Международные процессы, Том 16, № 4 (55), сс. 181–192
DOI 10.17994/IT.2018.16.4.55.11

ХОЛОДНО — О ГОРЯЧЕМ
Дискуссии

НОВЕЙШИЕ КИБЕРСТРАТЕГИИ США – ПРЕАМБУЛА ВОЙНЫ?

АНАТОЛИЙ СМИРНОВ
МГИМО МИД России, Москва, Россия

Резюме

Человечество входит в полосу тотальной ломки миропорядка. При этом инфогенный нарратив играет все более подрывную роль в столь важной для судеб мира проблеме. США, являясь свыше сорока лет драйвером информационно-коммуникационных технологий, адаптивно использует их в геополитической конкуренции. Киберстратегии США стали, по сути, определяющими в трендах глобального развития ИКТ. При этом США умело используют отсутствие юридически обязывающих международных норм поведения государств в информационном пространстве и под надуманными угрозами из России, КНР, Ирана, КНДР планируют проведение не только оборонительных, но и наступательных кибероперaций. Наиболее известный пример – атака боевым кибервирусом «Стакснет» иранских ядерных объектов. Данная политика США провоцирует другие страны к принятию своих доктринальных и концептуальных документов, подстёгивая гонку кибервооружений. Инициативы России и её партнеров по ШОС, БРИКС и иным форматам сотрудничества обеспечить создание системы международной информационной безопасности (МИБ) на площадках ООН, ОБСЕ, АТЭС встречают агрессивное противодействие со стороны Соединённых Штатов. В силу этого наряду с одобренной подавляющим большинством российской резолюцией по МИБ на 73 Генассамблее ООН США выдвинули альтернативную резолюцию, собравшую почти в три раза меньше голосов, в основном стран–участниц НАТО. Настоящая статья призвана оценить соотношение преемственности и новаций в американских доктринальных документах по международной информационной безопасности. В этой связи киберстратегии, принятые администрацией Дональда Трампа, сравниваются с документами его непосредственного предшественника. Кроме того, в статье рассматривается поощряемый США процесс расширения активности НАТО в сфере ведения кибероперaций. Наконец, в завершение представляется альтернативная повестка дня обеспечения стабильности в информационном пространстве, отстаиваемая Россией и её партнёрами.

Ключевые слова:

информационно-коммуникационные технологии; информационная война; кибервойна; информационные операции; международная информационная безопасность; НАТО; США; Россия.

Человечество входит в полосу тотальной ломки и перековки миропорядка. При этом инфогенный нарратив играет всё более подрывную роль в столь важной для судеб мира проблеме обеспечения стабильного развития. США, являясь свыше сорока лет драйвером информационно-коммуникационных технологий, виртуозно манипулирует ими в интересах геополитического соперничества. Киберстратегии США стали, по сути, определяющими в трендах глобального развития

Дата поступления рукописи в редакцию: 03.10.2018
Дата принятия к публикации: 22.03.2019

Для связи с автором / Corresponding author:
Email: aismirnov46@gmail.com

интернет-пространства. При этом США умело используют отсутствие юридически обязывающих международных норм поведения государств в информационной среде и под надуманными угрозами из России, КНР, Ирана, КНДР планируют проведение не только оборонительных, но и наступательных кибероперации. Данная политика США провоцирует другие страны к принятию своих доктринальных и концептуальных документов, подстёгивая гонку кибервооружений. Инициативы России и её партнёров по ШОС, БРИКС и иным форматам сотрудничества обеспечить создание системы международной информационной безопасности (МИБ) на площадках ООН, ОБСЕ, АТЭС встречают агрессивное противодействие со стороны Соединённых Штатов.

1

В принятой в декабре 2017 г. Стратегии национальной безопасности США обращает на себя внимание многократное употребление (45 раз!) термина «кибер»[1]. В документе подчёркивается, что ревизионистские силы, такие как Китай и Россия, используют технологии, пропаганду и принуждение, чтобы сформировать миропорядок, противоречащий интересам и ценностям Соединённых Штатов. Между тем ещё в феврале 2016 г. предшествующий американский президент Барак Обама распорядился создать двухпартийную комиссию по укреплению национальной кибербезопасности, поручив ей оценить текущее положение дел и рекомендовать шаги, которые правительство, частный сектор и нация в целом могут предпринять для повышения защищённости в современном цифровом мире[2]. В декабре 2016 г. члены Комиссии (среди которых лидеры промышленности и научных кругов, многие из которых имели опыт работы в правительстве) представили получившийся доклад[3]. В нём отмечалось, что обеспечение кибербезопасности – одна из крупнейших проблем, с которыми сталкиваются США как нация. В этой связи она стала приоритетом политики поддержания национальной безопасности.

При администрации Б. Обамы последовательно осуществлялась стратегия, ориентированная на три приоритета[4]:

1) повышение уровня кибербезопасности и защиты от киберугроз в государственном и частном секторах;

2) сдерживание и прекращение злонамеренной киберактивности, направленной на Соединённые Штаты или их союзников;

3) эффективное реагирование на инциденты в области кибербезопасности и восстановление систем после кибератак.

