ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ

ИНСТИТУТ ЕВРОПЫ РОССИЙСКОЙ АКАДЕМИИ НАУК

125009, МОСКВА, МОХОВАЯ УЛ., 11-3
ТЕЛ.: +7(495)692-10-51/629-45-07
E-MAIL: europe@ieras.ru
WWW.INSTITUTEOFEUROPE.RU

INSTITUTE OF EUROPE RUSSIAN ACADEMY OF SCIENCES

125009, MOSCOW, MOKHOVAYA STR., 11-3
TEL.: +7(495)692-10-51/629-45-07
E-MAIL: europe-ins@mail.ru
WWW.INSTITUTEOFEUROPE.RU

Статья в журнале «Аналитические записки Института Европы РАН»

(Выпуск II) №13, 2022 (№280)

Военные аспекты кибербезопасности в контексте специальной военной операции РФ на территории Украины

Шариков Павел Александрович

кандидат политических наук, старший научный сотрудник Отдела европейской интеграции Института Европы РАН

Аннотация. *В ходе развернувшегося конфликта между Россией, Украиной и странами НАТО недружественные действия включают в себя, среди прочих, наступательные и оборонительные операции в киберпространстве. Автор рассматривает доктринальные и организационные аспекты применения военного киберпотенциала в ходе конфликта.*

Ключевые слова: *кибербезопасность, НАТО, военный киберпотенциал, наступательные кибероперации.*

Военный киберпотенциал стран НАТО

К началу XXI века развитие национального киберпотенциала стало приоритетом государственной политики и национальной безопасности в странах Европы и США.

Автор. Павел Александрович Шариков *– кандидат политических наук, старший научный сотрудник Отдела европейской интеграции Института Европы РАН.* ***Адрес****: 125009, Россия, г. Москва, ул. Моховая, д. 11, стр. 3.* ***E-mail****: pasha.sharikov@gmail.com*
DOI: http://doi.org/10.15211/analytics21320220512

Внедрение информационных технологий (ИТ) во все сферы общественной жизни требовало разработки централизованной политики в области развития национального киберпотенциала. В 1990-е – начале 2000-х гг. в США и странах Европы создавались национальные государственные ведомства, координирующие технологическое развитие. По мере распространения ИТ возрастала уязвимость критической инфраструктуры из-за киберугроз. Проблема кибербезопасности стала неотъемлемым элементом национальной и международной безопасности. В США раньше других стран был поставлен вопрос о военных аспектах кибербезопасности. В частности, при администрации Дж. Буша младшего велись широкие дискуссии о полномочиях вооружённых сил в сфере защиты информации и информационной инфраструктуры. Принципиальное противоречие заключалось в том, что потенциальный ущерб мог быть нанесён гражданским структурам, а для обеспечения кибербезопасности широкие полномочия должны были получить вооруженные силы.

В 2010 году в США в структуре Стратегического командования было учреждено Кибер командование, в функции которого входила защита военной информационно-технологической инфраструктуры. В 2017 году Д. Трамп повысил статус военного подразделения до уровня самостоятельного единого боевого командования[1]. Это было продиктовано тем, что проблематика кибербезопасности вышла за рамки компетенции Стратегического командования, связанной со сдерживанием стратегических угроз, и стала самостоятельным направлением военной стратегии, особое внимание которой уделялось наступательному киберпотенциалу.

Согласно документу [2], принятому в 2019 году, США характеризуют российскую активность в киберпространстве (как и китайскую, иранскую, северокорейскую и пр.) как *persistent engagement*, т.е. постоянные информационные и кибератаки незначительного масштаба, наносящие определенный ущерб, но не провоцирующие другую сторону на ответные действия, так как не пересекают порог военных действий, не переходят в острую фазу конфликта. В документе упоминается «порог военных действий» (*threshold of armed conflict*), который ни разу не пересекался, и не говорится о том, что произойдёт, если данный порог будет пройден. Очевидно, что переход порога предполагает военный ответ, но нет ясности относительно того, каким об будет: симметричным (кибер против кибер) или ассиметричным (т.е. с применением обычных вооружений или других методов). Судя по всему, США считают, что кибератаки низкой интенсивности предшествуют военным действиям, их цель – отвлечение внимания руководства, частичное повреждение различных экономических объектов и инфраструктур.

