10.46272/2587-8476-2022-13-2-79-94

Эволюция национальных подходов к ведению кибервойны

Карасев Павел Александрович, ИМЭМО им. Е.М. Примакова, Центр проблем информационной безопасности ВМК МГУ, Москва, Россия

Контактный адрес: karpaul@iisi.msu.ru

АННОТАЦИЯ

Новейшие информационно-коммуникационные технологии (ИКТ) все чаще рассматриваются государствами как инструмент проецирования своей мощи и реализации национальных интересов. Наиболее значимые в военном отношении страны за последние 20 лет создали доктринальные, материально-технические и организационные основы ведения военной деятельности в ИКТ-среде, а отдельные государства уже открыто декларируют приоритет наступательных кибероперациий, что значительно повышает риски непреднамеренной эскалации. Текущая ситуация, связанная с военно-политическим освоением ИКТ-среды, предопределяет острую необходимость непрерывного анализа актуальных тенденций в этой сфере и поиска подходов к снижению напряженности. Для достижения этой цели в первой части статьи подробно рассмотрены релевантные доктринальные и стратегические документы США и других ключевых стран, выявлены этапы и особенности процесса эволюции их подходов. Далее, с учетом полученных результатов, рассмотрены и оценены факторы, которые оказывают влияние на военную стабильность в ИКТ-среде. Сделан вывод, что выявленные факторы в совокупности оставляют безальтернативной задачу выработки международных механизмов снижения эскалации в этой сфере. Эта задача приобретает особую остроту в условиях общей международной нестабильности. Международное сообщество в целом и отдельные страны (прежде всего, Россия и США) осознают опасность непреднамеренной эскалации в ИКТ-среде, особенно в контексте поддержания стратегической стабильности, и готовы делать шаги к выработке механизмов регулирования и предотвращения киберконфликтов. Актуальность сотрудничества сохраняется, т.к. проблему противодействия киберугрозам по-прежнему нельзя в полной мере решить только односторонними мерами. Вопрос в том, какую форму примет это сотрудничество, учитывая все политические реалии.

КЛЮЧЕВЫЕ СЛОВА

международная информационная безопасность, кибератаки, кибероружие, внешняя политика США, информационное пространство

Сегодня в экспертном сообществе и среди политических элит развитых государств есть уверенность в том, что информационные технологии являются важным инструментом реализации национальных интересов, который имеет множество предназначений и может быть использован во многих сценариях – от кибершпионажа до силового или информационно-психологического воздействия. Об этом говорят как исследования в этой области, так и национальные и наднациональные доктрины и стратегии. По некоторым оценкам[1], в 2015 г. уже более 60 государств мира обладали специализированными ИКТ-средствами – кибероружием. Ставший хрестоматийным пример использования вируса *STUXNET* в кибератаке против ядерных объектов Ирана в 2010 г. наглядно демонстрирует, что сегодня есть возможность оказывать воздействие на объекты физического мира посредством ИКТ-инструментов через виртуальную среду. В то же время сегодня нет согласованного и общепринятого определения как «кибервойны», так и того, что понимать под вооруженным нападением в киберпространстве.

Определение понятию «агрессия» было дано ООН в 1974 г.: «Агрессией является применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом Организации Объединенных Наций»[2]. Представляется, что действия в киберпространстве могут быть квалифицированы в качестве «применения вооруженной силы» в весьма ограниченных сценариях. Например, существует мнение, что с точки зрения международного права некоторые кибератаки в определенных условиях приобретают черты актов агрессии, например нарушение суверенитета и политической независимости государства[3].

На протяжении последних 20 лет непрерывно эволюционируют концептуальные, доктринальные и материально-технические рамки кибервойн. Анализ этого процесса и выявление тенденций позволят достигнуть основной цели исследования – актуализировать понимание текущей позиции государств и «красных линий» в ИКТ-среде, а также прийти к выводам относительно возможных путей снижения напряженности в этой сфере. Для этого необходимо, во-первых, рассмотреть имеющуюся терминологию и выявить концептуальные характеристики, присущие деструктивной военно-политической деятельности в киберпространстве. Во-вторых, необходимо провести сравнительный анализ различных зарубежных доктрин и иных документов стратегического планирования, относящихся к военному использованию ИКТ – при этом, ввиду особой роли США, эволюция подходов этой страны в указанной сфере может быть рассмотрена в качестве стереотипной модели в рамках концептуализации военного применения ИКТ. Кроме этого, стоит отметить, что многие исследования определяют США как страну с самыми развитыми кибервозможностями[4].

1 Jennifer Valentino-DeVries, and Danny Yadron, "Cataloging The World's Cyberforces," The Wall Street Journal, October 11, 2015, accessed May 25, 2022, https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.
2 Резолюция 3314 «Определение агрессии» (XXIX) Генеральной Ассамблеи от 14 декабря 1974 года // ООН. [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml (дата обращения: 28.03.2022).
3 Лобач et al. 2020, 63.
4 Например, США находятся на первом месте по кибермощи в докладе Белферского центра: Voo et al. 2020.

Вопросы терминологии

Международное сообщество уже более 10 лет назад согласилось с необходимостью разработки терминологического аппарата, который охватывал бы проблемы военно-политического использования ИКТ[1], но работа на этом направлении до сих пор не принесла ощутимых результатов. Так, согласованных терминов не содержится в докладах Группы правительственных экспертов (ГПЭ) ООН[2]. В то же время важно подчеркнуть, что ГПЭ в своих документах неизменно подтверждает наличие угрозы использования ИКТ в деструктивных военно-политических целях[3].

Значительные усилия по разработке согласованного терминологического аппарата предпринимаются научным сообществом. Так, в 2011-2013 гг. в рамках исследовательской работы, проведенной Институтом проблем информационной безопасности МГУ и американским Институтом Восток – Запад, были выпущены две методологически сильные публикации с важнейшими согласованными терминами в области международной информационной безопасности[4]. В 2014 г. вышел доклад аналитического центра *New America* «Компиляция существующих определений в области кибербезопасности и безопасности информации», который через сравнение терминологического аппарата множества документов продемонстрировал наличие как совпадающих взглядов, так и существенных различий[5].

