УДК 327.51
DOI: 10.31857/S2686673024090058
EDN: ZVMYUS

США против России: кибернатиск на Восток

Я.В. Селянин

Институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук (ИМЭМО РАН). Российская Федерация, Москва, Профсоюзная ул., 23.
ORCID: https://orcid.org/0000-0002-3802-0563 e-mail: yaroslav.selyanin@yandex.ru

Резюме. До начала специальной военной операции на Украине глава Киберкомандования США в июне 2022 года заявил о проведении его ведомством наступательных кибероперациий против России. В случае осуществления личным составом американских Вооружённых сил таких действий в других средах – на суше, на море или в воздушном пространстве – их можно было бы трактовать как агрессию против суверенного государства. Министерство обороны США начало активно развивать это направление с 2018 года. Пока американские официальные лица и экспертное сообщество спекулируют на тему правового обоснования законности данных действий, Вашингтон отрабатывает методику их проведения на Украине и готовится применить этот опыт против России на других направлениях.

***Ключевые слова**:* США, Россия, Украина, Средняя Азия, Киберкомандование США, киберпространство, наступательные кибероперации, постоянное взаимодействие, наступательная оборона, кибероперации переднего края.

Для цитирования: Селянин Я.В. США против России: кибернатиск на Восток. *США & Канада: экономика, политика, культура*. 2024; 54(9): 62–77.
DOI: 10.31857/S2686673024090058 EDN: ZVMYUS

U.S. vs. Russia: Cyber «Drang nach Osten»

Yaroslav V. Selyanin

Institute of World Economy and International Relations, Russian Academy of Sciences. 23, Profsoyuznaya Str., Moscow, 117997, Russian Federation.
ORCID: https://orcid.org/0000-0002-3802-0563 e-mail: yaroslav.selyanin@yandex.ru

Abstract: In June 2022, the commander of U.S. Cyber Command, Paul Nakasone, disclosed that his soldiers had conducted offensive cyberattacks against Russia before the Special military operation in Ukraine began. These so-called “hunt forward” operations are part of USCYBERCOM’s doctrine of persistent engagement. This doctrine involves the personnel of the Cyber Nation Mission Forces deploying to partner countries to work with their cyber defenders in their most critical networks and computer systems. Their mission is to search for and degrade enemy activities, while also researching their tools and tactics in cyberspace. This doctrine is one of Nakasone’s key innovations in Cyber Command’s course of action.

Previously, U.S. cyber operations required authorization from the U.S. President. This restriction made actions like persistent engagement and hunt forward operations nearly

impossible, as they require extensive activities within other countries' networks even before a cyberattack is prepared. It is impractical to expect the President to approve every such request. Nakasone changed this by removing the requirement for presidential authorization. Today, this allows Cyber Command to conduct such operations – both defensive and offensive – much more broadly, and they are taking full advantage of this opportunity.

The problem lies in the sphere of international law – both in the field of the law of war (jus in bello) and the right to war (jus ad bellum). U.S. politicians often claim that cyber operations can achieve strategic goals without crossing the threshold of armed conflict. In any other domain actions with similar effects could provoke war but not in cyberspace. This feature is its main advantage and the reason the U.S. sabotages other countries' initiatives (particularly Russian) to establish a legal regime for state use of cyberspace. However, there is no consensus among U.S. specialists about the legal basis that legitimizes such operations against another country, both internationally and domestically. Yet, this ambiguity seems to work in the U.S. favor. In fact, U.S. soldiers have attacked another country's (Russian) territory and this has not led to a direct war between Russia and the U.S.

U.S. officials consider the hunt forward operation experience in Ukraine as both successful and useful for refining U.S. strategies in cyberspace, including the National Cybersecurity Strategy and the DoD Cyber Strategy. They plan to use such tools more broadly against Russia. Currently, the U.S. is actively working in the Post-Soviet area against Russia to disrupt Russia's national interests. Among other things, Washington is attempting to coerce Central Asian states into alignment with U.S. interests. Hunt forward operations are an obvious tool of the United States, which Russia will most likely have to counteract there.

***Keywords**:* USA, Russia, Ukraine, Central Asia, U.S. Cyber Command, cyberspace, offensive cyber operations, persistent engagement, defend forward, hunt forward operations.

For citation: Selyanin, Y.V. U.S. vs. Russia: Cyber «Drang nach Osten». *USA & Canada: Economics, Politics, Culture*. 2024; 54(9):62–77.
DOI: 10.31857/S2686673024090058 EDN: ZVMYUS

ВВЕДЕНИЕ

Глава Киберкомандования США и по совместительству директор Агентства национальной безопасности Пол Накасоне в июне 2022 года заявил журналистам «Скайньюс», что американские военные проводили операции наступательного и оборонительного характера в киберпространстве в поддержку Украины. Хотя эти действия Вашингтон начал ещё до начала специальной военной операции (СВО), Накасоне позиционировал их как «ответ на российское вторжение» [1]. Заявление прозвучало на полях конференции по вопросам конфликтов в киберпространстве «СайКон» (*CyCon*), проводимой таллинским Центром передового опыта в области коллективной кибероборонe Североатлантического альянса. Неудивительно, что в своём докладе американский генерал оценил международное сотрудничество в этой сфере как стратегическое преимущество, ведь именно в его рамках эти операции и были проведены.