Развитие военного киберпотенциала в США оказало заметное влияние на европейские страны: в 2010-е – начале 2020-хх гг. в структурах их вооруженных сил были созданы

[1] Statement by President Donald J. Trump on the Elevation of Cyber Command. August 18, 2017 URL: https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/ (дата обращения: 07.04.2022)

[2] Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command, 2019 URL: https://nsarchive.gwu.edu/sites/default/files/documents/4421219/United-States-Cyber-Command-Achieve-and-Maintain.pdf (дата обращения: 07.04.2022)

подразделения, отвечающие за кибербезопасность. В их функции входит обеспечение кибербезопасности военной информационной инфраструктуры, защита национального киберпространства, проведение наступательных кибероперaций. Вашингтон, в основном в период администрации Б. Обамы, наладил двусторонние треки сотрудничества в сфере кибербезопасности с каждой из европейских стран, в том числе с основными союзниками: Германией [3] и Францией [4]. С Великобританией, самым близким союзником США, действует соглашение о сотрудничестве в области кибербезопасности [5]. Кроме того, американское киберкомандование проводит регулярные международные учения [6] по защите киберпространства, привлекая европейских союзников.

Коллективная кибероборона

Особое внимание США уделяют институциональному сотрудничеству в сфере кибербезопасности в рамках НАТО. В определённом смысле, развитие политики кибербезопасности в НАТО повторяет эволюцию политики кибербезопасности стран европейского региона и США. В 2012 году было учреждено Агентство по коммуникациям и информационным технологиям (*NATO Communication and Information Agency, NCIA*), в функции которого входят координация и управление ИТ-ресурсами стран НАТО, а также обеспечение коммуникации[7]. Кибербезопасность стала одним из приоритетов Североатлантического альянса. В 2014 году лидеры его государств-членов впервые согласились, что кибератака может стать основанием для применения пятой статьи Североатлантического договора. В 2016 году было решено отнести киберпространство к физическим пространствам – воздушному, наземному и морскому. В том же году на саммите в Варшаве было принято обязательство по кибероборонe (*NATO cyber pledge*)[8], согласно которому страны готовы принять схожие меры в сфере развития национальных киберпотенциалов.

Учитывая, что разные страны имеют различный киберпотенциал, возникали определённые разногласия относительно того, насколько применимо международное

[3] Joint Statement on U.S.-Germany Cyber Bilateral Meeting U.S.-Germany Cyber Bilateral Meeting, 24.03.2016. URL: https://www.auswaertiges-amt.de/en/newsroom/news/160323-cyber-konsultationen-usa/279470 (дата обращения: 07.04.2022)

[4] Fourth U.S.-France Cyber Dialogue, January 14, 2022. URL: https://www.state.gov/fourth-u-s-france-cyber-dialogue/ (дата обращения: 07.04.2022)

[5] U.S.-U.K. Cyber Agreement Opens Doors for Both Nations, September 8, 2016. URL: https://www.defense.gov/News/News-Stories/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/ (дата обращения: 07.04.2022)

[6] DOD's Largest Multinational Cyber Exercise Focuses on Collective Defense, December 6, 2021. URL: https://www.defense.gov/News/News-Stories/Article/Article/2863303/dods-largest-multinational-cyber-exercise-focuses-on-collective-defense/ (дата обращения: 07.04.2022)

[7] NCIA Who we are. URL: https://www.ncia.nato.int/about-us/who-we-are.html (дата обращения: 07.04.2022)

[8] Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (дата обращения: 07.04.2022)

право, в особенности военное право, к кибератакам и конфликтам в киберпространстве. Проработкой этого вопроса занимался учреждённый в Эстонии Центр превосходства по кибербезопасности. Одним из его наиболее заметных достижений является т.н. «Таллинский учебник» (*Tallin Manual*)[9], впервые опубликованный в 2012 году. В первой редакции были представлены наиболее общие аргументы, объясняющие юридическую сторону конфликтов в киберпространстве. Вторая редакция, вышедшая в свет в 2017 году, была посвящена исследованию ежедневных вызовов в киберпространстве, с которыми сталкиваются государства, а также правовых рамок реагирования на них. В настоящее время готовится третья редакция.