Используя определения, содержащиеся в национальных документах и документах различных организаций, можно попытаться выделить характерные черты того, что сегодня понимается под «кибервойной» или «боевыми действиями в киберпространстве».

В ряде документов можно встретить термин «информационная война», который определяется как «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»[6].

В документах США встречается термин «информационные операции», который определен как «комплексное использование в ходе военных операций информационных возможностей в сочетании с другими направлениями деятельно-

1 Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Одобрен на 65 сессии Генеральной Ассамблеи ООН 30 июля 2010 года // ООН. [Электронный ресурс]. URL: http://www.un.org/ru/documents/ods.asp?m=A/65/201 (дата обращения: 28.03.2022).

2 Группа правительственных экспертов (ГПЭ) ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

3 Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Одобрен на 70 сессии Генеральной Ассамблеи ООН 22 июля 2015 года // ООН. [Электронный ресурс]. URL: http://www.un.org/ru/documents/ods.asp?m=A/70/174 (дата обращения: 28.03.2022).

4 Rauscher et al. 2011.

5 Maurer et al. 2014.

6 Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года // Законодательство стран СНГ. [Электронный ресурс]. URL: http://base.spinform.ru/show_doc.fwx?rgn=28340 (дата обращения: 28.03.2022); Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве // Министерство обороны России. [Электронный ресурс]. URL: http://ens.mil.ru/files/morf/Strategy.doc (дата обращения: 28.03.2022).

сти для оказания влияния, подрыва, искажения или перехвата принятия решений противниками и потенциальными противниками»[1], а также термин «операции в киберпространстве» – «такое использование кибервозможностей, когда основной задачей является достижение целей в киберпространстве или через него»[2].

Национальная киберстратегия Великобритании определяет «наступательные действия в киберпространстве» как «добавление, удаление или манипулирование данными в системах или сетях для достижения физического, виртуального или когнитивного эффекта...»[3]. Министерство обороны Франции определяет кибератаки как «злонамеренный акт взлома в киберпространстве», к которому относятся «дезинформация, электронный шпионаж, воздействие на данные в ходе боевых действий, нарушение критически важной инфраструктуры страны»[4]. В Стратегии кибербезопасности Германии термин «кибератака» определяется как «воздействие на одну или несколько информационных систем через киберпространство, целью которого является полное или частичное нарушение их информационной безопасности с помощью ИКТ-средств»[5].

В публикации, подготовленной Институтом проблем информационной безопасности МГУ и Институтом Восток-Запад, приведено следующее определение термина «кибервойна»: «высшая степень киберконфликта между или среди государств, во время которой государства предпринимают кибератаки против киберинфраструктур противника как часть военной кампании; может быть формально объявлена одной (всеми) сторонами конфликта или не быть объявленной формально и проходить *de facto*»[6].

Приведенные определения позволяют выделить концептуальные характеристики, присущие действиям в киберпространстве. Важно отметить, что в мире сложилось два основных подхода к обеспечению безопасности ИКТ-среды. В России, Китае и ряде других государств – это информационная безопасность, в то время как в США и странах Запада – кибербезопасность. Информационная безопасность рассматривает угрозы не только информационно-технического характера (киберугрозы), но и информационно-гуманитарные, то есть те, что реализуются посредством целенаправленного вредоносного воздействия на сознание индивидов и общества. В документах стратегического планирования Российской Федерации термины с приставкой «кибер-» не используются. За последние несколько лет наметилось концептуальное сближение указанных парадигм (и это видно из рассмотренных выше определений), однако оно не трансформировалось в более успешное международное сотрудничество. Напротив, ярко проявили себя накопившиеся противоречия, и взаимодействие было фактически подорвано ввиду различий подходов, а не различий в понимании угроз.

1 "Department Of Defense Dictionary Of Military And Associated Terms," US Department of Defense, Joint Publication 1-02, November 8, 2010 (As Amended Through 15 February, 2016), accessed May 20, 2022, https://irp.fas.org/doddir/dod/jp1_02.pdf.
2 Ibid.
3 "National Cyber Strategy 2022," HM Government, accessed May 20, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.
4 "La cyberdéfense au ministère des Armées (Cyber defense at the Ministry of the Armed Forces)," Ministère des Armées (Ministry of the Armed Forces), accessed May 20, 2022, https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees#title-9319.
5 "Cyber-Sicherheitsstrategie für Deutschland (Cyber Security Strategy for Germany)," Bunderministerium des Innern (Federal Ministry of the Interior), 2016, accessed May 20, 2022, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheits-Strategie.pdf.
6 Rauscher et al. 2014, 32.

Очевидно, что сегодня военные действия в ИКТ-среде не ограничены только лишь информационно-техническим воздействием: информационно-гуманитарное или когнитивное воздействие на индивидуальное или коллективное сознание также является их составной частью. В то же время информационно-техническое воздействие не ограничивается виртуальным пространством и может приводить к физическим эффектам, в том числе в объектах критически важной инфраструктуры. Кибер- и информационные воздействия, в зависимости от конкретной доктрины, могут осуществляться как в качестве поддержки военных кампаний в традиционных оперативных пространствах, так и вне их, как самостоятельные действия – возможно, и в мирное время.

Подходы США к военной деятельности в киберпространстве

Соединенные Штаты Америки находятся на передовой процесса милитаризации ИКТ-среды, и эволюцию подходов этой страны к политическому и военно-стратегическому противостоянию в ИКТ-среде можно исследовать в качестве показательной модели. Рассмотрение США приоритетно также и ввиду того, что эта страна определяет политику военно-политического блока НАТО, куда входят 30 государств мира.

В начале 1990-х гг. в США сформировалось представление, что военный истеблишмент стремится воспользоваться теми новыми возможностями, которые появились вследствие информационной революции[1]. Научно-исследовательский центр RAND в 1996 г. опубликовал всеобъемлющее исследование *"Strategic Information Warfare: A New Face of War"*, где новую область противостояния, для которой характерно использование странами киберпространства, назвали «стратегическая информационная борьба»[2].

