перспективами апокалиптического будущего. Для остального человечества, предпочитающего мир, процветание и глобальную справедливость, такой поворот имел бы смысл.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Подполковник (в отставке, финские сухопутные силы) **Мика Керттунен**, доктор социологических наук (пол.), Директор по исследованиям Института киберполитики (Тарту, Эстония). Он окончил Финскую военную академию и курс офицеров Генерального штаба, а также Королевский норвежский командно-штабной колледж. Керттунен изучал мировую политику в Университете Хельсинки, и в своей диссертации 2009 года проанализировал внешнюю и ядерную политику Индии. После службы в армии он сосредоточил внимание на кибер-проблемах внешней политики и политики безопасности, разработке кибер-норм, а также разработке национальных стратегий кибербезопасности и военных кибер-доктрин. Д-р Керттунен является советником финской делегации в Группе правительственных экспертов ООН по информационной безопасности (2016-2017) и приглашенным преподавателем юридического факультета Тартуского университета.

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Мануэль Фишер, *Connections QJ* 18, № 1-2 (2019): 81-109
https://doi.org/10.11610/Connections.rus.18.1-2.05

Рецензированная статья

Концепция сдерживания и ее применимость в кибер домене

Мануэль Фишер

Европейский центр исследований по вопросам безопасности им. Джорджа К. Маршалла, http://www.marshallcenter.org

Резюме: Киберпространство, как пятый домен, вездесуще, и все развитые государства все больше осознают, что международные отношения и типичные области, охватываемые государством, меняются перед лицом глобальной дигитализации. С появлением технологий, меняющих правила игры, традиционные инструменты государственности, такие как сдерживание, кажутся устаревшими в процессе построения стратегии национальной безопасности. В частности, развитые государства сильно зависят от открытого и безопасного киберпространства, но в то же время страдают от множества уязвимостей. Недавнее прошлое показало, что изощренные кибератаки могут серьезно подорвать деятельность правительств, экономик и обществ и, следовательно, создать угрозу основным интересам безопасности. Как классический инструмент международных отношений, сдерживание может способствовать усилению защите интересов национальной безопасности, даже если киберпространство требует некоторых особых соображений. Поэтому в статье объясняются основные механизмы сдерживания в ядерном веке и при современных международных отношениях, правовые основы киберпространства и возможные способы применения сдерживания в киберпространстве. Статья призвана побудить мировых лидеров внимательно рассматривать сдерживание в киберпространстве как мощный актив, и предоставить политикам варианты действий.

Ключевые слова: кибербезопасность, кибероперации, сдерживание, правовая база.

Введение

Говорить о сдерживании в 21 веке – все равно что раскапывать остатки ушедшей эпохи. С появлением ядерных технологий и, главным образом, во времена Холодной войны, сдерживание было темой не только для политиков и академических кругов, но и влияло на повседневную жизнь миллионов людей, независимо от того, к какому «блоку» они принадлежали. С тех пор сдерживание уменьшило вес в общественном восприятии вместе с ядерными арсеналами великих держав. То, что осталось, по-прежнему имеет огромный потенциал, но как инструмент государственности, а не как основополагающий момент.

В частности, государства сталкиваются с постепенным изменением традиционно ориентированной на государство структуры международной системы, особенно в таких привычных областях государственных функций, как безопасность. Классическое понимание войны и конфликта размывается, а традиционные государственные структуры, кажется, не успевают реагировать с помощью классических инструментов, поскольку конфликт нового типа является многослойным (политическим, военным и экономическим, среди прочего), осуществляемым в основном невоенными средствами, такие как пропаганда и политическая агитация, и среди различных государственных и негосударственных субъектов.[1,2]

Перед лицом ежедневных и непрекращающихся атак на государства и их органы,[3] встает вопрос: что мешает игроку в киберпространстве снова и снова проводить одни и те же атаки или даже подниматься по лестнице эскалации и причинять необратимый ущерб, если это служит его интересам.

---

1 David J. Betz, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (London and New York: Routledge, 2017), 80.

2 Joseph S. Nye, Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security* 41, no. 3 (Winter 2016/2017): 44–71, цитата на с. 48, https://doi.org/10.1162/ISEC_a_00266.

3 Как это произошло в Германии в 2015 году, когда российская хакерская группа под названием «Fancy Bear» атаковала парламент Германии, шпионила по крайней мере за 16 его членами (включая Ангелу Меркель) и извлекла несколько частично конфиденциальных документов. К тому времени Федеральная канцелярия впервые за несколько десятилетий заговорила о (гибридной) войне и потенциальных ответных ударах. Смотри: Patrick Beuth, Kai Biermann, Martin Klingst, and Holger Stark, “Bundestags-Hack – Merkel und der schicke Bär,” *Zeit Online*, May 10, 2017, http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland. И тем не менее, то же самое произошло снова в конце 2017 года, когда сотрудники службы безопасности обнаружили предположительно российскую «устойчивую серьезную угрозу», нацеленную на министерство иностранных дел, которая скомпрометировала сеть на срок до года. Смотри: Thorsten Severin and Andrea Shalal, “German Government under Cyber Attack, Shores up Defenses,” *Reuters*, March 1, 2018, www.reuters.com/article/us-germany-cyber/german-government-under-cyber-attack-shores-up-defenses-idUSKCN1GD4C8.

Кажется, что в киберпространстве нет ни уважения, ни страха перед возмездием, ни серьезных технических барьеров – или, другими словами, нет никакого сдерживания.

В этой статье будет рассмотрен вопрос, эффективна ли концепция сдерживания только в том случае, если она связана с ядерным оружием, и становится ли она бесполезной в международной системе, которая больше не является доминируемой (чисто) ядерным оружием, а киберпреступлениями. Автор утверждает, что это не так! Даже в киберпространстве сдерживание может быть мощным инструментом государственности, способствовать защите интересов национальной безопасности государства. Чтобы доказать эту гипотезу, в этой статье будет тщательно исследована концепция сдерживания, заглянув в прошлое, которое дает разнообразные примеры по этой теме, чтобы, наконец, спроецировать результаты на настоящее. Поэтому будут изучены существующие концепции сдерживания и особые последствия для киберпространства вместе с правовой базой все более дигитализированной международной системы, чтобы в итоге найти эффективные способы применения сдерживания в киберпространстве.

Данное исследование проводится при следующих общих предположениях и исключениях:

- Появляющиеся мобильные технологии пятого поколения (5G) и облачные технологии будут стимулировать распространение Интернета вещей. Критические процессы будут постепенно перенесены на эти технологии, и кибер риски будут расти в геометрической прогрессии, поскольку новые устройства создают больше возможностей для потенциальных проникновений. Кроме того, контролируя физические активы, можно нанести даже физический вред.[4,5]
- Согласно «парадигме предположение о неизбежности проникновения», весьма вероятно, что каждый достаточно сложный программный продукт имеет критические уязвимости и что обновления либо не предоставляются, либо уязвимость держится в секрете.[6]
- Это исследование будет сосредоточено на политических киберугрозах и будет охватывать криминальную кибер-деятельность только в той мере, в какой она происходит в контексте конфликта. Традиционный шпионаж с помощью кибер-средств будет исключен из этого исследования.

---

[4] "BSI: Critical infrastructures – Definition," Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance, 2017, www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html.

[5] James Manyika, et al., *The Internet of Things: Mapping the Value beyond the Hype* (McKinsey & Company, June 2015), 11.

[6] "BSI: Critical Infrastructures," 18.

Механизмы сдерживания

Концепция сдерживания так же стара, как стремление человечества воевать друг с другом.[7] Термин «сдерживание» происходит от слова «террор», которое отражает страх перед издержками, связанными с определенным действием. В академической литературе иногда используется термин «разубеждение» для обозначения более широкого круга мер, которые направлены не только на несение издержек, но и на лишение противника определенных выгод.[8] Для четкого разграничения и ввиду преобладающего использования в политической и академической сферах, в этой работе термин «сдерживание» будет использоваться как общий термин, учитывая тот факт, что это понятие гораздо шире.

Джозеф Най также принимает во внимание оба значения, определяя сдерживание как [9]

> … отговаривать кого-то от каких-либо действий, заставляя его поверить, что затраты для него превысят ожидаемую выгоду.

Это означает сохранение статус-кво, не позволяя оппоненту проводить действия, которые считаются неблагоприятными. Речь не идет о принуждении противника к определенному поведению и, таким образом, изменении статус-кво.[10] Рассмотрение ключевых механизмов и их применение в международных отношениях (МО) поможет понять точки соприкосновения и проложить путь к киберсдерживанию.

Согласно теоретику сдерживания сэру Майклу Куинлану,[11] «не существует такого понятия, как государство, неподверженное сдерживанию».[12] В качестве основных условий для успешного сдерживания (независимо от того, в какой сфере) он рассматривает следующие пять пунктов: [13]

1. Вероятности
2. Способность и серьезное намерение

---

[7] Ранние упоминания восходят к работе Фукидида о Пелопоннесской войне, даже до появления христианского календаря, см. Richard Ned Lebow, “Thucydides and Deterrence,” *Security Studies* 16, no. 2 (2007): 163–188, цитата на стр. 163 https://doi.org/10.1080/09636410701399440.

[8] Michael Quinlan, “Deterrence and Deterrability,” in *Deterrence and the New Global Security Environment*, ed. Ian R. Kenyon and John Simpson (London: Routledge, 2006), 5.

[9] Nye, “Deterrence and Dissuasion in Cyberspace,” 45.

[10] Wyn Q. Bowen, “Deterrence and Asymmetry: Non-state Actors and Mass Casualty Terrorism,” *Contemporary Security Policy* 25, no. 1 (2004): 54-70, https://doi.org/10.1080/1352326042000290506.

[11] Бывший постоянный заместитель государственного секретаря Министерства обороны Великобритании; влиятельный стратег в области обороны и сдерживания.

[12] Quinlan, “Deterrence and Deterrability,” 7.

[13] Quinlan, “Deterrence and Deterrability,” 4.

3. Декларация сдерживания
4. Перспектива возникновения многосторонних затрат
5. Использование всего диапазона возможных ответов.

Вероятности

Идеальное сдерживание должно было бы работать с определенностями, например: «Если ты возьмешь мой обед, я сломаю твою игрушку». Но поскольку человеческое взаимодействие носит довольно сложный характер, возникает ряд неопределенностей, и неправильное восприятие и неверное толкование неизбежны. Чтобы принять это во внимание, необходимо учитывать вероятности.[14] Важную роль играют не только потенциальная выгода («обед») и стоимость проигрыша («игрушка»), но и вероятность успеха или проигрыша. Как следствие, параметры вероятности выигрыша («вы не можете быть уверены, что получите мой обед, потому что я попытаюсь его защитить») и вероятности проигрыша («если вы возьмете мой обед, я сделаю все возможное, чтобы уничтожить вашу игрушку» и, может быть, у меня все получится») необходимо добавить к следующему вычислению решения:[15,16]

*Значение выигрыша * Вероятность выигрыша < Величина потери * Вероятность проигрыша*

Эффективное сдерживание в неопределенной среде должно учитывать все четыре фактора неравенства, чтобы левая часть оставалась меньше правой в восприятии противника.

Способности и серьезное намерение

Способности – это основа, на которой противник может рассчитать ценность, которую он может получить или потерять. Однако существует также необходимость в убедительном намерении использовать эти возможности, чтобы оказать воздействие на вычисление вероятностей.[17] Мощные меры, обеспечивающие наступление, могут увеличить величину потерь, серьезность наступательных и защитных мер может изменить расчет вероятности выигрыша и проигрыша.

*Значение выигрыша * Вероятность выигрыша (↓) < Величина потери (↑)* Вероятность проигрыша (↑)*

---

[14] Quinlan, “Deterrence and Deterrability,” 4.

[15] Philip Bobbitt, *Democracy and Deterrence: The History and Future of Nuclear Strategy* (Basingstoke: Palgrave Macmillan, 1988), 8.

[16] Jeffrey R. Cooper, “A New Framework for Cyber Deterrence,” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Georgetown University Press, 2012): 105-120, 109.

[17] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham, Maryland: Rowman & Littlefield, 2017), 9.

В то время как способности – это, скорее, вопрос денег, а убедительное намерение может быть доказано только действием, тем не менее, оба требуют «демонстрации силы», чтобы они были восприняты оппонентом.[18]

Декларация сдерживания

Помимо способностей и убедительности, важное значение имеет эффективная передача правильного сообщения о сдерживании правильной аудитории.[19,20] Следовательно, очень важно указать какие действия будут запрещены, что (наступательные или оборонительные) способности для соответствующего реагирования имеются и что они будут задействованы.[21] Здесь чрезмерно точное, самоограничивающее определение не является необходимым и даже может быть вредным, поскольку оно открывает противнику путь для уклонения от ответа или для воспрепятствования ответа.[22] Эффективная коммуникация дает противнику определенные факторы для его расчетов и уменьшает количество неверных интерпретаций или неверных восприятий. Более того, сильное заявление о сдерживании само по себе может повлиять на восприятие вероятностей выигрыша и проигрыша.

*Значение выигрыша * Вероятность выигрыша (🡻) < Величина потери * Вероятность проигрыша (🡹)*

Нынешние эксперты, такие как бывший заместитель министра обороны США по вопросам политики Джеймс Миллер, отмечают, что «на самом деле вы не сдерживаете государства, вы сдерживаете отдельных лиц и группы лиц, принимающих решения …».[23] Это означает, что декларацию о сдерживании необходимо разработать в обратном порядке, начиная с желаемого

---

[18] США продемонстрировали новые способности во время вторжения в Панаму в 1989 году, применив стелс истребитель-бомбардировщик F-117, конечно, не из-за угрозы панамской ПВО, а для демонстрации новых способностей в наборе инструментов, см. Richard A. Clarke and Robert K. Knake, *Cyber War: What It Is and How to Fight It* (New York: HarperCollins, 2010), 194.

[19] Bowen, “Deterrence and Asymmetry,” 51.

[20] Jasper, *Strategic Cyber Deterrence*, 9.

[21] Хотя четко обозначенная красная линия отсутствует, США служат хорошим примером, публично предлагая ИТ-подрядчикам побороться за контракт почти на 500 миллионов долларов на разработку и, при необходимости, развертывание, смертоносного кибероружия. Исполнительный директор киберкомандования США заявил, что США ищут привлекающие внимание кибер инструменты, которые можно проследить до США. Смотри Jasper, *Strategic Cyber Deterrence*, 102.

[22] Quinlan, “Deterrence and Deterrability,” 4.

[23] Sean D. Carberry, “Why There’s no Silver Bullet for Cyber Deterrence,” *Federal Computer Week (FCW)*, June 06, 2017, https://fcw.com/articles/2017/06/06/carberry-cyber-deterrence.aspx.

эффекта и с учетом того, как она будет обрабатываться теми, кого она должна сдерживать.[24] Предположение о том, что противник действует рационально, довольно упрощено, поскольку для этого нужна точная информация и готовность принимать решения, основанные только на стратегических последствиях. Лица, принимающие решения, никогда не имеют точной информации, и на них оказывают влияние многие факторы, такие как эмоции или личные интересы.[25]

Перспектива возникновения многосторонних затрат

Создание защитных сооружений может лишить противника желаемого эффекта или, по крайней мере, уменьшить его. Это посеет семена сомнения в сознании противника, поскольку ему нужно больше времени и ресурсов, и вероятность обнаружения возрастает.[26] Короче говоря, меры лишения увеличивают альтернативные издержки претендента. Сочетание мер возмездия и лишения, а также увеличение разнообразия затрат мешают оппоненту заблаговременно подготовить и укрепить свои ценности.[27] Таким образом, увеличивается как величина потерь, так и вероятность потерь.

*Значение выигрыша * Вероятность выигрыша < Величина потери (↑) * Вероятность проигрыша (↑)*

Чтобы увеличить этот эффект, может быть, целесообразно адаптировать стратегию к конкретному противнику. Это требует контекстного знания мотивов данного актора, процессов принятия решений, структур командования и контроля и будет означать необходимость проведения существенных разведывательных действий и проявления понимания культуры оппонента.[28]

---

[24] То, как противник интерпретирует заявление о сдерживании, зависит от его истории и стратегической культуры и является источником неправильного толкования, основанного на различных предпочтениях и ожиданиях. Смотри James Andrew Lewis, “Rethinking Deterrence,” Report (Washington: Brzezinski Institute on Geostrategy, May 2016), 5, https://csis-website-prod.s3.amazonaws.com/s3fs-public/170713_Deterrence_Stability_0.pdf.

[25] Will Goodman, “Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–135, 107, https://www.hsdl.org/?view&did=18663.

[26] Bowen, “Deterrence and Asymmetry,” 50.

[27] Такое сочетание аспектов наказания и воспрещения имело место при администрации Джорджа Буша для сдерживания использования нетрадиционного оружия с вызывающими озабоченность режимами посредством сочетания возможностей воспрещения (разработка всеобъемлющей противоракетной обороны) и угрозы неукоснительного наказания. Смотри Bowen, “Deterrence and Asymmetry,” 50.

[28] Bowen, “Deterrence and Asymmetry,” 51.

Использование всего диапазона возможных ответов

Если демонстрируемые затраты не соответствуют средствам или размаху действий, которые пытаются предотвратить, можно сдержать даже противников разных размеров и с разными системами ценностей.[29] Использование всего диапазона возможных ответов затрудняет противнику возможность предугадать ответ и защитить себя. Таким образом, величина потерь, а также вероятность потерь могут быть увеличены.

*Значение выигрыша * Вероятность выигрыша < Величина потери (⬆) * Вероятность проигрыша (⬆)*

Поскольку государство обычно обладает монополией на применение силы и обладает широким спектром кинетических средств, это может быть преимуществом при столкновении с негосударственными противниками. Переключение областей реагирования на классические и знакомые области государственности может укрепить легитимность и убедительность.[30]

Особые последствия для кибер домена

С тех пор как государства и правительства начали взаимодействовать друг с другом на арене МО, сдерживание было ценным инструментом. Наиболее влиятельная эра сдерживания наступила с появлением ядерного оружия и, по существу, определила курс Холодной войны. Есть параллели с кибер-веком, которые могут оказать ценную помощь, но есть также аспекты, которые следует игнорировать.

Атомная бомбардировка Хиросимы и Нагасаки в 1945 году внезапно заставила мир встать лицом к лицу с новым военным потенциалом, который воспринимался как непреодолимый и приводящий к не выживанию. Стратегам потребовалось несколько лет, чтобы перейти от так называемого «массированного возмездия» НАТО через поворотные моменты, вызванные шоком «Спутник»-а и кубинским кризисом, и последующей концепции сдерживания через «взаимное гарантированное уничтожение» до всеобъемлющей стратегии «гибкого реагирования». Это была многоступенчатая концепция, переходящая от обычной обороны к стратегическому применению ядерного оружия. Она был основана на потенциале (обычные и ядерные силы) и, по крайней мере, на некоторой убедительности (США нанесли ядерный удар по Японии), полагаясь на весь спектр средств (от обычных ответных мер до тактических и стратегических ядерных средств), чтобы обещать многогранные затраты (удары по военным и экономическим целям на

[29] Quinlan, “Deterrence and Deterrability,” 4.

[30] Когда пропагандистская машина Исламского государства стала слишком сильной и неконтролируемой, правительство США обратилось к смертоносной силе в виде воздушных ударов по высокопоставленным оперативникам СМИ, которые стали законными мишенями в вооруженном конфликте из-за их связи с террористической группировкой. Смотри Jasper, *Strategic Cyber Deterrence*, 95.

поле боя и на родине), но не было самоограничения в способах реагирования (не было заранее определенной лестницы эскалации).[31]

Эта четко определенная стратегия действительно привнесла определенную стабильность в международную систему и основывалась на пяти факторах, которые характеризовали тогдашнюю современную концепцию войны (и, следовательно, сдерживания) в среде новых и сложных технологий [32]:

1. *Фактор времени:* Исключительно большой ущерб теперь можно было нанести за короткое время, практически без предварительного предупреждения.
2. *Фактор силы:* Немедленно наличные силы превосходили силы мобилизации из-за фактора времени.
3. *Фактор выживания:* необходимо было выжить при первом исключительно тяжелом ударе, чтобы начать контратаку.
4. *Фактор глобализации:* ядерная война немедленно охватила бы весь мир.
5. *Фактор обороны:* оборона НАТО должна была основываться на демонстрации сильных сторон, а не на защите слабых сторон.