В докладе подчёркивалось, что для укрепления государственной кибербезопасности в министерстве внутренней безопасности (*DHS*) был впервые учреждён пост главного сотрудника по информационной безопасности и защите критической инфраструктуры.

Комиссия отмечала, что США на международной арене:

– отстаивали применение международного права в киберпространстве[5];

– добивалась в «группе двадцати» и на других международных площадках принятия добровольных норм поведения государств в мирное время, обеспечив признание этих норм со стороны более тридцати стран;

– осуществили разработку мер укрепления доверия и заставили Китай и другие

[1] National Security Strategy of the United States. December 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 19.01.2018).

[2] Report on Securing and Growing the Digital Economy. Commission on Enhancing National Cybersecurity. 01.12.2016. URL: https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf (дата обращения: 01.13.2018).

[3] Report on Securing and Growing the Digital Economy. Commission on Enhancing National Cybersecurity. 01.12.2016. URL: https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf (дата обращения: 01.13.2018).

[4] Ibid.

[5] Только те его положения, которые отвечают национальным интересам США.

государства принять на себя обязательства по противодействию краже интеллектуальной собственности и коммерческой тайны;

– старались модернизировать процесс взаимной правовой помощи для более широкого трансграничного обмена данными между правоохранительными органами;

– разработали дополнительные инструменты, чтобы сдерживать и пресекать злонамеренную киберактивность, направленную против Соединённых Штатов.

Б. Обама, завершая свое президентство, заявил: «За последние восемь лет моя администрация добилась значительного прогресса в этом отношении. ...Теперь настало время для следующей администрации взять на себя эту обязанность и обеспечить, чтобы киберпространство продолжало оставаться драйвером процветания, инноваций и перемен — как в Соединённых Штатах, так и во всём мире»[6].

Силовой сценарий взаимодействия США с Россией объясняет многие факторы американской внешней политики, в том числе в области обеспечения международной информационной безопасности [Стрельцов, Смирнов 2017]. Рассмотрим перечень наиболее известных фактов в данной сфере. Соединённые Штаты отказались от взаимодействия с Россией по предотвращению инцидентов в сфере информационно-коммуникационных технологий, предусмотренного совместным заявлением президентов Российской Федерации и Соединенных Штатов Америки (2013). В 2015 г. США приняли Стратегию кибербезопасности, позволяющую вести наступательные кибервойны[7]. При этом, покидая свой пост, Б. Обама оставил в наследство Дональду Трампу заложенные в объекты критической информационной инфраструктуры России так называемые кибербомбы, которые можно привести в действие для подрыва экономической и социальной стабильности[8]. Кроме того, в открытый доступ просочились сведения о разработке Центральным разведывательным управлением США маскировочных программных средств проведения компьютерных атак, в том числе под «чужим флагом»[9].

Уже новый американский лидер Дональд Трамп 11 мая 2017 г. подписал закон об укреплении кибербезопасности федерального правительства и защите критической инфраструктуры страны от кибератак[10]. В период его правления Соединённые Штаты также отказались от достигнутой в ходе встречи 7 июля 2017 г. президентов двух стран в Гамбурге договорённости о создании рабочей группы по кибербезопасности. Вместо этого президент США 23 марта 2018 г. подписал закон о разъяснении законного использования данных за рубежом (*Clarifying Lawful Overseas Use of Data Act – CLOUD Act*[11]), который упростил национальным спецслужбам получение данных с технологического оборудования, поставленного американскими фирмами в любую страну.

Более того, при нём произошло повышение статуса Киберкомандования США до статуса независимой «командной единицы». Таким образом, оно впервые стало в один ряд с девятью другими стратегическими боевыми подразделениями США[12].

[6] Report on Securing and Growing the Digital Economy. Commission on Enhancing National Cybersecurity. 01.12.2016. URL: https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf (дата обращения: 01.13.2018).

[7] The Department of Defense Cyber Strategy. April 2015. URL: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата обращения: 16.02.2018).

[8] *Зубов Н.* Барак Обама приготовил «кибербомбы» для России // Коммерсант. 23.06.2017. URL: https://www.kommersant.ru/doc/3335422 (дата обращения: 06.10.2017).

[9] WikiLeaks: ЦРУ может устраивать кибератаки «под чужим флагом». ТАСС. 07.03.2017. URL: http://tass.ru/mezhdunarodnaya-panorama/4077772 (дата обращения: 06.12.2017).

[10] Белый дом: Трамп подписал указ об усилении кибербезопасности не в связи с РФ. ТАСС. 11.05.2017. URL: http://tass.ru/mezhdunarodnaya-panorama/4245924 (дата обращения: 16.02.2018).

[11] H.R.4943 – CLOUD Act. URL: https://www.congress.gov/bill/115th-congress/house-bill/4943 (дата обращения: 16.09.2018).