В том же году Министерство обороны США определило порядок проведения т.н. «информационных операций»[3], целью которых является воздействие на информацию и информационные системы противника[4]. В секретной директиве, которая регламентировала все аспекты информационных операций, отмечено, что они проводятся как в военное, так и в мирное время. По признанию экспертов, разработка операций в мирное время стала причиной секретности этой тематики в США в 1990-х гг.[5]

В новом тысячелетии в США продолжилось осмысление происходящей цифровизации военной деятельности и развитие подходов к использованию ИКТ в военно-политических целях. В «Концепции развития вооруженных сил США до 2020 г.», которая вышла в 2000 г., было зафиксировано, что США должны стремиться к доминированию во всех средах, в том числе и в информационном

1 Molander et al. 1996.
2 Ibid., 1–2.
3 "Department of Defense Directive S-3600.01," U.S. Department of Defense, 1996, accessed May 20, 2022, https://archive.org/details/DODD_S3600.1.
4 Ibid., 9.
5 Armistead 2004, 41.

пространстве[1]. В «Четырехлетнем обзоре обороны»[2] 2001 г. киберпространство было признано новой сферой противоборства.

Важным шагом по созданию практических возможностей осуществления военной деятельности в киберпространстве стало учреждение в 2010 г. соответствующей структуры – Киберкомандования[3], которое отвечает за кибероперации, защиту военных сетей и систем от кибератак, а также координацию кибероборонь. Для скорейшего достижения Киберкомандованием оперативной готовности был подписан специальный меморандум с Министерством внутренней безопасности[4], а также введена двойная должность – руководитель Киберкомандования одновременно является главой Агентства национальной безопасности США (АНБ), которое, помимо радиоэлектронной разведки и криптографии, занимается вопросами проникновения в информационные сети и системы потенциального противника. При этом Киберкомандование и географически расположено там же, где и АНБ – в Форт-Мид, штат Мэриленд.

В 2011 г. США закрепили свою позицию в том, что значимые кибератаки против США могут вызвать ответ любыми доступными средствами – не исключая и применение военной силы[5]. Определенное понимание того, что считать значимой кибератакой, можно получить из «Президентской директивы № 20»[6]. Согласно этому документу, ощутимые последствия включают в себя жертвы среди населения, значительные материальные потери, значительный экономический ущерб.

При Д. Трампе курс на дальнейшую милитаризацию ИКТ-среды еще более укрепился, что нашло отражение в «Киберстратегии Министерства обороны США 2018 г.», которая содержит две новые концепции – *persistent engagement u defend forward*[7]. Реализация «постоянного противодействия» и «обороны за передовой линией» в совокупности означает переход не просто к наступательной концепции кибероборонь, а к агрессивному противоборству, невзирая на возможные риски эскалации. Кроме этого, Киберкомандование было выведено из структуры Стратегического командования и получило большую самостоятельность, а административные барьеры[8], которые требовали длительного согласования наступательных кибероперациий, были сняты. Появление в 2019 г. в СМИ[9] информации о том, что объекты, связанные с выработкой и передачей электроэнергии в России, подверглись кибервторжениям со стороны спецслужб США, можно рассма-

1 "Joint Vision 2020," US Department of Defense, June 2000, p. 6, accessed May 20, 2022, https://www.hsdl.org/?view&did=446826.
2 "Quadrennial Defense Review 2001," US Department of Defense, 2001, p. 7, accessed May 20, 2022, https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/qdr2001.pdf.
3 "Cyber Command Fact Sheet," US Department of Defense, May 2010, accessed May 20, 2022, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf.
4 "Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," US Department of Homeland Security, October 2010, accessed May 20, 2022, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.
5 "International Strategy for Cyberspace," The White House, May 2011, p. 14, accessed May 20, 2022, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
6 "Fact Sheet on Presidential Policy Directive," US Government, January 2013, accessed May 20, 2022, http://epic.org/privacy/cybersecurity/Pres-Policy-Dir-20-FactSheet.pdf.
7 "2018 Department of Defense Cyber Strategy," US Department of Defense, 2018, p. 1, accessed May 20, 2022, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
8 David E. Sanger, "Trump Loosens Secretive Restraints on Ordering Cyberattacks," The New York Times, September 20, 2018, accessed May 20, 2022, https://www.nytimes.com/2018/09/20/us/politics/trump-cyberattacks-orders.html/.
9 David E. Sanger, and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," The New York Times, June 15, 2019, accessed May 20, 2022, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

тривать как неподтвержденное свидетельство практической реализации новой стратегии.

Дж. Байден еще до своего избрания в президенты неоднократно обещал заставить Россию ответить за свои действия в киберпространстве[1]. Он же заявлял, что стратегия «постоянного противодействия» будет пересмотрена, в том числе ввиду рисков непреднамеренной эскалации[2]. Хотя администрация Дж. Байдена еще не опубликовала значимых документов по вопросам военной кибербезопасности, в апреле 2021 г. был выпущен информационный бюллетень, в котором перечислены шаги по противодействию «вредоносной деятельности России за рубежом»[3]. В нем не говорится о пересмотре или смягчении политики Д. Трампа, равно как и не сказано о ее поддержке или развитии. До появления новой стратегии кибероборонны США это можно расценивать как согласие на продолжение реализации «постоянного противодействия» и «обороны за передовой линией».

Подводя краткий итог вышесказанному, можно отметить, что США на протяжении 30 лет последовательно развивают свои кибервозможности и сегодня обладают доктринальными, организационными и материально-техническими возможностями проведения как оборонительных, так и наступательных операций в ИКТ-среде. Киберпространство признано театром военных действий, а значительная кибератака может быть расценена как нападение – с соответствующими последствиями. При этом в документах стратегического планирования США зафиксирована возможность проведения кибероперация против потенциального противника в мирное время. Особенно опасным с точки зрения возможной эскалации представляется закрепление на уровне стратегии подходов, которые оправдывают и предписывают проведение военных кибероперация в мирное время на территории потенциальных противников.

Позиции европейских стран, НАТО и России

Военно-политический блок НАТО объединяет 30 государств в рамках общей политики безопасности, в том числе в ИКТ-среде. При этом нельзя отрицать того, что США играют в этой организации лидирующую и принципиальную роль. Сегодня можно констатировать, что Североатлантический Альянс последовательно развивает возможности наступательных и оборонительных операций в киберпространстве и в этих шагах следует по тому пути, который уже прошли Соединенные Штаты. Так, в 2014 г. было признано, что пятая статья Североатлантического договора (о коллективной обороне) применима к киберпространству[4]. В 2016 г. киберпространство было признано сферой оперативной деятель-

1 “Campaign 2020: Trump-Biden Second Debate,” C-Span, October 22, 2020, accessed May 20, 2022, https://www.c-span.org/video/?475796-1/trump-biden-debate&live.