НАТО по-прежнему является ядерным альянсом (в основном основанным на потенциале и решимости США), и ядерное сдерживание остается частью его оборонной стратегии. Тем не менее, после холодной войны мировые атомные арсеналы систематически сокращались, и появлялись различные неядерные технологии. Некоторые даже говорят, что в контексте мощных альтернатив, ядерному оружию отводится пассивная и символическая роль в МО.[33] В то же время вертикальное [34] и горизонтальное [35] распространение деструктивных технологий стало легче осуществлять и сложнее контролировать.[36]

---

[31] "Nuklearstrategie – Zwischen Abschreckung und Einsatzdoktrin," *Bundeszentrale für politische Bildung*, https://sicherheitspolitik.bpb.de/m6/articles/nuclear-strategy-between-deterrence-and.

[32] Bruno Thoß, *NATO-Strategie und nationale Verteidigungsplanung: Planung und Aufbau der Bundeswehr unter den Bedingungen einer massiven atomaren Vergeltungsstrategie 1952 bis 1960* (München: Oldenbourg Verlag, 2006).

[33] Lewis, "Rethinking Deterrence," 5.

[34] Увеличение количества и изощренности оружия установившихся обладателей такого оружия. Смотри Ian R. Kenyon and John Simpson, eds., *Deterrence and the New Global Security Environment* (Abingdon: Routledge, 2006).

[35] Распространение ядерной технологии среди других. См. Kenyon and Simpson, *Deterrence and the New Global Security Environment*.

[36] Фактически, признанные ядерные державы обеспокоены тем, что их ядерное сдерживание может быть обойдено или уничтожено с помощью современных обычных вооружений. Они не дойдут до ядерного порога, и таким образом,

Но даже если концепции ядерного сдерживания невозможно скопировать, все же можно узнать как можно разработать комплексную стратегию использования новых и мощных технологий.[37] Параллельно с ядерной эрой, кибер-эра означает развитие новой, созданной руками человека и трудной для понимания технологии, обладающей огромным потенциалом для гражданского использования и, в то же время, для невообразимого разрушения. Эти общие черты позволяют предположить, что те же факторы, что и в ядерном сдерживании, играют, по крайней мере, основную роль в киберсдерживании. В следующем параграфе будут рассмотрены ранее представленные факторы времени, сил, выживания, глобализации и обороны в киберсфере и добавлен к набору аспектов кибер-специфический фактор атрибуции.

Фактор времени

В кибер эпохе для самой атаки влияние фактора времени, похоже, стремится к нулю, поскольку искусственный интеллект использует алгоритмы для выполнения основных, но трудоемких задач, а участники по всему миру подключаются друг к другу за миллисекунды. Эта так называемая «сетевая скорость» создает одновременность причинно-следственной связи, которая устраняет необходимость дорогостоящего и трудного преодоления расстояния. Теперь даже небольшие субъекты могут влиять на состояние без предварительного предупреждения.[38] Однако это справедливо только для самой атаки. Как и во время Холодной войны, подготовка поля битвы – необходимое предварительное условие для атаки на сетевой скорости. Подобно выявлению командных бункеров, продвинутый кибер-атакующий должен проникнуть в систему и воспроизвести ее схему, получить доступ и разместить бэкдоры.[39,40] Это означает, что нужна долгосрочная кампания, которая не может быть проведена полностью с компьютера, а состоит из сложных операций агентурной разведки (HUMINT).[41]

нанесение удара, по силе равного ядерному, по жизненно важным объектам может остаться безнаказанным, см. Lewis, “Rethinking Deterrence,” 4.

37 Clarke and Knake, *Cyber War: What It Is*, 155.

38 Betz, *Cyberspace and the State*, 39.

39 Richard B. Andres, “The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence,” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 89–104.

40 Clarke and Knake, *Cyber War: What It Is*, 30.

41 Jeffrey Carr, “Responsible Attribution: A Prerequisite for Accountability,” Tallinn Paper No. 6 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014).

Фактор силы

Силы с новейшими технологическими знаниями и оборудованием, находящиеся непосредственно и постоянно в расположении, превосходили мобилизационные силы благодаря временному фактору. Все еще правительства используют те же концепции, что и для не кибератак, делегируя задачи защиты и сдерживания мелких субъектов местной полиции и используя федеральные агентства только против государственных субъектов или террористических групп.[42] Это означает фрагментацию ответственности и наличие непоследовательной стратегии. В то же время, технологические знания и оборудование стоят огромных денег и требуют гибких и специализированных структур. И то, и другое доступно только в определенной степени в государственных структурах, и поэтому все более значительная роль отводится частному сектору.

Особое внимание уделяется цепочке поставок программного и аппаратного обеспечения для ИТ. Часто вопросы кибербезопасности и защиты данных не рассматриваются на стадии разработки, и последующее исправление уязвимостей не всегда возможно.[43] Компрометируя оборудование на ранней стадии разработки, можно создать уязвимости и легко распространить их по цепочке поставок.[44] Это позволяет сфокусировать внимание на всю цепочку, вплоть до мельчайшего «умного клапана». Хотя такие мишени могут показаться незначительными, было оценено, что на них концентрируются особо изощренные агенты, представляющие собой угрозу.[45] Таким образом стало критически важно определять кто производит, испытывает и сертифицирует оборудование, откуда поступают запасные части и какие процессы производства и распределения должны находиться под постоянным национальным контролем.

Фактор выживания

Способность пережить первый удар и способность действовать были ключевым элементом в ядерной обстановке. Кибердомен также кажется средой, в которой доминируют наступательные действия, в которой атакующие имеют структурное преимущество перед обороняющимися, и опреде-

---

[42] Andres, “The Emerging Structure of Strategic Cyber Offense,” 91.

[43] ENISA, “Threat-Landscape-Report 2017” (Heraklion: European Union Agency for Network and Information Security), 107, www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport.

[44] Это явление связано не только с киберпространством. В течение многих лет Министерство обороны США борется с контрафактными деталями в своих важнейших цепочках поставок оборонной продукции. См. United States Government Accountability Office (GAO), “Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk” (Washington D.C.: US GAO, 2016), https://www.gao.gov/products/GAO-16-236.

[45] ENISA, “Threat-Landscape-Report 2017,” 110.

ленная защита невозможна. Более того, промышленно развитые и связанные страны кажутся более уязвимыми, чем менее развитые.[46,47] Это приводит к самосдерживанию мощных, промышленно развитых и связанных государств, как в эпоху ядерной войны. Осознавая свою собственную кибер-уязвимость, возникает нежелание использовать обычное превосходство в других областях (например, в обычных вооружениях).[48] Поскольку кажется невозможным снизить уровень взаимосвязанности в современных обществах, лучшим вариантом является усовершенствование сдерживания и способов защиты.[49]

Фактор глобализации

Подобно ядерной войне, кибератаки игнорируют барьеры и границы в реальном мире. Атакующему больше не нужно находиться рядом с местом действия или в зоне досягаемости обороняющихся.[50] Сетевая скорость сокращает пространственное расстояние до нуля и позволяет субъектам, находящимся за пределами юрисдикции государства, применять силу против него с хорошими шансами никогда не быть привлеченными к ответственности.[51] Это ведет к глобальной кибер-арене, где государственные субъекты часто связаны законами, тогда как нападающие легко ускользают от их действия.[52,53] Даже в большей степени, чем в ядерный век, такие атаки могут иметь широкий спектр последствий, что затрудняет прогнозирование их масштаба. Кибер-инструмент, такой как вирус, может отпрыгнуть назад, распространиться в другие страны или создать непредсказуемый глобальный хаос за считанные минуты.[54]

Еще одним аспектом глобализованной арены является геополитическая симметрия даже для государств, не соседствующих друг с другом. Если государство не обладает преимуществом осуществлять эскалацию (благоприятная асимметрия силы и средств), оно может изо всех сил пытаться адекватно отомстить, поскольку оно должно опасаться проиграть серию эскала-

---

[46] Jack L. Goldsmith, “How Cyber Changes the Law of War,” in *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, ed. Frederic Lemieux (London: Palgrave Macmillan, 2015), 51–61.

[47] Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, no. 1-2 (January 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

[48] Clarke and Knake, *Cyber War: What It Is*, 157.

[49] Clarke and Knake, *Cyber War: What It Is*, 149.

[50] Goldsmith, “How Cyber Changes the Law of War,” 53.

[51] Betz, *Cyberspace and the State*, 39.

[52] Clarke and Knake, *Cyber War: What It Is*, 30.

[53] Andres, “The Emerging Structure of Strategic Cyber Offense,” 92.

[54] Goodman, “Cyber Deterrence,” 116.

ций в конце концов в физической сфере.[55]

Фактор обороны

К сожалению, в киберпространстве отсутствуют четкие нормы того, что такое надлежащая защита и каковы соответствующие ответные меры.[56,57] Помимо того факта, что киберконфликт выходит за рамки традиционного поля боя и имеет место в повседневных системах (например, в банках, телекоммуникациях и управлении воздушным движением[58]), самая большая проблема для сдерживания заключается в том, что наступательные и оборонительные способности поддерживаются в соответствии с кодексом молчания. С одной стороны, противник может подготовить собственную защиту, если он знает о нападении противника, а с другой стороны, нет стимула раскрывать проникновение, поскольку это может испортить репутацию жертвы. Таким образом, нет шанса поучиться у других и разработать надлежащие средства защиты.[59] В контексте сдерживания это контрпродуктивно (поскольку постоянное информирование о четких и целенаправленных ухудшениях сдерживания является ключевым моментом) и должно преодолеваться компромиссом, заключающимся в сохранении в тайне как можно больше информации, но раскрывая и коммуникируя ее количество, достаточное для осуществления эффективного сдерживания.[60]

Фактор атрибуции

Атрибуция не была большой проблемой в ядерный век, и даже сегодня, когда только девять государств обладают ядерным оружием и хорошо известными идентификаторами изотопов каждого арсенала, это не вызывает особого беспокойства.[61] Но в отличие от ядерного оружия, киберсредства труднее отследить, и стопроцентное приписывание оружия к источнику редко возможно.[62] Широко распространено мнение, что это подрывает концепцию сдерживания, но на самом деле, даже при несовершенной атрибуции сдерживание возможно, если речь идет о трех аудиториях [63]:

---

[55] Эстония не хотела приписывать кибератаки 2008 года России (даже если у нее были веские доказательства) из-за геополитического дисбаланса и возможной физической эскалации против значительно превосходящих российских вооруженных сил. См. Goodman, “Cyber Deterrence,” 109.

[56] Carberry, “Why There’s no Silver Bullet for Cyber Deterrence.”

[57] Andres, “The Emerging Structure of Strategic Cyber Offense,” 101.

[58] Clarke and Knake, *Cyber War: What It Is*, 30.

[59] Andres, “The Emerging Structure of Strategic Cyber Offense,” 93.

[60] Goodman, “Cyber Deterrence,” 109; Andres, “The Emerging Structure of Strategic Cyber Offense,” 101.

[61] Nye, “Deterrence and Dissuasion in Cyberspace,” 50.

[62] Clarke and Knake, *Cyber War: What It Is*, 68.

[63] Nye, “Deterrence and Dissuasion in Cyberspace,” 51.

1. *Защищающееся государство* хочет получить относительно высокие гарантии от своих спецслужб и сетевых криминалистов;
2. *Атакующий государственный или негосударственный субъект* знает, что было сделано, но не может быть уверен, насколько хороши противостоящие криминалистика и разведка; даже если он отрицает нападение, он никогда не узнает, насколько правдоподобным был этот обман;
3. *Национальную и международную общественность* необходимо убедить в справедливости возмездия. Следовательно, необходимо раскрыть определенную степень подробностей, даже если при этом определенные методы криминалистической экспертизы могут стать бесполезными для будущих дел.

Качество атрибуции зависит от доступных ресурсов, наличного времени и изощренности противника. Чем меньше в наличии высококлассных криминалистов и высококвалифицированного персонала, тем ниже будет качество атрибуции. Чем выше давление времени для атрибуции, тем ниже будет качество. Чем более опытен оппонент и располагает большим финансированием, тем ниже будет качество атрибуции.[64]

Сегодня вопрос не столько в том, *можно ли* атрибутировать кибератаку, сколько в том, *сколько времени* это займет.[65] Пока все кибератаки следуют шаблону Cyber-Kill-Chain [66] и подразумевают участие человека-противника, будут ошибки, индивидуальные мотивы и отношения, которые сделают возможным отслеживание, противодействие и сдерживание.[67] Этот факт вызывает еще одну параллель с ядерным веком. Работать с людьми нельзя виртуально или из-за компьютера. Лучший способ приписать атаку после того, как она произошла, – это уже иметь развернутую разведывательную кампанию инфильтрации и создания доверенных контактов на месте.[68] Эти довольно традиционные методы агентурной разведки (HUMINT) снова становятся важными и могут опередить предпочитаемые в последнее время и

---

[64] Rid and Buchanan, “Attributing Cyber Attacks,” 32.

[65] Tim Maurer, “Here’s How Hostile States Are Hiding behind ‘independent’ Hackers,” *The Washington Post*, February 1, 2018, www.washingtonpost.com/news/monkey-cage/wp/2018/02/01/heres-how-hostile-states-are-hiding-behind-independent-hackers.

[66] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” *Leading Issues in Information Warfare & Security Research* 1, no. 1 (2011): 1–14, 5, www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[67] “Cybersecurity’s Maginot Line: A Real-World Assessment of the Defense-in-Depth Model,” Complimentary Report (Milpitas: FireEye Inc., June 2014), www.iqpc.com/media/1003877/33776.pdf.

[68] Carr, “Responsible Attribution,” 8.

удобные методы анализа сигналов (SIGINT).[69]

Правовая база киберпространства

Подобно появлению ядерного оружия, информационная эпоха принесла с собой революционные современные технологии, которые изменили представление о МО и их правовых рамках. Некоторые даже утверждают, что эти новые технологии опередили право и что современное законодательство не может полностью регулировать возникающие кибер способности.[70,71] Но поскольку изолированные решения отдельных участников не могут работать, только международное право (МП) может обеспечить правовую основу регулирования в кибер сфере. Международное общество по-прежнему пытается понять последствия дигитализированного мира, и ему нужно время, чтобы воплотить МП в кибер-специфические договоры и обычное право. До тех пор потенциал эскалации в киберпространстве остается значительным, поскольку государства могут полагаться на свободу действий, прибегая к различным позициям в интерпретации.[72] Единственный способ уменьшить этот деструктивный потенциал – обеспечить стабильную и приемлемую правовую основу.

В 2013 году Группа правительственных экспертов ООН согласилась с тем, что международное право – и, в частности, Устав ООН – применимо в кибер сфере.[73] Эта новаторская позиция всемирно признанного органа стала первым важным шагом к заполнению законодательного вакуума в киберпространстве. Она сопровождалась выпуском «Таллиннского руководства по

---

[69] Clarke and Knake, *Cyber War: What It Is*, 215.

[70] Это становится актуальным в контексте «презумпции законности» международного права, согласно которой действия, которые не запрещены, разрешены. Поскольку современные информационные технологии прямо не рассматриваются в международном праве, у государств есть большая свобода действий до тех пор, пока существующие пробелы не закрываются обычным правом или явными договорами. См. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York, NY: Cambridge University Press, 2016), 51, Rule 11.9.

[71] Michael N. Schmitt, "The Law of Cyber Targeting," Tallinn Paper No. 7 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/uploads/2018/10/TP_07_2015.pdf.

[72] Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," Tallinn Paper No. 5, Special Expanded Issue (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014), https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf.

[73] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (United Nations General Assembly, 2015), 12, https://digitallibrary.un.org/record/799853.

международному праву, применимому к кибервойне», а в 2017 году – Таллиннским руководством 2.0, которые были подготовлены как необязывающие исследования под руководством Совместного центра НАТО передового опыта по кибер защите (CCDCOE).[74] ЕС даже пошел дальше этого мнения, заявив в своей Стратегии кибербезопасности, что «те же законы и нормы, которые применяются в других сферах нашей повседневной жизни, применяются также и в киберсфере».[75]

Соответственно, для всех государств правила поведения в киберпространстве определяются условиями МП, и для нахождения эффективной и надежной позиции сдерживания необходимо прояснить следующие моменты:

- Как классифицировать кибератаку в соответствие с международным правом?
- Какая реакция на кибератаку является законной?
- Какие цели являются законными при обмене кибер атак?

Классификация кибератак в соответствие с международным правом

В Таллиннском руководстве 2.0 сказано, что «принцип государственного суверенитета применяется в киберпространстве», и, таким образом, государство может принимать все меры, не запрещенные МП, которые оно считает необходимыми и подходящими для работы со своей кибер-инфраструктурой, с участниками киберпространства или с кибер-деятельностью на своей территории.[76,77] Следовательно, любая враждебная кибероперация, направленная против кибер и не кибер-инфраструктуры государства, означает нарушение суверенитета в случае причинения физического вреда или травм.[78] Не так обстоят дела, если при атаке происходит манипулирование или удаление баз данных с целью подорвать экономику или повлиять на политические процессы. Хотя некоторые теоретики требуют включения этих

[74] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/.

[75] Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace (Brussels: European Union, 2013), 3, https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en.

[76] Michael N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York: NATO Cooperative Cyber Defence Centre of Excellence, 2017), 11.

[77] Cited in Jasper, *Strategic Cyber Deterrence*, 142.

[78] Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law*, 54, (2014): 697-732.

нефизических эффектов, они все еще выходят за рамки общей интерпретации.[79]

Кибероперации не являются кинетическими по своей природе и поэтому часто ошибочно воспринимаются как несиловые, хотя их последствия могут варьировать от простого беспокойства до причинения смерти. Таким образом, кибератаки необходимо оценивать в соответствии с их воздействием на реальный мир и, если они имеют результат, сопоставимый с кинетической атакой, они представляют собой «применение силы».[80,81] Однако государству разрешается проводить силовые защитные действия только в случае «вооруженного нападения», что означает, что применение силы должно достигнуть определенного порога.[82,83] Этот уровень иногда сохраняется в состоянии стратегической двусмысленности, чтобы противнику было сложнее прогнозировать потенциальные действия самообороны.[84] Таллиннское руководство 2.0 становится конкретным только для актов сбора кибер разведданных, кибер-кражи и кратковременного прерывания несущественных услуг, которые не квалифицируются как вооруженные нападения из-за отсутствия серьезных травм или смертей или причинения серьезного

---

79 Michael N. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," *Villanova Law Review* 56, no. 3 (2011): 569-605, 574; Schmitt and Vihul, "The Nature of International Law Cyber Norms," 17.

80 Устав ООН запрещает применение силы или угрозу силой, требуя: «все члены должны воздерживаться в своих международных отношениях от угрозы силой или ее применения против территориальной целостности или политической независимости любого государства или любым другим способом, несовместимым с целями Объединенных наций». См. United Nations, "Charter of the United Nations" (United Nations, 2016), Article 2 (4).

81 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 573.

82 Это также может иметь место, если серия киберинцидентов (каждый из которых по отдельности находится ниже порога вооруженной атаки) суммируется. Следовательно, они должны иметь один и тот же источник, должны быть связаны друг с другом и, вместе взятые, должны иметь необходимый масштаб. См. Schmitt, *Tallinn Manual on the International Law*, 56, Rule 13.8.

83 United Nations, "Charter of the United Nations," Article 51.

84 В соответствии с этим, на саммите НАТО в Уэльсе в 2014 году было решено определять, приведет ли кибератака к применению статьи 5 (и таким образом, будет считаться вооруженным нападением) в каждом конкретном случае. См. See Schmitt and Vihul, "The Nature of International Law Cyber Norms," 26. По мнению Lewis, "Rethinking Deterrence," 9, эта стратегическая двусмысленность пороговых значений создает путаницу и ослабляет сдерживающий эффект. Ядерная стратегия НАТО «Гибкое реагирование», напротив, держала свою лестницу эскалации в стратегической двусмысленности (понимая, что способности были известны в любом случае), но делала красные линии очень четкими. См. Kenyon and Simpson, *Deterrence and the New Global Security Environment*.

