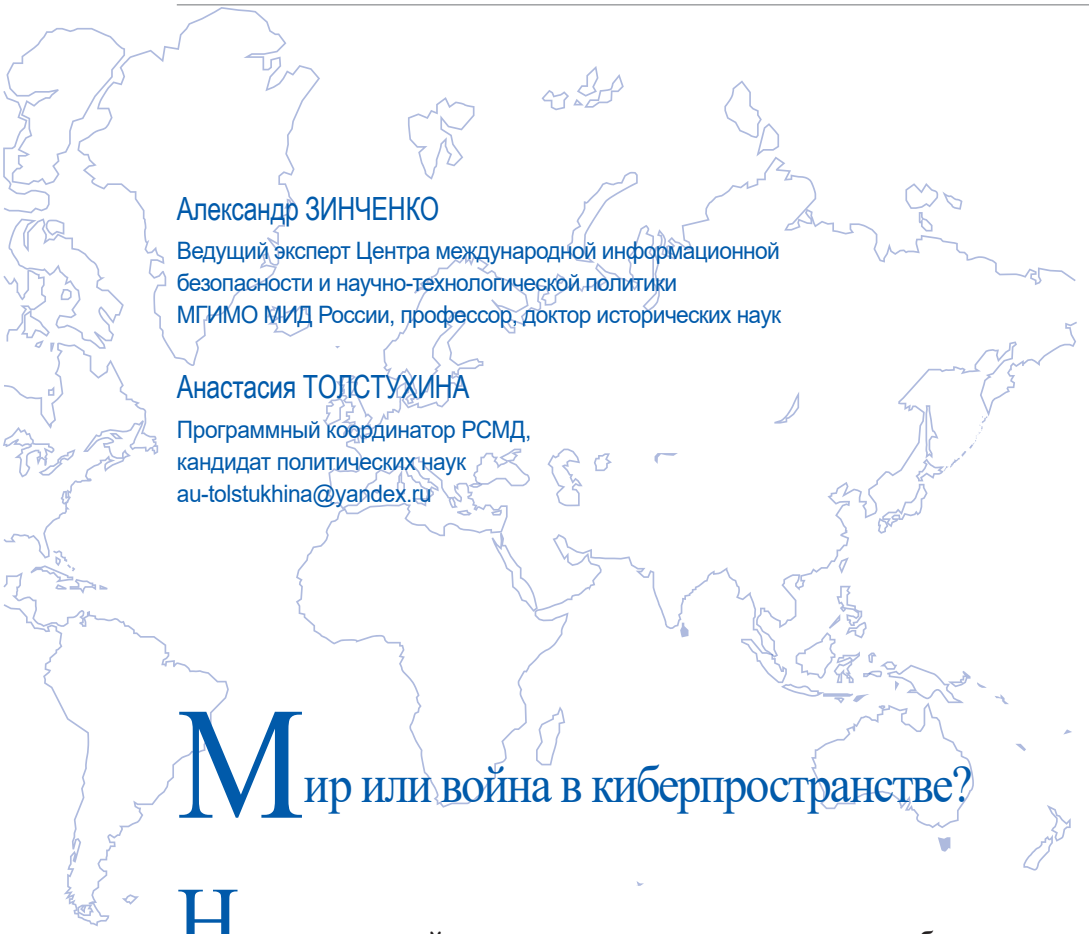

Александр ЗИНЧЕНКО
Ведущий эксперт Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России, профессор, доктор исторических наук

Анастасия ТОЛСТУХИНА
Программный координатор РСМД, кандидат политических наук
au-tolstukhina@yandex.ru

Мир или война в киберпространстве?

На сегодняшний день человечество столкнулось с беспрецедентным масштабом развития информационно-коммуникационных технологий (ИКТ). Однако нынешнего уровня защищенности в цифровой сфере для стабильного и поступательного мирового развития явно недостаточно. Проблемы, связанные с обеспечением информационной безопасности, тормозят инвестиции в высокотехнологичные секторы. Научно-технический прогресс - искусственный интеллект, «облачные» технологии, «большие данные», «Интернет вещей», электронная медицина и финансы - становится заложником отсутствия международно признанных стандартов поведения в информпространстве.

Вызывает опасение возросшая в связи с этим степень уязвимости всех без исключения стран перед лицом киберугроз. К сожалению, вместо объединения усилий всего мирового сообщества по укреплению глобальной информационной безопасности отдельные государства являются проводниками деструктивной политики на данном направлении.

