СТРАТЕГИЧЕСКИЕ РИСКИ И ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Ромашкина Н.П.[1], Стефанович Д.В.[2]

Аннотация.

Цель статьи: *на основе анализа и систематизации по различным параметрам исходящих из киберсферы рисков и угроз международной безопасности и глобальной стабильности выявить актуальные на текущем этапе проблемы стратегической стабильности, связанные с деструктивным влиянием информационно-коммуникационных технологий (ИКТ), разработать сценарии реализации киберугроз, ведущих к снижению уровня стратегической стабильности для выработки соответствующих предложений, которые могут заложить основу политики сдерживания в сфере ИКТ.*

Метод исследования: *анализ, синтез и научное прогнозирование, экспертная оценка, компаративный анализ киберсферы в рамках системного подхода.*

Полученный результат: *в статье представлены анализ и систематизация по различным параметрам исходящих из киберсферы рисков и угроз международной безопасности и глобальной стабильности. Доказывается влияние ускоренного развития информационно-коммуникационных технологий (ИКТ) на уровень стратегической стабильности, при обеспечении которой особого внимания требует кибербезопасность ракетно-ядерных вооружений. Поставлены глобальные проблемы стратегической стабильности на текущем этапе и обоснованы выводы о том, что защита стратегических вооружений, систем предупреждения о ракетном нападении, противовоздушной и противоракетной обороны, связи, командования и контроля над ядерными вооружениями от вредоносных ИКТ являются актуальными глобальными проблемами современности. Предложены конкретные сценарии реализации киберугроз, ведущих к снижению уровня стратегической стабильности ниже необходимого и достаточного, а также сформулированы предложения по минимизации соответствующих угроз эскалации. Предлагаются меры, которые могут заложить основу для создания политики сдерживания в ИКТ-среде так, как это было сделано в период биполярности в отношении ядерных вооружений, стать фундаментом для более широких международных соглашений о контроле над вооружениями в так называемом информационно-ядерном пространстве в будущем.*

Ключевые слова: *информационно-коммуникационные технологии (ИКТ), информационное пространство, кибероружие, информационная угроза, киберугроза, кибератака, стратегическая стабильность, системы боевого управления, ядерное оружие, критически важные объекты государственной инфраструктуры.*

DOI:10.21681/2311-3456-2020-05-77-86

Введение

Ускоренное развитие информационно-коммуникационных технологий (ИКТ) в настоящее время является, пожалуй, самой характерной особенностью современного мира, предоставляя исключительные возможности и неся новые опасности во всех областях жизни. В настоящее время в рамках международных и внутринациональных дебатов в разных странах обсуждается широкий спектр вопросов, связанных с киберугрозами миру, международной безопасности и стабильности. Это и деятельность ООН по обеспечению международной информационной безопасности; и меры доверия, формальные обязательные соглашения по киберпространству; и технические, этические, а также юридические вопросы использования искусственного интеллекта в военной сфере; и инициативы по контролю над кибервооружениями; и предложения по запрету кибератак на критически важную государственную инфраструктуру, особенно на мирные и военные ядерные объекты, и так далее.

В то время как еще совсем недавно связь между кибер и ядерными проблемами в военной сфере, так же, как и возрастающая угроза влияния новейших ИКТ на уровень стратегической стабильности почти полностью отрицались, сегодня эта проблематика уже осознана научным и экспертным сообществом. Во многом это связано с лавинообразным ростом конкретных фактов применения вредоносных ИКТ в военных конфликтах, разжигании межнациональной розни и в целях смены руководства страны; с увеличением количества кибератак на критически важную государственную инфраструктуру и искусственные спутники Земли; с уже не гипотетической, а реальной возможностью примене-

1 Ромашкина Наталия Петровна, кандидат политических наук, руководитель Группы проблем информационной безопасности Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН, Москва, Россия. E-mail: Romachkinan@yandex.ru

2 Стефанович Дмитрий Викторович, научный сотрудник Центра международной безопасности Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН, Москва, Россия. E-mail: stefanovich@imemo.ru, ORCID 0000-0002-8694-8040

ния военной силы даже не в ответ, а в целях предотвращения кибератаки; с соответствующими изменениями, которые вносятся в доктринальные документы все большего количества стран. Таким образом, в контексте проблемы обеспечения международной безопасности и стабильности, важнейшими с точки зрения необходимости предотвращения являются исходящие из цифрового пространства риски и угрозы, которые носят стратегический, глобальный характер [1].