ущерба.[85,86] Для атак, которые не достигают порога вооруженного нападения, но представляют собой незаконное применение силы, могут применяться только контрмеры, направленные на прекращение нападения.[87] Если применение силы сводится к вооруженному нападению, осуществляемому с помощью классической военной силы, которое вызывает или может привести к уничтожению имущества и ранениям или смерти, тогда разрешаются силовые оборонительные действия. Если кибероперация является составной частью общей военной операции, она представляет собой вооруженное нападение, даже если в отдельности не может быть квалифицирована как таковое.[88] Следовательно, у государств есть стимул быстро рассматривать чистые кибероперации как вооруженное нападение, чтобы оправдать силовой оборонительный ответ, что значительно увеличивает вероятность эскалации.[89]

Законные меры реагирования на кибератаки

Государство, ставшее жертвой незаконной кибероперации, имеет определенные права в соответствии с международным правом, если атака достигает как минимум уровня применения силы. Это всегда начинается с законного требования компенсации за физические или финансовые потери и с ненасильственных ответных действий, таких как блокирование входящей передачи данных. Кроме того, в ответ на выявленное применение силы могут быть приняты типичные технические, политические или экономические контрмеры, направленные на прекращение и возмещение ущерба. Эти меры могут включать ограниченную степень применения военной силы и обычно противоречат международным обязательствам, но являются закон-

---

85 Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law*, 339.

86 Цитируется в Jasper, *Strategic Cyber Deterrence*, 142.

87 Таллиннское руководство 2.0 гласит в правиле 20, что государства имеют право принимать контрмеры (кибермеры или не кибермеры) в ответ на нарушение международно-правовых обязательств другим государством. Правило 69 гласит, что кибероперация представляет собой применение силы, если они имеют сопоставимые эффекты, такие как операции, не связанные с киберпространством, которые можно квалифицировать как применение силы. Контрмеры в этом случае могут быть направлены только на устранение существующего ущерба, пока существует угроза, а не на цели возмездия. Кроме того, противник должен быть предупрежден заранее, чтобы дать ему возможность прекратить атаку. См. Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law*, цитируется в Jasper, *Strategic Cyber Deterrence*, 174.

88 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 587.

89 Подход США в этом вопросе несет в себе именно эту опасность, но кажется эффективным на кибер-арене, поскольку любое использование силы рассматривается как вооруженное нападение и может подвергаться силовому ответу. См. Schmitt, "'Below the Threshold' Cyber Operations," 730.

ными, если они соразмерны нанесенному ущербу и ниже порога вооруженного нападения. Однако необходимо заранее призвать противостоящее государство воздерживаться от продолжения или принять меры для прекращения действий, исходящих с его территории.[90,91] Право принимать контрмеры сохраняется за государствами, даже если существуют частные ИТ-компании, чьи кибер-возможности превышают арсенал государства. Тем не менее, Таллиннское руководство 2.0 прямо упоминает право потерпевшего государства обращаться к частным фирмам для проведения кибероперациий от его имени. Конечно, ответственность за контрмеры, проводимые капером, лежит на государстве.[92,93]

Если применение силы достигает уровня вооруженного нападения (независимо от того, было ли оно инициировано государством или негосударственным субъектом), применяется право на самооборону, и могут проводиться необходимые и соразмерные силовые действия против атакующего противника.[94] Поскольку нет международного консенсуса относительно границы между применением силы и вооруженным нападением, это становится вопросом интерпретации и убедительности потерпевшего государства, поскольку МП не диктует уровень достоверности атрибуции, чтобы начать действия в целях самообороны.[95] Возникает вопрос, как реагировать на действия негосударственных субъектов, которые, по определению, не могут нарушать запрет на применение силы по международному праву, установленный для государств. В таких случаях ответственность государства предлагает возможность в любом случае применить МП. Государство несет ответственность не только за действия своих правительственных органов, но и за поведение отдельных лиц или групп, которые действуют по указанию или под контролем государства.[96] Более того, государство может быть привлечено к ответственности за противоправные действия негосударственных субъектов на его территории, если оно не принимает надлежащих мер для прекращения атак или не предоставляет всю доступную

---

[90] Schmitt, *Tallinn Manual on the International Law*, 36, Rule 9.

[91] Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 581.

[92] Schmitt, "'Below the Threshold' Cyber Operations," 727.

[93] Jasper, *Strategic Cyber Deterrence*, 179.

[94] Schmitt, *Tallinn Manual on the International Law*, 54, Rule 13.

[95] Carr, "Responsible Attribution," 7.

[96] Международный Суд (ICJ) создал прецедент решением по делу Никарагуа, в котором он признал США ответственными за нарушения международного гуманитарного права, совершенные повстанческой группировкой, которую США «эффективно контролировали». См. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 578.

поддержку для расследования инцидентов.[97,98] Если такое государство не желает или неспособно выполнять свои юридические обязанности, пострадавшее государство может действовать в порядке самообороны и остановить атаку кинетическими или кибер-средствами даже на территории другого государства. Но самооборона возможна не только в ответ на продолжающееся вооруженное нападение. Ее также можно проводить в условиях неминуемой атаки (о чем свидетельствуют враждебные действия, такие как подготовительные кибероперации, которые приведут к последствиям на уровне вооруженной атаки), без какой-либо другой разумной надежды на ее отражение, кроме немедленного ответа.[99]

Законные цели при обмене кибератаками

Если ситуация доходит до того, что силовая самооборона или возмездие становится законным вариантом, возникает вопрос о том, как и что атаковать. Киберсфера характеризуется повсеместной инфраструктурой двойного назначения, которая может быть предназначена для использования в гражданских целях, но по характеру, местоположению, назначению или применению может использоваться в военных целях.[100] Поэтому, в соответствии с международным гуманитарным правом (МГП) эта инфраструктура становится законной военной мишенью, поскольку ее полное или частичное разрушение, захват или нейтрализация предлагает прямое и конкретное военное преимущество. В конечном итоге, это означает, что из-за сильной зависимости от гражданских продуктов и гражданской инфраструктуры, диапазон целевых объектов на кибер-арене расширяется, и системы с важными гражданскими функциями могут стать законным объектом воздействия.[101] В случае силового ответа в обмене кибератак это дает определенную гибкость в выборе целей, но, в то же время, кибер-средства сталкиваются с проблемой сложной масштабируемости и специфического выбора мишеней. МГП требует, чтобы применяемое оружие позволяло отличать комбатантов от гражданских лиц и гражданских объектов от военных. Если кибероружие не может быть направлено на конкретный военный объект

[97] Международный Суд создал прецедент в деле о проливе Корфу, приняв решение о том, что государство нарушает свои международные обязательства, если оно позволяет сознательно использовать свою территорию для противоправных действий против других государств. См. Schmitt, “Cyber Operations and the *Jus Ad Bellum* Revisited,” 578.

[98] Goodman, “Cyber Deterrence,” 108.

[99] Schmitt, “Cyber Operations and the *Jus Ad Bellum* Revisited,” 592.

[100] Это могут быть системы управления воздушным пространством или линии связи, которые частично используются в военных целях.

[101] Schmitt, “The Law of Cyber Targeting,” 11.

или создает неконтролируемые последствия, его применение запрещено.[102] Эти ограничения не применяются к защитным мерам и к ненасильственным средствам, таким как вредоносные программы, которые не вызывают травм, повреждений или потери функциональности систем, даже если они могут распространиться на гражданские системы.[103] Если в кибератаке участвуют некомбатанты, не связанные с организованной вооруженной группой и не находящиеся под контролем государства, они могут стать целью на время, пока они принимают непосредственное участие во враждебных действиях. В киберпространстве такое участие может начаться со сбора и распространения военной разведывательной информации с помощью кибер-средств, зондирования систем противника для выявления уязвимостей или разработки программного обеспечения, предназначенного для атак.[104]

Применение сдерживания в кибердомене

При рассмотрении опыта, накопленного с основными механизмами сдерживания, и с учетом особых последствий и правовых характеристик кибердомена, становится ясно, что киберсдерживание не может применяться изолированно, но должно быть одним из жизненно важных компонентов всеобъемлющей стратегии безопасности.[105,106] В отличие от ядерных концепций, защита и устойчивость являются фундаментальной отправной точкой для лишения противника шансов на успех.[107] Помимо *воспрещения* посредством обороны, важную роль как сдерживающий фактор играет классический аспект *возмездия*, как угроза наказания. Поскольку это исследование основано на более широком понимании сдерживания, в центре внимания находятся еще два пути: сдерживание путём *обвязывания* и установление *нормативных табу*.[108]

Сдерживание воспрещением

Сосредоточение внимания на обороне становится все более важным, поскольку число потенциальных противников государства с наступательными

[102] Несмотря на это, если кибероружие является альтернативой кинетическому оружию и оказывает аналогичное воздействие на противника, его следует предпочесть, поскольку в большинстве случаев сопутствующий ущерб менее вероятен, см. Schmitt, “The Law of Cyber Targeting,” 18.

[103] Schmitt, “The Law of Cyber Targeting,” 16.

[104] Schmitt, “The Law of Cyber Targeting,” 14.

[105] Nye, “Deterrence and Dissuasion in Cyberspace,” 46.

[106] Cooper, “A New Framework for Cyber Deterrence,” 105.

[107] Carberry, “Why There’s no Silver Bullet for Cyber Deterrence.”

[108] Nye, “Deterrence and Dissuasion in Cyberspace,” 54.

кибер-возможностями постоянно растет.[109] Сдерживание посредством воспрещения направлено на повышение устойчивости и способности восстанавливаться. Таким образом, выгоды от атаки для противника могут быть уменьшены до такого уровня, что нападение станет бесполезным, а после удара можно будет гарантировать, что имеются кибер- и некибер военные ответы для возмездия. Существуют методы различной изощренности и с разными затратами,[110] но все они имеют общую цель – съедать ресурсы и время противника и нарушать его расчет предполагаемой вероятности и ценности выигрыша.[111,112] Согласно «парадигме предполагаемого прорыва», невозможно предотвратить успешное проникновение в чьи-либо сети. Но использование уязвимостей можно сделать сложным и утомительным. Тогда нападающий издает больше «шума», ему требуется больше времени, и его становится легче идентифицировать, поскольку он оставляет больше следов.

На пути к культуре устойчивости жизненно важную роль играют публично-частное партнерство (ПЧП) и обеспечение кибер страховок. ПЧП объединяют, с одной стороны, государство (как законодателя с богатыми ресурсами рабочей силы, которая ориентирована не на прибыль, а на результативность, и может полагаться на разведывательные службы) с частными лицами, ориентированными на эффективность (которые обладают большим опытом и технически специализируются в кибернетической области, где они имеют доступ к большому количеству данных и информации).[113] С другой стороны, обязательное обеспечение кибер страховок в экономике способствует повышению системной устойчивости и предотвращению того, что экономика страны может подвергнуться угрозе. Установление цены на различные частные кибер практики порождает стимул к более высоким

---

[109] The Worldwide Threat Assessment of the US Intelligence Community shows a rise from probably three states in 2007 to over 30 states in 2017. См. Daniel R. Coats, “Worldwide Threat Assessment of the US Intelligence Community” (Washington D.C.: Director of National Intelligence, February 2018), 6, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[110] Примером сложных и дорогостоящих мер является накопление резервных промышленных генераторов энергии и трансформаторов. Пример простых и дешевых мер: обучение военных астронавигации на случай потери систем глобального позиционирования. См. Nye, “Deterrence and Dissuasion in Cyberspace,” 56.

[111] Nye, “Deterrence and Dissuasion in Cyberspace,” 56.

[112] Jasper, *Strategic Cyber Deterrence*, 111.

[113] Правительство США подчеркивает этот подход в своей Стратегии национальной безопасности: «В соответствии с принципами защиты гражданских свобод и неприкосновенности частной жизни правительство США расширит сотрудничество с частным сектором, чтобы мы могли лучше обнаруживать и атрибутировать атаки». См. *National Security Strategy of the United States of America* (Washington D.C.: The White House, 2017), с. 13, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

стандартам и к соблюдению «элементарной кибергигиены» там, где противник может срывать низко висящие фрукты и быстро добиваться успеха.[114] Более того, создание отчетов и систематизирование данных, связанных с атаками, можно значительно улучшить за счет получения выгоды от комплексных центров и процессов кризисного реагирования в страховой отрасли.[115] Таким образом, информационная асимметрия между частниками и правительством может быть наконец уменьшена, время реакции может быть увеличено, и может быть обеспечена основа для создания культуры обмена информацией, основанной на доверии. Чтобы дополнительно стимулировать частно-государственное сотрудничество, необходимо внедрить «соглашения об ответственном раскрытии информации»[116] и «временные допуски».[117]

Дальнейшие отправные точки для повышения устойчивости и способности к восстановлению можно найти в самой структуре защиты. Недостаточно защитить только внешние периметры системы. Поскольку взлом возможен в любое время, существуют меры для глубокой защиты, способные обнаружить злоумышленника внутри системы, отследить, идентифицировать и побеспокоить его. Такой подход может поддерживаться сегментированными сетями и сегментированными секторами, которые не позволяют, когда злоумышленник проник внутрь, получить доступ ко всей системе. На первый взгляд, сохранение жизненно важных способностей посредством дублирования может быть дорогостоящим, но значительно снижает вероятность получения выигрыша для противника. Наконец, необходима защита цепочки поставок, чтобы избежать проникновения противника. Это

---

[114] При соответствующем обучении для повышения осведомленности пользователей можно избежать до 50 % инцидентов. См. “ENISA Threat Landscape Report 2016” (Heraklion: European Union Agency for Network and Information Security, 2017), 81, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport.

[115] Umar Choudhry, *Der Cyber-Versicherungsmarkt in Deutschland: Eine Einführung* (Wiesbaden: Springer, 2014).

[116] Соглашение между специалистом по поиску уязвимостей и производителем программного обеспечения о соблюдении крайнего срока публикации. Поисковик избегает риска быть ответственным за использование уязвимости, производитель получает необходимое время для анализа и исправления уязвимости, а пользователь может полагаться на тот факт, что исправления не продолжаются больше, чем необходимо. См. *Die Lage der IT-Sicherheit in Deutschland 2017* (Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2017), с. 21, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf.

[117] Ограниченно по времени, связанное с конкретным делом, приостановление ограничения доступа спецслужбами для оперативной группы, чтобы обеспечить эффективный обмен информацией между агентствами и привлеченными частниками.

требует интенсивного обсуждения вопросов встроенной при проектировании безопасности с последующей проверкой производителей и поставщиков услуг и оценкой того, какие части критически важных цепочек поставок должны находиться под национальным контролем.

Сдерживание путем воспрещения – это больше, чем просто отражение кибератаки. Проводимое комплексно, оно может повысить влияние фактора времени и фактора выживания, восстановить значение фактора силы и обеспечить основу для фактора атрибуции, на основе которого становится возможным возмездие. При надлежащем коммуникировании способности защиты государства могут значительно повлиять на расчет оппонента в отношении ценности и вероятности выигрыша, а также дать правительству свободу действий для реагирования на основные угрозы в киберпространстве.[118]

Сдерживание возмездием

Ответить на нежелательное поведение наказанием – это самый известный способ сдерживания. Цель состоит в том, чтобы пообещать нанести противнику расходы, которые перевешивают выгоды, ожидаемые от первоначальной атаки.[119] Это работает только в том случае, если атака может быть атрибутирована злоумышленнику в достаточной степени, а атрибуция адресована трем вышеупомянутым аудиториям.[120] Возмездие не обязательно должно оставаться в киберпространстве, но может принимать форму дипломатических, информационных, военных и экономических действий, адаптированных к противнику и с учетом потенциальных эффектов обратной связи из-за международной взаимозависимости.[121] Кроме того, ключевую роль играет геополитическая симметрия. Месть противнику может означать инициирование серии эскалации ответных действий за пределами киберпространства, что в конечном итоге может привести к выигрышу только в том случае, если доминирование эскалации будет на одной стороне.[122]

Меры противодействия в киберсфере могут быть самыми разнообразными и находиться на различных уровнях агрессивности.[123] За пределами

---

[118] Nye, “Deterrence and Dissuasion in Cyberspace,” 56.

[119] США «… будут применять меры с быстрыми и дорогостоящими последствиями к иностранным правительствам, преступникам и других субъектам, которые предпринимают значительные злонамеренные действия в киберпространстве». См. *National Security Strategy of the United States of America*, 13; Goodman, “Cyber Deterrence,” 106.

[120] Nye, “Deterrence and Dissuasion in Cyberspace,” 51.

[121] Jasper, *Strategic Cyber Deterrence*, 13.

[122] Goodman, “Cyber Deterrence,” 109.

[123] Как предлагается в порядке возрастания в Jasper, *Strategic Cyber Deterrence*, 177:

- разрешать злоумышленникам красть фальшивые файлы или встраивать маяки, которые показывают их местоположение;

кибердомена санкции являются наиболее распространенной реакцией на нежелательное поведение, хотя в большинстве случаев они затрагивают население государства больше, чем правительство. Поэтому более эффективным оказывается инвестировать ресурсы в выявление злоумышленников и нацеливать санкции на этих лиц.[124] Даже если имя конкретного человека не может быть названо, все же возможно направить ответные меры на отношения и социальные сети, в которых участвуют злоумышленники. Это работает, поскольку все злоумышленники связаны зависимостями, и их расчет выигрыша и потерь может быть затронут косвенно. Подозреваемые группы могут быть лишены таких привилегий, как участие в финансовом сообществе, и общественное возмущение можно использовать для внутреннего давления на преступников и даже для объявления их вне закона до такой степени, что сеть повернется против них, чтобы избежать несения ущерба.[125]

Эффективное возмездие требует использования факторов времени, силы, выживания и атрибуции в качестве основы, чтобы способствовать фактору защиты. Кинетические средства оказались эффективными инструментами государства для ответа на кибератаки. В результате могут быть выбраны как обычные военные средства, так и ядерный ответ в чрезвычайно тяжелых случаях.[126]

Сдерживание обвязыванием

Современная международная система характеризуется различными зависимостями, взаимосвязями и общими уязвимостями. Сдерживание путём

- файлы-приманки с вредоносным ПО, чтобы сфотографировать злоумышленников с помощью веб-камеры;
- инфильтрация сетей злоумышленников для извлечения, изменения или удаления украденных данных;
- внедрение вредоносных программ для повреждения или программ-вымогателей для блокировки компьютеров-исполнителей;
- вставление логических бомб в файлы перед кражей, чтобы повредить компьютеры при открытии;
- использование DDoS-атак, чтобы помешать вредоносной деятельности.

[124] Президент Обама сделал именно это, подписав Указ о блокировании собственности и интересов людей, которые вмешиваются в работу ИТ-систем критически важной инфраструктур. См. Jasper, *Strategic Cyber Deterrence*, 97.

[125] Cooper, “A New Framework for Cyber Deterrence,” 114.

[126] В недавно разработанной ядерной стратегии США прямо предусмотрена возможность ядерного возмездия за разрушительные кибератаки. См. David E. Sanger and William J. Broad, “Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms,” *The New York Times*, January 16, 2018, www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html.

обвязывания пытается поощрять ответственное поведение государства, делая упор на отдачу от сотрудничества во имя взаимных интересов.[127] Если атака имеет отрицательный сопутствующий эффект для атакующего и способствует статус-кво и его продолжению, злонамеренное взаимодействие теряет привлекательность. Связанность усиливает значение факторов выживания и глобализации, а также увеличивает восприятие противником ценности выигрыша и вероятности потерь, даже если от атаки активно не защищаются или нет страха возмездия. Эффект сдерживания зависит от сложных международных отношений сдерживания и работает лучше, когда взаимозависимость сильнее.[128]

Для усиления эффекта связанности подходящим инструментом являются меры укрепления доверия для укрепления международного мира и безопасности за счет расширения межгосударственного сотрудничества, прозрачности, предсказуемости и стабильности.[129] В киберпространстве возможными вариантами являются горячие линии связи, региональные центры связи, предварительные уведомления и соглашения о неприменении атак на конкретные цели, которые могут быть дополнены криминалистической помощью в случае ИТ-инцидентов и соглашениями о невмешательстве в работу групп реагирования на компьютерные чрезвычайные ситуации. Только установление режима контроля над кибероружием сталкивается с некоторыми трудностями. Большинство технологий, которые можно охарактеризовать как кибероружие, имеют двойное назначение (например, программы оценки уязвимости, которые могут либо найти бреши в безопасности для защиты системы, либо для ее использования), и в результате нет единого мнения о том, что такое кибер- оружие действительно.[130] Кроме того, проверка арсеналов кибероружия практически невозможна, поскольку это оружие нельзя потрогать и оно может быть легко спрятано или воссоздано после удаления.[131] Чтобы решить эту проблему, необходимо обращать внимание на «последствия», а не на «использованное оружие».[132] Кроме того, могут быть установлены нормативные табу, что является последним из четырех способов киберсдерживания.

---

[127] Jasper, *Strategic Cyber Deterrence*, 16.