США, безусловно, относятся к числу стран-лидеров в сфере ИКТ. Однако в последние годы все чаще наблюдается открытое намерение Вашингтона развивать и использовать информационные технологии в военных целях, активно милитаризировать информационное пространство, развязывая тем самым гонку кибервооружений. Подтверждением тому служит множество фактов.

В 2011 году США разработали и применили в отношении Ирана вирус «Stuxnet». Эта атака стала своего рода «киберхиросимой» и тревожным сигналом для всего мирового сообщества, поскольку данные агрессивные действия могли бы привести к непоправимым последствиям не только для Ирана, но и для всего региона в целом. Таким образом, именно США фактически впервые в новейшей истории применили кибероружие против государства и тем самым отбросили реализацию его мирной атомной программы на несколько лет.

В 2009 году под руководством Пентагона было создано Кибернетическое командование (USCYBERCOM), которое полноценно заработало уже в следующем году[1]. В новой военно-управленческой структуре объединились как оборонительные, так и наступательные полномочия, которые осуществляются на основе полученной информации от главного разведывательного органа - Агентства национальной безопасности (АНБ).

В августе 2017 года указом Президента США Киберкомандование было выделено в самостоятельную структуру и поднято до статуса объединенного боевого командования. Таким образом, новая «командная единица» встала на одну прямую с девятью другими боевыми подразделениями США[2]. В настоящее время Киберкомандование проводит активную работу по найму нескольких сотен квалифицированных кибероператоров, способных участвовать в защитных и наступательных операциях. Планируется, что в кадровый состав данной структуры в конечном итоге будет включено около 6200 сотрудников и 133 подразделения. По сообщениям некоторых СМИ, эти подразделения заработают на полную мощь к концу 2018 года[3].

Генерал-лейтенант Пол Накасоне, глава АНБ и Киберкомандования, считает, что Вашингтону требуется более агрессивный подход к противникам в киберпространстве[4]. В связи с этим в марте 2018 года была разработана новая «Дорожная карта» Киберкомандования США под названием «Достижение и поддержание превосходства в киберпространстве». Согласно новой стратегии, американские военные должны практически ежедневно совершать рейды по зарубежным сетям и вы-

водить из строя подозрительные серверы до того момента, как они попытаются запустить вредоносные программы[5]. Для того чтобы работа Киберкомандования была более продуктивной, Пентагон в настоящее время разрабатывает передовую систему кибероружия «Объединенная платформа» (United Platform). Подробности о том, что́ она станет собой представлять, не разглашаются, однако известно, что на ее основе будут осуществляться как защита государственных структур США от хакерских атак, так и наступательные онлайн-операции[6].

Согласно замыслу разработчиков, новая киберстратегия сможет навязывать дополнительные стратегические затраты противникам, заставляя их увеличивать ресурсы на оборону и уменьшать количество кибератак[7]. При этом предполагается, что Киберкомандование будет действовать «на грани войны», то есть таким образом, чтобы его шаги нельзя было квалифицировать как акт военной агрессии по отношению к другому государству. Стоит отметить, что данные инициативы Киберкомандования нашли отражение в доктринальном документе высшего военно-политического руководства США - Стратегии национальной обороны 2018 года (NDS, National Defense Strategy)[8].

Как сообщает газета «The New York Times», некоторые нынешние и бывшие американские чиновники предупреждают, что действия США в зарубежных сетях могут привести к ответным ударам по американским банкам, финансовым рынкам или сетям связи[9]. Кроме того, сами авторы новой киберстратегии не исключают определенных дипломатических рисков, ведь главными противниками Соединенных Штатов, согласно «новому видению» Киберкомандования, являются вовсе не криминальные субъекты, такие как террористы, преступники и хакеры, а государства - Китай, Россия, Иран и т. д.[10].

Параллельно с реформированием американских киберструктур в настоящее время в Вашингтоне ведется работа и на законодательном уровне. В рамках форума по кибербезопасности, проведенного Министерством внутренней безопасности (МВБ) США 31 июля 2018 года, вице-президент США М.Пенс призвал сенаторов поддержать законопроект о создании специализированного агентства при МВБ[11]. На ассигнование новой структуры, которая должна выступить централизованным хабом и объединить ресурсы американского национального правительства, М.Пенс запросил у Конгресса «рекордные» 15 млрд. долларов[12].

Борьба США за монополию в киберпространстве с каждым годом становится все более ожесточенной. Она становится особенно опасной, когда в рамках инициатив Президента США Д.Трампа традици-

онная система контроля Белого дома над американской наступательной и оборонительной кибератвностью ликвидируется, а новая только формируется.