В 2018 году было объявлено, что НАТО планирует открыть центр проведения кибероперaций (*Cyber Operations Center, CYOC*) – аналог национальных военных киберкомандований. Пресса со ссылкой на высокопоставленных военных сообщала, что новый центр начнёт полноценную работу в 2023 году[10].

В 2020 году Министерство обороны Великобритании опубликовало первую редакцию «Доктрины операций в киберпространстве Объединённого командования НАТО»[11]. Центральное понятие доктрины кибербезопасности НАТО – суверенитет в информационном пространстве. Утверждается, что наступательные кибероперации будут производится посредством механизма добровольного определения влияния киберэффектов на суверенитет (*Sovereign Cyber Effects Provided Voluntarily by Allies, SCEPVA*). Судя по всему, в НАТО до сих пор нет консенсуса относительно планирования оборонительных и наступательных кибероперaций.

Доктринально политика НАТО в области кибербезопасности имеет много общего с американской. Подобно доктринальным документам США, в НАТО считается, что агрессия в киберпространстве – это угроза, требующая пристального внимания и оборонительных мероприятий, однако она не считается полноценной военной угрозой, так как не пересекает «порог военных действий» и, соответственно, не требует ответного удара вооружёнными силами.

Военный киберпотенциал в ходе конфликта на Украине

На практике этот тезис подтверждается развитием событий вокруг конфликта между Россией и Украиной в 2022 году. Ещё в декабре 2021 года в Киев отправились американские и британские специалисты по кибербезопасности, чтобы консультировать

[9] Schmitt M.N. (general editor). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013.
[10] Emmott, R., NATO cyber command to be fully operational in 2023, October 16, 2018. URL: https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9 (дата обращения: 07.04.2022)
[11] NATO Standard AJP-3.20, Allied Joint Doctrine for Cyberspace operations. Edition A Version 1 JANUARY 2020
URL:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (дата обращения: 07.04.2022)

украинские власти по отражению возможной киберагрессии[12]. Дмитрий Альперович, известный американский специалист в области кибербезопасности российского происхождения, тогда предполагал, что действия России в киберпространстве – это подготовка к наземной военной операции.

В начале февраля 2022 года, с визитом в Европу отправилась Энн Нойбергер, советник президента США по вопросам кибербезопасности. Она провела встречи с руководителями НАТО, ЕС, а также Болгарии, Чехии, Эстонии, Венгрии, Латвии, Литвы, Польши, Румынии, Словакии, Германии и Франции[13]. Цель визита Энн Нойбергер заключалась в том, чтобы разработать коллективные инструменты реагирования на кибератаки со стороны РФ, а также оказать поддержку Украине в случае возможной киберагрессии. Американские официальные лица утверждали, что Россия уже совершала кибератаку против энергетических объектов на территории Украины, и предупреждали, что подобные атаки могут повториться. О таких атаках сообщали и компании частного сектора. В частности, компания *Microsoft*[14] заявила о том, что РФ ведёт «не только полномасштабные кинетические, но и информационные военные действия». Президент *Microsoft* заявил, что сотрудничает с властями Украины, США, стран Европы и НАТО в области разработки защиты от кибератак.

При этом на официальном уровне отсутствуют признаки того, что разрабатывается военный ответ на подобные действия. Напротив, у США и европейских союзников большие опасения относительно того, что Россия, не желая перерастания военного конфликта в крупномасштабную войну против НАТО, будет использовать кибероружие.

24 февраля 2022 года, в первый день специальной военной операции, впервые была введена в действие Группа быстрого реагирования на кибератаки (*Cyber rapid response teams and mutual assistance in cybersecurity, CRRT*) в рамках Постоянного структурного сотрудничества по вопросам безопасности и обороны (*PESCO*). По просьбе[15] Украины в Киев отправилась группа экспертов из Хорватии, Эстонии, Литвы, Нидерландов, Польши и Румынии для консультаций и оказания помощи против киберугроз.