[128] Китай, который выводит легитимность своей правящей партии из экономического роста, и таким образом, зависит от Интернета, гораздо больше связан с западным миром, чем довольно изолированная Северная Корея. См. Nye, “Deterrence and Dissuasion in Cyberspace,” 58.

[129] Jasper, *Strategic Cyber Deterrence*, 150.

[130] Jasper, *Strategic Cyber Deterrence*, 16.

[131] Nye, “Deterrence and Dissuasion in Cyberspace,” 60.

[132] Goodman, “Cyber Deterrence,” 116.

Сдерживание с использованием нормативных табу

При установленных строгих нормах, агрессивный субъект несет репутационные потери, которые вредят его мягкой силе, превышающие выигрыши, полученные от атаки. Если государство нарушает табу (например, использует ядерное оружие в незначительном конфликте против более слабого государства), оно сталкивается с опасностью подвергнуться остракизму со стороны международной системы. Этот эффект сдерживания работает, хотя нет активной защиты или гарантированного возмездия, но требует определенной степени достоверности атрибуции. Исторически сложилось так, что международное сообщество согласовало несколько подразумеваемых и явных норм, таких как запрет химического и биологического оружия в Женевской конвенции.[133]

В киберпространстве первым важным шагом стало принятие нормативного соглашения о применимости международного права и Устава Организации Объединенных Наций. В 2013 году «Группа правительственных экспертов ООН по развитию в области информации и телекоммуникаций в контексте международной безопасности» предложила базовые нормы, такие как выполнение международных обязательств в случае, если противоправное деяние приписывается государству, отказ от использования прокси субъектов и недопущения использования негосударственными субъектами территории государства для совершения противоправных действий.[134] Кроме того, мощной нормой для сдерживания и коммуникирования предупреждающего послания может быть использование международных трибуналов и Международного уголовного суда для преследования киберпреступников, террористов и государственных акторов.[135] Нормы, связанные с киберпространством, могут направлять поведение государства и повышать предсказуемость, доверие и стабильность в киберпространстве, а также снижать вероятность конфликта из-за неправильных восприятий. Это работает только в том случае, если нормы принимаются большинством государств и со временем институционализируются, например под эгидой ООН.[136] Нормативные табу могут в определенной степени способствовать контролю над кибероружием, даже если установить режим контроля над

[133] Хотя это табу не помешало Башару аль-Асаду использовать химическое оружие против своего населения, международная реакция (уничтожение сирийского химического оружия в 2014 году и ответные удары США в 2018 году) отразила возросшие затраты на нарушение нормативного табу. См. Nye, “Deterrence and Dissuasion in Cyberspace,” 60.

[134] Jasper, *Strategic Cyber Deterrence*, 17.

[135] Quinlan, “Deterrence and Deterrability,” 8.

[136] Jasper, *Strategic Cyber Deterrence*, 145.

кибероружием невозможно. Они должны быть направлены на табуированные результаты и цели, и таким образом, помогать различать, какое поведение терпимо, а какое подвергается остракизму.[137]

Заключение

Становится очевидным, что основные механизмы сдерживания работают во всех сферах, в том числе и в киберпространстве. Тем более, что ядерное сдерживание теряет актуальность в МО, а текущие конфликты все больше характеризуются кибер-компонентами, необходимость во всестороннем понимании киберсдерживания неоспорима. Более того, было показано, что пять основных факторов (времени, силы, выживания, глобализации, защиты) новой технологии, меняющей правила игры, такой как атомная бомба, могут быть адаптированы к киберпреступности. Кроме того, в киберпространстве решающую роль играет атрибуция, и ее необходимо добавить в обсуждение. Стало ясно, что международная система все еще находится на ранней стадии применения МП в киберпространстве и что законодательство должно пройти долгий путь, чтобы догнать технологические разработки.

Выведенные четыре способа применения сдерживания в кибербезопасности (воспрещение, возмездие, связанность и нормативные табу) обеспечивают реальный подход к интеграции аспектов киберсдерживания в стратегию кибербезопасности государства (зная, что киберсдерживание может быть только одним из столпов) общей стратегии безопасности). Однако эти способы никогда не работают изолированно, а скорее в комплексном пакете с переменным весом отдельных элементов.[138] Благодаря соблюдению основных механизмов сдерживания и адаптации их пакета к конкретным субъектам угрозы, универсальное и надежное сдерживание становится возможным.

Таким образом, высказанная в этой работе гипотеза может быть подтверждена: *даже в кибер-веке сдерживание может быть мощным инструментом государства и способствовать защите интересов национальной безопасности государства!*

Тем не менее, эффективное сдерживание не возникает само по себе. Над ним нужно осуществлять стратегический менеджмент, иначе его последствия нельзя будет контролировать. Политики и стратеги всего мира должны подготовиться к новой и требовательной эпохе сдерживания, чтобы избежать превращения лунатизма в настоящую кибервойну.

В следующей статье полученные результаты будут применены к примеру Германии. Будет объяснено, как Германия, как важный игрок во все

[137] Nye, “Deterrence and Dissuasion in Cyberspace,” 60.

[138] Например, против довольно изолированной Северной Кореи связанность не может быть основной частью стратегии, тогда как против могущественной России связанность играет гораздо большую роль, чем возмездие.

более дигитализированной международной системе, может подойти к стратегии киберсдерживания, чтобы поддержать свои интересы национальной безопасности.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Мануэль Фишер – профессионал в области безопасности, работающий в оборонном секторе Германии и специализирующийся на решениях по борьбе с БПЛА. Он имеет двенадцать лет службы в немецкой армии (Бундесвере) в качестве офицера военной полиции. За это время он получил степень магистра экономики и организационных наук в Университете Федеральных вооруженных сил в Мюнхене. После службы в армии он учился в Европейском центре исследований по вопросам безопасности им. Джорджа Маршалла, где окончил магистерскую программу исследований в области международной безопасности, посвященную кибербезопасности.
E-mail: fischermanuel@web.de.

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Т. Малярчук, Ю. Данык & Ч. Бриггс
Connections QJ 18, № 1-2 (2019): 110-129
https://doi.org/10.11610/Connections.rus.18.1-2.06

Рецензированная статья

Гибридная война и кибер воздействия на энергетическую инфраструктуру

***Тамара Малярчук,*[1] *Юрий Данык*[2] *и Чад Бриггс*[3]**

[1] *Житомирский государственный университет им. Ивана Франко, https://zu.edu.ua/en_index.html*

[2] *Национальный технический университет Украины «КПИ им. Игоря Сикорского», https://kpi.ua/en*

[3] *Университет Аляски, Анкоридж, США, https://www.uaa.alaska.edu/*

Резюме: Энергия – неотъемлемая часть всех отраслей экономики и социальной сферы, играющая особую роль в обеспечении безопасности развития современного общества. Поэтому энергетическая инфраструктура стала важнейшим компонентом гибридной войны. Деструктивный кибер шантаж в ней, как правило, сопровождается цепными и синергетическими эффектами, которые систематически оказывают влияние и охватывают все остальные сферы жизни общества и государства как в обычных, так и в особенно критических условиях. Авторы систематически и всесторонне проанализировали и представили в статье результаты исследований особенностей деструктивных кибер воздействий в национальной энергетике Украины и способов противодействия и защиты критической энергетической инфраструктуры.

Ключевые слова: гибридная война, энергетический комплекс, энергетическая инфраструктура, кибербезопасность, кибератака.

Введение

Дискуссии о гибридной войны часто концентрировались на дебатах об определениях точной природы термина и о том, охватывает ли термин «гибридная» то, что другие военные эксперты называют нелинейной войной,

войной полного спектра, войной четвертого поколения или другими подобными терминами. Точно так же при обсуждении киберконфликтов это явление рассматривалось как отдельная область, как если бы использование кибер-инструментов оставалось отличным от других форм конфликта. Гибридная война, которая *де-юре* ведется на территории Украины и *де-факто* охватывает большее количество участников со всего мира, по своему содержанию, формам и методам ведения может рассматриваться как специфический вариант четвертого поколения войны (4GW).

В гибридных конфликтах любой интенсивности боевые действия (операции) являются элементом других (несиловых) действий, взаимно скоординированных по единому плану, в основном экономического, политического, дипломатического, информационного, психологического, кибернетического, когнитивного и др. характера.[1] Это порождает дестабилизирующие внутренние и внешние процессы в государстве, являющемся объектом агрессии, такие как беспокойство и недовольство населения, миграция и акты гражданского неповиновения. Гибридные войны не объявляются и, следовательно, не могут быть завершены в классическом понимании окончания войн и военных конфликтов. Это своего рода перманентная война переменной интенсивности в нескольких секторах, с каскадными воздействиями и синергетическими деструктивными проявлениями, в которую в определенной степени сознательно или неосознанно вовлечено все население страны и международное сообщество. Воздействие ощущается во всех сферах жизни, во всех слоях общества и во всем государстве. Благодаря использованию инновационных технологий стало возможным переключить конфликт с преимущественно открытых и силовых (кинетических) средств на менее очевидные стратегии, ориентированные на структурную уязвимость противников, включая (что важно) достижение когнитивного преимущества над ними.

Применительно к событиям на Украине с 2013 года основное внимание часто уделялось вторжению России в Крым в 2014 году и последующему содействию поддерживаемым Россией анклавов в восточных украинских регионах Донбасса и Луганска. Эти операции – от появления так называемых «зеленых человечков» в Симферополе до крушения рейса № 17 Малазийских авиалиний несколькими месяцами позже – сфокусированы на довольно обычных (хотя и нерегулярных) формах конфликта. Часто упускаются из виду более широкие стратегические цели противника при проведении кампании гибридной войны и широкий спектр инструментов, используемых для достижения этих целей.

Как считают многие авторы, гибридная война – явление не новое, поскольку она представляет собой скоординированные действия как государственных, так и негосударственных субъектов по проведению кампании

[1] Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, “Hybrid War: High-tech, Information and Cyber Conflicts,” *Connections: The Quarterly Journal* 16, no. 2 (2017): 5-24, https://doi.org/10.11610/Connections.16.2.01.

действий, которые варьируют от информационной войны до прямого кинетического конфликта.[2] Стратегия Российской Федерации в отношении Украины после Майдана в основном направлена на дестабилизацию и делегитимацию правительства, что является частью усилий по предотвращению интеграции Украины с западноевропейскими институтами и предотвращению эффективного вмешательства со стороны западных стран или стран НАТО. Хотя оккупация Крыма и продолжающийся конфликт на востоке Украины служат этой цели, был предпринят более широкий, но менее заметный набор действий, направленных на эрозию устойчивости украинских институтов. Вместо того, чтобы сосредотачиваться на самой гибридной войне или киберсфере как отдельного домена враждебных действий, цель этой статьи – проиллюстрировать и объяснить использование кибероружия против энергетической инфраструктуры.

Опять же, хотя это и не новая стратегия, осуществляемая повстанцами или кампаниями стратегических бомбардировок, нацеливание на энергетическую инфраструктуру является эффективным способом повышения уязвимости государства или общества, одновременно давая сигнал другим потенциальным противникам об их собственной уязвимости и возможностях наносить ущерб крупным отраслям их экономики. Кибер-инструменты обеспечивают асимметричное преимущество без учета географического расстояния, а это означает, что небольшие группы могут наносить широкомасштабный ущерб, избегая при этом обычной атрибуции и правил сдерживания.[3] Во время Холодной войны Соединенные Штаты проводили гибридные операции в таких странах, как Филиппины в начале 1950-х годов и Вьетнаме в 1960-х годах, используя целый ряд методов – от создания газет и радиостанций до поддержки повстанцев и наемников и активного участия боевых частей США. Опыт США может быть поучительным, поскольку он иллюстрирует две очень разные стратегические цели при использовании гибридных методов – либо попытки стабилизировать, либо дестабилизировать иностранный режим. В то время как в некоторых случаях, например на Филиппинах, усилия по стабилизации были в значительной степени успешными, в ряде примеров от Вьетнама до Афганистана, США добились гораздо меньшего успеха в своих усилиях по стабилизации. С другой стороны, дестабилизация, по-видимому, является более успешным применением методов

[2] Robert Wilkie, “Hybrid Warfare: Something Old, Not Something New,” *Air and Space Power Journal* 23, no. 4 (Winter 2009): 13-18; NicuPopescu, “Hybrid Tactics: Neither New Nor Only Russian,” *EUISS Issue Alert* 4 (European Union Institute for Security Studies, January 2015), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf.

[3] Dinos Kerigan-Kyrou, “Critical Energy Infrastructure: Operators, NATO, and Facing Future Challenges,” *Connections: The Quarterly Journal* 12, no. 3 (Summer 2013): 109–17, http://dx.doi.org/10.11610/Connections.12.3.06.

гибридной войны, как, например, в контролируемых США действиях в Центральной Америке и Чили, или в Иране в 1953 году.[4]

Для целей этой и последующих статей гибридная война определяется как полное использование государственных и негосударственных инструментов для изменения стабильности и легитимности ключевых систем и институтов в данном регионе. Обратите внимание, что теоретически это означает, что методы гибридной войны могут использоваться в законных целях, а также для дестабилизации, и это часто делается при атаке противника и одновременной поддержке своего государства и союзников / прокси-субъектов. В то время как двойное использование гибридных инструментов не так очевидно в энергетическом секторе, эта статья является одной из серии, в которой также исследуется социальная устойчивость и роль иностранного вмешательства (например, отношения Европейского Союза с Украиной), где играть несколько ролей становится все более важным, и где кибер-методы затрудняют отслеживание этих усилий. Энергетическая инфраструктура и кибератаки – удачное место для начала исследования из-за существующей истории атак и сходства между государствами в их потребности защищать источники энергии и их уязвимости для кибер-инструментов.

Такими возможностями располагает не только Россия. Червь Stuxnet (приписываемый, возможно, Израилю и США) эффективно наносил физический ущерб центрифугам с ядерным топливом, не подключенным к какой-либо внешней сети и рассматриваемым иранцами как безопасные в отношение внешнего вмешательства или нападения. Stuxnet был элегантной программой, которая могла легко перемещаться без обнаружения с компьютера на компьютер, не причиняя вреда и не вмешиваясь в работу какой-либо системы, пока, наконец, не нашла свой путь к конкретным центрифугам с компьютерным управлением в Иране. Оказавшись там, червь вносил небольшие изменения в работу высокоскоростных машин, сдвигая калибровку ровно настолько, чтобы повредить или уничтожить их, не вызывая подозрений, что происходит внешняя атака.[5] Точно так же Китай и даже более мелкие государства, такие как Северная Корея, обладают антиэнергетическим кибер-потенциалом, а заметный потенциал кибератак против энергетики также продемонстрировали такие негосударственные субъекты, как Аль-Каида и ИГИЛ.[6]

---

[4] Max Boot, *The Road Not Taken: Edward Lansdale and the American Tragedy in Vietnam* (New York: Liveright Publishing, 2018).

[5] Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy* 9, no. 3 (May-June 2011): 49-51.

[6] Lukáš Tichý and Jan Eichler, "Terrorist Attacks on the Energy Sector: The Case of Al Qaeda and the Islamic State," *Studies in Conflict & Terrorism*, 41:6 (2018): 450-473, https://doi.org/10.1080/1057610X.2017.1323469.

Концепция устойчивости

Как писали Конклин и Конке, большая часть кибербезопасности была построена вокруг концепции «ограждения» компьютерных систем от внешних злоумышленников и вокруг защиты данных, а не на сосредоточении внимания на устойчивости системы в целом. Их предложение состояло в том, чтобы сосредоточить внимание в большей степени на функциональности, а не на отдельных атаках, подход, который уже существует в энергетическом секторе, но который указывает на несоответствие между энергетической безопасностью и уязвимостями, присутствующими в инфраструктуре из связанных с кибер-системами систем.[7] Таким образом, энергетическая безопасность в отношение кибератак опирается на более широкую концепцию устойчивости, которая связана не только с фактическим производством и передачей энергии, но и с теми системами, которые энергетика поддерживает и узаконивает. Если общество лишается энергии, особенно сильно индустриальное и технологически зависимое, тогда пресловутая коверная дорожка выдергивается из-под ног всех систем обеспечения.

Сети устойчивости могут быть смоделированы в соответствии с типом и схемой соединений (топологией) между различными частями системы, будь то отдельные лица, электрические соединения или экологические отношения. Поскольку сетевые соединения являются функциональными, они редко бывают случайными, а наоборот, сосредоточены на критических узлах, которые обеспечивают важные связи внутри системы. В экологических науках эти критические узлы часто называют «ключевыми видами», которые, даже если они не являются наиболее заметными представителями экосистемы, имеют решающее значение для ее эффективного функционирования. В социальных системах такими критическим узлами могут быть ключевые люди или центры активности сообщества, которые обеспечивают связь между людьми, которые в противном случае не могут взаимодействовать. А в отношение Интернета критическими узлами являются либо наиболее заметные центры активности, такие как Google, либо могут быть представлены в виде ключевых серверов или линий связи. Однако во всех вышеперечисленных случаях эти сети часто называют «безмасштабными», что означает, что они имеют тенденцию быть устойчивыми, поскольку случайные отказы в любой части системы могут быть компенсированы.[8]

Энергетические сети часто конфигурируются по-другому, поскольку вместо того, чтобы быть устойчивыми и позволять перенаправлять мощность в

---

[7] William Arthur Conklin and Anne Kohnke, “Cyber Resilience: An Essential New Paradigm for Ensuring National Survival,” in *Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018*, National Defence University, Washington D.C., USA, 8-9 March 2018, ed. Dr. John S. Hurley and Dr. Jim Q. Chen (Reading, UK: Academic Conferences and Publishing International Limited, 2018), p. 126.

[8] Sarah Dunn and Sean Wilkinson, “Hazard Tolerance of Spatially Distributed Complex Networks,” *Reliability Engineering & System Safety* 157 (2017): 1-12.

случае сбоя, традиционная энергетическая инфраструктура была построена на централизованных узлах. Образец энергетической инфраструктуры двадцатого века представлял собой крупная электростанция (на ископаемом или ядерном топливе), которая затем передает электроэнергию в населенные пункты с соответствующими подсетями электрических трансформаторов.[9] Большая часть работы по повышению устойчивости энергетических систем была направлена на предотвращении каскадных отказов в электрических сетях, где отказ нескольких критических узлов приводит к отключению электроэнергии в больших географических районах, что неоднократно наблюдалось в Северной Америке. Это была форма устойчивости, но в сочетании с элементами хрупкости, что означало, что система была хрупкой и ее можно было легко сломать с помощью достаточной внешней силы. Пуэрто-Рико после урагана Мария в 2017 году является ярким примером.[10] Гражданская устойчивость в энергетическом секторе в меньшей степени сосредоточена на самих электростанциях, хотя экологические факторы все чаще нарушают способность крупных электростанций противостоять наводнениям и другим экологическим опасностям. Хотя наиболее ярким примером была катастрофа на Фукусиме в 2011 году, энергетические сооружения в Северной Америке и Европе становятся все более уязвимыми.[11]

Социальные, политические и энергетические сети не работают независимо, а «вложены» друг в друга. Высокоустойчивые социальные и политические связи основаны на деятельностях, которые не могут осуществляться долго без более фундаментальных энергетических и экологических сетей. Это делает уязвимыми даже самые прочные социальные сети в случае нарушения энергоснабжения. Как основная потребность, коммунальные услуги, такие как поставка энергии, поставка воды и канализация, дают отражение на легитимность управляющих властей, и доверие к этим учреждениям быстро ослабевает, когда основные услуги не могут быть удовлетворены. В Косово, например, несмотря на высокое общественное доверие к безопасности, обеспечиваемой НАТО/ KFOR в стране, электроэнергетические компании KEK и KEDS подвергались публичной критике и недоверию, и несмотря на приватизацию, все же негативно и серьезно повлияли на общественное восприятие легитимности правительства и доверия к его способ-

---

[9] Dong Hwan Kim, Daniel A. Eisenberg, Yeong Han Chun, and Jeryang Park, "Network Topology and Resilience Analysis of South Korean Power Grid," *Physica A: Statistical Mechanics and Its Applications* 465 (January 2017): 13-24, https://doi.org/10.1016/j.physa.2016.08.002.

[10] Maria Gallucci, "Rebuilding Puerto Rico's Grid," *IEEE Spectrum* 55, no. 5 (May 2018): 30-38, https://doi.org/10.1109/MSPEC.2018.8352572.

[11] Cleo Varianou Mikellidou, Louisa Marie Shakou, Georgios Boustras, and Christos Dimopoulos, "Energy Critical Infrastructures at Risk from Climate Change: A State of the Art Review," *Safety Science* 110, Part C (December 2018): 110-120, https://doi.org/10.1016/j.ssci.2017.12.022.