Заявление Накасоне ставит несколько вопросов. *Во-первых*, как такие действия согласуются с нормами международного права? *Во-вторых*, как американская

сторона расценивает результаты и полученный опыт? *В-третьих*, на каком ещё направлении можно ожидать аналогичных действий со стороны Вашингтона?

НАСТУПАТЕЛЬНАЯ ОБОРОНА ПОСТОЯННОГО ВЗАИМОДЕЙСТВИЯ КИБЕРКОМАНДОВАНИЯ США

Глава Киберкомандования хорошо знал, о чём рассказывал журналистам. Ведь «операции в поддержку Украины» были кибероперациями переднего края, КПК (*hunt forward operations, HFO*), – составной частью доктрины постоянного взаимодействия (*persistent engagement*). Она была одним из ключевых элементов программы, которую Накасоне представил конгрессменам в марте 2018 года, когда его утверждали на должность главы ведомства. Позднее доктрина постоянного взаимодействия дополнилась концепцией наступательной обороны (*defend forward*). Суть обоих терминов состоит в том, что подразделения кибервойск США – в данном случае речь идёт о киберсилах миссий национального значения, КМНЗ (*Cyber Nation Mission Force, CNMF*), не дожидаясь кибератаки со стороны противника, начинают действовать за пределами американских сетей, проникают в его сети и «изучают» его подходы и инструменты обороны и проведения кибератак.

Выступая перед конгрессменами, П. Накасоне представлял им идеи, родившиеся на основе практического опыта функционирования и действий подразделений КМНЗ, которые он непосредственно возглавлял до назначения на пост главы Киберкомандования. Важность решаемых КМНЗ задач настолько высока, что в декабре 2022 года они получили особый статус (*sub-unified command*) в структуре Киберкомандования [2], что дало им большую свободу действий, в том числе при проведении государственных закупок.

По-видимому, во время командования КМНЗ П. Накасоне сильно досаждала сложность и забюрократизированность процедуры получения разрешения на проведение операций в киберпространстве. Последнее и сейчас остаётся для высшего военно-политического руководства чем-то малопонятным, а тогда, в 2018 году, понимания было ещё меньше. Поэтому во избежание опасных недоразумений президентская директива № 20 «Политика США по проведению кибероперацій» (*PPD-20*) времён Б. Обамы требовала одобрения президента для проведения наступательных и оборонительных операций в киберпространстве (*Offensive Cyber Effects Operations* и *Defensive Cyber Effects Operations*) за пределами сетей США [3]. Забегая вперёд, отметим, что это настолько сковывало деятельность КМНЗ, что к началу 2019 года, спустя лишь несколько месяцев после снятия этого требования в рамках существенного расширения полномочий Киберкомандования и изменений в законодательстве, Киберкомандование провело операций больше, чем за предыдущие десять лет [4].

Старая процедура фактически делала невозможным внедрение новой концепции о постоянном взаимодействии кибервойск США с киберсилами, как это

тогда называлось, соперников. Ими считались Россия, Китай, Северная Корея и Иран. Требовались изменения нормативно-правовой базы, которые были проведены в 2018 году.

Во-первых, изначально засекреченная, но раскрытая Эдвардом Сноуденом, президентская директива № 20 была заменена закрытым президентским меморандумом в области национальной безопасности № 13 (*NSPM-13*) [5], который унаследовал название предшествующего документа, поскольку также описывает процесс одобрения руководством США наступательных и оборонительных кибероперацій, в том числе за пределами сетей США. *Во-вторых*, был принят закон «Об ассигнованиях на национальную оборону» на 2019 фин. год (*NDAA-2019*), одно из положений которого квалифицировало «тайную военную деятельность или операции в киберпространстве» (*clandestine military activity or operation in cyberspace*) как обычную военную деятельность. Для решения об её осуществлении достаточно полномочий министра обороны [6]. Утверждение плана операции у президента больше не требуется. По словам военных, это позволило им осуществлять некоторые действия, необходимые «для подготовки операции», включая «подготовку среды» [7] (то есть части неамериканского сегмента киберпространства, где предполагается проведение операции киберсилами США). Тогда же Минобороны США получило широкие полномочия «предпринимать уместные и пропорциональные действия в киберпространстве иностранных государств для срыва и сдерживания <…> активной, систематической и проводимой в данный момент времени вредоносной кампании против правительства и населения США» уже упомянутыми Россией, Китаем, Северной Кореей или Ираном. Перечень таких действий включал кибер- и информационные операции.

Приятые меры дали Киберкомандованию свободу действий. К моменту начала специальной военной операции (СВО) России на Украине американские специалисты уже активно действовали в рамках концепции наступательной обороны. Кроме работы с территории США передовые оперативные группы КМНЗ выезжали на территории государств-партнёров для совместной работы со специалистами принимающей стороны, конечно, по её приглашению и просьбе помочь с защитой своего киберпространства. Эти «выезды в поле» и получили название кибероперацій переднего края.

По официальным данным Киберкомандования, к ноябрю 2022 года КМНЗ провели более 20 таких операций в «16 различных странах, включая Украину, Эстонию и Литву». Из них 11 было проведено в девяти странах для «защиты выборов от иностранного влияния и вмешательства» в одном только 2020 году [8]. В сентябре 2023 года Киберкомандование объявило, что КПК в общей сложности проводились уже 50 раз более чем в 23 странах [9].