Так, по сведениям «The Wall Street Journal», Д.Трамп 16 августа 2018 года росчерком пера «переиграл» президентскую политическую директиву 20 (Presidential Policy Directive 20), регламентирующую порядок применения кибероружия в отношении противников Вашингтона. Этот секретный документ был подписан Б.Обамой еще в 2012 году[13]. По данным американского издания, пересмотр директивы обусловлен стремлением Вашингтона снять ограничения на применение кибероружия против иностранных государств в наступательных целях, так как у американской стороны есть опасения, что якобы некие хакеры планируют атаки на избирательную систему во время промежуточных выборов в Конгресс в ноябре этого года[14].

Как видим, США в настоящее время меняют оборонительную и сдерживающую киберстратегию, которая существовала при администрации Б.Обамы, на агрессивные наступательные действия в сфере ИКТ, вплоть до проведения превентивных кибератак, нацеленных на информационные структуры суверенных государств.

Помимо подготовки специальных структур к проведению кибероперациий, Соединенные Штаты уже с 1947 года ведут глобальный шпионаж в рамках радиоэлектронного проекта «ЭШЕЛОН» (ECHELON). Современные ИКТ-технологии позволили Вашингтону значительно расширить возможности разведслужб. Ярким тому подтверждением является государственная программа «ПРИЗМА» (PRISM, Program for Robotics, Intelligents Sensing and Mechatronics), которая действует с 2007 года и представляет собой комплекс мероприятий массового негласного сбора цифровой информации без санкций судебных органов. Документальные факты, представленные экс-сотрудником ЦРУ Э.Сноуденом в 2013 году, показали, что с помощью программы «ПРИЗМА» американские спецслужбы имеют доступ к центральным серверам девяти ведущих интернет-компаний - «Microsoft», «Yahoo», «Google», «Facebook», «Paltalk», «YouTube», «AOL», «Skype» и «Apple».

Таким образом, разведчики собирают глобальную базу данных, в которую входят аудио- и видеофайлы, фотографии, электронные письма и документы, личные данные пользователей социальных сетей[15]. Более того, Э.Сноуден поведал миру, что с помощью программы «ПРИЗМА» АНБ прослушивало телефонные переговоры 35 глав различных государств и иностранных дипломатов. Эксперты утверждают, что спецслужбы США

в рамках сотрудничества с британской штаб-квартирой правительственной связи (ШКПС) незаконно взламывали практически все применяемые в Сети интернет-стандарты криптографии, используя для этого суперкомпьютеры и услуги высокопрофессиональных хакеров[16].

Таким образом, деятельность Вашингтона по наращиванию кибероружия и глобальный кибершпионаж ставят под угрозу безопасность во всем мире. В подобных условиях любое государство без особых доказательств может быть обвинено в хакерских атаках и подвержено агрессии со стороны США и их союзников, в том числе и военной (недаром в Стратегии действий Министерства обороны США в киберпространстве (The DOD Cyber Strategy) за 2015 г. подчеркивается возможность военного возмездия на кибератаки[17]). В частности, в последнее время со стороны западных политиков во главе с Вашингтном в адрес России сыпятся обвинения во всех «кибергрехах». По сложившейся практике, никаких подтверждений вредоносной активности России в информационном пространстве не предоставляется. Муссированием темы «мифических» российских хакеров и фейковыми новостями вытесняется тот факт, что Россия сама становится жертвой масштабных кибернападений: в 2017 году на российские объекты государственной критической инфраструктуры было совершено более 70 млн. атак.

Почти 20 лет назад Россия стала первой страной, поднявшей в ООН вопрос о вызовах и угрозах, зарождающихся в информационном пространстве. Она выступила с прорывной на тот момент политической инициативой по обеспечению международной информационной безопасности (МИБ) - проектом резолюции ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», который с 1998 года ежегодно включается в повестку дня Генассамблеи. В прошлом году для обеспечения непрерывности дискуссии по МИБ в ООН Россия совместно с более чем 60 соавторами предложила Генассамблее принять процедурное решение о сохранении данной тематики в повестке дня ее 73-й сессии. Это решение было одобрено консенсусом.

Помимо указанной резолюции, российская сторона выступила инициатором ооновского переговорного процесса по мирному обустройству международной информационной сферы. Таким переговорным механизмом стала на долгие годы Группа правительственных экспертов (ГПЭ) по МИБ. Этой группе удалось согласовать несколько важнейших положений, затрагивающих следующие значимые аспекты: источники угроз в киберпространстве, необходимость борьбы с кибер-

преступностью и кибертерроризмом, применимость международного права к сфере использования ИКТ и многие другие. Группа консенсусом приняла три подробных доклада, которые в качестве рекомендаций вынесли на рассмотрение международного сообщества нормы ответственного поведения государств в информационном пространстве. Кроме того, в 2015 году в ООН в качестве официального документа Организации была распространена инициатива государств - членов ШОС «Правила поведения в области обеспечения МИБ», ключевой особенностью которой является ее миротворческий характер и нацеленность на предупреждение конфликтов в информационном пространстве.