ности обеспечивать безопасность.[12] В Ираке вооруженные силы США провели исследование, которое выявило сильную связь с поддержкой повстанцев в тех районах Багдада (особенно в Садр-Сити), где повстанцы перекрыли доступ к воде, электричеству и канализации.[13] Разжигание нестабильности с помощью базовых услуг может быть эффективным и надежным способом подорвать устойчивость общества и сделать его более уязвимым. Для таких стран, как Украина, с ее травматическим опытом чернобыльской катастрофы 1986 года, связь между энергетической безопасностью и легитимностью правительства может быть еще более хрупкой.

Атаки и уязвимости в Украине

Современное общество практически полностью зависит от состояния защищенности информации и кибер-инфраструктуры во всех сферах жизнедеятельности человека. Возможность использовать как информационные, так и кибертехнологии, а также информационно-коммуникационные сети для достижения своих целей имеют не только государственные структуры стран, но и криминальные и террористические организации. В связи с этим обеспечение кибер и информационной безопасности критически важной инфраструктуры государства стало решающим условием для обеспечения обороноспособности государства и его экономического и социального развития. В январе 2018 года Сенат США выпустил доклад,[14] в котором отмечалось, что с 2014 года Россия неустанно и по разному использует киберпространство Украины в качестве кибер театра и полигона для испытания кибероружия. Во многих случаях кибератаки были нацелены на украинскую систему распределения электроэнергии, в результате чего на долгое время выводились из строя секторы экономики, инфраструктуры и жилья. После атаки России на украинскую энергосистему американские представители Министерства энергетики, Министерства внутренней безопасности, ФБР и Североамериканской корпорации по надежности электроснабжения увеличили свое участие в работе по электроснабжению. Признавая необходимость изучения этих кибер-воздействий, они работали вместе, чтобы понять тактику и практику российского правительства, спрогнозировать типы буду-

[12] Mentor Vrajolli, *Kosovo Security Barometer,* Seventh Edition (Pristina: Kosovar Centre for Security Studies, 1 February 2018), http://www.qkss.org/en/Reports/Kosovo-Security-Barometer-Seventh-Edition-1050.

[13] David E. Mosher, Beth E. Lachman, Michael D. Greenberg, Tiffany Nichols, Brian Rosen, and Henry H. Willis, *Green Warriors: Army Environmental Considerations for Contingency Operations from Planning Through Post-Conflict* (Santa Monica, CA: Rand Corporation, 2008), 90-91.

[14] "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations United States Senate, One Hundred Fifteenth Congress, Second Session (U.S. Government Publishing Office, January 10, 2018), https://www.hsdl.org/?view&did=806949.

щих кибератак и разработать эффективные меры защиты от них. Сотрудничество с Украиной в противодействии этим угрозам, опять же, считается важнейшим элементом киберзащиты США.

Глубокое проникновение энергетики во все отрасли экономики и в социальную сферу определяет ее особую роль в обеспечении безопасности современного развития общества. Энергетическая безопасность характеризует степень выполнения энергетическим комплексом его функций в обществе и государстве в обычных, критических и чрезвычайных обстоятельствах.[15] Предприятия и учреждения энергетического сектора играют ведущую роль в развитии государства.[16] Промышленность остается основным потребителем электроэнергии, хотя ее доля в общем потреблении электроэнергии в мире снижается. В промышленности электроэнергия используется для приведения в действие различных механизмов и технологических процессов. На сегодняшний день коэффициент электрификации силового привода в промышленности составляет 80 %. При этом около 1/3 электроэнергии тратится непосредственно на технологические нужды.[17] Объекты энергетического сектора являются стратегически важными и должны непрерывно функционировать и обеспечивать предоставление качественных услуг.[18]

На территории Украины в каждом регионе есть энергетические системы, которые относятся к критической инфраструктуре. Каждая из них обладает так называемыми «критическими узлами», нарушение работы которых приводит к нарушению функциональности сети и потенциально вызывает каскадные отказы в сетях. Схематично этот комплекс представлен в таблице 1.

Все структурные элементы энергетики относятся к определенной иерархии, системе контроля и системе безопасности. Основой электроэнергетики является единая энергосистема Украины, которая централизует поставки электроэнергии внутренним потребителям, а также ее экспорт и импорт. Система объединяет восемь региональных энергосистем (Днепровская, Донбасса, Западная, Крымская, Южная, Юго-Западная, Северная, Центральная), соединенных между собой системообразующими и межгосударственными высоковольтными линиями электропередачи. По данным Государственного комитета статистики Украины, наибольшая доля электроэнергии вырабатывается на тепловых электростанциях (около 50 %), на атомных станциях (45 %) и на гидроэлектростанциях (5 %).

---

[15] Концепция развития сектора безопасности и обороны Украины, введенная в действие Указом Президента Украины от 14 марта 2016 г. № 92/2016.

[16] Стратегия кибербезопасности Украины, утвержденная Указом Президента Украины от 15 марта 2016 г. № 96 (Officer Vision of Ukraine, 2016), # 23.

[17] Закон Украины «Основные принципы кибербезопасности Украины» № 2163-VIII от 5 октября 2017 года, http://zakon.rada.gov.ua/laws/show/2163-19.

[18] Стратегия национальной безопасности Украины, утвержденная Указом Президента Украины от 26 мая 2015 г. № 287/2015 г., http://zakon.rada.gov.ua/287/2015.

Таблица 1. Энергетический комплекс Украины.

<table>
<tr><th colspan="2">Топливная промышленность</th><th colspan="4">Электроэнергетика</th><th>Инфраструктура генерации</th></tr>
<tr><td colspan="2">1. Угольная промышленность</td><td colspan="4">1.Тепловые электростанции</td><td>1. Транспорт</td></tr>
<tr><td colspan="2">2. Газовая промышленность</td><td colspan="2">Государственная региональная электростанция</td><td colspan="2">Теплоэлектроцентраль</td><td>a) Трубопроводный</td></tr>
<tr><td colspan="2">3. Нефтяная промышленность</td><td colspan="4">2. Гидроэлектростанции</td><td>b) Железнодорожный</td></tr>
<tr><td>a) Добыча нефти</td><td>b) Нефтепереработка</td><td colspan="2">Гидро-электростанции</td><td colspan="2">Гидроаккумулирующие электростанции</td><td>c) Водный</td></tr>
<tr><td colspan="2" rowspan="2">4. Торфяная промышленность</td><td colspan="4" rowspan="2">3. Атомные электростанции</td><td>d) Автомобильный</td></tr>
<tr><td>e) Воздушный</td></tr>
<tr><td colspan="2" rowspan="3">5. Сланцевая промышленность

6. Химическая промышленность</td><td colspan="4">4. Альтернативные источники энергии</td><td>2. Линии электро-передач</td></tr>
<tr><td>a) Ветряные электростанции</td><td>b) Солнечные электро-станции</td><td>c) 3D альтернативные ПЭЯ</td><td>d) Биотопливные электростанции</td><td rowspan="2">3. Водоснабжение
a) Система управления;
4. Система поддержки персонала</td></tr>
<tr><td colspan="2">e) Топливные электростанции</td><td colspan="2">f) Геотермальные станции</td></tr>
</table>

Угрозы в энергетическом секторе

Весь набор угроз, которые могут повлиять на функционирование энергосистем, можно условно разделить на обычные угрозы (вероятные сбои и аварии) и чрезвычайные угрозы (они уникальны по происхождению, характеру развития и последствиям). Различные формы резервирования мощностей, разработки и транспортировки топливно-энергетических ресурсов, системы гарантированного энергоснабжения, создание резервов топливно-энергетических ресурсов служат для противодействия обычным угрозам в энергосистемах. Обыденные явления практически исключают создание угрозы энергетической безопасности в условиях развития и функционирования национальной экономики. Напротив, необычные воздействия могут негативно повлиять на энергетический комплекс в целом. Среди чрезвычайных угроз ведущую роль играют киберугрозы. Киберугрозы способны спровоцировать такие проблемы, как нарушение обеспечения энергоресурсами и

чрезвычайные ситуации в энергетическом комплексе государства. Они реализуются в виде разнообразных деструктивных кибер-воздействий.

Разрушительные кибер воздействия могут вызывать:

- Целенаправленные атаки (повышенная постоянная угроза);
- Воздействия на системы управления;
- Воздействия через социальные сети;
- Атаки на банковские системы (кража денег);
- Аппаратные ошибки (инструментальные ошибки) в микросхемах и прошивках компьютерного и сетевого оборудования.

Такие киберугрозы могут быть реализованы путем воздействия как на весь энергетический комплекс в целом, так и на его элементы в отдельности, а также путем достижения синергии результатов. Воздействие может осуществляться комплексно, одновременно, последовательно или смешанно на автоматизированные системы управления, на персонал, на финансовую систему энергетики, на программно-аппаратный комплекс. Самым уязвимым местом в единой энергосистеме являются автоматизированные системы управления.

Анализ кибер воздействий на объекты критической инфраструктуры энергетики в 2014-2018 гг.

Проблема кибербезопасности государственного энергетического сектора имеет решающее значение для национальной безопасности и национальной обороны, а также для экономического и социального развития.

В 2014–2018 годах были осуществлены хорошо спланированные синхронизированные кибератаки на элементы энергетического комплекса Украины. На какое-то время нарушителям удалось управлять комплексом, а в некоторых случаях даже нарушать функционирование как системы управления, так и нормальное функционирование элементов энергокомплексов. Целями этих атак, возможно, были проверка надежности системы кибербезопасности этой критически важной инфраструктуры, установление особенностей функций системы кибербезопасности энергетических компаний и их реакции на различные кибер воздействия и инциденты. Было показано, что чрезмерно сложный контроль над информационными системами может сделать комплексные энергетические объекты уязвимыми для кибератак. Наиболее опасными кибер-воздействиями на объекты энергетического комплекса являются те, которые вызывают или сопровождаются цепными деструктивными воздействиями непосредственно на энергетический объект, который затем подключается к другим объектам инфраструктуры и сферам повседневной жизни нации.

Еще одной особенностью кибератак на объекты энергетического комплекса Украины было начальное рассредоточение с конечной направленностью на определенные систематические многоспектральные результаты и разноплановые последствия.

В ходе анализа кибератак выяснилось, что атаки не были одиночными, а проводились синхронно. Все они оказывали разрушительное воздействие на АСУ энергетических объектов. Основной синхронный деструктивный киберэффект был сосредоточен на уязвимых элементах автоматизированных систем управления. Перед основной кибератакой осуществлялась предварительная кибератака на сервисно-диспетчерскую систему с целью отказа в обслуживании потребителей. Применение нескольких деструктивных концентрированных кибератак на энергокомплекс осуществлялось в рамках масштабной кибероперации, направленной на нарушение одновременно нескольких объектов энергокомплекса Украины.

Группы, ответственные за многие украинские кибератаки, Telebots, BlackEnergy и Gray Energy, были более тесно или более слабо связаны с российскими государственными спецслужбами, подобными британской GCHQ.[19] Однако отсутствие прямой атрибуции не умаляет значение стратегического использования таких инструментов для дестабилизации и делегитимации украинского государства. Напротив, такие замаскированные подходы к конфликту являются яркими примерами того, как кибер-инструменты могут быть использованы в современных концепциях гибридной войны, когда уязвимости критически важной инфраструктуры подвергаются атакам, чтобы ослабить государственную поддержку и функционирование и усилить недоверие потенциальных внешних партнеров. Второстепенная цель кибератак на энергетическую инфраструктуру может заключаться в том, чтобы дать сигнал другим (например, Великобритании, США, Германии) об их уязвимостях, причем украинские атаки служат подтверждением концепции. В любом случае действия кибер-атакующих сильно скоординированы, их трудно отследить и атрибутировать, и они представляют собой крайне асимметричные некинетические атаки. Эти атаки являются новыми техническими областями конфликта, особенно в тех случаях, когда целью является непрекращающееся состояние нестабильности, а не традиционная концепция «полной победы» на поле боя.

Одной из важных составляющих энергосистемы Украины является система управления. Система управления энергосистемой играет ведущую роль в функционировании всего энергетического комплекса Украины. На автоматизированную систему управления может быть оказано мощное кибер воздействие, которое может привести к нарушению управления отдельными объектами энергетики или энергетическим комплексом в целом. Автоматизированная система управления энергосистемой должна быть устойчивой к кибер-воздействиям и иметь соответствующую комплексную систему противодействия кибератакам.

[19] Jack Stubbs, “Hackers Accused of Ties to Russia Hit Three East European Companies: Cybersecurity Firm,” *Reuters*, October 17, 2018, https://uk.reuters.com/article/us-russia-cyber/hackers-accused-of-ties-to-russia-hit-three-east-european-companies-cybersecurity-firm-idUKKCN1MR1BO.

В декабре 2015 года была зафиксирована повышенная постоянная угроза (APT) в автоматизированной системе управления энергосистемой. Атаке подверглись внутренние сети украинской энергокомпании Прикарпатьеоблэнерго (ПАО).[20] В результате этой кибератаки значительная часть области и областной центр остались без электроснабжения в течение нескольких часов. Было остановлено 30 подстанций. Около 230 тысяч человек лишились энергоснабжения на срок от одного до шести часов. В ходе атаки использовалось вредоносное ПО BlackEnergy.[21] Группа BlackEnergy начала атаку на украинскую электросеть с помощью семейств ПО BlackEnergy и KillDisk. Это было последнее известное использование вредоносного ПО BlackEnergy в реальном мире. После атаки выяснилось, что группа BlackEnergy состоит как минимум из двух подгрупп: TeleBots и GrayEnergy.

Основная цель группы TeleBots – осуществление кибератак с целью проведения диверсий в Украине, что достигается за счет атак на компьютерные сети (CNA). Эта группа совершила множество разрушительных атак, в том числе:

- серия атак в декабре 2016 года с использованием обновленной версии того же вредоносного ПО KillDisk, разработанного для операционных систем Windows и Linux;
- известная атака Petya / NotPetya в июне 2017 года с использованием бэкдоров, встроенных в украинскую бухгалтерскую программу MEDOC;
- атака с использованием семейства ПО BadRabbit в октябре 2017 г.

Специалисты ESET в течение нескольких лет отслеживали деятельность группы GreyEnergy. Группа GreyEnergy использует уникальное семейство вредоносных программ. Дизайн и архитектура этого вредоносного ПО очень похожи на уже известное семейство BlackEnergy. Помимо концептуального сходства вредоносного ПО, ссылки указывают на то, что группа, стоящая за вредоносным ПО GreyEnergy, тесно сотрудничает с группой TeleBots. В частности, в декабре 2016 года команда GreyEnergy разработала червя, похожего на NotPetya, а позже еще более продвинутая версия этой вредоносной программы использовалась группой TeleBots во время атаки в июне 2017 года. GreyEnergy имеет более широкие цели, чем группа TeleBots. GreyEnergy в первую очередь интересуется промышленными сетями различных организаций, отвечающие за критическую инфраструктуру, и, в отличие от TeleBots, группа GreyEnergy не ограничивается только Украиной.

В конце 2015 года специалисты ESET впервые обнаружили вредоносное ПО GreyEnergy, нацеленное на энергетическую компанию в Польше. Но

---

[20] Kim Zetter, “Russia’s Hacking Attack on the Ukrainian Power System: How It Was,” *Texty.org.ua*, http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak.

[21] Bruce Middleton, *A History of Cyber Security Attacks: 1980 to Present* (New York: Auerbach Publications, 2017).

позже, как и в случае с BlackEnergy и TeleBots, фокус группы GreyEnergy сместился на Украину. Злоумышленники сначала проявляли интерес к энергетическому сектору, а затем к транспортной инфраструктуре и другим важным объектам. О последнем использовании вредоносного ПО GreyEnergy было сообщено в середине 2018 года.

Вредоносное ПО GreyEnergy является модульным, и в отличие от Industroyer, специалисты ESET не обнаружили никаких модулей, управляемых ПСУ, а это означает, что оно нацелено именно на промышленные системы управления, но такая система может быть объектом воздействия с использованием и других методов. По крайней мере, операторами был обнаружен один случай использования этого вредоносного ПО. Модуль может стереть диск, чтобы нарушить бизнес-процессы в компании и скрыть следы.[22] Одна из наиболее ярких деталей, выявленных в ходе исследования ESET, заключается в том, что один из обнаруженных образцов GreyEnergy был подписан действующим цифровым сертификатом, который, вероятно, был украден у тайваньской компании, производящей оборудование для ПСУ. Другими словами, группа GreyEnergy буквально следовала методам разработки Stuxnet.

Кроме того, синхронные атаки были осуществлены на энергокомпании «Черновцыоблэнерго» и «Киевоблэнерго», но с меньшими последствиями. 23 декабря 2015 года несанкционированная группа лиц вмешалась в работу информационно-технологической системы удаленного доступа к телеуправлению оборудованием подстанций 35-110 кВ ПАО «Киевоблэнерго». С 15:31 до 16:30 по местному времени было полностью или частично отключено пятнадцать городов и сел в Мироновском, Макаровском, Белоцерковском, Фастовском, Сквирском, Рокитнянском, Кагарлыкском, Иванковском и Яготинском административных округах. Более 80 000 потребителей остались без электричества. В результате атаки произошли сбои в системе удаленного доступа. Отключено было 30 станций, снабжающих несколько стратегических объектов области: предприятия, учреждения, организации, население. Электричество восстановили 23 декабря 2015 года в 18:56.[23]

Система управления была уязвима для подобных кибератак. Ответ на кибератаку был несвоевременным, а система безопасности не справилась со своими функциями. С помощью вредоносного ПО злоумышленник может контролировать и в некоторых приложениях управлять частью или всей автоматизированной системой управления. Последствия такой атаки могли быть использованы для проверки работы системы безопасности и системы реагирования энергетической компании на критическую ситуацию.

---

[22] "GreyEnergy: A Successor to BlackEnergy," White Paper (GreyEnergy, October 2018), www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf.

[23] «Крупнейшие кибератаки на Украину с 2014 года», *Новое время*, 24, 7 июля 2017, https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

В целом кибератака была комплексной и в определенной степени систематически организована через:

- Предварительное заражение сетей с помощью поддельных писем;
- Получение контроля над автоматизированной системой управления путем отключения операций на подстанциях;
- Отказ элементов АСУ;
- Удаление информации на серверах и рабочих станциях (утилита Kill Disk);
- Атак на телефонную сеть колл-центров с целью отключения обслуживания текущих абонентов.

В период с 19 по 20 января 2016 года была проведена кибератака с помощью кибер-инструмента Joint Conflict and Tactical Simulation Enhancements, которая также была направлена на нарушение работы системы управления путем установки вредоносного ПО, присланного электронной почтой.[24] Другая кибератака, проведенная в ночь с 17 на 18 декабря 2016 г., была менее масштабной. Произошел срыв работы подстанции «Северная» энергокомпании «Укрэнерго». Потребители в северной части Киева и прилегающих районах остались без электричества. Нападавшие не причинили значительного ущерба; целью нападения была «демонстрация силы». Как и в предыдущих случаях, это нападение было частью операции против государственных учреждений Украины.[25]

Основные особенности продвинутых постоянных угроз (Advanced Persistent Threats) заключаются в том, что они, как правило:

- нацелены на элементы критической инфраструктуры
- проводятся группой высококвалифицированных хакеров
- тщательно маскируются с помощью специально разработанных программных средств (например, специальных Shell-кодов, Root Kitta)
- долгое время остаются неизвестными
- сопровождаются разведывательными или деструктивными действиями
- и являются элементами разведывательных и диверсионных операций.

Анализ кибер воздействий представлен в таблице 2.

---

[24] "Zillya! Antivirus Has Analyzed the Cyber Attacks on Infrastructure Objects in Ukraine," February 17, 2016, Antivirus Zillya, Certificated for use by public and state authorities, https://zillya.ua/zillya-antivirus-provela-analiz-kiberatak-na-infrastrukturni-ob-kti-ukra-ni.

[25] Vitaliy Tchervonenko, "Was There an Attack on the Regional Power Company," BBC Ukraine, January 6, 2016, https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc.

Таблица 2. Анализ кибер атак.