2 “Cyber Policy,” The New York Times, 2020, accessed May 20, 2022, https://www.nytimes.com/interactive/2020/us/politics/2020-democrats-cyber-policy-foreign-policy.html.

3 “FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government,” US Government, April 2020, accessed May 20, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

4 Заявление по итогам встречи на высшем уровне в Уэльсе // НАТО. [Электронный ресурс]. URL: http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=ru (дата обращения: 28.03.2022).

ности[1], а в феврале 2017 г. были приняты обновленный «План кибероборонны»[2] и дорожная карта по военному освоению киберпространства. В ноябре того же года было принято решение[3] о создании Центра кибероперациий НАТО.

Важнейшие в военном отношении европейские страны также идут по пути наращивания своих оборонительных и наступательных возможностей в ИКТ-среде. Согласно данным за 2021 г.[4], США, Великобритания, Франция и Германия в совокупности покрывают 86% расходов НАТО, и на текущий момент у всех этих государств в том или ином виде есть свои кибервойска.

В декабре 2016 г. было объявлено о создании структуры, подобной Киберкомандованию США, во Франции. Одновременно Ж.-И. ле Дриан, бывший тогда министром обороны Франции, заявил, что в определенных условиях кибератака может считаться актом войны и вызвать ответные действия с использованием наступательного потенциала киберкомандования[5]. В 2018 г. был принят «Стратегический обзор кибероборонны», который положил начало пересмотру и усилению подходов Франции к военным действиям в ИКТ-среде. Одно из главных изменений заключается в разделении киберзащиты и кибернападения. В частности, передача функций киберзащиты из разведывательного сообщества специальной структуре «способствует принятию вмешательства государства в вопросы безопасности информационных систем – в госуправлении и экономике»[6]. В полной версии документа также рассматривается вопрос ответных действий на кибератаку, которые допускаются при условии, что предотвращение, сотрудничество и переговоры не сработают. Ответ может быть дан с использованием кибер- или иных средств. В стратегии также подчеркивается, что крупная кибератака может быть истолкована как вооруженная агрессия в соответствии со ст. 51 Устава ООН[7]. В 2019 г. вышла наступательная военная доктрина, которая интересна тем, что в ней представлен принцип управления рисками при подготовке и проведении наступательных операций: снижение риска эскалации в асимметричной обстановке, или риска побочного ущерба, или непредвиденного косвенного воздействия на гражданскую инфраструктуру[8].

Формирование киберсил Великобритании началось в 2011–2013 гг., когда была создана Группа оборонных кибероперациий[9]. В «Национальной стратегии

1 Заявление по итогам встречи на высшем уровне в Варшаве // НАТО. [Электронный ресурс]. URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=ru. (дата обращения: 28.03.2022).
2 Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Defence Ministers," NATO, February 2017, accessed May 20, 2022, https://www.nato.int/cps/ru/natohq/opinions_141340.htm.
3 Министры обороны стран НАТО встречаются, чтобы продолжить адаптацию Североатлантического союза к XXI веку // НАТО. [Электронный ресурс]. URL: https://www.nato.int/cps/ru/natohq/news_148357.htm?selectedLocale=ru (дата обращения 28.03.2022).
4 "Defence Expenditure of NATO Countries (2014–2021)," NATO, June 2021, p. 7, accessed May 20, 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210611-pr-2021-094-en.pdf.
5 "Worried by Hacker Threat, France Prepares Army Response," Phys.org, December 2016, accessed May 20, 2022, https://phys.org/news/2016-12-hacker-threat-france-army-response.html.
6 "Revue stratégique de cyberdéfense (Strategic Review of Cyber Defence)," Secrétariat général de la défense et de la sécurité nationale (General Secretariat of Defense and National Security), February 2018, p. 5, accessed May 20, 2022, http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf.
7 Ibid.
8 "Éléments publics de doctrine militaire de lutte informatique offensive (Public Elements of Military Doctrine of Offensive Computer Struggle)," Ministère des Armées (Ministry of the Armed Forces), 2019, p. 9, https://www.defense.gouv.fr/sites/default/files/ema/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf.
9 "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World," Cabinet Office, November 2011, p. 26, accessed May 20, 2022, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

кибербезопасности 2016–2021» подтверждено наличие наступательных кибер-средств и заявлено, что реагирование на кибератаки будет осуществляться с использованием наиболее подходящих возможностей, в том числе наступательных кибероперациий[1]. В 2018 г. были обнародованы детали, касающиеся процесса поиска уязвимостей, подобного тому, что ранее был запущен в США. Центр правительственной связи Великобритании и Национальный центр кибербезопасности непрерывно работают над обнаружением уязвимостей безопасности, однако раскрывают лишь часть из них, в то время как другие могут быть использованы в разведывательных целях в интересах Великобритании[2]. Стоит отметить, что т.н. «уязвимости нулевого дня» – то есть те, для которых не создано защиты – фактически являются компонентами, необходимыми для создания кибероружия.

Германия создала Командование кибер- и информационного пространства в 2016–2017 гг. Выступая на церемонии открытия этой структуры, министр обороны Германии У. фон дер Ляйен заявила, что «если сети немецких военных будут атакованы, мы сможем защитить себя. Как только нападение ставит под угрозу функциональную и оперативную боеготовность наших вооруженных сил, мы можем ответить наступательными мерами»[3]. На сегодняшний момент численность задействованного персонала составляет 14448 военнослужащих и гражданских специалистов[4]. В части «Стратегии кибербезопасности Германии», касающейся кибероборонь, сказано, что она должна быть интегрирована в планирование, структуры и процессы общей защиты. Для того чтобы вооруженные силы Германии могли выполнять свои задачи в киберпространстве, расширяются их возможности, консолидируется архитектура безопасности их *IT*-систем, а ранее разрозненные структуры объединяются в рамках новой, самостоятельной военно-организационной области[5].