Спустя три недели после начала специальной военной операции Россия столкнулась с беспрецедентным давлением в киберпространстве. Хакерская группировка *Anonimous* в течение нескольких недель атаковала российские государственные сайты. Это были действия, скорее, похожие на хулиганство, чем на государственную киберагрессию. Тем

---

[12] Sanger D., Barnes J.E., U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault, New York Times, December 20, 2021. URL: https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.html (дата обращения: 07.04.2022)

[13] Chalfant M., Top White House cyber official to meet with Europeans amid Russia tensions, The Hill, February 1, 2022. URL: https://thehill.com/homenews/administration/592198-top-white-house-cyber-official-to-meet-with-europeans-amid-russia (дата обращения: 07.04.2022)

[14] Smith B., Digital technology and the war in Ukraine. February 28, 2022. URL: https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/ (дата обращения: 07.04.2022)

[15] Украина не является членом ЕС, но 15 апреля 2021 года установила сотрудничество со странами ЕС в рамках PESCO.
Ukraine-EU cooperation in the military-political, military and military-technical spheres, April 15, 2021. URL : https://ukraine-eu.mfa.gov.ua/en/2633-relations/spivpracya-ukrayina-yes-u-sferi-zovnishnoyi-politiki-i-bezpeki/spivpracya-ukrayina-yes-u-ramkah-spilnoyi-politiki-bezpeki-i-oboroni (дата обращения: 07.04.2022)

не менее, они наносили весьма заметные репутационные потери. Об инцидентах с кибератаками других государств против России не сообщалось. Информации о проведении или подготовке каких-либо наступательных информационных операций в открытом доступе нет. Наоборот, обсуждаются меры по обеспечению кибербезопасности в свете дальнейших кибератак со стороны РФ[16].

Согласно официальным заявлениям МИД РФ, «помимо подготовленных США и другими натовцами украинских спецподразделений информационно-технического воздействия в ведение этой кибервойны против нас все шире вовлекаются анонимные взломщики и провокаторы»[17]. Отмечается, что страны НАТО участвуют в подготовке украинских специалистов, но при этом, если и участвуют в киберагрессии против России, то анонимно, не давая оснований обвинить руководство своих стран в ведении военных действий.

В ходе встречи министров иностранных дел стран НАТО 7 апреля генеральный секретарь Йенс Столтенберг отметил, что «Украине оказывается масштабная помощь в сфере кибербезопасности»[18]. Судя по всему, основную поддержку оказывают США. На прошедших во вторник слушаниях в комитете по вооруженным силам Палаты Представителей глава Киберкомандования Пол Накасоне заявил [19], что с начала специальной операции команды передовых поисковых операций (*hunt forward teams*) американского Киберкомандования активно сотрудничали с союзниками по НАТО и Украиной для обнаружения уязвимостей в сетях и обеспечения безопасности критических инфраструктур.

Эксперты утверждают[20], что противоречия, связанные с отсутствием у стран-членов НАТО единого определения киберсуверенитета, объясняют и отсутствие консолидированной позиции по предполагаемым российским кибератакам против Украины и стран-членов.

С точки зрения международных отношений, проблема кибератак относится не столько к военной, сколько к публично-политической сфере. Ни одна из противоборствующих сторон не может убедительно доказать, что атака была организована государственными органами, специальными службами или вооруженными силами второй стороны. Любые

---

[16] Blessing J., Get ready for Russia's cyber retaliation, The Hill, March 3, 2022. URL: https://thehill.com/opinion/cybersecurity/596623-get-ready-for-russias-cyber-retaliation (дата обращения: 07.04.2022)

[17] Заявление МИД России в связи с продолжающейся киберагрессией со стороны «коллективного Запада». 29 марта 2022 г. URL: https://mid.ru/ru/foreign_policy/news/1806906/ (дата обращения: 07.04.2022)

[18] Press conference by NATO Secretary General Jens Stoltenberg following the meetings of NATO Ministers of Foreign Affairs, April 7, 2022. URL: https://www.nato.int/cps/en/natohq/opinions_194330.htm (дата обращения: 08.04.2022)

[19] Posture statement of Gen. Paul M. Nakasone, commander, U.S. Cyber Command before the 117th Congress. URL: https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/ (дата обращения: 08.04.2022)

[20] Shmitt M., Expert Backgrounder: NATO Response Options to Potential Russia Cyber Attacks Understanding the legal framework. Just Security, February 24, 2022. URL: https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks/ (дата обращения: 07.04.2022)

декларации вряд ли повлекут за собой судебные разбирательства или компенсации. Все обвинения друг друга в информационных атаках – форма политической эскалации. Даже атаки группировки *Anonymous* нельзя однозначно трактовать как натовские, а противодействовать им через международные институты невозможно из-за осложнившихся дипломатических отношений.