Кроме того, Дональд Трамп отменил правила по осуществлению кибератак, утверждённые директивой Б. Обамы[13]. При этом приоритетное значение Соединённые Штаты придают усилению информационной составляющей потенциала ведения гибридной войны, созданию системы глобальной электронной слежки и роботроллинга в социальных сетях, направленного на инспирирование «кибербунта» в России.

2

В сентябре 2018 г. Д. Трамп подписал Национальную киберстратегию США. Она вызвала одобрительную реакцию в самих Соединённых Штатах. Сторонники жёсткой линии были довольны тем, что в новом документе нашёл отражение дух экспансионизма, а их оппоненты – удовлетворены возрождением интереса к теме киберпространства, учитывая, что ранее Трамп упразднил пост координатора по кибервопросам в Белом доме и сократил расходы на эту область. При этом 40-страничный документ 2018 г. во многом повторяет разработки времён предыдущего президента.

В заявлении министерства внутренней безопасности США указывается, в частности, что ведомство «использовало свои полномочия для того, чтобы государственные учреждения... удалили антивирусные продукты лаборатории Касперского из своих систем». Упоминание российской компании не случайно: Москва определена как активный противник США[14]. Выходу национальной киберстратегии предшествовало появление новой киберстратегии министерства обороны США[15]. Документы достаточно схожи.

В частности, в киберстратегии Пентагона говорится: «Мы участвуем в долгосрочном стратегическом соперничестве с Китаем и Россией. Расширяя соперничество, эти государства включили в него постоянные кампании в киберпространстве, которые создают долгосрочный стратегический риск для нации, а также для наших союзников и партнёров. Китай разрушает военное преимущество США и экономическую жизнеспособность нации, систематически используя конфиденциальную информацию из учреждений государственного и частного секторов США. Россия применяла киберинформационные операции для оказания влияния на наше население и бросает вызов нашим демократическим процессам... Северная Корея и Иран также использовали злостную кибердеятельность, чтобы нанести ущерб гражданам США и поставить под угрозу интересы Соединённых Штатов... Растущая зависимость США от киберпространства... становится неприемлемым риском для нации»[16].

Схожий посыл содержится и в Национальной киберстратегии Соединённых Штатов: «Россия, Иран и Северная Корея провели безрассудные кибератаки, которые нанесли ущерб американскому и международному бизнесу, а также нашим союзникам и партнёрам... Китай занимается киберэкономическим шпионажем и кражей триллионов долларов интеллектуальной собственности... Россия, Китай, Иран и Северная Корея используют киберпространство, чтобы бросить вызов Соединённым Штатам, их союзникам и партнёрам... Эти противники используют кибертехнологии для подрыва нашей экономики

[12] Киберкомандование США. US Cybercom. URL: http://tadviser.ru/a/353528 (дата обращения: 26.08.2018).

[13] *Volz D.* Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive. The Wall Street Journal. 15.08.2018. URL: https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721 (дата обращения: 26.08.2018).

[14] Statement by Secretary Kirstjen M. Nielsen on the Release of the National Cyber Strategy. 20.09.2018. URL: https://www.dhs.gov/news/2018/09/20/statement-secretary-kirstjen-m-nielsen-release-national-cyber-strategy (дата обращения: 01.10.2018).

[15] Прежняя киберстратегия минобороны США вышла в 2015 г.

[16] Department of Defense Cyber Strategy 2018. Summary. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (дата обращения: 01.10.2018).

и демократии, воруют нашу интеллектуальную собственность и вносят разлад в нашу демократическую систему...»[17]. Существенно, что США уже не первый раз в своих доктринальных документах официально называют Россию противником.

В национальной киберстратегии содержатся два раздела, в которых говорится о глобальной кибербезопасности на морских коммуникациях и в космическом пространстве. При этом контроль над ними с использованием новейших технических средств рассматривается как один из национальных приоритетов.

Среди поставленных Стратегией задач значатся[18]:

– модернизация электронного наблюдения, дающая возможность спецслужбам контролировать потоки данных;

– передача новых полномочий силовым органам;

– разработка новых механизмов для преследования лиц, находящихся за пределами США (в том числе граждан других государств);

– активные действия: «для предотвращения и сдерживания злонамеренной киберактивности против Соединённых Штатов могут быть использованы все инструменты государственной власти. К ним относятся дипломатические, информационные, военные, финансовые, интеллектуальные, общественные и правоохранительные возможности».

Советник президента США по национальной безопасности Джон Болтон, выступая на пресс-конференции в Вашингтоне по случаю обнародования новой киберстратегии, заявил, что Белый дом «разрешил наступательные кибероперации... для создания структур сдерживания, которые продемонстрируют противникам, что стоимость их участия в операциях против нас выше, чем они рассчитывают»[19]. При этом весь опыт американской политики сдерживания говорит, что данным понятием охватывается и организация государственных переворотов, и открытая интервенция. В киберпространстве это может означать осуществление DDoS-атак, внедрение вредоносных и шпионских программ, нанесение ударов по уязвимым местам противника – критической информационной инфраструктуре, инспирирование «кибербунтов» в социальных сетях через армии «умных» ботнетов и др. Далеко не все государства будут в состоянии эффективно и безболезненно отразить такие атаки.