Позиция России по вопросам военно-политического использования ИКТ-среды также прошла несколько этапов развития. Впервые она была подробно изложена в документе 2011 г. «Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве». В нем предлагается «разрешение конфликтов в информационном пространстве осуществлять, в первую очередь, путем переговоров, примирения, обращения к Совету Безопасности ООН или к региональным органам, или соглашениям, или иными мирными средствами»[6]. Одновременно возможно «в условиях эскалации конфликта в информационном пространстве и перехода его в кризисную фазу воспользоваться правом на индивидуальную или коллективную самооборо-

1 "National Cyber Strategy 2016–2021," HM Government, accessed May 20, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016.pdf.
2 "The Equities Process," GHCQ, November 2019, accessed May 20, 2022, https://www.gchq.gov.uk/information/equities-process.
3 "German Military Can Use 'Offensive measures' Against Cyber Attacks: Minister," Reuters, April 5, 2017, accessed May 20, 2022, https://www.reuters.com/article/us-germany-cyber-idUSKBN1771MW.
4 "Personalzahlen der Bundeswehr (Personnel numbers of the Armed forces)," Bundeswehr, January 2022, accessed May 20, 2022, https://www.bundeswehr.de/de/ueber-die-bundeswehr/zahlen-daten-fakten/personalzahlen-bundeswehr.
5 "Cyber-Sicherheitsstrategie für Deutschland (Cyber Security Strategy for Germany)," Bunderministerium des Innern (Federal Ministry of the Interior), 2016, accessed May 20, 2022, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheits-Strategie.pdf.
6 Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве // Министерство обороны Российской Федерации. [Электронный ресурс]. URL: https://ens.mil.ru/science/publications/more.htm?id=10845074%40cmsArticle&ysclid=l1apyn31fn (дата обращения: 28.03.2022).

ну с применением любых избранных способов и средств, не противоречащих общепризнанным нормам и принципам международного права»[1]. В актуальной Военной доктрине «отражена приверженность Российской Федерации к использованию для защиты национальных интересов страны и интересов ее союзников военных мер только после исчерпания возможностей применения политических, дипломатических, правовых, экономических, информационных и других инструментов ненасильственного характера»[2].

В 2017 г. министр обороны Российской Федерации С. Шойгу заявил, что в России за последние четыре года созданы войска информационных операций[3], соответственно, решение об их создании было принято в 2014 г., что подтверждается сообщениями СМИ. При этом одной из поставленных перед этими подразделениями задач является контрпропаганда, то есть нейтрализация вредоносного информационного воздействия, что соответствует принятой в России концепции информационной безопасности.

На внешнеполитическом контуре усилия российской дипломатии с самого начала были направлены на недопущение милитаризации ИКТ-среды вплоть до заключения соглашения о запрете на деструктивное военно-политическое использование ИКТ. Россия еще в 1998 г. на уровне ООН отметила опасность возникновения «информационных войн»[4] и фактически «стала первым государством, которое на международном уровне подняло вопрос о появлении принципиально новых (информационных) угроз национальной и международной безопасности в XXI веке»[5]. В 2015 г. А.В. Крутских, являющийся специальным представителем Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, отметил, что позиция России и ее партнеров по ШОС и БРИКС заключается в том, чтобы «не легализовывать и не регулировать конфликты в информационном пространстве, а предотвращать использование ИКТ в военно-политических целях»[6]. Эта внешнеполитическая позиция неоднократно подтверждалась и в дальнейшем[7].

Исходя из вышесказанного, можно констатировать, что ведущие государства НАТО в построении доктринальных, организационных и материально-технических возможностей проведения кибероперации пошли по пути США, но с учетом некоторых национальных особенностей и приоритетов. До сих пор ни

1 Ibid.
2 Военная доктрина Российской Федерации (утверждена Президентом Российской Федерации 25 декабря 2014 г., № Пр-2976) // Совет Безопасности Российской Федерации. [Электронный ресурс]. URL: http://www.scrf.gov.ru/security/military/document129/ (дата обращения: 28.03.2022).
3 В Минобороны РФ создали войска информационных операций // Interfax. [Электронный ресурс]. URL: https://www.interfax.ru/russia/551054 (дата обращения: 28.03.2022).
4 Роль науки и техники в контексте международной безопасности, разоружения и других связанных с этим областей. Письмо Постоянного представителя Российской Федерации при Организации Объединенных Наций от 23 сентября 1998 года на имя Генерального секретаря // ООН. [Электронный ресурс]. URL: http://www.un.org/ru/documents/ods.asp?m=A/C.1/53/3 (дата обращения: 28.03.2022).
5 Крутских 2007.
6 Нам удалось договориться в условиях конфронтации и санкций // Коммерсантъ. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/2790234 (дата обращения: 28.03.2022).
7 МИД РФ: усилия по обеспечению кибербезопасности особенно актуальны на фоне коронавируса // ТАСС. [Электронный ресурс]. URL: https://tass.ru/politika/8180805 (дата обращения: 28.03.2022); Максим Федоренко: Россия – признанный интеллектуальный лидер в сфере международной информационной безопасности // Внешнеэкономические связи. [Электронный ресурс]. URL: https://eer.ru/article/mnenie/u72/2021/12/29/5965 (дата обращения 28.03.2022); Спецпредставитель президента: Россия против развязывания гонки информационных вооружений // ТАСС. [Электронный ресурс]. URL: https://tass.ru/politika/4374464? (дата обращения: 28.03.2022).

одна из этих стран не приняла в чистом виде политику «постоянного противодействия» и «обороны за передовой линией», однако нет уверенности, что это не произойдет в ближайшее время[1]. Если сравнить позицию России с позицией других стран, можно отметить, что Россия идет в русле последних тенденций и создала свое «информационное командование» и соответствующие подразделения. В то же время с доктринальной точки зрения Россия не ставит своей задачей проведение наступательных операций в информационном пространстве, что можно объяснить политикой «предотвращения» конфликтов в информационном пространстве. При сохранении общей направленности внешней политики на поиск путей предотвращения или ограничения конфликтов в ИКТ-среде, создание кибер- и информационного потенциала является неизбежным следствием необходимости обеспечения национальной безопасности на фоне развития наступательных и оборонительных кибервозможностей в других государствах.