В основе российской позиции лежит необходимость предотвращения войн и конфликтов в информационном пространстве, которые могут быть развязаны для достижения военных и политических целей. В этой связи категорически неприемлемыми являются любые концепции, допускающие возможность применения в нем силы.

Россия выступает за равноправный, справедливый миропорядок в цифровой сфере, при котором были бы защищены интересы всех стран вне зависимости от уровня их технологического развития. Принципиально важно обеспечить соблюдение принципов государственного суверенитета, неприменения силы, невмешательства во внутренние дела других государств, основных прав и свобод человека, а также равные права для всех государств на участие в управлении сетью Интернет.

Для обеспечения мирного информационного пространства необходимо, чтобы была решена ключевая задача - создание универсальных, согласованных всеми государствами правил ответственного поведения в информационном пространстве. Как основоположник ооновской дискуссии по МИБ, Россия призывает все страны сделать решительный шаг в направлении их выработки и принятия. В этом году российские дипломаты намерены обратиться к Генассамблее ООН с предложением одобрить первоначальный перечень правил ответственного поведения государств в информационном пространстве и в ходе ее 73-й сессии внести соответствующий проект резолюции в Первый комитет ГА ООН. В данном документе обобщены все ранее наработанные рекомендации ГПЭ в 2010, 2013 и 2015 годах. Проект резолюции содержит 25 правил поведения государств, среди которых следующие принципиально важные положения:

- использовать ИКТ исключительно в мирных целях;

- нацелить международные усилия на предотвращение конфликтов в этой сфере;

- соблюдать в ней принципы Устава ООН, включая суверенное равенство государств, неприменение силы или угрозы силой, невмешательство во внутренние дела государств;

- избегать голословных обвинений в злонамеренном использовании, подкреплять любые обвинения доказательствами;

- не использовать ИКТ для вмешательства во внутренние дела других государств;

- не использовать посредников для кибератак;

- предотвращать распространение вредоносных ИКТ-инструментов и скрытых вредоносных функций («закладок»).

Предполагается, что эти 25 правил составят первоначальный список, который впоследствии будет дорабатываться, корректироваться и расширяться.

Серьезной угрозой для международного сообщества является также беспрецедентный рост преступлений, совершаемых с использованием ИКТ. О лавинообразном уровне киберпреступности свидетельствуют данные, представленные Генеральным секретарем ООН А.Гутеррешем: ежегодный ущерб от деятельности преступников в информационном пространстве достигает 1,5 трлн. долларов.

Существующие региональные международно-правовые механизмы, такие как Конвенция Совета Европы о киберпреступности 2001 года (так называемая Будапештская конвенция), не могут справиться с этими вызовами. Более того, данный документ буквально навязывается западниками мировому сообществу, в том числе России, как единственно возможный формат международного правового регулирования в сфере противодействия информационной преступности.

Позиция Москвы в отношении Будапештской конвенции остается неизменной. Она неоднократно обращала внимание на неприемлемое для нее положение, содержащееся в статье 32b, в соответствии с которым государствам под предлогом расследований фактически разрешено проникать в содержимое любого компьютера, не только не запрашивая на то разрешение, но даже без какого-либо уведомления соответствующих заинтересованных государств.

По мнению российской стороны, назрела необходимость разработки нового универсального инструмента в области борьбы с использованием ИКТ в противоправных целях. Более того, данный тезис закреплен в итоговой декларации стран - членов БРИКС в конце июля 2018 года. В связи с этим Россия намерена запустить в этом году полномасштабное обсуждение этого вопроса в Третьем комитете ГА ООН посредством внесения

в него проекта резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

Кроме того, именно Россия представила в качестве вклада в работу ООН на этом направлении проект универсальной конвенции о сотрудничестве в сфере противодействия информационной преступности, который 28 декабря 2017 года стал официальным документом Генассамблеи ООН и был призван стать «пищей к размышлению».

Очевидно, что в информационной сфере абсолютно все государства находятся «в одной лодке» и в большей или меньшей степени уязвимы в отношении угроз, исходящих от противоправного применения ИКТ. Притом, сами Соединенные Штаты с их многочисленными структурами, отвечающими за кибербезопасность, здесь не исключение. В условиях, когда в мире активно орудуют кибербанды, просто необходимо общими усилиями всего мирового сообщества бороться с реальными угрозами и преступниками, а не с фейками.