Что касается киберстратегии Пентагона, то в этом документе подчёркивается необходимость «создания более смертоносных сил (lethal force)»[20]. Таким образом, это уже открытое выражение агрессивных намерений, и администрация Д. Трампа даёт Пентагону зелёный свет для кибератак по всему миру. Учитывая, что в международном праве ясного определения «злонамеренных действий в киберпространстве» нет, то под такие операции можно подвести всё что угодно. И ещё один важный аспект: «Национальная киберстратегия сохранит в долгосрочной перспективе открытость Интернета, что поддержит и заново обозначит американские интересы»[21]. Таким

[17] Statement by Secretary Kirstjen M. Nielsen on the Release of the National Cyber Strategy. 20.09.2018. URL: https://www.dhs.gov/news/2018/09/20/statement-secretary-kirstjen-m-nielsen-release-national-cyber-strategy (дата обращения: 01.10.2018).

[18] Ibid.

[19] The Cybersecurity 202: Trump administration seeks to project tougher stance in cyberspace with new strategy. The Washington Post. 21.09.2018. URL: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/21/the-cybersecurity-202-trump-administration-seeks-to-project-tougher-stance-in-cyberspace-with-new-strategy/5ba3e85d1b326b7c8a8d158a/?noredirect=on&utm_term=.a2a77a27737a (дата обращения: 01.10.2018).

[20] Department of Defense Cyber Strategy 2018. Summary. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (дата обращения: 01.10.2018).

[21] President Donald J. Trump is Strengthening America's Cybersecurity. 20.09.2018. URL: https://www.globalsecurity.org/security/library/news/2018/09/sec-180920-whitehouse01.htm?_m=3n%252e002a%252e2390%252ero0ao07f9a%252e277u (дата обращения: 01.10.2018).

образом, США продолжают отвергать обсуждение проблем интернационализации управления сетью и национальной юрисдикции в Интернете.

Из вышеизложенного можно сделать промежуточный вывод о том, что «ответственное поведение» в киберпространстве должно сводиться к следованию правилам, которые установят Соединённые Штаты. Даже сам отказ от принятия этих правил может трактоваться как ведение войны против США.

3

В условиях резкого обострения российско-американских отношений внимания заслуживает вышедшая в июне 2017 г. в США разоблачительная книга Д. Ковалика «Заговор, делающий Россию козлом отпущения: как ЦРУ и "глубинное государство" сговорились, чтобы очернить Путина» [Kovalik 2017][22].

По мнению автора, на обвинения в адрес Москвы о «вмешательстве в выборы в США» следует смотреть в широком историческом контексте[23]. В частности, Ковалик характеризует конфронтацию США и СССР в период «холодной войны» и после её окончания и пишет, что Соединённые Штаты неоднократно вмешивались во внутренние дела России, нарушали обещания и унижали Москву. Разговоры о «российских хакерах» представляются Д. Ковалику попыткой сделать Москву «козлом отпущения», которая чревата не чем иным, как новой опасной конфронтацией с Россией. Автор, в частности, пишет, что были ли «русские хакеры», уже мало кого волнует, а следствие сосредоточилось на том, пытался ли президент Д. Трамп помешать расследованию, когда уволил директора ФБР Дж. Коми.

Д. Ковалик сравнивает ситуацию с послевоенной эпохой маккартизма, когда антикоммунистические настроения в американском обществе нашли выражение в поисках, предании правосудию, а иногда и расправе над «антиамерикански» настроенными гражданами. Не только он, но и многие рядовые американцы, даже находясь под мощным информационным давлением, в том числе спецслужб США, пытаются отстаивать свою точку зрения в глобальных социальных сетях, несмотря на муссирование русофобских измышлений.

4

Уже несколько лет у России с НАТО практически нет совпадающей повестки дня в сфере безопасности. Североатлантический альянс всё более отчетливо навязывает Москве некое военное соревнование. Генетический код НАТО, который закладывался при его создании, сохранился, а его проявления видны и сегодня: поиск врага на Востоке, от которого якобы надо обороняться. На это надо тратить огромные ресурсы, вести пропаганду, чтобы показать, что у блока есть «серьёзное дело» в области безопасности, хотя тупиковость этого пути всё более очевидна.

На саммитах НАТО в Бухаресте (2008) и Лиссабоне (2010) обсуждалось и было впервые включено в стратегическую концепцию НАТО *положение о киберпространстве как новой, пятой, сфере военной деятельности альянса*. Данное направление получило динамичное развитие на саммите НАТО в Уэльсе (2014) и стало одним из ключевых на последующих, в том числе парламентских, ассамблеях организации[24]. Ещё в 2010 г. в концепции альянса, получившей название *NATO's Bi-Strategic Command Capstone Concept*, были официально определены гибридные угрозы как угрозы для НАТО, создаваемые противником одновременно в

[22] *Д. Ковалик* — известный американский журналист, юрист и активист движения за мир, профессор юриспруденции Питтсбургского университета в Пенсильвании.