Анализ доказывает, что все факторы, дестабилизирующие систему международной безопасности, связаны сегодня с развитием ИКТ. Так, в современных конфликтах с нарастающей скоростью применяются новые разрушительные ИКТ-инструменты [2, 3]. А практика международных отношений в целом уже в полной мере включает использование новых цифровых технологий для достижения политических и военных целей [4, 5]. В качестве наиболее ярких примеров можно вспомнить использование компьютерных вредоносных программ Stuxnet, Duqu, Wiper, Flame и др. для комплексных массированных кибератак на критически важные объекты государственной инфраструктуры, в частности, предприятия мирной ядерной энергетики Ирана (АЭС в г. Бушер и завод по обогащению урана в г. Натанз), а также на объекты нефтеперерабатывающей промышленности ряда стран [6, 7]. Кроме того, постоянно развиваются и совершенствуются технологии вмешательства во внутренние дела государства («цветные» революции, демонстрации, протесты и т.д.) [8]. Поэтому ускоренное развитие деструктивного ИКТ и связанных с ним угроз информационной безопасности (киберугроз) целесообразно выделять в качестве отдельного глобального дестабилизирующего фактора. При этом каждый из других ранее существовавших дестабилизирующих факторов в настоящий период усугубляется и обостряется использованием ИКТ в деструктивных военно-политических целях, милитаризацией мирных информационных технологий, а также легкостью, внезапностью и быстродействием как информационно-технологического [9, 10], так и информационно-психологического оружия [11]. Обязательные глобальные механизмы управления в этой сфере пока отсутствуют, что, в частности, сказывается на снижении уровня стратегической стабильности[3] по сравнению с периодом биполярности [12, 13].

Кибербезопасность и стратегическая стабильность: глобальные проблемы современного этапа

Проблема 1. Рост вероятности выведения из строя или уничтожения ядерного оружия (ЯО) посредством кибервоздействия [14]. Этот процесс уже сегодня оказывает влияние на будущее процессов ядерного разоружения и нераспространения. С одной стороны, развитие таких новых возможностей может стать для государств – обладателей ЯО поводом для ускоренного сокращения таких вооружений. А с другой стороны, что более вероятно, может послужить серьезной причиной для масштабной модернизации ЯО, создания более сложных и защищенных систем, что приведет к качественной и/или количественной гонке ядерных вооружений, и как следствие – снижению уровня стратегической стабильности. Кроме того, вопросы кибербезопасности уже влияют не только на будущие, но и на существующие ограничительные режимы.

Проблема 2 связана с самой серьезной, хотя пока и маловероятной, угрозой – влияние ложной информации, полученной от ИКТ, на рост вероятности ошибочного санкционированного запуска баллистических ракет (БР), а также на принятие решения о применении ЯО [15]. Задача защиты БР от ошибочных пусков возникла с момента создания первых ракет. И всякий раз решается заново при создании новых БР, постановке их на дежурство, при подготовке и проведении испытательных, учебно-боевых и контрольно-боевых пусков. Несмотря на то, что и США, и Россия (СССР) всегда уделяли этому большое внимание, за десятилетия существования ЯО в обеих странах были случаи технических сбоев и человеческих ошибок, которые могли бы спровоцировать ядерный запуск. Уменьшение вероятности ошибочного запуска, которая никогда не равна нулю, будет стоять более остро по мере перехода войск стратегического назначения в разных странах на цифровые технологии передачи информации. Так, по данным Минобороны России, наши Ракетные войска стратегического назначения (РВСН) должны полностью перейти на цифровые технологии в 2020 г.[4]

Эта проблема продиктована следующими возможностями ИКТ:

- получение ложной информации от систем предупреждения о ракетном нападении (СПРН) о запуске баллистических ракет с ЯО со стороны противника;
- вредоносное внедрение в управление коммуникационными системами в командных пунктах РВСН для создания ситуаций ошибочного санкционированного пуска или предотвращения использования наступательных средств, т.е. блокирования санкционированного пуска [16];
- непосредственное внедрение в электронные системы управления, связи, командования и контроля над ЯО (автоматизированные системы боевого управления (АСБУ) – в российской терминологии, Nuclear Command, Control, and Communications (NC3) – в западной терминологии).