Интересно, что в ноябре 2022 года в официальном разъяснении о том, что КПК представляют собой, указано, что это «строго оборонительные кибероперации» [8]. Однако, *во-первых*, в упомянутом интервью генерала Накасоне говорится о проведении передовой оперативной группой на Украине

оборонительных, наступательных и информационных операций. *Во-вторых*, в Обзоре ключевых шагов по защите нации в 2022 году, опубликованном Киберкомандованием в январе 2023 года, указано, что проводящие КПК «КМНЗ – это объединённые киберсилы Вооружённых сил США, задача которых – защищать нацию в киберпространстве посредством наступательных, оборонительных и информационных операций». На Украине «КМНЗ развернули самую большую в истории передовую оперативную группу для проведения кибероперацій», состоявшую из личного состава Военно-морских сил и Корпуса морской пехоты США [10].

При этом не стоит путать кибероперации переднего края и деятельность экспедиционных групп кибер- и электромагнитных операций 11-го кибербатальона 780-й бригады военной разведки из состава киберкомандования сухопутных войск ВС США. В преддверии начала СВО, в 2022 году, такая группа была направлена в Европу и обеспечивала работу регионального штаба сухопутных войск США по направлению радиоэлектронной борьбы, информационных операций, оборонительных и наступательных кибероперацій [11].

Глава Киберкомандования США признался в участии американских вооружённых сил в проведении наступательных кибероперацій против России на Украине, но не раскрыл точные сроки их проведения и суть. В интервью каналу «Скайньюс» П. Накасоне заявил, что его подчинённые прибыли на Украину в декабре 2021 года, пробыли там «почти 90 дней» и, как остальной личный состав МО США, были выведены с её территории в феврале – до начала СВО [1]. Если взглянуть на календарь, то в случае прибытия на Украину 1 декабря 2021 года и убытия в первый день СВО 24 февраля 2022 года, получится, что личный состав КМНЗ пробыл бы на Украине 86 дней. Срок близкий к заявленному. Хотя в ноябре 2022 года Киберкомандование уточнило, что его специалисты находились на территории Украины с декабря 2021 года по март 2022 года, а после покидания последней продолжили оказывать ей поддержку [12].

Можно констатировать, что США являются стороной киберсоставляющей конфликта на Украине. 6 июня 2022 года об этом заявил и спецпредставитель Президента России по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских. Отвечая на вопрос газеты «Коммерсант», он подчеркнул, что США «развязали киберагрессию против России и её союзников. Используют в качестве тарана "режим Зеленского" и созданную им "ИТ-армию" для совершения компьютерных атак против нашей страны. Нападения с использованием ИКТ на объекты критической инфраструктуры в России постоянно увеличиваются» [13].

С учётом информации о заблаговременной подготовке со стороны ВСУ к атаке на ДНР и ЛНР, возникает вопрос: не было ли у представителей кибервойск США, находившихся на Украине, задачи по непосредственному участию в обеспечении этого нападения?

В любом случае, несмотря на спешное покидание территории Украины личным составом КМНЗ в связи с началом СВО (если верить расходящимся друг с другом официальным данным), их деятельность признана в США успешной. Практику проведения кибероперациий переднего края, включая действия наступательного характера, США будут расширять.

Согласно принятой в марте 2023 года Стратегии национальной кибербезопасности, США намерены использовать весь спектр доступных им средств для дезорганизации и разгрома противника, угрожающего интересам их национальной безопасности: дипломатические, информационные, военные (включая кинетические и киберсредства), финансовые, разведывательные и правоохранительные. Конкуренты превратились в противников. Главная угроза – Китай, затем – Россия. Упомянуты Иран и КНДР, преступные группировки. Цель состоит в том, чтобы сделать проведение кампаний с использованием киберпространства против национальной и общественной безопасности США невозможным, а за «неподобающее поведение» в интернете Вашингтон (в компании с другими странами) намерен наказывать провинившихся. Кроме мер, например, дипломатического и экономического характера, предусмотрены ответные кибероперации (*counter-cyber operations*) [14].

Стратегия говорит о планах предоставлять партнёрам помощь в реагировании на инциденты, поскольку это способствует достижению целей внешней политики и кибербезопасности США [14]. По-видимому, это положение включает в себя деятельность передовых оперативных групп КМНЗ в рамках проведения кибероперациий переднего края. Они действительно продвигают цели внешней политики и кибербезопасности США, поскольку дают личному составу передовых кибергрупп Министерства обороны доступ к инфраструктуре других стран. Полученная информация в дальнейшем может облегчить Вашингтону проведение в ней уже собственных операций.