[23] В США вышла книга, оспаривающая теорию о «вмешательстве России» в выборы. РИА Новости. 26.06.2017. URL: https://ria.ru/world/20170626/1497276092.html (дата обращения: 14.07.2018).

[24] NATO told to speed up info campaign in response to Russia, Daesh moves. 07.10.2017. URL: https://www.nato-pa.int/news/nato-told-speed-info-campaign-response-russia-daesh-moves (дата обращения: 26.08.2018).

дипломатической, экономической, военной и информационной сферах[25]. Во многом *интерес к этой тематике обусловлен тем, что гибридный вариант действий не подпадает под определение агрессии*.

При этом, действуя по принципу «держи вора!», в экспертных кругах НАТО для обозначения якобы негативной роли участия России в тех или иных конфликтах, как правило, ей приписывают ведение гибридных войн. Рассмотрим наиболее яркий пример – пункт из заявления по итогам саммита НАТО 8–9 июля 2016 г. в Варшаве[26]: «Дуга нестабильности и отсутствия безопасности простирается на периферии НАТО и за её пределами. Североатлантический союз сталкивается с рядом вызовов и угроз безопасности, исходящих с востока и с юга, от государственных и негосударственных субъектов, от вооружённых сил и террористических, *кибернетических или гибридных нападений*. *Агрессивные действия России, в частности провокационная военная деятельность на периферии территории НАТО и проявленная Россией готовность добиваться политических целей с помощью угрозы силой и применения силы* (выделено автором), являются одним из источников региональной нестабильности, представляют собой фундаментальный вызов, брошенный Североатлантическому союзу, наносят урон евроатлантической безопасности и угрожают нашей давней цели – созданию единой, свободной и мирной Европы».

Таким образом, НАТО совершенно бездоказательно пытается навязать всему миру имидж Москвы как агрессора, использующего в том числе кибернетические и гибридные операции на периферии территории альянса, «забывая» о том, что сам блок расширялся и вплотную подошёл к границам России.

Важную роль в разработке международно-правовых аспектов обоснования кибермилитаризации, а также в проведении конференций и крупномасштабных учений играют *Центры передового опыта НАТО*. Рассмотрим лишь некоторые аспекты их деятельности, профильные для тематики статьи. Объединённый *Центр в области кибероборонь НАТО (CCD COE)* в Таллинне был создан в 2008 г. и имеет статус военной организации. Его главная задача – консультирование, обучение специалистов и исследования в области кибербезопасности и международного права[27]. Центр укомплектован и финансируется рядом стран–участниц НАТО (Бельгия, Великобритания, Венгрия, Германия, Греция, Испания, Италия, Латвия, Литва, Нидерланды, Польша, Словакия, США, Турция, Франция, Чехия, Эстония. Намерение участвовать в работе Центра выразили Норвегия и Румыния). Австрия, Финляндия и Швеция имеют статус участников, не входящих в альянс.

В 2013 г. огранизация опубликовала Таллиннское руководство по вопросам применения международного права к условиям конфликтов в киберпространстве [Tallinn Manual 2013]. 300-страничный документ привлёк к себе внимание тем, что ряд его положений санкционирует применение широкого спектра кинетического оружия против источника киберугрозы, силовые действия военных в отношении гражданских лиц, причастных к кибератакам (за счёт причисления их к комбатантам), а также военные кибероперации, направленные против критической информационной инфраструктуры. Наличие подобных положений позволило ряду экспертов и дипломатов утверждать, что Таллиннское руководство даёт государствам международно-правовую базу для ведения наступательной кибервойны. *Россия и*

[25] Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats. August 2010. URL: http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf (дата обращения: 26.05.2018).

[26] 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: http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (дата обращения: 26.05.2018).

[27] The NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/ (дата обращения: 13.06.2018).

её партнёры активно занимают противоположную позицию, выступая за предотвращение использования информационно-коммуникационных технологий в военных целях.

Документ по сути легитимировал конфликты в киберпространстве как форму поведения государств и действующих в их интересах посредников (*proxy actors*)[28]. В частности, *следуя логике Таллиннского руководства, после атаки боевого кибервируса Stuxnet в 2010 г. на информационные системы центрифуг по обогащению урана Иран был бы правомочен в ответ применить кинетическое оружие.* Бывший аналитик ЦРУ М. Барроуз указывал, что червь Stuxnet «смог, пусть и на короткое время, приостановить иранскую ядерную программу. Он нарушил работу почти 1000 центрифуг для обогащения уранового топлива. По мнению экспертов, иранцы, обнаружив вирус и избавившись от 1000 заражённых устройств, смогли предотвратить больший ущерб» [Барроуз 2015: 193]. Между тем государственный секретарь США Х. Клинтон в 2011 г. заявила, что проект по разработке вируса *Stuxnet* оказался успешным и иранская ядерная программа, таким образом, будет отброшена на несколько лет назад[29].