Объект воздействия	Использованные инструменты	Способ проникновения	Воздействие	Последствия
2015				
«Прикарпатье Облэнерго»	DoS-атака на коллцентры «Облэнерго» методом «отказа в обслуживании»[26]	Сеть Интернет	Насыщение сетевого оборудования большим количеством внешних запросов	Потребители не могли сообщать об отключении электроэнергии
	Расширенная постоянная угроза (Advanced Persistent Threat)	Сеть SCADA, установка вредоносного ПО «BlackEnergy»	Перехват управления системы в сети SCADA через украденные аккаунты; отправка команд на отключение систем бесперебойного питания, которые уже были реконфигурированы. После этого отключение систем безопасности, приводящее к прерыванию подачи электроэнергии	Отключено около 30 подстанций, около 230 тыс. человек остались без электричества от одного до шести часов.
«Черновцы облэнерго»	DoS-атака на коллцентры «Облэнерго» методом «отказа в обслуживании»	Сеть Интернет	Насыщение сетевого оборудования большим количеством внешних запросов	Потребители не могли сообщать об отключении электро-энергии
	Утилита Kill Disk	Сеть Интернет	Уничтожение информации на серверах и рабочих станциях	Отказ элементов ИТ-инфраструктуры
	APT-атака, обнаружение вредоносного ПО «BlackEnergy»	Сеть SCADA	Захват управления автоматизированными диспетчерскими систем с проведением остановок на подстанциях	Перерыв в подаче электроэнергии составил от 1 до 3,5 часов. Всего недодано 73 МВтч

[26] Государственная энергетическая компания Украины.

				(0,015% суточного потребления Украины)
«Киевское облэнерго»	Расширенная постоянная угроза (APT)	Система удаленного доступа	Несанкционированное вмешательство в АСУ	Более 80 378 потребителей без электричества. Отключено электроснабжение 30 узловых подстанций, питающих ряд стратегических объектов, более 80 тыс. потребителей остались без электричества в течение одного-трех часов.
2016 год				
«Киевское облэнерго»	Вредоносное ПО Crash Override (атака была полностью автоматизирована)	Сеть Интернет	Перехват управления энергосистемой, автоматическая разгрузка подстанций	Подстанция «Пивничная» с питанием для собственных нужд от подстанции полностью отключена. Снижение нагрузки на 144,9 МВт ПАО «Киевэнерго» и 58 МВт ОАО «Киев-облэнерго». Киевская АЭС тоже была отключена от системы с потерей мощности для собственных нужд.

Основные кибератаки различаются по своим последствиям и способам действия. Атаки на энергокомпании в 2015 году не были полностью самоорганизованными. В 2016 году вредоносные программы, которые уже предусматривали самоорганизацию действий в процессе атак и работы, стали более работоспособными. Также, проведя исследование специалисты компании ESET, констатировали, что «Crash Override» способен физически разрушать энергосистемы. Программное обеспечение CrashOverride [27] имеет возможность отправлять команды в электросеть на включение или отключение питания. По их данным, Crash Override может использовать известную уязвимость оборудования Siemens, в частности цифрового реле Siprotec. Такие реле устанавливаются для защиты и управления распределительными и передающими электросетями. Майк Ассанте из американской компании по кибербезопасности SANS Institute установил, что отключение цифрового реле может привести к тепловой перегрузке электросети. Это очень серьезная угроза для трансформаторов и любого оборудования, находящегося под напряжением. Таким образом, Crash Override может обеспечить спланированную атаку на несколько «критических узлов» энергетического комплекса. Тогда есть вероятность отключения электроэнергии во всем государстве, поскольку нагрузка перемещается из одного региона в другой.

Автоматизированные энергосистемы энергетических комплексов уязвимы для кибератак. В результате нашего анализа кибератак мы можем выделить следующие категории возможных кибератак:

- Направленные на целевые компоненты: электронные вычислительные устройства, такие как удаленные терминалы (RTU) или человеко-машинный интерфейс (HMI),[28] обычно имеют интерфейс для удаленной настройки или управления. С помощью удаленного доступа злоумышленник может перехватить управление устройством и вызвать сбои, например, внести изменения в данные, передаваемые оператору, повредить оборудование или вызвать полный или частичный отказ устройства.
- Ориентированные на протоколы: почти все современные протоколы передачи данных хорошо документированы, а их описание открыто. Например, стандарт DNP3 распространен в системах управления энергопотреблением в Северной Америке.[29] Его спецификация доступна

[27] Middleton, *A History of Cyber Security Attacks*.

[28] Muhammad Baqer Mollah and Sikder Sunbeam Islam, “Towards IEEE 802.22 Based SCADA System for Future Distributed System,” in *Proceedings of 2012 International Conference on Informatics, Electronics & Vision (ICIEV)*, Dhaka, Bangladesh, 18-19 May 2012, https://doi.org/10.1109/ICIEV.2012.6317474.

[29] Salman Mohagheghi, Mirrasoul Mousavi, J. Stoupis, and Z. Wang, “Modeling Distribution Automation System Components Using IEC 61850,” in *Proceedings of the 2009 IEEE Power & Energy Society General Meeting*, Calgary, AB, Canada, July 26-30, 2009, https://doi.org/10.1109/PES.2009.5275841.

каждому по невысокой цене. Злоумышленник может внести изменения в эту информацию, что может привести к значительным финансовым затратам из-за перепроизводства электроэнергии, включения ЛЭП во время работы на них, повреждения оборудования, перегрузки системы.

27 июня 2017 года на украинские учреждения и организации была совершена масштабная деструктивная хакерская атака («Petya»). Атаке подверглись непосредственно и «критические узлы» энергетики (Укрэнерго, Киевоблэнерго, Днепроэнерго, Запорожьеоблэнерго, Чернобыльская АЭС). Эта кибератака была направлена на нарушение работы веб-сайтов компаний и систем поддержки клиентов. Ущерб информационным системам украинских компаний произошел из-за обновления программного обеспечения, предназначенного для отчетности и документооборота M.E.Doc, путем установки бэкдора в пакете обновления программного обеспечения M.E.Doc. Одновременно с установкой пакета обновлений на компьютеры учреждений и организаций был установлен бэкдор, способствовавший установке вируса «Petya».

23 мая 2018 года эксперты Cisco предупредили о заражении более 500 000 маршрутизаторов и систем в 54 странах, но главной целью для масштабных кибератак могла быть Украина.[30] Для проведения такой атаки можно использовать деструктивное программное обеспечение «VPN Filter», которое позволяет злоумышленникам перехватывать весь трафик, проходящий через пораженное устройство (включая данные авторизации и персональные данные платежных систем), собирать и выгружать информацию, удаленно управлять зараженным устройством, да еще и вывести его из строя. Также имеются функции для мониторинга протоколов Modbus SCADA, используемых в автоматизированных системах управления.

В предыдущих разделах были оценены все известные кибератаки, повлиявшие на функционирование критических объектов инфраструктуры в энергетическом секторе.

Заключение

В этой статье рассмотрены пути и направления выбора и реализации рациональных подходов к решению комплексной защиты от деструктивного кибер воздействия на государственный энергетический комплекс. Проанализированы все крупные кибератаки на энергетический комплекс Украины в период с 2014 по 2018 год, которые оказали влияние на функционирование объектов критической инфраструктуры в энергетике. Выяснилось, что кибератаки не были одиночными, а проводились систематически. Они оказывали комплексное разрушительное воздействие на системы энергоменедж-

[30] "Global Ransomware Attack Causes Turmoil," *BBC News Ukraine*, June 28, 2017, https://www.bbc.com/news/technology-40416611.

мента. Установлено, что основные деструктивные кибер воздействия сосредоточены на уязвимых элементах (критических узлах) систем управления объектами энергетического комплекса. Перед основной кибератакой проводилась предварительная атака на систему обслуживания и диспетчеризации с целью отказа в обслуживании потребителей. Применение нескольких деструктивных концентрированных кибератак на энергетический комплекс осуществлялось в рамках масштабной кибератаки, направленной на одновременное нарушение работы нескольких объектов энергетики.

Установлено, что система производства и поставки электроэнергии зависит от уровня киберустойчивости энергообъектов. Анализ кибератак показал, что минимальное значение уровня устойчивости может привести к разрушению функционирования энергосистемы (объекта, сети).

Описаны методы реализации гибридных распределенных кумулятивных кибератак с цепным воздействием на объекты критической инфраструктуры. Определены уязвимости этих объектов. Установлено, что кибератаки, осуществленные через электронную почту, обеспечивали доступ к основным серверам для получения информации о состоянии работы системы для перехвата контроля над объектами энергетической инфраструктуры в целом, и затем изменялись параметры их функционирования.

Авторы разработали методику обнаружения гибридных распределенно-концентрированных кибератак с цепными эффектами с использованием модели интеллектуального распознавания киберугроз. Они также разработали организационные и технические меры для обеспечения кибербезопасности в энергетическом секторе. Показано, что систематические меры, направленные на своевременное обнаружение киберугроз, предотвращение и противодействие кибератакам, обеспечат необходимый уровень функциональной устойчивости систем энергокомплекса к деструктивным кибер-воздействиям. Это обеспечит их адекватное реагирование на актуальные и потенциальные угрозы, рационально используя имеющиеся возможности и ресурсы государства.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами авторов и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторах

Тамара Малярчук, кандидат наук, работала в ООО «УкрЭнерджи» с 2016 по 2018 год. Доктор Малярчук был членом рабочей группы НАТО по реализации программы DEEP в Вооруженных силах Украины. Она была аналитиком в Житомирском военном институте им. С. Королева в Украине и работала с американскими военными в области языковой и киберзащиты. Она проводит исследования в области электронного обучения, инновационных технологий в области обнаружения и лечения посттравматического стрессового расстройства, манипулятивных технологий в веб-среде.
E-mail: maliarchuktamara@gmail.com

Генерал-майор **Юрий Даныk**, профессор, доктор технических наук, начальник Института информационных технологий Национального университета обороны Украины им. Ивана Черняховского. Он является экспертом в области военного искусства, национальной обороны и безопасности, информации и кибербезопасности, электронных и ИТ-технологий, проектирования и применения робототехнических комплексов, подготовки спецподразделений. Имеет боевой опыт применения передовых оборонных технологий в условиях современной войны. *E-mail*: zhvinau@ukr.net

Д-р **Чад Бриггс** – доцент и директор департамента государственной политики и администрации Университета Аляски в Анкоридже. Доктор Бриггс имеет практический опыт в области информационных и гибридных войн, а также в разработке оборонительных стратегий для защиты критически важных систем в Восточной Европе и на Балканах. Он имеет докторскую степень в области политологии Карлтонского университета в Канаде, а ранее был старшим советником Министерства энергетики США и программы Минерва, а также профессором по энергетической и экологической безопасности в Академии ВВС США (USAF). Он является автором (вместе с Мириам Матеджовой) книги *«Безопасность при бедствиях: использование разведывательных данных и военного планирования для оценки энергетических и экологических рисков»*. *E-mail*: cbriggs9@jhu.edu

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Весна Павичич, *Connections QJ* 18, № 1-2 (2019): 130-148
https://doi.org/10.11610/Connections.rus.18.1-2.07

Рецензированная статья

Проблема ориентации Сербии и пути ее преодоления

Весна Павичич

Министерство безопасности Боснии и Герцеговины, http://msb.gov.ba/

Резюме: Сербия, самая большая страна на Западных Балканах, стоит перед историческим выбором относительно своей будущей политической ориентации. Хотя этот выбор стоял в повестке дня с конца 1990-х годов, он еще некоторое время останется нерешенным. Преобразование страны продвигается вперед. Однако без интеграции в западные институты, прежде всего в Европейский Союз, этот процесс неполный, и другие крупные игроки в международной системе, в первую очередь Россия, но в некоторой степени также и Китай, пытаются повлиять на Белград в направлении, благоприятном для их интересов. Рациональный выбор в отношении экономической интеграции, торговли и инвестиций, а также последствия консолидации демократии должны подтолкнуть Сербию к Западу. Однако, как показывают некоторые примеры, помимо рационального выбора есть и другие факторы. Эмоциональная ассоциация с Россией, ортодоксальное христианство, поддержка Россией Сербии в споре последней с Косово, а также изощренное влияние Москвы на пошаговое продвижение и колебания Запада помогают России лучше утвердить свое положение в Сербии. Это приводит к безрезультатной ситуации, требующей внимания, чтобы избежать продолжения колебаний и неопределенности в долгосрочной перспективе. Китай потенциально предлагает альтернативу, прежде всего как торговый партнер и инвестор. Однако его интересы в будущей ориентации Сербии могут отличаться от интересов Москвы, поскольку его инвестиции могут принести тем более высокую прибыль, чем раньше Белград станет членом Европейского Союза.

Ключевые слова: Европейский Союз, российское влияние, Сербия, Западные Балканы, Китай.

Введение

Эта статья занимается рассмотрением исторического вызова и дилеммы, с которой Сербия сталкивается в течение некоторого времени и перед которой будет стоять в ближайшие годы. Сербия должна завершить свой переход к демократии, как одну из сложных задач. Внутренняя демократизация должна идти рука об руку с продолжением модернизации, а также с продолжающимся сближением с Западом и интеграцией в институты, которые в дальнейшем будут способствовать консолидации преобразований в Сербии. Однако было бы преждевременно делать вывод о том, что Сербия безвозвратно приняла решение ориентироваться на Запад, поскольку она продолжает взвешивать варианты, и некоторые из ее партнеров, похоже, предлагают альтернативы.

Основные атрибуты национальной идентичности, а именно: «а) историческая территория или родина; б) общие мифы и исторические воспоминания; в) общая массовая публичная культура; г) общие юридические права и обязанности для всех членов и д) общая экономика с территориальной мобильностью для членов», играют важную роль в политической риторике России в отношении Сербии.[1] Этнонациональная принадлежность, по-видимому, является важнейшей опорой и дифференцирующей переменной социальной идентификации членов крупнейших национальных сообществ в Сербии.[2] Важно решить, какие атрибуты – материальные или нематериальные – имеют большее значение при построении идентичности. Другой важный вопрос – являются ли эти атрибуты объективными или воспринимаемыми, присутствуют ли они в обществе или «построены» через официальные и социальные дискурсы. Наконец, вопрос в том, могут ли внешние игроки способствовать формированию идентичности, напрямую обращаясь к сербскому обществу или оказывая влияние на ее политический истеблишмент. Если предположить, что присутствие внешних игроков в Сербии играет важную роль в формировании идентичности последней, то мы должны задуматься какие из атрибутов на чем основаны. Политическое разделение между ее «западной» и «восточной» идентичностью продолжает оставаться вызовом для внешнего восприятия Сербии как игрока на международной политической арене.

Проевропейская ориентация Сербии явно прослеживается с начала века и с момента ухода режима Слободана Милошевича с поста и власти. Однако оставались сомнения в том, что готовность на словах можно подкрепить действиями и принятием болезненных решений, которые, по всей видимости, были необходимы. Следовательно, результат оставался под вопросом.

---

1 Antoni D. Smit, *Nacionalni Identitet* (Belgrade: Biblioteka XX vek, 1998), 29-30.

2 Jovan Komšić, Dragomir Pantić, and Zoran Đ. Slavujević, *Osnovne Linije Partijskih Podela i Mogući Pravci Političkog Pregrupisavanja u Srbiji* (Belgrade: Friedrich Ebert Stiftung, Institute of Social Sciences, 2003), 55-77.

В 2003 году, когда ЕС предоставил Западным Балканам перспективу членства, организованная преступность продемонстрировала свою силу, казнив премьер-министра Сербии. Убийство премьер-министра Зорана Джинджича было одним из факторов, «повлиявших на смещение вектора внешней политики Сербии на Восток».[3] Другим фактором была ответственность за военные преступления 1990-х годов. Тот факт, что многие в Сербии расценили суровые наказания сербских преступников, как «Siegerjustiz» (правосудие победителей), выражающимся в дисбалансе вынесения множества приговоров сербам, но гораздо меньшему числу хорватов и босняков, также способствовал восприятию «несправедливости Запада». Это некоторые из причин, по которым Белград придерживается декларативной прозападной политической ориентации, не рассматривая полное участие и исключая другие варианты. Готовность Белграда остается под вопросом. Сегодня это неоднозначно ориентированная страна, где политические элиты тяготеют к разным направлениям и ориентируются на различные центры силы.

Страны Западных Балкан все еще переживают непростой процесс консолидации. Несмотря на значительные различия, они часто заинтересованы во взаимодействии одновременно с западными государствами и с Россией, в то время как фактор Китая также присутствует в их экономике. Некоторые из них завершили процесс интеграции в ЕС и/или НАТО, но влияние России заметно в их политике. Весьма часто возникает сомнение в том, что Россия присутствует и в их экономической сфере. Как будет показано позже, экономическое участие Москвы в двусторонней торговле с Белградом (а также с другими странами) весьма ограничено. Однако, когда нужно вернуться к вопросу о различных атрибутах присутствия и влияния, присутствие Москвы очень заметно и подчеркнуто символикой.

Сербия смотрит на ЕС – ЕС неуверенно бросает ответный взгляд

Несмотря на то, что Европейский Союз «не так привлекателен, как раньше», Сербия все еще надеется присоединиться к ЕС. Это было подтверждено в 2016 году заявлением тогдашнего премьер-министра Александра Вучича (ныне президента Сербии): «Мы рациональные люди, и мы знаем, что это лучшее для нашей страны».[4] В 2016 году премьер-министр Сербии также заявил, что «подавляющее большинство сербских граждан выступает за продолжение европейского пути, сохраняя при этом тесные связи с Китаем и Россией».[5] Однако вопрос о том, как долго Сербия сможет балансировать

[3] Helsinki Committee for Human Rights in Serbia, “The Warp of the Serbian Identity: Anti-westernism, Russophilia, Traditionalism,” *Ogledi i Studies* No. 17 (Belgrade, 2016), 188, https://www.helsinki.org.rs/doc/Studies17.pdf.

[4] Подробнее по этому вопросу: “Vucic Says EU Membership Has ‘Lost Magic Power’ for Balkans,” *Radio Free Europe/Radio Liberty*, February 23, 2016, http://www.vucic-says-eu-membership-has-lost-magic-power-for-balkans-migrant-crisis-brexit.

[5] Reuters online: https://www.reuters.com/article/us-serbia-election/serbias-vucic-confirms-domination-with-presidential-win-idUSKBN1733VI.

между Западом и Востоком, не ставя под угрозу свои перспективы вступления в ЕС, все еще остается в силе. Заметное разочарование Сербии вызвано рядом факторов. Со времени перехода к демократии в начале века, за которым в 2003 г. последовало решение ЕС, обеспечившее «европейскую перспективу» для Западных Балкан, прошла жизнь полпоколения. В июне 2003 года в Салониках саммит ЕС-Западные Балканы принял декларацию, одобренную Европейским советом. В декларации говорилось: «Будущее Балкан находится в Европейском Союзе. Продолжающееся расширение ... вдохновляет и побуждает страны Западных Балкан идти по тому же успешному пути».[6] Хотя обязательства ЕС оставались расплывчатыми и не упоминались какие-либо сроки, тем не менее, некоторые государства на Западных Балканах, должно быть, были уверены, что эти перспективы будут реализованы в ближайшем времени.

Десять лет спустя, когда была сформирована Комиссия ЕС Жан-Клода Юнкера, новый председатель Комиссии заявил следующее: «В следующие пять лет к нам в Европейский Союз не присоединятся никакие новые члены. … Тем не менее, переговоры будут продолжаться, и другим европейским народам и европейским странам потребуется заслуживающая доверия и честная европейская перспектива. Это особенно относится к Западным Балканам».[7] Прошло пять лет, и после того, как Комиссия ушла в отставку, можно сказать, что если и было обещание, которое Юнкер сдержал, так это то, что в течение этих пяти лет не было дальнейшего расширения ЕС. Ближе к концу срока полномочий Комиссии, Европейский союз, возможно, заметил, что отсутствие ощутимой перспективы расширения снижает влияние ЕС в регионе и только увеличивает влияние других держав. Поэтому в сообщении, опубликованном в феврале 2018 года, туманное обещание было подтверждено несколько более четко: «Переговоры о присоединении уже идут полным ходом с Черногорией и Сербией. В случае наличия сильной политической воли, проведения реальных и устойчивых реформ и окончательного решения споров с соседями, они потенциально могут быть готовы к членству в 2025 году. Эта перспектива чрезвычайно амбициозна. Достижение этого будет полностью зависеть от объективных достижений и результатов каждой страны».[8] Официально расширение ЕС почти не становилось

---

[6] Declaration, EU–Western Balkans Summit, C/03/163, Thessaloniki, June 21, 2003, 10229/03 (Presse 163), point 2.