Во время хакерских нападений могут быть повреждены или разрушены каналы коммуникаций, созданы помехи в системе управления вооруженными, в том числе, ядерными, силами, а также снижена уверенность военных, принимающих решения, в работоспособности и эффективности систем связи, командования и контроля (например, нападавшие могут использовать DDoS-атаки для нарушения систем коммуникации,

3 Стратегическая стабильность военно-политической системы – состояние мира (отсутствие широкомасштабной войны) в рамках этой системы, которое поддерживается даже при постоянно действующих возмущениях (дестабилизирующих факторах) в течение определенного (заданного) периода времени.

4 К 2020 году РВСН полностью перейдут на цифровые технологии передачи информации. Сайт Министерство обороны Российской Федерации (Минобороны России). // https://structure.mil.ru/structure/forces/strategic_rocket/news/more.htm?id=12142122%40egNews.

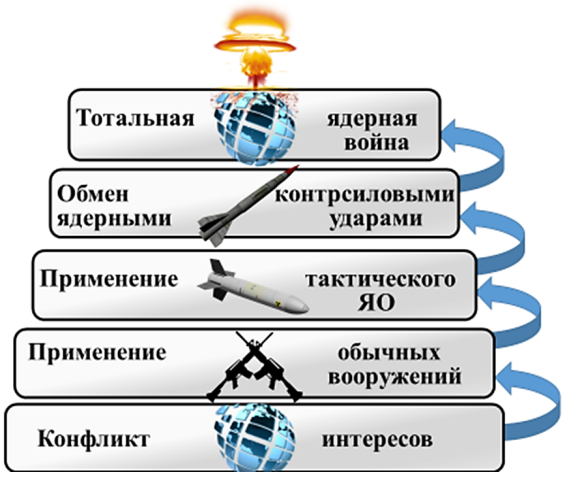

Рис. 1. Лестница эскалации ядерной войны

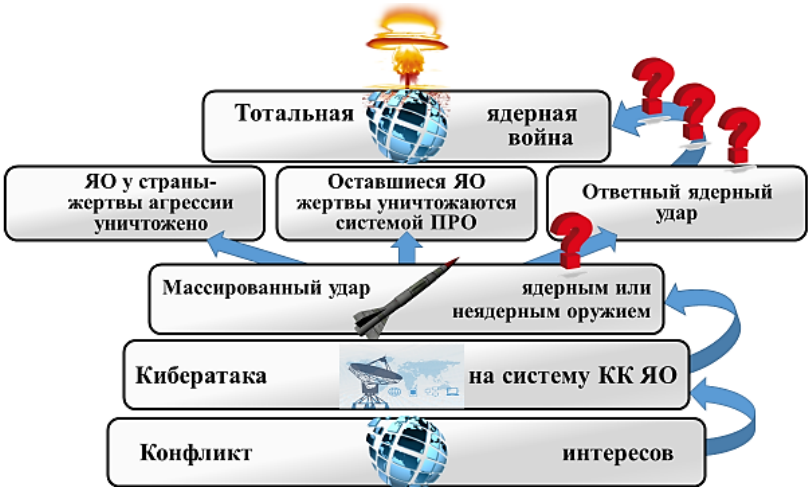

Рис. 2. Лестница эскалации конфликта с применением ИКТ

управления и целеполагания). В кризисной ситуации кибернападения могут негативно повлиять на принятие решения об ответных действиях. Угроза выведения из строя систем военного назначения под воздействием ИКТ-средств может сократить поиск альтернатив военным действиям и создать значительные проблемы для успешного доведения информационных сообщений и команд. Таким образом «лестница эскалации конфликтов» сократится, что, в свою очередь, может вызвать соблазн победить в войне без получения ответного удара, что разрушает концепцию ядерного сдерживания (рисунки 1, 2).