Факторы эскалации и деэскалации

Сегодня кибератаки, в том числе направленные на различные объекты критически важной инфраструктуры, осуществляются ежеминутно, и их интенсивность непрерывно возрастает. Так, по информации Ю.И. Борисова, заместителя председателя Правительства Российской Федерации по вопросам оборонно-промышленного комплекса, за первую половину 2021 г. количество хакерских атак, направленных на объекты критической информационной инфраструктуры России, превысило общий объем атак 2020 г.[2] Одновременно следует подчеркнуть, что на сегодняшний момент кибератаки не привели к значительной эскалации, в первую очередь в военной сфере. Представляется, что этого не происходит благодаря совокупности нескольких факторов. Во-первых, ИКТ-среда является рукотворным пространством и обладает свойствами трансграничности, анонимности, глобальности. Все эти свойства, которые проистекают из технических и технологических особенностей построения глобальных информационных сетей, значительно затрудняют проведение быстрой и точной атрибуции – то есть определения источника кибератаки. И это, в свою очередь, повышает риски ошибочного реагирования и непреднамеренной эскалации, особенно если говорить о возможных автоматических ответных хакерских атаках. Во-вторых, все основные игроки реализуют стратегию сдерживания путем определения, какие кибератаки и какой ущерб неприемлемы и приведут к ответным действиям. Например, в июне 2021 г. страны Североатлантического Альянса признали, «что воздействие значительной злонамеренной накапливающейся кибердеятельности может при определенных обстоятельствах считаться равнозначным вооруженному нападению»[3].

1 Так, политика «активной киберзащиты», которая содержится в Национальной Стратегии Кибербезопасности Великобритании прямо не говорит о вторжении в сети потенциального противника (“National Cyber Strategy 2016–2021,” HM Government, accessed May 20, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016.pdf.

2 Борисов заявил о росте числа кибератак на критическую инфраструктуру // РБК. [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/13/12/2021/61b377649a7947d59106869f (дата обращения: 28.03.2022).

3 Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 14 июня 2021 года // НАТО. [Электронный ресурс]. URL: https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=ru (дата обращения: 28.03.2022).

С другой стороны, ряд факторов усугубляют ситуацию с возможной эскалацией. Во-первых, отсутствуют международно-правовые механизмы, которые могли бы способствовать снижению рисков в ИКТ-среде, так как принятые в рамках ООН нормы, правила и принципы ответственного поведения государств являются частью «мягкого» права – то есть необязательны для исполнения. Более того, до сих пор нет четкого механизма их применения и отсутствует юридически закрепленное определение множества важных понятий, необходимых для реализации как упомянутых норм, так и международного права в целом. Например, нет юридически закрепленной трактовки, что понимать под государственными границами в ИКТ-среде и где пролегает зона ответственности государств. Профессор А.А. Стрельцов отмечает, что «отсутствие признанных международным сообществом механизмов делимитации границ государств в ИКТ-среде и, соответственно, международных договоров, закрепляющих границы национальных сегментов ИКТ-среды, не позволяет использовать суверенитет государства в данной среде как средство добросовестного выполнения международных обязательств»[1]. Во-вторых, рядом государств, особенно США[2], продвигается концепция т.н. «публичной атрибуции», в рамках которой виновный определяется не через установление фактов, должное разбирательство и доказательство вины, а путем «назначения» – зачастую из политических соображений. В-третьих, порог обладания т.н. «кибероружием», то есть специализированным программным обеспечением, и его использования остается низким. Его «компоненты», в том числе описание новых уязвимостей, можно приобрести на черном рынке. Там же можно нанять и соответствующих специалистов. Эта ситуация ведет к существенному расширению круга акторов: кибероружием могут обладать не только государства, но и террористы. Соответственно, учитывая сложности атрибуции, нельзя исключить возможность проведения третьими сторонами атак под ложным флагом с целью провоцирования конфликта. Похожая оценка этого фактора приводится в исследовании Белферского центра, где прямо сказано, что наступательные кибервозможности дешевле традиционных инструментов и их труднее отследить. Кроме того, в исследовании отмечается асимметричный характер кибервозможностей, который означает, что небольшие страны могут оказывать большее влияние с помощью киберсредств, чем с помощью традиционных инструментов[3]. В-четвертых, в определенных военных кругах распространено мнение[4], что киберсредства позволяют лучшим образом соблюдать принципы международного гуманитарного права (МГП) – пропорциональность и избирательность[5]. Однако исследования говорят о том, что на данный момент невозможно гарантировать соблюдение принципов МГП при применении кибероружия[6]. Так, по мнению экспертов, вредоносная программа STUXNET, с помощью которой в 2010 г. были поражены некоторые предприятия

1 Стрельцов 2017, 98.
2 "The National Cyber Strategy," The White House, September 2018, accessed May 20, 20222, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
3 Voo et al. 2020.
4 "Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Defence Ministers," NATO, November 2017, accessed May 20, 2022, https://www.nato.int/cps/en/natohq/opinions_148417.htm?selectedLocale=en.
5 Международное гуманитарное право. Общий курс // МККК. [Электронный ресурс]. URL: https://www.icrc.org/ru/document/mgp-obshchiy-kurs (дата обращения: 28.03.2022).
6 Карасев 2018.

ядерной программы Ирана, распространилась далеко за пределы своей первоначальной цели[1]. Специалисты в области права отмечают, что выполнение положений международного гуманитарного права в ИКТ-среде затруднено по причине отсутствия для нее механизма идентификации гражданских и военных систем[2].

Самым существенным фактором является то, что на сегодняшний момент у ряда стран есть не только доктринальные, материально-технические основы, но и намерение более активно использовать ИКТ-возможности в военно-политических целях, невзирая на возможные риски. В этой связи можно вспомнить, что в актуальных документах стратегического планирования США[3] Россия и Китай названы основными противниками, а Дж. Болтон, будучи советником президента США по национальной безопасности, в июне 2019 г. заявил: «Цель [наступательных действий в киберпространстве]. состоит в том, чтобы заявить России или кому-либо еще, кто осуществляет против нас кибероперации: „Вы за это поплатитесь“»[4]. В июне 2019 г. в газете *The New York Times* была опубликована статья[5] о том, как российские объекты производства и передачи электроэнергии подверглись кибервторжению со стороны спецслужб США.