В сентябре 2023 года была принята свежая редакция Киберстратегии Министерства обороны США. Комментируя её содержание, представители ведомства констатировали, что использование киберпространства в ходе СВО сильно отличается от предположений американских специалистов о его использовании, которые делались до начала конфликта. *Во-первых*, США ожидали гораздо большей интенсивности действий в киберпространстве, а этого не случилось. *Во-вторых*, они пришли к мысли, что одного только киберпотенциала недостаточно для сдерживания противника, и поэтому его необходимо использовать совместно с иными инструментами. Вывод довольно неожиданный для военных США, много говоривших о важности совместного использования различных инструментов и придумавших термин «многосферные боевые действия» (*multi-domain battle*). Кроме того, заместитель помощника министра обороны по киберполитике М. Эоянг указала на то, что проведение операций в киберпространстве требует длительной заблаговременной подготовки: нужно проникнуть в сети и системы противника, закрепиться там и изучить их, проработать варианты воздействия на

них. А одним из уроков назвала эффективность использования облачных хранилищ, позволивших киевскому режиму перемещать данные за пределы территории страны при сохранении доступа к ним [15].

Одновременно США предостерегают другие страны от допуска иностранных государств в свои сети и фактически сами же обозначают риски для своих партнёров при проведении кибервойсками США операций типа КПК. Например, глава Министерства внутренней безопасности А. Майоркас предостерёг страны Латинской Америки от сотрудничества с Китаем в сфере телекоммуникаций. По его мнению, китайское оборудование и технологии могут быть использованы китайскими хакерами для проведения кибератак. В качестве примера он привёл приписываемую КНР атаку на Малайзию после того, как страна решила рассмотреть «возможность отказаться от железнодорожного проекта, поддерживаемого Китаем» [16]. Двойные стандарты со стороны США уже мало кого удивляют. Тем не менее будет не лишним напомнить, что это предостережение прозвучало от представителя страны, чьи спецслужбы, например, собирали информацию по программе ПРИЗМ (*PRISM*), раскрытой Сноуденом. Более того, специалисты утверждают, что действия США в отношении «Хуавей» были обусловлены в том числе тем, что с расширением использования в мире китайского телекоммуникационного оборудования и смартфонов целые сегменты киберпространства в наиболее интересующих американские спецслужбы странах выпадают из их поля зрения [17].

В случае же проведения кибероперациий переднего края американские военнослужащие получают доступ к наиболее важным сетям (уже не столь важно, на чьём оборудовании они построены) других стран в режиме наибольшего благоприятствования. Специалисты принимающей стороны сами вводят гостей в курс дела. Понятно, что это даёт гораздо более полное представление о сетях, чем тайное проникновение и изучение их максимально аккуратным образом, чтобы избежать обнаружения несанкционированного доступа извне.

Стоит также отметить следующее. На фоне опыта СВО представители сухопутных войск США заговорили о формировании новой триады по аналогии с ядерной. Речь о взаимодействии космических, кибер- и сил специальных операций для проведения мероприятий, которые нельзя было бы расценить в качестве повода для начала боевых действий, то есть не превышая порога начала вооружённого конфликта. Эксперименты по проведению совместных действий этих трёх видов вооружённых сил будут продолжены для того, чтобы выработать модели их использования. Как заявил глава командования сил специальных операций СВ генерал-лейтенант Дж. Брага, указанная триада имеет три основных направления применения. *Во-первых*, заблаговременная подготовка сред ведения боевых действий. *Во-вторых*, обеспечение доступа в сети противника через «человеческое измерение, киберпространство или космические системы». *В-третьих*, разгром сетей противника [18]. Если отбросить свойственное американскому менталитету заблаговременное преувеличение своих успехов, можно

констатировать, что в США активно ведётся поиск наиболее эффективных подходов к применению кибервойск с учётом полученного практического опыта.

ИМЕЮТ ЛИ ПРАВО?

Правовой аспект проведения американских наступательных кибероперациий можно разделить на две составные части: соответствие национальному и международному законодательству. К слову, причина возмущения американцев упомянутой программой ПРИЗМ была не в том, что спецслужбы в принципе осуществляли массированную слежку. В конце концов, на то АНБ и занимается радиотехнической разведкой, чтобы перехватывать информацию, передаваемую по сетям электросвязи. Основой кампании в американской прессе против действий Агентства было то, что оно превысило полномочия согласно национальному законодательству США и следило за гражданами своей страны без соответствующего решения суда.

По заявлениям американских официальных лиц, наступательные операции США в киберпространстве вполне законны и не противоречат намерениям США избегать прямого столкновения с Россией. Например, глава Киберкомандования утверждает, что, *во-первых*, его ведомство находится «под гражданским контролем над военными», *во-вторых*, они действовали в рамках права вооружённого конфликта (*within the law of armed conflict*), *в-третьих*, это вообще вопрос политического решения руководства страны. Пресс-секретарь Белого дома К. Жан-Пьер на соответствующий вопрос ответила предельно ясно: с точки зрения США – не противоречит [19]. А посол США по особым поручениям в области киберпространства и цифровой политики Н. Фик заявил, что наступательные действия в киберпространстве – это «инструмент национальной мощи, так же как и любой другой военный разведывательный, экономический, дипломатический, информационный. Необходим надёжный демократический надзор за соблюдением принципа верховенства закона. Но это законные операции, которые точно могут продвигать наши национальные интересы, и они являются одним из многих инструментов, имеющихся в распоряжении нашего политического руководства» [20].

При этом лишь П. Накасоне вспомнил про международное право, хотя и он сказал фактически только о соблюдении права войны (*jus in bello*), регулирующего ведение боевых действий безотносительно того, было ли у государства право их начинать. О том же, как ведение наступательных кибероперациий действующими военнослужащими США против иностранного государства (России) соотносится с правом на ведение войны (*jus ad bellum*) не сказал и он, фактически переложив ответственность на политическое руководство.