Таллиннское руководство активно вплетает правила ведения кибервойн в ткань международного права, да ещё с акцентом на проактивных операциях, то есть на кибернападении. Именно в легитимации конфликтов в информационном пространстве российские эксперты видят главный порок этого документа, который противоречит ключевому посылу России и её партнёров о недопустимости информационных войн.

Таллиннское руководство – 2.0, вышедшее в феврале 2017 года, равно как и другие многочисленные работы Центра в области кибероборонь НАТО, показывают, что его позиция не меняется [Tallinn Manual 2.0 2017]. Например, в прошедших в Эстонии 23–27 апреля 2018 г. учениях «Сомкнутые щиты» (*Locked Shields*) приняли участие порядка 1 тыс. экспертов из 30 стран. Было задействовано около 4000 виртуальных систем с имитацией кибернападений. Информация о мероприятии подтвердила наступательный характер разрабатывавшихся сценариев, так как число компьютерных атак на легендированную страну за 4 дня превышало 2500[30]. В июне 2018 г. в Таллинне прошла 10-я Международная конференция по киберконфликтам (*CyCon*-2018), организованная Центром. В мероприятии приняли участие свыше 700 киберэкспертов из более чем 40 стран. На 28–31 мая 2019 г. запланирована 11-я конференция *CyCon*-2019 на тему «Тихая битва» (*Silent Battle*)[31].

Среди Центров передового опыта НАТО особое место в информационной войне против России занимает *Центр в области стратегических коммуникаций (Стратком) в Риге (Strategic Communications Centre of Excellence)*[32]. Он был создан в 2014 году, но открыт 20 августа 2015 года. На церемонии, помимо президентов Латвии Р. Вейониса и Литвы Д. Грибаускайте, присутствовала делегация американских сенаторов во главе с Дж. Маккейном. Суть их выступлений: *в арсенале Центра есть средства, способные заставить врагов потерять волю к борьбе и возненавидеть собственную страну, что приведёт к бескровной победе*[33].

Стратегические коммуникации НАТО – достаточно новая концепция, включающая спектр средств публичной дипломатии и общественных отношений, от убеждения с

[28] «Таллиннское руководство» — апология кибервойны? URL: http://infoshos.ru/ru/?idn=11516 (дата обращения: 13.11.2017).

[29] Rumors mount as Bushehr nuclear plant readies for power launch. RT. 17.01.2011. URL: https://www.rt.com/russia/rosatom-bushehr-safe-viruses/ (дата обращения: 13.06.2018).

[30] NATO Won Cyber Defence Exercise Locked Shields 2018. URL: https://ccdcoe.org/nato-won-cyber-defence-exercise-locked-shields-2018.html (дата обращения: 13.07.2018).

[31] Cycon 2019 Theme Silent Battle Cyber Space. URL: https://ccdcoe.org/cycon-2019-theme-silent-battle-cyber-space.html (дата обращения: 13.06.2018).

[32] NATO Stratcom Center of Excellence. URL: http://www.stratcomcoe.org/ (дата обращения: 13.06.2018).

помощью психологических операций до применения силы. Одна из главных *целей Страткома – это дискредитации политического и военного руководства России*, распространение панических и пораженческих настроений среди населения[34]. Под видом борьбы с российскими СМИ и вербовщиками ИГИЛ Центр решает важнейшую для США и НАТО задачу – сдерживание России и обеспечение глобального информационного доминирования. Об этом убедительно говорят и названия практически всех работ и мероприятий Центра.

При этом Североатлантический альянс продолжает наращивать киберпотенциал. 8 ноября 2017 г. генеральный секретарь организации по итогам встречи министров обороны заявил: «Сегодня министры договорились о создании нового Центра кибероперациий в рамках проекта адаптированной структуры органов военного управления НАТО. Это позволит усилить нашу киберзащиту и поможет интегрировать её в планирование и операции НАТО на всех уровнях. Кроме того, мы приняли решение о том, что сможем интегрировать национальные средства киберзащиты союзников в миссии и операции НАТО»[35]. Как стало известно по итогам саммита альянса в Брюсселе в июле 2018 года, штат Центра кибероперациий в бельгийском Монсе будет состоять из 70 экспертов, которые станут получать разведданные и обрабатывать огромные массивы информации в режиме реального времени[36].

* * *

5 декабря 2018 г. Генеральная Ассамблея ООН приняла российскую резолюцию по международной информационной безопасности: «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/73/27)[37]. Её поддержало подавляющее большинство государств. Более 30 стран из всех регионов мира стали её соавторами[38]. Данный документ открыл новый этап в глобальной дискуссии по международной информационной безопасности (эта проблема была впервые включена в повестку дня ООН в 1998 г. по инициативе России). Генеральной Ассамблее удалось принять прорывные решения, нацеленные на реальное укрепление этой дискуссии. Главная задача – защитить интересы всех стран в цифровой сфере, вне зависимости от того, на каком уровне технологического развития они находятся.