Кибератаки, направленные против информационных систем критической инфраструктуры, особенно на объектах, содержащих опасные силы[6], а также атаки на военную инфраструктуру несут наибольший риск эскалации с учетом возможных материальных и людских потерь. Стремление ядерных держав в рамках модернизации своих ядерных сил насыщать информационно-управляющие системы цифровыми технологиями неизбежно ведет к возникновению потенциальных киберуязвимостей и возрастанию рисков непреднамеренной эскалации в сфере, связанной с поддержанием стратегической стабильности[7]. Также до сих пор недостаточно изучены потенциальные риски применения в военной сфере автономных систем с элементами искусственного интеллекта.

***

В условиях острого дефицита доверия и геополитической нестабильности крайне сложно реализовать как эффективное предотвращение, так и регулирование конфликтов в ИКТ-среде. Факты говорят о гонке кибервооружений, где отдельные страны открыто заявляют о возможном использовании наступательных кибероперации. Непрерывно возрастающие киберриски, особенно на фоне нестабильности международной обстановки, обостряют необходимость поиска путей и механизмов деэскалации напряженности в ИКТ-среде.

1 Stuxnet: первые жертвы // SecureList. [Электронный ресурс]. URL: https://securelist.ru/stuxnet-pervye-zhertvy/24277/ (дата обращения: 28.03.2022).

2 *Стрельцов, А.* Основные проблемы применения международного права к ИКТ-среде // Digital Report. [Электронный ресурс]. URL:https://digital.report/osnovnyie-problemyi-primeneniya-mezhdunarodnogo-prava-k-ikt-srede/ (дата обращения: 28.03.2022).

3 “2018 Department of Defense Cyber Strategy,” US Department of Defense, September 2018, accessed May 20, 2022, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

4 “‘They will Pay a Price’: Bolton Says US has Expanded ‘Offensive Cyber Operations’ Against Russia,” RT, June 11, 2019, accessed May 20, 2022, https://www.rt.com/news/461622-bolton-us-expanded-cyber-war-russia/.

5 David E. Sanger, and Nicole Perlroth, “U.S. Escalates Online Attacks on Russia’s Power Grid,” The New York Times, June 15, 2019, accessed May 20, 2022, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

6 Статья 56. Дополнительного Протокола I к Женевским конвенциям от 12 августа 1949 года // Система ГАРАНТ. [Электронный ресурс]. URL: http://base.garant.ru/2540377/#ixzz5RAhTQHgB (дата обращения: 28.03.2022). Согласно этой статье, к таким установкам и сооружениям относятся плотины, дамбы и атомные электростанции.

7 Более подробно о киберуязвимостях информационно-управляющих систем стратегических сил: Futter 2016; Unal et al. 2018.

Опыт разработки правил ответственного поведения государств в ИКТ-среде выявил существенные противоречия между странами, что на практике выразилось в отсутствии консенсуса по докладу группы правительственных экспертов (ГПЭ) ООН в 2017 г., а также в формировании в 2018 г. двух параллельных групп – новой ГПЭ, где ведущую роль играли США, и Рабочей группы открытого состава (РГОС) с неформальным лидерством России и Китая[1]. Несмотря на оформившееся разделение, обсуждение актуальных проблем безопасности ИКТ-среды продолжилось, причем не только на многосторонней основе[2], но и в двустороннем формате.

На Саммите Россия – США в июне 2021 г. обсуждению вопросов кибербезопасности было уделено особое внимание, и по итогам переговоров было объявлено о создании совместной консультативной группы. Одна из задач, которая поставлена перед ее участниками, – выработать общее понимание, какая критически важная инфраструктура находится за пределами «красных линий»[3]. Представляется, что принятые решения придали позитивный импульс двустороннему и международному взаимодействию. Об этом можно судить исходя из того, что ГПЭ ООН и РГОС завершили свою работу в позитивном ключе, а в конце 2021 г. Генеральной Ассамблеей ООН была принята Резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий», подготовленная совместно Россией и США.

Подобное объединение усилий и, в некоторой степени, согласование позиций, безусловно, является позитивным сигналом – и необходимо развить успех, реализовав, как отмечено в Резолюции, «возможность разработки в будущем, при необходимости, дополнительных имеющих обязательную силу обязательств»[4]. С учетом всех рисков необходимость в выработке обязательных механизмов деэскалации в ИКТ-среде очевидна уже сегодня. В условиях острейшей напряженности в международных отношениях и дефицита времени на принятие решения любой значительный инцидент в ИКТ-среде – то есть тот, который какая-либо из сторон воспримет как переход «красных линий», – может спровоцировать эскалацию с применением все более разрушительных мер противодействия. Представляется важным обратить первоочередное внимание на выработку общего понимания киберугроз военной и стратегической стабильности, а затем – механизмов предотвращения киберинцидентов в этой сфере. Одновременно стоит вернуться к рассмотрению возможности реализации озвученного в 2020 г. президентом России предложения заключить глобальную договоренность о ненанесении первого кибердара – по аналогии с отказом от нанесения ядерного удара первыми[5].

1 Доклад Генерального секретаря A/72/327 // UNdocs.org. [Электронный ресурс].URL: https://undocs.org/ (дата обращения: 20.05.2022); Доклад Первого комитета A/73/505 // UN.org. [Электронный ресурс]. URL: https://www.un.org/ru/ga/first/73/first_res.shtml (дата обращения: 20.05.2022).

2 США принимали участие в работе РГОС, а Россия вошла в ГПЭ.

3 "Remarks by President Biden in Press Conference," The White House, June 16, 2021, accessed May 20, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4/.

4 Ibid.

5 Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности // Президент России. [Электронный ресурс]. URL: http://www.kremlin.ru/events/president/news/64086. (дата обращения 28.03.2022 г.)

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Карасев, П.А. Милитаризация киберпространства // Безопасность и контроль над вооружениями 2017–2018: Преодоление разбалансировки международной стабильности / Отв. ред.: А.Г. Арбатов, Н.И. Бубнова. – Москва: ИМЭМО РАН, Политическая энциклопедия, 2018. – С. 247–259.