Вместе с тем вопрос правовой стороны дела начал обсуждаться сразу же после публичного представления кандидатом в командующие Киберкомандования П. Накасоне концепции постоянного взаимодействия.

В апреле 2018 года, до того, как в августе того же года был принят закон «Об ассигнованиях на национальную оборону» *(National Defense Authorization Act)*, издание «Сайберскуп» (*Cyberscoop*) писало, что деятельность Киберкомандования, как боевого командования, подпадает под действие раздела 10 «Вооружённые силы» Свода законов США, а потому «может действовать только в пределах объявленной зоны военных действий», а это вступает в противоречие с глобальным характером интернета. А вот разведсообщество (включая возглавляемое тем же П. Накасоне АНБ) регулируется разделом 50 «Война и национальная оборона», «который позволяет им осуществлять шпионаж практически в любой зарубежной стране», что лучше подходит к киберпространству. В то время вопрос о применимости к нему раздела 10 был открытым. Кибератаки, проводимые вооружёнными силами, попадали в «своего рода юридическую "серую зону"», поскольку не было понимания, как они соотносятся с международным правом [21].

Существовал юридический спор о том, к какому разделу – 10 или 50 – лучше отнести деятельность Киберкомандования и проводимые им операции. Так, в том же 2018 году на портале «Лофээ» (*Lawfare*) была опубликована короткая заметка под названием «Вопросы, относящиеся к разделам 10 и 50, в случае воздействия операций в компьютерных сетях на третьи страны». Автор указал, что разведывательные действия через киберпространство, то есть тайные операции подпадают под раздел 50 и должны соответствовать только Конституции и иным законам США. В случае же вывода их под раздел 10, операции теряют «такую защиту» от применения международного права. «Действуя в рамках раздела 10, Киберкомандование столкнулось бы с целым набором проблем в области международного права», в том числе в случае наступления негативных «последствий для серверов в третьих странах без (получения Соединёнными Штатами. – *Я.С.*) разрешения этих стран» на проведение кибероперациий [22].

В ответной статье было разъяснено, что Киберкомандование при проведении военных кибероперациий не может действовать в рамках раздела 50, поскольку к нему относится только разведывательная деятельность (*intelligence operations*) в киберпространстве, при которой «сохранение секретности – обязательное условие». Это относится к задачам, например АНБ. «Военные» (*military*) и «наступательные» (*offensive*) кибероперации по определению вызывают последствия вроде повреждения или уничтожения данных, размещённых в сети или в процессе их передачи [23], что входит в задачи Киберкомандования. То есть оно никак не может действовать в рамках раздела 50, только – в рамках раздела 10, что и было затем прямо прописано в упомянутом законе. Американские теоретики (в том числе из состава специально созданной в соответствии с положением упомянутого закона Комиссия по киберпространству *(Cyberspace Solarium Commission*) позже попытались обосновать, почему наступательные кибероперации якобы частично являются оборонительными. Утверждалось, что «действия военных киберсил США, которые на оперативном уровне можно было бы определить как наступательные (то есть получение доступа и перемещение внутри и сквозь неамериканское

киберпространство), несмотря на это, подразумеваются служащими оборонным стратегическим целям – укреплению обороноспособности и устойчивости США в киберпространстве» [24]. Киберкомандование в рамках концепции наступательной обороны занимается не только подрывом боеспособности противника. Совместно с Минфином, Министерством внутренней безопасности, ФБР и АНБ оно собирает данные о вредоносных программах противника, затем частично публикуемых в открытом доступе [24]. Но проблема в том, что грань между сбором информации и подрывом боеспособности может быть очень тонка. Внесение неопределённости в данном случае может быть попыткой затруднить выдвижение обвинений против американских военных.

Вместе с тем сегодня даже в США озвучивается точка зрения, что соответствие кибероперациий переднего края праву вооружённого конфликта (*conventions of armed conflict*, т.е. *jus in bello*), по-видимому, является вопросом «спорным и неурегулированным» [25].

Причём США сделали всё возможное, чтобы такие действия остались в «серой зоне». Они придерживаются позиции, что специальных норм международного права для регулирования деятельности в киберпространстве не требуется, достаточно уже существующих. Ещё в 2017 году Научный совет Министерства обороны США опубликовал доклад рабочей группы по киберсдерживанию, где говорилось, что «преимущества наступательных киберсредств велики и продолжают расти, проверка соблюдения режима контроля над (кибер-. – *Я.С.*) вооружениями невозможна, а атрибуция сильно затруднена» из-за технических особенностей этой среды. Давалась рекомендация обеспечить готовность осуществлять киберсдерживание собственными средствами, по возможности определив правила поведения в этой среде, которых сами будут придерживаться [26].

Конечно, США имеют право на свою точку зрения. Однако из-за их позиции не удалось выработать даже международно признанную терминологию в этой сфере. В силу сложности проведения атрибуции атак и в более спокойные времена было крайне сложно доказать причастность к ним конкретного государства. Ведь даже в случае атаки на иранскую ядерную программу специалисты в области информационной безопасности официально не указывают прямо на США и Израиль, хотя её результат наиболее всего соответствовал интересам именно этих двух стран, и косвенные улики указывали на их причастность. Сегодня же в условиях, когда со стороны Вашингтона приводится аргументация «у нас есть доказательства, но мы вам их не покажем, потому что они секретные», собрать доказательную базу так, чтобы неопровержимо продемонстрировать причастность США к атакам, например, в рамках тех же кибероперациий переднего края, представляется практически невыполнимой задачей. В результате ситуация сводится к тому, что действует право сильного.