[7] Jean-Claude Juncker, Candidate for the President of the European Commission, "A New Start for Europe (Speech/14/567)," Strasbourg, July 15, 2014, http://europa.eu/rapid/press-release_SPEECH-14-567_en.htm.

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A Credible Enlargement Perspective for and Enhanced EU Engagement with the Western Balkans," Strasbourg, February 6, 2018, COM (2018) 65 final, https://ec.europa.eu/commission/sites/beta-political/files/communication-credible-enlargement-perspective-western-balkans_en.pdf.

ближе, и это делает понятными сомнения политиков, дипломатов, неправительственных организаций и ученых относительно присоединения любой страны Западных Балкан к ЕС к 2025 году.[9]

Определенное развитие событий указывает на отсутствие прорыва в плане расширения на Западных Балканах. Количество закрытых или открытых глав в переговорах с Белградом о присоединении увеличилось до двух гипотетически закрытых и 17 открытых глав из 35.[10] Поскольку переговоры продолжаются с 2014 года, это свидетельствует о медленном, нерегулярном движении вперед. Однако также важно отметить, что экономические отношения расширились. По состоянию на 2017 год ЕС является крупнейшим торговым партнером Сербии, на долю которого приходится более 60 процентов ее экспорта и импорта. Торговля с ЕС превышает объемы торговли с любым другим партнером в отношении почти 8: 1 по импорту и 11:1 по экспорту по сравнению со вторым крупнейшим партнером. Что касается импорта, вторым по величине партнером Сербии является Китай (8,1 процента); по экспорту – Российская Федерация (5,9). В общем, ЕС не имеет альтернативы во внешней торговле Сербии. Ситуация еще больше склоняется в сторону ЕС, поскольку приток прямых иностранных инвестиций (ПИИ) из ЕС в период 2010-2017 гг. составляет примерно 73 процента от общего объема. Вторым по величине инвестором является Россия, на долю которой приходится менее 10 процентов. Совокупные ПИИ ЕС в семь с половиной раз выше, чем Российской Федерации.[11] В общем, если оценивать ситуацию в Сербии исключительно с точки зрения экономической рациональности, у ЕС нет альтернативы. Однако эта информация должна доходить до большей части сербского населения, на которую могут оказывать воздействие другие соображения, на которые влияют послания, касающиеся эмоций и солидарности в отношении вопросов идентичности. Более того, даже исходя из чисто экономических соображений, необходимо учитывать, что часть торговли, прямых иностранных инвестиций и других видов активов сосредото-

[9] Julija Simić, "Serbia in the EU in 2025 – Mission (Im)possible," *Euractiv.rs*, April 5, 2019, https://www.euractiv.com/section/enlargement/news/serbia-in-the-eu-in-2025-mission-impossible.

[10] К концу мая 2019. См. Commission Staff Working Document, *Serbia 2019 Report*, в сочетании с документом "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2019 Communication on EU Enlargement Policy," COM (2019) 260 final, Brussels, May 29, 2019, SWD(2019) 219 final, 4, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-serbia-report.pdf.

[11] The Delegation of the European Union to the Republic Serbia, FDI to Serbia, Imports to Serbia, Exports from Serbia, http://europa.rs/serbia-and-the-eu/trade/fdi-in-serbia/?lang=en; http://europa.rs/serbia-and-the-eu/trade/serbia-total-imports/?lang=en; http://europa.rs/serbia-and-the-eu/trade/serbia-total-exports/?lang=en.

чена в определенных стратегических отраслях экономики, таких как энергетика (Россия) и телекоммуникации (Китай), что может оказывать влияние на восприятие экономической зависимости.

Также важно отметить, что приверженность ЕС к Сербии как стране-кандидату выходит за рамки торговли и инвестиций. А именно, Сербия является «крупнейшим получателем безвозмездной помощи ЕС на Западных Балканах и одним из крупнейших в мире».[12] Это понятно в свете того факта, что Сербия является крупнейшей экономикой и самой густонаселенной страной Западных Балкан, и трудно представить следующее расширение ЕС в регионе без присоединения Белграда. Европейский Союз является крупнейшим донором Сербии, «оказавшим более 3 миллиардов евро безвозвратной помощи за последние 15 лет… и партнером номер один страны в поддержке развития и текущих реформ». Гранты, предоставленные за последние 15 лет, были направлены на содействие развитию во всех областях, начиная от верховенства закона, государственной административной реформы, социального развития, образования, окружающей среды, улучшения инфраструктуры и сельского хозяйства.[13]

Ясно, что есть проблемы с продвижением Сербии к членству в ЕС с обеих сторон. Наиболее важные из них перечислены ниже:

1. Колебания ЕС вызваны как факторами, проистекающими из ситуации в Сербии, так и другими, не связанными с этим. Что касается Сербии, то конечно не помогает то, что долгосрочная политическая ориентация страны, включая присоединение страны к Западу, не так однозначна, как в случае центрально европейских государств в 1990-е годы, когда они впервые продемонстрировали свое стремление примкнуть к Западу и стать членами ЕС (и НАТО). Международная политическая ориентация страны должна быть исключена из политики межпартийного соперничества, по крайней мере в качестве стратегической цели. Есть и другие вопросы, по которым улучшения могли бы быть более убедительными, например снижение уровня коррупции, надлежащее управление и другие.

2. Колебания ЕС также связаны с проблемами, не имеющими отношения к Сербии. Конец 1990-х годов характеризовался энтузиазмом в европейской политике; у политиков создалось впечатление, что Европа находится на пути к объединению и прочному миру. В конце 2010-х многие в Европе настроены скептически, Европа производит впечатление вновь разъединенного континента, а Западные Балканы могут быть последним неспокойным регионом в дополнение к некоторым бывшим советским республикам (Украине и Грузии). На европейском континенте нет прочного мира. Между Западом и Россией существует геополитическое соперничество. Кроме того,

---

[12] The Delegation of the European Union to the Republic Serbia, “EU and Serbia at Work,” http://europa.rs/eu-assistance-to-serbia/eu-and-serbia-15-years-of-partnership/?lang=en.

[13] The Delegation of the European Union to the Republic Serbia, “EU and Serbia at Work.”

некоторые новые члены ЕС, вступившие в ЕС с 2004 года, не особенно хорошо выполняют свои обещания. Система сдержек и противовесов не соблюдается, независимость судебной системы нарушается, права человека подрываются такими мерами, как господство в СМИ нескольких лояльных акторов и подельников, политическая власть используется для обогащения членов политического истеблишмента и наблюдается все такой же высокий уровень коррупции среди других. Совершенно очевидно, что ЕС не хочет совершить еще одну большую ошибку и принять государства, которые не выполняют обещаний после вступления в ЕС. ЕС не хочет видеть новых членов, которые рассматривают членство как «дойную корову», не соблюдая при этом некоторые из основополагающих ценностей Союза и не проявляя солидарность по важнейшим вопросам.

Тот факт, что ЕС с момента публикации февральского документа 2018 года занимался расширением Западных Балкан как рутинным делом, был обусловлен различными факторами. Единственная наиболее важная причина то, что ЕС был занят другими вопросами, начиная от BREXIT и заканчивая разногласиями по поводу миграции и оспаривания некоторыми печально известными членами согласованных ценностей. Более того, смена караула на нескольких руководящих должностях, включая Комиссию ЕС, Европейский парламент, Европейский совет и Европейский центральный банк, отвлекла внимание, по крайней мере, на время. Параллельно этому так называемый берлинский механизм, посвященный Западным Балканам, угасает из-за ослабления приверженности Германии к расширению. Сделает ли ЕС под новым руководством расширение на Западных Балканах своим приоритетом, еще предстоит увидеть.

Сербия имеет серьезные поводы для недоверия по отношению к НАТО, обусловленные 78 ночами бомбардировок в марте-июне 1999 года. Это также страна, которая регулярно подтверждает свой нейтралитет. Однако это не означает, что она не имеет отношения к Атлантическому альянсу. Она участвует в программе «Партнерство ради мира» (ПРМ), подписала Программу индивидуального партнерства (IPAP) и участвует в учениях со странами-членами НАТО. Отсюда можно сделать вывод, что Сербия проводит векторную внешнюю политику и политику безопасности в определенных пределах. Хотя членство Сербии в НАТО не является актуальной проблемой, и ситуация не изменится в ближайшее время, остается вопрос, можно ли повлиять на ситуацию с безопасностью Белграда каким-либо иным образом. Есть одна региональная проблема, которая тесно связана с безопасностью Сербии. А именно, поскольку Белград приближается к ЕС и, возможно, станет его членом в следующем десятилетии, проблема состоит в том, как избежать резкого разрыва между Сербией и Боснией и Герцеговиной. Ясно, что с его нынешним прогрессом и с его конституционной системой Сараево не может стать членом ЕС. Однако, если Белград станет членом ЕС без каких-либо перспектив для Боснии и Герцеговины, у боснийских сербов будет

два варианта: стать сербскими гражданами, как индивидуумы, или присоединиться к Сербии с территорией Республики Сербской. Хотя членство в НАТО не решит эту проблему, оно может облегчить ее решение.[14]

Как и в случае с более ранними расширениями, важно сохранять стратегический приоритет и политическое внимание, поскольку без этого стремление к расширению рассеется в руках технократов. У различных сил на Западных Балканах уже складывается такое впечатление.[15] Стратегический подход, вероятно, поможет сделать различные выводы относительно сроков и некоторых подробностей условий присоединения. Однако возникает деликатный вопрос: в какой степени ЕС должен идти на компромисс с условиями вступления во имя признания того, что оно является частью геополитического соперничества, прежде всего с Российской Федерацией. Это также поднимает вопрос о том, в какой степени кандидаты могут использовать стратегическую важность расширения и, следовательно, изменить дискурс в свою пользу. Несомненно, обе стороны осознают эту дилемму и рассматривают подход к расширению как инструмент.

Встречные интересы России и ее средства

Российская Федерация никогда не покидала Западные Балканы. Ее присутствие было постоянным, хотя его интенсивность, акценты и последствия российской политики изменились с 1990-х годов. С тех пор, как войны в бывшей Югославии подошли к концу, интересы России были сосредоточены на принятии неизменных обязательств без вкладывания больших материальных ресурсов или, в том же плане, лучших людей туда. Такое отношение может быть связано с признанием того, что малые и средние государства Западных Балкан менее важны, чем великие державы, с которыми Москва считает себя членами одной и той же лиги, или чем государства-преемники Советского Союза с традиционно более высоким значением для России.

Отношения между Россией и Западными Балканами строятся на схожей основе:

1. Политическое ангажирование основано на различных дискурсах в соответствии с ожиданиями принимающей страны и ее населения.
2. Политика идентичности является ее неотъемлемой частью. В Хорватии речь идет о славянских корнях; в Сербии это дополняется упором на православие, и то же самое касается сербов в других странах региона.

---

[14] Я не отрицаю, что такое решение является вторым по желательности. Безусловно, было бы лучше преодолеть наследие Дейтона и поставить Боснию и Герцеговину на путь членства в ЕС. Однако в нынешних условиях это может быть иллюзией.

[15] Для более обстойного обзора такой позиции см. European Movement Serbia and Embassy of the Federal Republic of Germany in Serbia, “Twelve Proposal for EU Enlargement from the Western Balkans” (Belgrade, June 2018), http://www.emins.org/wp-content/uploads/2018/06/Twelve-Proposals-web.pdf.

3. Российское присутствие и вклад усиливаются специально подобранными информационными сообщениями. Россия инвестировала в это через новостную программу на сербском языке каналов RT и Sputnik News. Последний обращается к сообществам на разных языках. Они часто поддерживают политиков, находящихся у власти в соответствующих государствах, подрывают доверие к оппозиции, говорят об их жестокости во время восстания,[16] и пытаются отчуждать население от Запада.[17]
4. Определенную роль играет также искажение истории, включая представление преувеличенной роли Советского Союза в освобождении Югославии во Второй мировой войне. Трудности, которые характеризовали советско-югославские отношения конца 1940-х годов, вычеркнуты из истории, в то время как поддержка Россией Сербии в Дейтонском мирном соглашении и даже больше, в так называемой войне в Косово 1999 года, часто подчеркивается.
5. Отношения между Россией и Западными Балканами часто визуализируются посредством символических встреч на высшем уровне в контексте хорватов, сербов и боснийских сербов. Это включает в себя президентские встречи, в том числе высокопоставленный визит президента Путина в Сербию в 2019 году. Такой визит является заметным и включает литургические элементы.
6. В контексте Сербии, государства, которое, в отличие от большинства государств Западных Балкан, не является ни членом НАТО, ни приближается к нему, сотрудничество имеет важный символический военный компонент, включая военную помощь России.
7. Российская политическая поддержка распространяется на Сербию и в том, что касается ее притязаний на принадлежность Косово Сербии.
8. В целом российский экономический след относительно невелик. Торговля Западных Балкан с Россией составляет примерно 4 процента от общего объема, включая 3,1 процента от экспорта и 4,9 процента от импорта.[18]

---

[16] Смотрите отчет RT о поведении протестующих против правительства в Белграде: “Serbian Anti-govt Protesters Break through Police Cordon & Block Presidential Palace,” *RT*, March 17, 2019, https://www.rt.com/news/454071-serbia-vucic-protest-police/.

[17] Достаточно упомянуть обширные репортажи Sputnik News о широко распространенном непристойном поведении на Западе, включая гомосексуальность и наготу, которые имеют целью оттолкнуть многих мусульман. См. https://sputniknews.com/tags/tag_Albania/.

[18] См. Eurostat, “Western Balkans Countries-EU – International Trade in Goods Statistics,” *Eurostat: Statistics Explained*, May 2019, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Western_Balkans-EU_-_international_trade_in_goods_statistics&oldid=480316.

В общем, российское присутствие на Западных Балканах имеет неоднозначную основу, включая сильные и слабые стороны, перечисленные выше. Сербия принадлежит к тем государствам, которые из-за размеров, исторических и религиозных связей (и некоторой загадочности) и предстоящего спора по Косово привлекают к себе внимание Москвы. При этом создается впечатление, будто Москва является альтернативой для Белграда. Если мы более внимательно посмотрим на некоторые из этих факторов, картина станет более нюансированной.

1. Относительно низкая интенсивность экономических отношений между Россией и Западными Балканами в целом и с Сербией в частности, с точки зрения как торговли, так и инвестиций, не означает незначительность России во взаимных отношениях.

- В Сербии компании, принадлежащие России или косвенно связанные с ней, контролируют около 13 процентов доходов национальной экономики.
- Прямая зависимость дополняется косвенными элементами, такими как зависимость от российского сырья, экспорт в Россию и задолженность за поставки газа.
- Сербия сильно зависит от поставок газа «Газпром»-ом и в значительной степени зависит от поставок нефти «Лукойл»-ом. Местные политические посредники препятствуют диверсификации энергетических рынков.
- Зависимость от газа будет еще больше увеличиваться из-за транзита, связанного с продолжением «Турецкого потока», и сотрудничества с Россией в снабжении некоторых частей Сербии сжиженным природным газом, где трубопроводы не достигают мест проживания.
- Зависимости способствуют российские кредитные схемы.[19]
- Российский государственный Сбербанк вышел на рынок Сербии в 2012 году и приобрел «банковское подразделение Volksbank International в Центральной и Восточной Европе».[20]

2. Связь с Россией очень заметна в военных вопросах. Сербские офицеры учатся в военных академиях России. Сербские военные проводят учения с российскими военными. С 2013 года Сербия имеет статус наблюдателя при Организации Договора о коллективной безопасности (ОДКБ) и имеет «дей-

[19] Centre for the Study of Democracy (CSD), "Assessing Russian Economic Footprint in Serbia," *Policy Brief* no. 72, January 29, 2018, https://csd.bg/publications/publication/policy-brief-no-72-assessing-russias-economic-footprint-in-serbia, 1.

[20] CSD, "Assessing Russian Economic Footprint in Serbia," 12.

ствующее соглашение о военном сотрудничестве с Россией, которое позволяет российским военным базироваться в аэропорту Ниша».[21] Наконец, что не менее важно, Сербия получила российское вооружение и технику из России, в том числе разведывательные и патрульные машины БРДМ-2, боевые танки Т-72 и боевые самолеты МиГ-29. Несмотря на то, что это выглядит впечатляюще, на самом деле они довольно устаревшие, и в случае с МиГ-29 затраты на модернизацию должна нести Сербия.

3. Россия оказывает дипломатическую поддержку находящимся у власти в Белграде, что очень важно, когда руководство оказывается под угрозой. Хотя это выражается несколько двусмысленно, например, когда министр иностранных дел России Сергей Лавров подтвердил, что Россия чрезвычайно заинтересована в долгосрочной стабильности и процветании всего региона Западных Балкан, это все же было заявлено.[22] Это можно было рассматривать только как циничное заявление всего через несколько месяцев после попытки Российской Федерации осуществить государственный переворот против избранных лидеров Черногории и попыток вбить клин между политическими силами в (как она сейчас называется) Республике Северная Македония. Однако Россия, безусловно, заинтересована в стабильности Сербии, поскольку маловероятно, что нестабильность (или любые потрясения) пойдут на пользу Москве.

В совокупности, Российская Федерация намерена надолго остаться в уравнении Западных Балкан. Ее внимание сосредоточено на государствах, которые не были прочно ориентированы на Запад в отношении институционального сближения с ЕС и НАТО. Другие факторы, такие как экономические возможности, безусловно, также играют роль, например, это сохранило интерес России к Хорватии как инвестору в агропромышленность и в другие области. Сербия находится на пересечении этих двух факторов. Основная цель России – не допустить завершения западной интеграции всего региона. Для этого Москва использует различные средства, в том числе полностью законные, сомнительные с моральной точки зрения, нелегитимные и прямо незаконные. С помощью такого сочетания различных средств удалось создать впечатление, что Сербия не является прочно и бесповоротно определившейся страной в том, что касается ее политической ориентации. При ее ограниченных средствах это максимум, на что Россия может надеяться. Имея ограниченные средства, трудно вносить значительный положительный вклад. Однако этого может быть достаточно, чтобы быть помехой,

---

[21] Официальный сайт Министерства обороны Республики Сербия, www.mod.gov.rs/lat/11655/unapredjenje-standarda-i-modernizacija-vojske-prioriteti-ministarstva-odbrane-11655.

[22] Ministry of Foreign Affairs of the Russian Federation, “Foreign Minister Sergey Lavrov’s remarks and answers to media questions at a news conference following talks with Deputy Prime Minister and Minister of Foreign and European Affairs of Croatia Davor Ivo Stier, Moscow, May 23, 2017,” www.mid.ru/en/web/guest/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/2763697.

особенно когда Запад по-прежнему колеблется в быстром продвижении вперед по завершению интеграции Западных Балкан.

Китай как дополнительный осложняющий фактор

Российская Федерация является актором, который постоянно и с помощью сложного набора средств пытается оказывать влияние на политику Западных Балкан. Это понятно, так как она рассматривает этот регион как последний неспокойный регион Европы. России трудно принять тот факт, что некоторые суверенные государства на территории бывшего Советского Союза могут также захотеть определить свое будущее, а не принимать опеку России. Хотя постепенное приближение Западных Балкан к Западу неоспоримо, пока этот процесс не завершен, Россия чувствует, что у нее есть шанс напрячь свои мускулы.

У Китая не было особого интереса к этому региону после распада Югославии. Однако в результате его глобальной экономической экспансии, которая наконец дошла до всей Европы в последние годы 2010-х годов, когда из-за глобального финансового кризиса старый континент стал более привлекательным, Западные Балканы также достигли порога внимания Китая. Китай проявлял более активный интерес к инициативе «Один пояс – один путь» (теперь «Пояс и путь»), а затем к инициативе 16 + 1 (17 + 1), открыто направленной на Восточно-Центральную и Юго-Восточную Европу. Интерес по-прежнему сосредоточен на экономике и, похоже, не выходит за рамки экономических отношений. Конечно, экономическое взаимодействие зависит от политической стабильности. Мнение о том, что Пекин отдает предпочтение сотрудничеству с политическими системами, аналогичными китайской, широко распространено на Западе, хотя его трудно обосновать доказательствами. Тем не менее, есть свидетельства того, что:

- Китай, как торговый и инвестиционный партнер, более коррумпирован, чем большинство западных экономик;
- Китай предпочитает межправительственные отношения в своих сделках и создает устойчивые зависимости, которые делают его заинтересованным в длительной политической стабильности;
- Большинство его предприятий принадлежат государству, а 35-процентная доля частных компаний (не считая крупнейших) также зависит от китайских политических властей.