Очевидно, что, как в отдельных странах Европы и Северной Америки, так и в структуре Североатлантического альянса ведется разработка наступательных и оборонительных кибероперации. При этом вряд ли натовская доктрина кибербезопасности будет содержать декларации о применении киберагрессии, так как любая атака может быть расценена как акт государственной военной агрессии и неизбежно привести к настоящей военной эскалации.

Выводы

Можно констатировать, что кибероборона Североатлантического альянса в настоящее время находится на завершающем этапе институционального становления. Киберпотенциал развивался в каждой из стран-членов НАТО с учётом национальной специфики (последнее киберкомандование было открыто в Польше в феврале 2022 г.). В середине 2010-х гг. начался процесс унификации военных киберпотенциалов стран-членов НАТО. В начале 2020-х гг. наметилось учреждение объединённого киберкомандования НАТО, исполняющего функции как оборонительных, так и наступательных операций в киберпространстве.

В преддверии и в ходе специальной операции на Украине все стороны, принимающие участие в конфликте (включая союзников), отмечали, что количество и масштаб кибератак заметно возрос. Украина, не будучи членом НАТО и ЕС, тем не менее, получила масштабную поддержку против предполагаемых кибератак со стороны РФ. Помощь оказывалась на институциональном уровне (*PESCO*) и в двусторонних форматах (прежде всего с США, Великобританией и рядом соседних государств Европы). Наименьшую поддержку при этом Украина получила от НАТО. На институциональном уровне лишь 4 марта было объявлено, что Украина будет принята в качестве «участника, вносящего вклад»[21] (*contributing participant*) в натовский центр киберпревосходства в Эстонии.

Обращает на себя внимание масштабная помощь со стороны коммерческого ИТ-сектора как пример стихийного государственно-частного партнёрства. Оценить потенциальный ущерб, который отдельные страны-члены НАТО могут нанести России, на основе открытых данных не представляется возможным. Информация о военных потенциалах, как правило, носит закрытый характер. Информация о предполагаемых атаках со стороны России, а также об ответных действиях стран-членов НАТО распространяется

[21] Ukraine to be accepted as a Contributing Participant to NATO CCDCOE. The NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/ (дата обращения: 07.04.2022)

посредством публичных заявлений официальных лиц со ссылкой на данные разведки. В этой связи особого внимания заслуживают доктринальные положения наступления и обороны в киберпространстве.

В среднесрочной перспективе сохранится отношение к военным аспектам кибербезопасности как к форме агрессии, не переходящей порог войны. Такая агрессия требует принятия мер обороны и безопасности, но не предполагает активной разработки ответных действий. Важным аспектом является сдерживание, которое обеспечивается высокой степенью секретности (отсутствие информации о том, какие действия повлекут за собой ответ и каким он будет). Большое влияние окажут меры в области экспортного контроля высоких технологий, принятые США и ЕС в начале специальной военной операции.

Меры по противодействию киберугрозам предполагают интенсивное взаимодействие с частным сектором и гражданским обществом, но лидирующую роль играют государственные национальные институты. В Европе происходит консолидация информационных ресурсов на региональном уровне, при этом национальные киберстратегии превалируют над региональными и многосторонними усилиями. Идет поиск оптимальной модели взаимодействия государства (в лице правоохранительных и военных органов) и гражданского общества и бизнеса. Стратегическая цель такой модели – обеспечить конкурентоспособность, сохранив безопасность всех заинтересованных сторон.

Дата выпуска: 11 апреля 2022 года

Military cybersecurity issues in the context of Russia's special military operation in Ukraine

Author. Pavel Sharikov*, Candidate of Science (Politics), Leading researcher of Department of European Integration, Institute of Europe, Russian Academy of Sciences. Address: 11-3, Mokhovaya Street, Moscow, Russia, 125009. E-mail: pasha.sharikov@gmail.com*

Abstract*. The unfolding conflict between Russia, Ukraine and NATO includes offensive and defensive cyberoperations. The author investigates doctrinal and organizational aspects of the use of military cyber capabilities in the conflict.*

Keywords*: cyber security, NATO, military cyber capabilities, offensive cyber operations.*

DOI: http://doi.org/10.15211/analytics21320220512

http://www.zapiski-ieran.ru

Release date: April 11, 2022.