Речь идёт о ряде исторических новаций в документе. *Во-первых*, это свод из тринадцати правил, норм и принципов ответственного поведения государств в информационном пространстве. По сути, это первые в истории «правила дорожного движения» в цифровой сфере. Их смысл – заложить основу мирного взаимодействия государств в ней, обеспечить предотвращение войн, конфронтации и любых агрессивных действий.

Среди принятых норм такие принципиально важные положения, как обязательства

[33] *Родин Ю., Горячев О.* ПБК: Центр пропаганды НАТО в Риге выиграет войну без единого выстрела. RT. 21.08.2015. URL: https://russian.rt.com/inotv/2015-08-21/PBK-Centr-propagandi-NATO-v (дата обращения: 13.08.2018).

[34] В сети опубликованы планы психологической войны НАТО и Украины против России. Правда.ру. 10.04.2015. URL: http://www.pravda.ru/news/society/10-04-2015/1255842-internet-0/ (дата обращения: 13.06.2018).

[35] Пресс-конференция генерального секретаря НАТО Й. Столтенберга по итогам заседания совета министров обороны. 08.11.2017. URL: https://www.nato.int/nato_static_fl2014/assets/audio/audio_2017_11/20171108_171108c-ru.mp3 (дата обращения: 14.01.2018).

[36] Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018. URL: https://www.nato.int/cps/en/natohq/official_texts_156624.htm (дата обращения: 14.11.2018).

[37] Resolution adopted by the General Assembly on 5 December 2018. 73/27.Developments in the field of information and telecommunications in the context of international security. URL: https://undocs.org/A/RES/73/27 (дата обращения: 14.12.2018).

[38] О принятии Генассамблеей ООН российской резолюции по международной информационной безопасности. 07.12.2018. URL: http://www.mid.ru/ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3437775 (дата обращения: 14.12.2018).

использовать информационно-коммуникационные технологии исключительно в мирных целях, соблюдать в информационном пространстве принцип государственного суверенитета, сотрудничать в борьбе с применением современных технологий в преступных и террористических целях, предотвращать распространение скрытых вредоносных функций в ИТ-продукции («закладок»). Кроме того, в принятом своде зафиксированы следующие принципы:

– любые обвинения в злонамеренном использовании ИКТ должны быть доказаны;

– государства не должны использовать посредников для злонамеренного применения информационно-коммуникационных технологий;

– ООН должна играть ведущую роль в дискуссиях по международной информационной безопасности;

– суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с информационно-коммуникационными технологиями, и к их юрисдикции над интернет-инфраструктурой, расположенной на их территории;

– государства несут главную ответственность за поддержание безопасной и мирной информационной среды.

Кроме того, в российском документе предлагается демократизировать переговорный процесс по международной информационной безопасности в ООН, сделать его подлинно открытым, демократическим, инклюзивным и прозрачным. В этих целях *в рамках Организации впервые создаётся рабочая группа открытого состава по этой проблематике (РГОС). Это означает, что в её работе смогут участвовать все без исключения государства–члены ООН.* Таким образом, мировое сообщество выразило убеждённость, что эпоха «клубных» договорённостей прошла и что все страны, вне зависимости от уровня их технологического развития, имеют право принимать прямое участие в переговорах по международной информационной безопасности, влияя на принятие решений. Каждый голос важен и должен быть учтён. Лишь таким образом можно заложить основу справедливого и равноправного миропорядка в цифровой сфере.

Планируется, что РГОС будет уполномочена рассматривать весь спектр вопросов обеспечения международной информационной безопасности. Приоритетное внимание она должна уделить дальнейшей работе над нормами, правилами и принципами ответственного поведения в информационном пространстве, вопросам применимости в нём международного права и наращиванию цифрового потенциала развивающихся стран. Такой мандат переговорная структура ООН получает впервые. Кроме того, РГОС повышает сам статус дискуссии по международной информационной безопасности. В отличие от прежней группы правительственных экспертов (ГПЭ) ООН новая структура – это полноценный орган Генеральной Ассамблеи, который может вырабатывать и рекомендовать государствам-членам любые документы вплоть до проектов международных договоров.

Новым элементом мандата РГОС стало изучение возможности проведения регулярного институционального диалога с широким кругом участников под эгидой ООН. Иначе говоря, рабочая группа должна рассмотреть варианты создания постоянно действующей переговорной структуры по международной информационной безопасности. В резолюции впервые предусмотрен механизм межсессионных консультаций РГОС с негосударственными игроками – бизнесом, неправительственными организациями и научным сообществом для обмена взглядами по вопросам, входящим в мандат группы. Это даст возможность подключить их к дискуссии по принципиально важным аспектам использования информационно-коммуникационных технологий.