На Западных Балканах опасения, исходящие из предыдущих пунктов, в том числе то, что многие политики в регионе не застрахованы от коррупции, дополняются размером экономики. Они могут легко стать зависимыми от крупного партнера, такого как Китай, как инвестора и кредитора. Китай – неоднозначное благо для стран Западных Балкан, не входящих в ЕС, поскольку китайские инвестиции не должны соответствовать требованиям ЕС по снижению финансовой непрозрачности, способствовать прозрачности и соблюдению определенных стандартов в отношении прибыльности и

охраны окружающей среды. Опыт некоторых стран Южной Азии и Африки должен служить предупредительным сигналом.

Ситуация варьируется от страны к стране на Западных Балканах: от Черногории с крупной задолженностью с 78 процентами ее суверенного долга на ВВП до Сербии, где она достигает лишь 12 процентов. Сербия привлекла более 2,5 млрд евро китайских проектов, среди которых самый крупный – модернизация железнодорожного сообщения между Белградом и Будапештом,[23] проект, который вызывает сомнения в своей рентабельности. Однако, поскольку она также представляет 44 процента экономик региона, не входящих в ЕС, ей меньше угрожает доминирование Китая, чем ее более мелким региональным партнерам. Похоже, Белград довольно осторожен с китайскими инвестициями и кредитами, которые он рассматривает как проявление неоколониализма. Еще неизвестно, изменится ли это в свете китайских обещаний и принятия двух соответствующих китайских документов, Руководящих принципов финансирования развития инициативы «Один пояс, один путь» и Рамочной основы устойчивости долга для участия страны в инициативу «Один пояс, один путь».[24] Хотя Китай не признал провозглашение независимой государственности Косово, его присутствие в Сербии (как и в целом на Западных Балканах) сохранило свою экономическую направленность, а поддержка Сербии Китаем не стала особенно заметной. Хотя это может измениться в будущем, необходимо отметить, что экономический аспект в настоящее время является почти исключительным направлением продвижения Китая на Западных Балканах. Растущее общее влияние Пекина без серьезных изменений в его политике и без гораздо более прямого влияния ЕС может создать проблемы в плане распространения надлежащего управления на Западных Балканах. Это, в свою очередь, может подорвать шанс расширения ЕС и его выгоды как для ЕС, так и для жителей государств Западных Балкан.

Болото Косово: отягчающий фактор

Косово перешло от *де-факто* к *де-юре* независимости, провозгласив независимую государственность в феврале 2008 года, которая была признана многими,[25] поскольку Белград больше не мог убедительно выступать за многонациональность. Сербия не смогла найти решение этого вопроса в сотрудничестве с Косово. Поскольку Белград не в состоянии официально принять независимость Косово, он сохранил свою реваншистскую позицию. Это

[23] Valbona Zeneli, “China in the Balkans: Chinese Investment Could Become a Challenging Factor for the European Future of the Western Balkans,” *The Globalist,* April 9, 2019, https://www.theglobalist.com/Balkans-china-fdi-belt-and-road-eu.

[24] Amine Bennis, “China’s Inroads into the Balkans,” *The World Today* (Chatham House, June-July 2019), https://www.chathamhouse.org/publications/twt/china-s-inroads-balkans.

[25] Всего за первые десять лет после провозглашения независимости (февраль 2008) Косово признали 117 государств. См. https://www.kosovothanksyou.com.

не означает, что он был бы готов использовать силовые средства, чтобы изменить статус-кво. Тем не менее, для Сербии этот вопрос не решен. История учит нас, что государства, преследующие реваншистские цели (за исключением самых сильных держав мира), обычно пытаются найти поддержку своим стремлениям. Это создает привязанности и зависимость от их сторонников. Многие государства попали в эту историческую ловушку и дорого заплатили за свою ошибку. Поскольку Российская Федерация открыто поддерживала Сербию в ее стремлении «восстановить» свою территориальную целостность, Москва внесла свой вклад в зависимость, которую оба государства считают выгодной. Если вернуться к корням вопроса, становится ясно, что резолюция 1244 Совета Безопасности ООН, принятая по окончании войны в Косово, оставила неясность относительно территориального статуса Косово.[26] Это произошло, среди прочего, благодаря существенному вкладу Российской Федерации в достижение урегулирования, которое повлекло за собой прекращение военного конфликта НАТО против Белграда.

Право вето России в Совете Безопасности ООН, используемое для блокирования дальнейшего развития государственности Косово, связало внешнюю политику Сербии с Россией. В 2008 году сербское правительство решило, что его политическим приоритетом будет сохранение территориальной целостности страны, что означает также сохранение Косово, а также интеграцию в ЕС. Такой подход способствовал созданию «двухвекторной внешней политики», которая представляет собой биполярную коммуникацию, «балансирующую между Брюсселем и Москвой, и которая стала неизменной для всех сербских правительств».[27] Несмотря на «свое официальное обязательство по интеграции в ЕС, сербское правительство… продолжало проводить внешнюю политику, согласованную как с ЕС, так и с Россией».[28]

Прогресс нормализации остается в некоторой степени неубедительным. Сербия и Косово подписали два соглашения о нормализации отношений при сильном поощрении и содействии ЕС. «После сделок при посредничестве ЕС в 2013 и 2015 годах отношения с Сербией, похоже, нормализуются, но независимость не обязательно привела к демократическому и подотчетному управлению».[29] Официальные представители ЕС оценили подписание соглашений в Брюсселе как «ключевой шаг в нормализации отношений между Сербией и Косово, но также как обязательную предпосылку для продвижения к интеграции в ЕС».[30] Влияние ЕС продолжало усаживать Сербию

[26] Resolution 1244 (1999), adopted by the Security Council at its 4011th meeting, on June 10, 1999, S/RES/1244 (1999), https://digitallibrary.un.org/record/274488.

[27] Helsinki Committee for Human Rights in Serbia, *The Warp of the Serbian Identity*, 191.

[28] Helsinki Committee for Human Rights in Serbia, *The Warp of the Serbian Identity*, 191.

[29] Lana Pašić, "Democracy, 25 years after Yugoslavia," *openDemocracy*, April 3, 2016, https://www.opendemocracy.net/can-europe-make-it/lana-pasic/democracy-25-years-after-yugoslavia.

[30] Dušan Vučićević, "Parlamentarni Izbori u Srbiji 2016," *Političke Analize* 7, no. 25 (2016), 26.

и Косово за стол переговоров. Однако в январе 2018 года лидер косовских сербов был застрелен в Митровице в тот день, когда должны были возобновиться переговоры между двумя сторонами.[31] Это свидетельствует о противодействии процессу примирения. Неоднозначное заявление ЕС, нашедшее отражение в прессе как некое туманное обещание, что Сербия и Черногория могут стать членами Союза в 2025 году, оказало влияние на ведущие переговоры стороны.[32] Косово могло сделать вывод, что урегулирование его статуса через признание в качестве независимого государства будет более актуальным для Белграда, поскольку очевидно, что Сербия не может стать членом ЕС без этого. Как мы знаем, сторона, ощущающая безотлагательную необходимость, будет более склонна к поиску компромисса. Это привело к просчету. Короче говоря, Белград продолжал блокировать членство Приштины в некоторых международных организациях, в то время как последняя ввела стопроцентные таможенные пошлины на сербские, боснийские и герцеговинские товары, что *де-факто* означало, что у них не было шансов на рынке в Косово. Наконец, чтобы способствовать устойчивому решению, возникла идея решить некоторые спорные вопросы между Сербией и Косово путем обмена территориями. Однако это означало бы отход от позиции так называемой Контактной группы, которая существовала с начала 21 века. Есть страны, которые активно поддерживают такое решение, например, США; другие, как Франция, колеблются, а некоторые опасаются хаоса, например, Германия. Этот вопрос также вызывает разногласия во внутренней политике, поскольку некоторые лидеры поддерживают его, например президент Косово, в то время как другие, например, бывший премьер-министр страны, выступают против него. Если не будет консенсуса, вопрос останется без решения.

Российская Федерация никогда не заявляла, что не признает независимость Косово; скорее Россия выразила мнение, что она присоединится к соглашению, которое Сербия считает приемлемым. Во второй половине десятилетия Москва начала осознавать приближение решения вопроса о государственности Косово. Это уменьшило бы влияние России на Западных Балканах. Москва предприняла ряд мер, чтобы предотвратить это неблагоприятное развитие событий. Россия выразила готовность выступить посредником между сторонами, чтобы подорвать монополию ЕС в сербско-косовских отношениях. Однако было очевидно, что Россия хочет лишь затянуть процесс и получить влияние. Москва также стала активно способствовать отмене признания косовской независимости. В целом во второй половине

[31] John R. Schindler, "Mysterious Balkan Assassination Threatens Regional Peace," *Observer*, 16 January 2018, http://observer.com/2018/01/assassination-of-oliver-ivanovic-threatens-peace-in-balkans.

[32] Communication from the Commission to the European Parliament, "A Credible Enlargement Perspective," point 5.1.

2010-х годов 14 малых государств отказались от государственного признания Косово. В Белграде это расценили как успех, а Россия, по понятным причинам, не афишировала свою роль в этом процессе.[33]

В течение первой половины 2010-х годов правительство Сербии измеряло изменение общественного мнения и рассматривало вопрос предложить ли Косово и когда признание его государственности.[34] В июле 2015 года 72 процента сербского населения полагали, что Сербия будет вынуждена признать Косово, чтобы присоединиться к Европейскому Союзу, в то время как 57 процентов придерживались мнения, что Сербия должна отказаться принять это, даже если это будет означать, что она останется вне ЕС. Снижение желания населения к вступлению в ЕС показано в следующей статистике: в октябре 2009 года интеграцию в ЕС поддержали 76 процентов, в августе 2010 года 71 процент, в апреле 2011 года 69. К ноябрю 2015 года этот процент снизился до 49.[35] Опросы, проведенные в 2019 году, показывают, что 78 процентов респондентов не поддержали бы решение о признании независимости Косово в обмен на более быстрое вступление Сербии в ЕС. В то же время 27 процентов респондентов считают, что правительство Сербии признает государственность Косово. Эти результаты особенно интересны учитывая, что 47 процентов респондентов считают, что Косово потеряно для Сербии.[36] Важно внимательно следить за тенденциями, поскольку сербские политики могут не захотеть рисковать своим будущим ценой признания Косово, в то время как трудно представить продолжение процесса расширения ЕС Сербией без такого признания. Однако мониторинг общественного мнения может иметь значение не только для сербских политиков, но и для официальных лиц ЕС и политиков стран-членов. Это привело бы к странной ситуации, если бы ближе к переговорам о вступлении ЕС «проснулся» и пришел к выводу, что население Сербии (и, следовательно, политический класс) не желает платить цену за вступление, признавая *де-факто* территориальный статус-кво.

Способы смягчения этой дилеммы – выводы

Принимая во внимание все еще существующую ориентацию Сербии на Европейский Союз, процесс интеграции следует ускорить. Усилия обеих сторон, ЕС и Сербии, должны быть сосредоточены на углублении понимания

[33] Сайт, на котором перечислены страны, признавшие независимость Косово, не содержит информации о странах, отозвавшие признание. См.: www.kosovothankyou.com.

[34] Centre for Insight in Survey Research, “Survey of Serbian Public Opinion: November 24 – December 3, 2015,” http://www.iri.org/sites/default/files/wysiwyg/serbia_november_2015_poll_public_release.pdf.

[35] Centre for Insight in Survey Research, “Survey of Serbian Public Opinion.”

[36] “Većina građana Srbiji smatra da je Kosovo traino izgubljen,” *SEEbiz,* March 31, 2019, по состоянию на 23 ноября 2018, http://rs.seebiz.eu/vecina-gradana-srbije-smatra-da-je-kosovo-trajno-izgubljeno/ar-191944.

демократии и европейской идентичности. Политический диалог необходимо активизировать в сфере безопасности, политических и экономических рамках для развития безопасности Сербии и социально-экономической системы в ясном направлении. Развитие страны, повышение уровня жизни, обеспечение большей прозрачности и свободы прессы, изменение политической риторики в конечном итоге будут способствовать переходному процессу и интеграции в ЕС.

Усиление роли гражданского общества в развитии и защите свободных СМИ ослабит разжигание ненависти и препятствия на пути демократических процессов. «Роль средств массовой информации занимает центральное место в жизни многих людей в Сербии…», и Европейский Союз должен использовать механизмы для поддержки «свободных и независимых СМИ в Сербии, а также для возвращения (или на деле введения) в страну международных медиа порталов».[37] Роль СМИ в формировании общественного мнения неоспорима. Кроме того, инвестиции в соответствующее образование молодежи подготовят будущие поколения к пониманию демократических стандартов и их соблюдению.

Несмотря на факт, что «сербская общественность выразила свое недовольство условиями ЕС», Европейский Союз должен вернуть себе репутацию и «прояснить требования Сербии в отношении Косово» и «учесть чувствительные вопросы Сербии в процессе присоединения»,[38] в противном случае Россия и Китай проявят более широкую заинтересованность в улучшении своего «безусловного» сотрудничества. Большая гибкость и четкий диалог по важнейшим вопросам могут способствовать прогрессу. Европе следует более серьезно рассмотреть возможные последствия для нее от наличия различных геополитических интересов на Балканах, а не создавать жесткие, часто технические условия для членства. Дальнейшая отсрочка интеграции всех остальных западно-балканских стран может привести к потере региона. Однако государства западных Балкан, которые стремятся к членству в ЕС, также должны найти способы более эффективной борьбы с теми явлениями, которые создают препятствия для членства в ЕС (включая коррупцию и недостаточный управленческий потенциал).

Сохраняющаяся напряженность в регионе требует интенсивного участия и более сильного присутствия Соединенных Штатов, а также поощрения Евросоюза к вступлению стран Западных Балкан. Программы Соединенных Штатов по укреплению экономического роста, верховенства закона и

[37] European Parliament, "Serbia's Cooperation with China, the European Union, Russia and the United States of America," EP/EXPO/B/AFET/2017/09 (Directorate-General for External Policies, Policy Department, November 2017), 44, https://www.europarl.europa.eu/cmsdata/133504/Serbia%20cooperation%20with%20China,%20the%20EU,%20Russia%20and%20the%20USA.pdf.

[38] European Parliament, "Serbia's Cooperation with China," 45-47.

борьбы с коррупцией по-прежнему важны для евроатлантической интеграции региона,[39] но недостаточны. Крайне необходимо укрепление политического диалога и более активное участие руководства США в делах на Балканах.

Следовательно, это может быть еще одна возможность, что «ЕС и США нуждаются в совместной стратегии, которая должна включать общую политику по устранению угроз региональной безопасности, четкую перспективу членства в ЕС и НАТО, а также разработку общей энергетической политики».[40] В настоящее время это может быть проблематично, поскольку у США и ЕС, а также у некоторых более крупных членов ЕС есть много других спорных вопросов в повестке дня, которые затрудняют преодоление и переориентацию внимания на Западные Балканы. Однако у США, похоже, есть четкое представление о том, как выйти из тупика Сербия-Косово, и их вклад в этом вопросе может оказаться незаменимым. Общие интересы Запада и стран Западных Балкан должны заключаться в поддержке стабильности, экономического развития, демократического перехода и восстановления возможностей интеграции в ЕС.

Безопасная среда может способствовать увеличению иностранных инвестиций, что положительно скажется на развитии. Государству следует повышать осведомленность общественности о важности ЕС, его преимуществах и последствиях для будущего социально-экономического развития Сербии. Интеграция Сербии в ЕС также является неотложной задачей для защиты ее от иностранного вмешательства, которое может привести страну, а вместе с ней и регион, к политической стагнации и изоляции. Сегодня внешняя политика Сербии опирается на четыре основные внешние фактора: Европейский Союз, Соединенные Штаты, Российская Федерацию и Китай. В краткосрочной перспективе Сербия может поддерживать «неустойчивое равновесие». Однако дальнейший прогресс на пути к вступлению в ЕС может означать, что Сербии придется «пожертвовать некоторой независимостью в иностранных делах».[41] ЕС, в свою очередь, должен найти способы быть более заметным в Сербии и на Западных Балканах в целом и «лучше продавать» свой существенный вклад в развитие региона.

Важно понимать роль России в попытке дестабилизировать Балканский регион, которая скрывается за панславянской политической риторикой.

---

[39] John McCain, “The Balkans Are Heating Up Again - and Washington Is Nowhere to Be Seen,” *The Washington Post*, April 27, 2017, https://www.washingtonpost.com/news/democracy-post/wp/2017/04/27/the-balkans-are-heating-up-again-and-washington-is-nowhere-to-be-seen/.

[40] Ernst M. Felberbauer and Predrag Jureković, “A Region in Limbo: South East Europe in the Light of Strained Western-Russian Relations,” Study Group Information Band 26/2015 (Republic of Austria, Federal Ministry of Defense and Sports, September 2015), https://www.bundesheer.at/wissen-forschung/publikationen/publikation.php?id=936, 114-115.

[41] European Parliament, “Serbia’s Cooperation with China,” 1-38.

Превосходство России в формировании идентичности населения Сербии может быть сигналом Европейскому Союзу о его неэффективности и неспособности сделать то же самое. Стратегическое партнерство, «оправданное» экономическим сотрудничеством, нереально в свете расстояния между Сербией и Россией, а также из-за того, что Сербия уже осуществляет большую часть своей торговли и прямых иностранных инвестиций со странами ЕС.

Если Сербия желает присоединиться к Европейскому Союзу, необходимо прекратить балансирование между Брюсселем и Москвой. «Западные Балканы стали частью новой геополитической конкуренции».[42] Политика, которой следует придерживаться, это внешняя политика Европейского Союза. С другой стороны, Брюссель должен сделать все возможное, чтобы не допустить дальнейшего препятствования Россией европейской и евроатлантической интеграции в будущем. Сила России в Сербии – это слабость ЕС.

Отказ от ответственности

Об авторе

Весна Павичич – госслужащий Министерства безопасности Боснии и Герцеговины. С 2018 года она служит в Специальной мониторинговой миссии (СММ) ОБСЕ в Украине.

[42] Felberbauer and Jureković, “A Region in Limbo,” 114.

Connections: The Quarterly Journal
Правила подачи рукописей

Журнал *Connections* принимает рукописи в объеме от 2 000 до 5 000 слов, в ясном стиле, для целевой аудитории, включающей компетентные лица, занимающиеся практикой или академической деятельностью, связанной с обороной и безопасностью. Все рукописи подаются в редакционный отдел журнала *Connections* в электронном виде по адресу PfPCpublications@pfp-consortium.org. В верхней части первой страницы должны быть указаны имя автора, учреждение, с которым в настоящее время связан автор и предварительное название статьи. В случае необходимости рукопись снабжается подстрочными замечаниями. Кроме того, авторы должны предоставить рукопись резюме и ключевых слов.

В число предпочтительных тем для будущих выпусков журнала входят:

- Эксплуатация и безопасность Арктики
- Контроль над вооружениями и перевооружение Европы
- Вызовы и возможности общего использования разведывательных ресурсов
- Противодействие и превенция насильственного экстремизма
- Кибербезопасность
- Строительство институций обороны
- Будущие сценарии безопасности
- Гибридная война
- Ограничения военно-морской мощи
- Миграция и беженцы
- Нестабильная периферия НАТО
- Россия Путина: угроза миру или угроза для себя?
- Терроризм и иностранные боевики
- Тенденции в организованной преступности

По вопросам, касающимся подстрочных замечаний и ссылок, пожалуйста, используйте *Chicago Manual of Style*. Инструкции на оформление можно найти по адресу: www.chicagomanualofstyle.org/tools_citationguide.html.

Рукописи, выходящие за рамки приоритетных тем, принимаются в порядке поступления по усмотрению Редакционного совета.

Теория сдерживания возникла с появлением ядерного оружия, чтобы решить проблемы подготовки к полномасштабной ядерной войне между США и СССР и ее предотвращения. Материалы для этого специального выпуска связаны с контекстом периода после окончания Холодной войны с возрождающейся и агрессивной Россией. Набор статей кратко излагает теорию сдерживания, текущую практику ее применения в сдерживании и, в случае необходимости, в защите НАТО и восточного фланга Европы с использованием против агрессии обычных сил, а также критический анализ его связи с кибер и гибридной войной.

По всем вопросам, касающимся журнала CONNECTIONS, пожалуйста связывайтесь с:

Partnership for Peace - Consortium
Managing Editor
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
Телефон: +49 8821 750 2256
Адрес электронной почты:
PfPCStratCom@marshallcenter.org

ISSN 1812-1101