Альтернатива кибергонке существует - это тот самый «мирный план», который предлагает Россия и страны, выступающие за укрепление мира и безопасности в информационном пространстве. Результаты по итогам поддержки в ООН ключевых российских инициатив в области МИБ прольют свет на тех, кто действительно выступает за укрепление мира в информационной среде, и тех, кто за «ширмой» манипуляций и фейков скрывает намерение развязать кибервойну. Ответственность за кибермир лежит на каждом суверенном члене международного сообщества.

---

[1]Киберготовность США 2.0 // URL: http://www.potomacinstitute.org/images/CRI/CRI2_0USA_Russian.pdf

[2]https://www.reuters.com/article/us-usa-defense-cyber/pentagons-cyber-command-gets-upgraded-status-new-leader-idUSKBN1I52MS

[3]Пентагон запустит новейшую систему кибероружия // URL: https://rg.ru/2018/07/03/pentagon-zapustit-novejshuiu-sistemu-kiberoruzhiia.html

[4]Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict // URL: https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news

[5]Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command // URL: https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf

[6]Pentagon is developing a 'cyber carrier' to launch online attacks against Islamic State and protect the US from hostile government hackers // URL: http://www.dailymail.co.uk/sciencetech/article-5912561/Pentagon-begins-work-cyber-aircraft-carrier.html

[7]Achieve and Maintain Cyberspace…

[8]2018 National Defense Strategy // URL:https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

[9]Pentagon Puts Cyberwarriors…

[10]Achieve and Maintain Cyberspace…

[11]DHS Hosts Successful First-Ever National Cybersecurity Summit // URL: https://www.dhs.gov/news/2018/08/01/dhs-hosts-successful-first-ever-national-cybersecurity-summit

[12]Белый дом запросил «рекордные» $15 млрд на обеспечение кибербезопасности // URL: https://www.kp.ru/online/news/3191033/

[13]Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive // URL: https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721

[14]Ibit.

[15]The Guardian от 24 октября 2013 // http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data 20.06.2017

[16]См. подробнее: *Смирнов А.И.* Современные информационные технологии в международных отношениях: монография. М.: МГИМО-Университет, 2017.

[17]The DOD Cyber Strategy // URL: https://docviewer.yandex.ru/view/348335116/?*=6a%2Fjbq4gIUMTNeDs4myi71KmCqt7InVybCI6Imh0dHBzOi8vd3d3LmRlZmVuc2UuZ292L1BvcnRhbHMvMS9mZWF0dXJlcy8yMDE1LzA0MTVfY3liZXItc3RyYXRlZ3kvRmluYWxfMjAxNV9Eb0RfQ1lCRVJfU1RSQVRFR1lfZm9yX3dlYi5wZGYiLCJ0aXRsZSI6IkZpbmFsXzIwMTVfRG9EX0NZQkVSX1NUUkFURUdZX2Zvcl93ZWIucGRmIiwidWlkIjoiMzQ4MzM1MTE2IiwieXUiOiIyMzY1MDE1NTgxNDY3Mjc0NzM3Iiwibm9pZnJhbWUiOnRydWUsInRzIjoxNTM0NzUwNDQ4MTIyLCJzZXJwUGFyYW1zIjoibGFuZz1lbiZuYW1lPUZpbmFsXzIwMTVfRG9EX0NZQkVSX1NUUkFURUdZX2Zvcl93ZWIucGRmJnRtPTE1MzQ3NTA0MjcmdGxkPXJ1JnRleHQ9UGVudGFnb24lMjBjeWJlciUyMHN0cmF0ZWd5JTIwMjAxNSZ1cmw9aHR0cHMlM0ElMkYlMkZ3d3cuZGVmZW5zZS5nb3YlMkZQb3J0YWxzJTJGMSUyRmZlYXR1cmVzJTJGMjAxNSUyRjA0MTVfY3liZXItc3RyYXRlZ3klMkZGaW5hbF8yMDE1X0RvRF9DWUJFUl9TVFJBVEVHWV9mb3Jfd2ViLnBkZiZscj0yMTMmbWltZT1wZGYmbDEwbj1ydSZzaWduPTg4ZTQ5Njg2NzBjNjYyOTM5MmY5MzY2ZGQyMDI0OTlkJmtleW5vPTAifQ%3D%3D&page=1&lang=en

Ключевые слова: ИКТ, Киберкомандование США, кибероружие, ГПЭ по МИБ.