Кроме того, эта проблема связана с возможностями использования так называемого «ложного флага» при кибервмешательстве, когда операции проводятся таким образом, чтобы создавалось впечатление, что они были выполнены другим субъектом. Не исключена также вероятность восприятия каких-то действий в качестве начального этапа перехода к условиям гарантированного взаимного уничтожения. Все это повышает вероятность ошибочного запуска БР, а, следовательно, снижает уровень стратегической стабильности.

Эти угрозы дополнительно усиливаются в связи с развитием ударных роботизированных средств с дистанционным управлением [17], искусственного интеллекта в военных целях, машинного обучения, возможностями автономной работы различных систем и подсистем, автоматизированных систем принятия решений и т.д. [18, 19], которые могут подвергаться ИКТ-атакам, средств кибер-электромагнитной деятельности, активно развивающейся в США и включающей в себя кибероперации, электронную, войну, электронные атаки в мирное время, операции по управлению электромагнитным спектром, подавление целей активными и пассивными помехами, а также электромагнитную дезинформацию.[5]

Одна из современных возможностей снижения ИКТ-угроз в военной сфере – разработка квантовых крипто-

5 Cyber Electromagnetic Activities. Field Manual No. 3-38, Headquarters Department of the Army, Washington, DC, February 12, 2014. // https://info.publicintelligence.net/USArmy-CEMA.pdf.

DOI:10.21681/2311-3456-2020-05-77-86

графических систем для защиты информации, в том числе, оборонного характера [20]. По данным министерства обороны РФ, у России тоже есть потенциал для производства таких систем, в том числе, и военного назначения.[6] Отметим, что квантовая криптография — метод защиты коммуникаций, основанный на принципах квантовой физики в отличие от традиционной криптографии на основе математических методов. Процесс отправки и приёма информации в квантовой криптографии выполняется физическими средствами, например, при помощи электронов в электрическом токе или фотонов в линиях волоконно-оптической связи. Таким образом, обеспечивается постоянная и автоматическая смена ключей при передаче каждого сообщения в режиме одноразового «шифроблокнота». Технология опирается на принципиальную неопределённость поведения квантовой системы – невозможно измерить один параметр фотона, не исказив другой. Поэтому можно создать такую систему связи, которая всегда будет обнаруживать вмешательство: попытка измерения параметров в квантовой системе вносит в неё нарушения, разрушая или искажая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать, что действует перехватчик. На сегодняшний день это единственный вид шифрования со строго доказанной криптографической стойкостью.

Проблема 3. Использование ЯО для предотвращения и в ответ на кибернападения на военные и другие критически важные объекты государственные инфраструктуры. Пока эта угроза является чисто теоретической. Но с учетом ускоренного роста вызовов, исходящих из ИКТ-пространства, необходимо отдавать себе отчет в том, что ядерная и информационная сферы, видимо, будут еще более взаимосвязаны в будущем, и этот вопрос может встать более остро. Эти опасности возрастают с учетом Углубленной политики киберзащиты НАТО от 2014 г., в рамках которой признается применимость к киберпространству статьи 5 Североатлантического договора. Однако из-за сложности атрибуции кибератаки под удар могут попасть непричастные к ней государства. При этом признание киберпространства сферой оперативной ответственности НАТО подразумевает формирование соответствующих командных структур, привлечение необходимых сил и средств. Кроме того, важнейшей информацией к размышлению является факт первого в истории применения реальной военной силы даже не факту кибератаки, а только с целью ее предотвращения, когда в мае 2019 г. воздушные силы Израиля осуществили удар по зданию на территории Сектора Газа, откуда осуществлялась деятельность хакеров, готовящих кибератаки. По заявлению представителей израильских вооруженных сил, кибернападение было направлено на урон качеству жизни граждан Израиля.[7] Таким образом, то, что еще совсем недавно рассматривалось в качестве абсолютно гипотетической возможности, сегодня стало прецедентом. Проблема создания системы сдерживания в этих условиях становится максимально актуальной.

Таким образом, можно выделить основные факторы влияния ИКТ на стратегическую стабильность:

- использование ИКТ в деструктивных военно-политических целях;
- соблазн одержать победу в широкомасштабной войне, связанный с развитием новых кибертехнологий, подталкивающих к приобретению стратегических преимуществ;
- тенденция к исчезновению границ между мирным состоянием государств и переходом их в состояние войны, размытие рамок между обороной и нападением в военном планировании;
- изменение логики глобального противоборства, когда комплексное применение невоенных методов с использованием вредоносных ИКТ приводит к достижению целей войны даже без вооруженной борьбы;
- сокращение «лестницы» эскалации конфликта, связанное с ростом вероятности ИКТ-атак на элементы военной ракетно-ядерной инфраструктуры.