Против столь очевидных прогрессивных идей коллективно выступили западные страны, прежде всего США и государства-члены ЕС. Тем самым они де-факто противопоставили себя международному сообще-

ству. Симптоматично, что именно эти государства активно нагнетают в СМИ атмосферу недоверия и раскручивают обвинения в кибератаках в адрес третьих стран. Напрашивается вывод, что в реальности они преследуют собственные цели и не заинтересованы в объективном и прагматичном решении проблем, связанных с обеспечением международной информационной безопасности, а также в придании переговорному процессу по этой теме открытого и прозрачного для всех участников характера.

Между тем протащенная США Резолюция Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» предполагает создание новой группы правительственных экспертов на основе справедливого географического распределения. Последняя начнёт работу в конце 2019 года[39]. Сам факт принятия двух резолюций ООН по тематике международной информационной безопасности показывает высокую значимость проблемы. Россия уже высказалась за координацию и взаимодействие групп, но Соединённые Штаты хранят молчание. Как всегда.

Список литературы

Барроуз М. Будущее: рассекречено. Каким будет мир в 2030 году. М.: Манн, Иванов и Фербер, 2015. 352 с.

Стрельцов А.А., Смирнов А.И. Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям // Международная жизнь. 2017. № 11. URL: https://interaffairs.ru/virtualread/ia_rus/112017/files/assets/basic-html/page74.html (дата обращения: 26.08.2018).

Kovalik D. The Plot to Scapegoat Russia: How the CIA and the Deep State Have Conspired to Vilify Putin. Skyhorse, 2017. 240 p.

Tallinn Manual on the International Law Applicable to Cyber Warfare / M.N. Schmitt. Cambridge University Press, 2013. 300 p.

Tallinn manual 2.0 on the international law applicable to cyber operations / ed. by M.N. Schmitt. Cambridge University Press, 2017. 638 p.

REVISION OF THE U.S. CYBERSTRATEGY UNDER DONALD TRUMP: PREAMBLE FOR AGGRESSION?

ANATOLY SMIRNOV
MGIMO University, Moscow 119454, Russia

Abstract

Mankind has entered the critical zone of breaking the world order. The more and more disruptive in this process is the infogenic narrative. The United States, as one of the leaders of information and communication technologies (ICT), has been adaptively developing and using its cyberpotential in

[39] Резолюция, принятая Генеральной Ассамблеей 22 декабря 2018 года. 73/266. Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности. URL: https://undocs.org/ru/A/RES/73/266 (дата обращения: 23.12.2018).

geopolitical competition for over 30 years to implement the doctrine of global information dominance. The US cyber strategies are largely predetermining global trends in the use of ICT. The absence of legally binding international norms and rules of behavior of states in the information space allowed the United States in the latest cyber strategies under false threats to conduct against Russia, the PRC, Iran and the DPRK not only defensive, but also offensive operations both in war and in peacetime in the context of conducting hybrid wars The US intimidates the Western public with "Russian hackers," attributing to them "hacking" of computer networks almost all over the world. This policy provokes other countries to adopt their cyber doctrine, stimulating the information arms race. Attempts by Russia and its partners in the SCO, BRICS and other formats of cooperation to ensure international information security (IIS) at the UN, OSCE, APEC sites, etc. meet more and more aggressive opposition from the United States and its satellites. This, in particular, was reflected in the failure of the adoption of the final document by the UN Group of Governmental Experts on the IIS in 2017. Against the background of these events, the development under the UN auspices of the global rules of responsible behavior of states in the information space is becoming even more relevant. Russia submitted a draft resolution to the First Committee of the 73rd session of the UN General Assembly, as well as the development of a Convention on Cybercrime in the Third Committee.

Keywords:

hybrid warfare; information and communications technology; information war; cyber warfare; cyberstrategy; cybercrime, international information security; USA; Russia.

References

Burrows M. (2015). *Buduschee: rassekrecheno. Kakim budet mir v 2030 godu* [The Future, Declassified: Megatrends That Will Undo the World Unless We Take Action]. Moscow: Mann, Ivanov i Ferber. 352 p.

Kovalik D. (2017). *The Plot to Scapegoat Russia: How the CIA and the Deep State Have Conspired to Vilify Putin.* Skyhorse. 240 p.

Schmitt M.N. (ed.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press. 300 p.

Schmitt M.N. (ed.) (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations.* Cambridge University Press, 2017. 638 p.

Strel'tsov A.A., Smirnov A.I. (2017). Rossijsko-amerikansloe sotrudnichestvo v oblasti mezhdunarodnoj informatsionnoj bezopasnosti: predlozheniya po prioritetnym napravleniyam [Russian-American Cooperation in the Field of International Information Security: Suggestions on Priority Directions]. *Mezhdunarodnaya zhizn'*. No. 11. URL: https://interaffairs.ru/virtualread/ia_rus/112017/files/assets/basic-html/page74.html (date of access: 26.08.2018).