Поэтому, *во-первых*, в Стратегии национальной кибербезопасности 2023 года сказано, что поддержка союзников и партнёров «будет продвигать реализацию целей внешней политики и кибербезопасности США», и предписано разработать

политику для определения, в каких случаях предоставление такой помощи будет соответствовать национальным интересам [14]. Аналогичный механизм прорабатывается в ЕС.

Во-вторых, Киберстратегия Министерства обороны США, опубликованная в 2023 году, предусматривает использование кибероперациий таким образом, чтобы это не могло стать причиной вооружённого конфликта. Этому способствует и опыт конфликта на Украине, показавший, что «проактивность в сфере кибербезопасности по своей сути не приводит к эскалации» [27].

Н. Фик заявил о том, что Госдепартамент прорабатывает официальный механизм содействия иностранным государствам в области киберпространства, цифровых и новых технологий [20].

В борьбе против России со стороны США участвуют не только государственные структуры. «Западные страны и компании предоставили Украине свои средства кибероборонbы. Со стороны Киберкомандования это выразилось в развёртывании передовых оперативных групп для проведения кибероперациий переднего края (отдельно подчёркивается, что "до вторжения"). Со стороны ЕС были задействованы группы быстрого реагирования в киберпространстве. ФБР и Агентство по кибербезопасности и защите инфраструктуры США (*Cybersecurity and Infrastructure Security Agency, CISA*) предоставляют Украине разведданные. "Майкрософт" (*Microsoft*) бесплатно обеспечивает перенос данных украинских госструктур в более безопасные места» [28].

В экспертной среде также ведётся обсуждение того, какое кибероружие США и НАТО могли бы с минимальными рисками передавать третьим странам, рассматривая в качестве получателей в первую очередь Украину и Грузию, и о том, как оценить вероятность и масштаб допустимого ущерба, который может быть нанесён России их применением данными государствами. Заявленная цель такой передачи – не в сдерживании РФ от действий в киберпространстве, а «в усилении арсенала асимметричных вооружений» у партнёров США. В случае кризиса наличие таких договорённостей ускорило бы передачу этим странам кибероружия такого действия, которое было бы адекватно интересам передающих стран. Рассматривается возможность использования площадок для коллективной помощи странам по запросу (в качестве примера приводится *Sovereign Cyber Effects Provided Voluntarily by Allies* блока НАТО, *SCEPVA*), но таким образом, чтобы другие не узнали о том, кто и как помог, во избежание раскрытия реальных возможностей участников такой площадки. Вместе с тем единства по этому вопросу в альянсе нет. Некоторые страны – участницы НАТО опасаются, что действия США по проведению наступательных кибероперациий могут превратить таких «помощников» в сторону конфликта [28].

Тем не менее на Западе активно обсуждается тема выработки механизма для предоставления помощи в киберпространстве [29]. Так, на саммите НАТО в Вильнюсе в 2023 году был запущен проект «Виртуальные силы и средства поддержки при киберинцидентах» (*Virtual Cyber Incident Support Capability*) «для поддержки

национальных усилий по смягчению последствий в ответ на вредоносную киберактивность со значительными последствиями». В Стратегии национальной кибербезопасности 2023 года этот механизм приведён в качестве примера того, что должны делать США [29].

ЗОНЫ РИСКА

Отработав указанные выше механизмы на Украине, США и страны НАТО могут зайти уже с отработанной методикой действий в другие страны. Например, в бывшие советские республики, включая среднеазиатские, которые стали пользоваться повышенным вниманием со стороны США. Почему вероятность согласия этих стран принять «по своей просьбе» такие группы велика? Потому что на территории некоторых из этих стран (Азербайджан, Армения, Казахстан, Таджикистан, Узбекистане) уже расположены американские военные биолаборатории, чья деятельность носит явно антироссийский характер, включая исследования по усилению функций опасных патогенов [30].

19 сентября 2023 года в Нью-Йорке президент США Дж. Байден встретился с президентами Казахстана, Киргизии, Таджикистана, Туркмении и Узбекистана. Подробностей о встрече мало, однако она входит в длинный перечень действий по отрыву этих стран от России. В случае успеха Вашингтона на этом направлении в киберпространстве данных стран вероятно появление передовых оперативных групп американского Киберкомандования для проведения кибероперации переднего края.

Это может значительно улучшить для США условия для действий в киберпространстве против России, Китая и других стран – от шпионажа до деструктивных кибератак – посредством использования «сети своих союзников и партнёров», наличие которой, согласно Киберстратегии Минобороны, представляет для Вашингтона «стратегическое преимущество» [31]. *Во-первых*, это может облегчить им проведение операций «под ложным флагом» против России и Китая. В случае если союзники и партнёры США, перечисленные выше, предоставят доступ к общим с РФ информационным системам (тем более, что среди них есть открыто взявшие антироссийский курс), это существенно затруднит обеспечение их информационной безопасности, поскольку, как минимум, перестанет работать принцип «безопасность через неясность» (*security by obscurity*). Интересно, что в Киберстратегии Министерства обороны США 2023 года подчёркивается аналогичная опасность для их собственных сетей в случае компрометации сетей союзников и партнёров [31]. *Во-вторых*, знание американской стороной сетей «союзников» может быть использовано для провокаций против последних посредством имитации атаки якобы со стороны России или Китая.