Возможные сценарии реализации киберугроз в сфере стратегической стабильности

В рамках сценариев реализации киберугроз в сфере стратегической стабильности под угрозами в сфере информационно-коммуникационных технологий (ИКТ-угрозами, киберугрозами) предлагается понимать потенциальную возможность вмешательства в нормальное функционирование различных подсистем управления ядерным оружием и его носителями с использованием кибернетических и иных информационных технологий, то есть так называемое «кибервоздействие». Отметим, что принципиально кибервоздействие незначительно отличается от воздействия с использованием средств радиоэлектронной борьбы (РЭБ) – по сути, воздействие тем или иным образом ведет к тому, что называется «отказом» в системах массового обслуживания [21]. Варианты такого воздействия в обобщенном виде представлены на рисунке 3 [22]. Можно выделить несколько базовых видов воздействия, исходя из используемых инструментов, представленных на рисунке 4.

При этом следует напомнить несколько важных особенностей вредоносного ПО, применяемого, в том числе, в военных операциях (кибероружия). Одной из них является невозможность достоверно определить цель противника, даже при обнаружении вредоносного ПО. Идентичные образцы могут использоваться и для деструктивного кибервоздействия, и для разведывательных мероприятий. Данная ситуация связана с другой особенностью кибероружия, роднящей его с оружием ядерным: разделение условных «носителя» и «полезной нагрузки». В связи с этим, особенно в условиях эскалации конфликта, принятие решений сторонами резко осложняется: после успешного внедрения «безвредной» боевой части (БЧ) в сеть при дальнейшей эскалации напря-

6 Инфофорум-2018. Минобороны РФ обдумывают идею разработки квантовых криптомашин. Сайт «Национальный форум информационной безопасности «Инфофорум». // https://infoforum.ru/news/infoforum-2018-minoborony-rf-obdumyvaut-ideu-razrabotki-kvantovyh-kriptomashin.

7 Israel forhindret dataangrep ved å bombe bygg med hackere. digi.no, 6 мая 2019. // https://www.digi.no/artikler/israel-forhindret-dataangrep-ved-a-bombe-bygg-med-hackere/464464.