Karasev, Pavel A. "Militarizaciya Kiberprostranstva." In *Security And Arms Control 2017–2018: Overcoming The Imbalance Of The International Stability,* edited by Alexey Arbatov, and Natalia Bubnova, 247–259. Moscow: IMEMO, 2018 [In Russian].

Крутских, А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. – 2007. – № 1. С. 28–37.

Krutskikh, A. "On Legal and Political Foundations of Global Information Security." *International Trends (Mezhdunarodnyye protsessy),* no. 1 (2007): 28–37 [In Russian].

Лобач, Д.В., Смирнова, Е.А. Компьютерные сетевые атаки как акт агрессии в условиях развития современных международных отношений: pro et contra // Российский журнал правовых исследований. – 2020. – № 4. – С. 59–65. https://doi.org/10.17816/RJLS46326.

Lobach, Dmitriy V., and Evgeniya A. Smirnova. "Computer Network Attacks as an Act of Aggression in the Context of the Development of Modern International Relations: Pros and Cons." *Russian Journal of Legal Studies (Moscow)* 7, no. 4 (March 14, 2021): 59–65. [In Russian].

Стрельцов, А.А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. – 2017. – № 4.

Streltsov, Anatoliy. "Suverenitet i yurisdikciya gosudarstva v srede informacionno-kommunikacionnyh tekhnologij v kontekste mezhdunarodnoj bezopasnosti." *International Affairs.* no. 4 (2017) [In Russian].

Armistead, Leigh. *Information Operations: The Hard Reality of Soft Power.* Washington, D.C.: Potomac Books, 2004.

Futter, Andrew. *Cyber Threats and Nuclear Weapons New Questions For Command And Control, Security And Strategy.* London: RUSI, 2016.

Maurer, Tim, and Robert Morgus. *Compilation of Existing Cybersecurity and Information Security Related Definitions.* New America, 2014. http://www.jstor.org/stable/resrep10487.

Molander, Roger, Andrew Riddile, and Peter Wilson. *Strategic Information Warfare: A New Face of War.* RAND Corporation, 1996. https://doi.org/10.7249/MR661.

Rauscher, Karl, and Valeriy Yashchenko. *Critical Terminology Foundations 1*. Ebook. New York: EWI/IISI, 2011.

Rauscher, Karl, and Valeriy Yashchenko. *Critical Terminology Foundations 2.* Ebook. New York: EWI/IISI, 2014.

Unal, Beyza, and Patricia Lewis. *Cybersecurity Of Nuclear Weapons Systems: Threats, Vulnerabilities And Consequences*. London: The Royal Institute of International Affairs, 2018. https://www.chathamhouse.org/publication/cybersecurity-nuclear-weapons-systems-threats-vulnerabilities-and-consequences.

Voo, Julia, Hemani, Ifran, Jones, Simon, DeSombre, Winnona, Cassidy, Dan, and Anina Schwarzenbach. *Reconceptualizing Cyber Power.* Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2020.

Сведения об авторе

Карасев Павел Александрович,

к.полит.н., с.н.с., Национальный исследовательский институт мировой экономики и международных отношений имени Е.М.Примакова РАН,

Россия, Москва, Профсоюзная ул., 23,

Центр проблем информационной безопасности ВМК МГУ,

Россия, Москва, Ленинские горы, МГУ имени М.В.Ломоносова, д. 1, стр. 52.

e-mail: karpaul@iisi.msu.ru

Дополнительная информация

Поступила в редакцию: 11 марта 2022.

Переработана: 31 мая 2022.

Принята к публикации: 1 июня 2022.

Конфликт интересов

Автор заявляет об отсутствии потенциального конфликта интересов.

Цитирование

Карасев, П.А. Эволюция национальных подходов к ведению кибервойны // Международная аналитика. – 2022. – Том 13 (2). – С. 79–94.

https://doi.org/10.46272/2587-8476-2022-13-2-79-94

Evolution of National Approaches to Cyber Warfare

ABSTRACT

The latest information and communication technologies (ICTs) are increasingly considered by nation-states as a means to project their power and promote national interests. Over the past 20 years the major militarily significant powers have created the doctrinal, logistical and organizational foundations for conducting military activities in the ICT environment and some states have already openly declared the priority of offensive cyber operations, which increases the risks of crossing "red lines" and inadvertent escalation. The current situation related to the military-political exploitation of the ICT environment predetermines the urgent need for continuous analysis of current trends in this area and the search for approaches to reduce tension, which is the goal of this article. To achieve this goal, the first part of the article considers in detail relevant doctrinal and strategic documents of the United States and other key countries and identifies certain stages and aspects of evolution of their approaches. Further, the article considers and evaluates factors that influence military stability in the ICT environment, taking into account the previously obtained results. It is concluded that the identified factors make the task of developing international frameworks to reduce the escalation in this area uncontested. This task is of particular urgency in the context of general international instability. Analysis of the current international environment in the relevant sphere allows to conclude that international community as a whole and the major players in particular (primarily Russia and the US) are aware of the danger of unintentional escalation in the ICT environment, especially when linked to strategic stability, and are ready to take steps towards developing the framework aimed at regulation and prevention of cyber conflicts. It is very actual now in new political reality but the question mostly is about finding the possible format.

KEYWORDS

International information security, cyberattacks, cyber warfare, US foreign policy, information space

Author

Pavel A. Karasev,

Ph.D. Political sciences, Senior researcher at Primakov National Research Institute of World Economy and International Relations, Russian Academy of Sciences,
Russia, Moscow, Trade Union street, 23,
Center for Information Security Issues at the Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University,
Russia, Moscow, Leninskie Gory, Lomonosov Moscow State University, 1, p. 52.
e-mail: karpaul@iisi.msu.ru

Additional information

Received: March 11, 2022. Revised: May 31, 2022. Accepted: June 1, 2022.

Disclosure statement

No potential conflict of interest was reported by the author.

For citation

Karasev, Pavel A. "Evolution of National Approaches to Cyber Warfare."
Journal of International Analytics 13, no. 2 (2022): 79–94.
https://doi.org/10.46272/2587-8476-2022-13-2-79-94