ЗАКЛЮЧЕНИЕ

Украина стала полигоном, на котором Киберкомандование США отрабатывает проведение в киберпространстве операций наступательного характера в условиях боевых действий против государства, также имеющего высокий потенциал в этой сфере – России. Кибероперации переднего края, предусматривающие выезд специалистов ВС США на территорию страны-партнёра для обнаружения активности киберподразделений третьих стран, изучения их подходов к обороне и нападению, а также выявления их инструментария, начали проводиться ещё до начала специальной военной операции. Затем личный состав был выведен за территорию Украины, но продолжил «оказывать ей содействие». Кроме государственных структур, то же делают и частные американские ИКТ-компании, такие как «Майкрософт».

Вопрос законности проведения наступательных кибероперации против другого государства, с которым США формально не находятся в состояния войны, является открытым даже среди американских специалистов. Тем не менее представители военного и политического руководства США открыто признают осуществление таких действий против России. При этом они пользуются правовой неопределённостью, сохранённой усилиями Вашингтона, и правом сильного, обеспеченным долгое время развиваемым киберпотенциалом, а обоснование законности или «забалтывание» незаконности этих действий оставляют своим экспертам и дипломатам.

Россия объявлена Соединёнными Штатами одним из главных противников, в том числе в киберпространстве, поэтому очевидно, что их кибернатиск на Восток будет продолжаться. Особое беспокойство вызывает постсоветское направление, включая среднеазиатское. Вашингтон последовательно работает над отрывом этих государств от России. С учётом наличия у них общих с Россией информационных систем, Вашингтон может рассматривать их в качестве места очередной зарубежной командировки передовых оперативных групп Киберкомандования США. Руководство этих стран может оказаться неспособным противостоять давлению США, если те «настойчиво предложат» им стать ещё одним (после Украины) полигоном для проведения наступательных кибероперации против России, как это случилось в случае появления в некоторых из них биолабораторий, работающих по американских военным программам.

ИСТОЧНИКИ

1. Martin, A. U.S. military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command. *Sky News*. 2022. June 01. Available at: https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (accessed 25.12.2023).

2. Pomerleau, M. Cyber National Mission Force declared sub-unified command. *DefenseScoop*. 2022. December 19. Available at:

https://defensescoop.com/2022/12/19/cyber-national-mission-force-declared-sub-unified-command/ (accessed 19.12.2023).

3. Presidential Policy Directive/PPD-20. *Federation of American Scientists*. 2012. October 16. Available at: https://irp.fas.org/offdocs/ppd/ppd-20.pdf (accessed 10.11.2023).

4. Pomerleau, M. New authorities mean lots of new missions at Cyber Command. *C4ISRNET*. 2019. May 08. Available at: https://www.c4isrnet.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/ (accessed 27.10.2023).

5. National Security Presidential Memoranda [NSPMs]. *Federation of American Scientists.* Available at: https://irp.fas.org/offdocs/nspm/ (accessed 10.11.2023).

6. John, S. McCain National Defense Authorization Act for Fiscal Year 2019. *GovInfo*. 2018. Available at: https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf (accessed 11.11.2023).

7. Pomerleau, M. Defense officials taking advantage of new cyber authorities. *C4ISRNET*. 2018. November 27. Available at: https://www.c4isrnet.com/dod/cybercom/2018/11/27/defense-officials-taking-advantage-of-new-cyber-authorities/ (accessed 27.10.2023).

8. CYBER 101: Hunt Forward Operations. *U.S. Cyber Command*. 2022. November 15. Available at: https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/ (accessed 27.10.2023).

9. "Building Resilience": U.S. returns from second defensive Hunt Operation in Lithuania. *U.S. Cyber Command*. 2023. September 12. Available at: https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/ (accessed 27.10.2023).

10. Kass, D.H. U.S. Cyber Command Year in Review 2022 Shows Major Steps to Defend Nation from Cyber Adversaries. *MSSP Alert*. 2023. January 06. Available at: https://www.msspalert.com/news/u-s-cyber-command-year-in-review-2022-shows-major-steps-to-defend-nation-from-cyber-adversaries (accessed 27.10.2023).

11. Pomerleau, M. Army's tactical cyber and electronic warfare unit gets new commander. *DefenseScoop*. 2023. June 30. Available at: https://defensescoop.com/2023/06/30/armys-tactical-cyber-and-electronic-warfare-unit-gets-new-commander/ (accessed 27.10.2023).

12. Before the Invasion: Hunt Forward Operations in Ukraine. *U.S. Cyber Command*. 2022. November 28. Available at: https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/ (accessed 27.10.2023).

13. Ответ специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности МИД России А.В. Крутских на вопрос газеты «Коммерсант». *Министерство*

иностранных дел Российской Федерации. 2022. 6 июня. Available at: https://www.mid.ru/ru/foreign_policy/news/1816353/ (accessed 30.10.2023).

14. National Cybersecurity Strategy 2023. *The White House*. 2023. March 1. Available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed 26.12.2023).

15. Pomerleau, M. Russia-Ukraine conflict forces DOD to revise assumptions about cyber's impact in war. *DefenseScoop*. 2023. September 18. Available at: https://defensescoop.com/2023/09/18/russia-ukraine-conflict-forces-dod-to-revise-assumptions-about-cybers-impact-in-war/ (accessed 25.12.2023).

16. Vasquez, C. Mayorkas warns Latin American leaders of Beijing's technology influence. *CyberScoop*. 2023. September 28. Available at: https://cyberscoop.com/mayorkas-latin-america-china/ (accessed 30.10.2023).

17. Гладков, А. Твой телефон – ключ доступа к тебе. Про российские мобильные ОС @MobileDeveloper. *Канал Максима Горшенина на YouTube*. 2023. May 06. Available at: https://www.youtube.com/watch?v=DwZGInVBKvU (accessed 10.11.2023).

18. Pomerleau, M. New triad is evolving deterrence for joint force. *DefenseScoop*. 2023. October 11. Available at: https://defensescoop.com/2023/10/11/new-triad-is-evolving-deterrence-for-joint-force/ (accessed 30.10.2023).

19. Martin, A. Ukraine war: US cyber chief on Kyiv's advantage over Russia. *Sky News*. 2022. June 8. Available at: https://news.sky.com/story/ukraine-war-us-cyber-chief-on-kyivs-advantage-over-russia-12628869 (accessed 25.12.2023).

20. US Leadership in Tech Diplomacy: A Conversation with Ambassador Nathaniel C. Fick. *Hudson Institute*. 2023. June 21. Available at: https://www.hudson.org/events/us-leadership-tech-diplomacy-conversation-ambassador-nathaniel-c-fick (accessed 02.11.2023).

21. Bing, C. Command and control: A fight for the future of government hacking. *CyberScoop*. 2018. April 11. Available at: https://cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/ (accessed 03.11.2023).

22. Chesney, R. Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries. *The Lawfare Institute*. 2018. April 12. Available at: https://www.lawfaremedia.org/article/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries (accessed 02.11.2023).

23. Lonergan, E.D. Cyberspace Is Neither Just an Intelligence Contest, nor a Domain of Military Conflict; SolarWinds Shows Us Why It's Both. *The Lawfare Institute*. 2021. May 12. Available at: https://www.lawfaremedia.org/article/cyberspace-neither-just-intelligence-contest-nor-domain-military-conflict-solarwinds-shows-us-why (accessed 02.11.2023).

24. Borghard, E.D., Lonergan, S.W. U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace. *Council on Foreign Relations*. 2020. April 22.

Available at: https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace (accessed 02.11.2023).

25. Elgan, M. What cybersecurity teams can learn from the US Cyber Command's «hunt forward». *SecurityIntelligence*. 2022. July 15. Available at: https://securityintelligence.com/articles/what-cybersecurity-teams-learn-us-cyber-command-hunt-forward/ (accessed 02.11.2023).

26. Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence. *Federation of American Scientists*. 2017. February. Available at: https://irp.fas.org/agency/dod/dsb/cyber-deter.pdf (accessed 16.11.2023).

27. Vićić, J., Winger, G.H. What the Defense Department's Cyber Strategy Says About Cyber Conflict. *The Lawfare Institute*. 2023. October 19. Available at: https://www.lawfaremedia.org/article/what-the-defense-department-s-cyber-strategy-says-about-cyber-conflict (accessed 03.11.2023).

28. Weber, V. The Benefits and Risks of Extending Weapons Deliveries to the Cyber Domain. *The Lawfare Institute*. 2022. December 02. Available at: https://www.lawfaremedia.org/article/benefits-and-risks-extending-weapons-deliveries-cyber-domain (accessed 03.11.2023).

29. Lostri, E. What Will Mechanisms for Cybersecurity Aid Look Like? *The Lawfare Institute*. 2023. September 12. Available at: https://www.lawfaremedia.org/article/what-will-mechanisms-for-cybersecurity-aid-look-like (accessed 03.11.2023).

30. В Минобороны рассказали о работе США над патогенами в Средней Азии и Закавказье. *Лента.ру*. 2023. 10 марта. Available at: https://lenta.ru/news/2023/03/10/usa_labs/ (accessed 25.12.2023).

31. 2023 DOD Cyber Strategy Summary. *U.S. Department of Defense*. 2023. September 12. Available at: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF (accessed 26.12.2023).

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

СЕЛЯНИН Ярослав Владиславович, научный сотрудник Центра североамериканских исследований Института мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук (ИМЭМО РАН).

Российская Федерация, Москва 117997, Профсоюзная ул., д. 23.

Yaroslav V. SELYANIN, Research Fellow, Center for North American Studies, Institute of World ·Economy and International Relations, Russian Academy of Sciences (IMEMO RAS).

23, Profsoyuznaya St., 117997 Moscow, Russian Federation.

Статья поступила в редакцию 11.04.2024 / Received 11.04.2024.
Поступила после рецензирования 30.04.2024 / Revised 30.04.2024.
Статья принята к публикации 5.05.2024 / Accepted 5.05.2024.