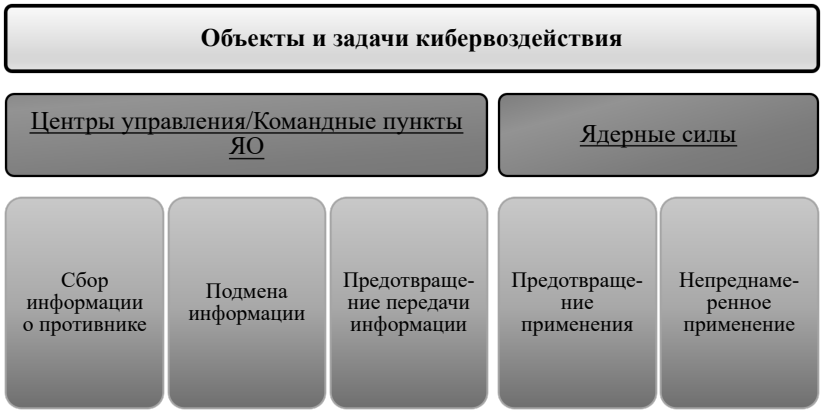

Рис.3. Кибервоздействие и ядерное оружие

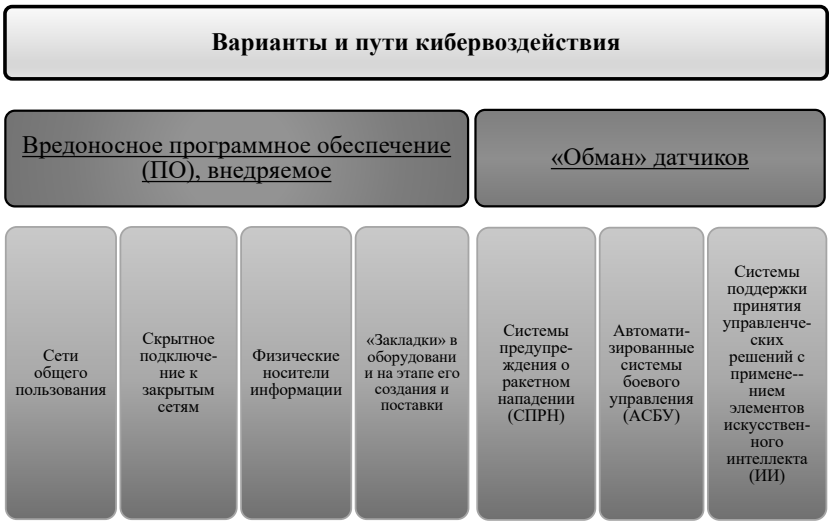

Рис.4. Варианты и пути кибервоздействия

женности напрашивается попытка замены «безвредной» БЧ на «деструктивную». При этом другая сторона может своевременно обнаружить атаку и в условиях отсутствия достоверной информации о планах противника принять решение об ответных действиях, в том числе, не ограничивая себя киберпространством. Естественно, в данной ситуации речь идет о сетях, напрямую связанных с ЯО, и, следовательно, с выживанием государства.

Таким образом, представляется целесообразной следующая классификация кибервоздействий с акцентом на цели враждебного воздействия:

- сбор информации о противнике;
- «подмена» информации, используемой противником;
- вывод оборудования противника из строя;
- предотвращение применения ядерных сил противника;
- непреднамеренное применение ядерных сил противника, прежде всего, против третьих стран.

Кроме того, можно определить основные категории субъектов, которые могут «работать» на стыке ядерного и кибернетического оружия:

- государства;
- организации, действующие под руководством и в интересах государственных органов (т.н. «прокси»), в т.ч. на территории третьих стран;
- частные структуры (в т.ч. террористические);
- хакеры-одиночки.

Государства в этой классификации являются наиболее мощным актором и наиболее вероятным объектом кибервоздействия. Остальные субъекты могут действовать как в роли подрядчиков государственных организаций, так и в собственных интересах.

Как упоминалось, наибольшие угрозы связаны с вредоносным кибервмешательством в АСБУ ядерных сил, а также в СПРН. АСБУ сил и средств ядерного сдерживания могут быть, в том числе, и физически разделены, однако принципиальное решение о применении ЯО принимается высшим руководством страны[8]. Кроме того, необходимо учитывать возможности средств

8 Указ Президента Российской Федерации от 2 июня 2020 г. № 355 «Об Основах государственной политики Российской Федерации в области ядерного сдерживания».

DOI:10.21681/2311-3456-2020-05-77-86

радиоэлектронной борьбы (РЭБ) (Electronic Warfare в терминологии США), как составной части информационного противоборства в технической сфере, в целях «обмана» СПРН и ПРО.

Опубликованные в июне 2020 года Основы государственной политики Российской Федерации в области ядерного сдерживания[9] включают в себя важное обновление условий перехода России к применению ЯО: угрозы самому ядерному оружию и его системам боевого управления. В пункте 19 «в» «Основ» прямо указывается: *«воздействие противника на критически важные государственные или военные объекты Российской Федерации, вывод из строя которых приведет к срыву ответных действий ядерных сил».* Фактически, это означает вмешательство любого рода в гражданскую или военную инфраструктуру, подрывающее потенциал ядерного возмездия. Весьма вероятно, что сюда также входит и кибервоздействие. Критические объекты, которые могут быть ему подвержены посредством ИКТ, включают в себя военные и гражданские командные пункты, АСБУ ядерных сил, инфраструктуру ядерных сил и СПРН (в том числе космического эшелона [23]). Соответственно, злонамеренное вмешательство в работу этих объектов может привести к катастрофическим последствиям.

Рассмотрим возможный сценарий внедрения страной А[10] некого вредоносного ПО в узлы АСБУ стратегических ядерных сил (СЯС) страны Б. Можно предполагать, что «гражданская» часть АСБУ будет более легкой целью. Задачи такого внедрения могут быть различными: сбор разведданных, нарушение связности АСБУ, деструктивные действия (отключение АСБУ, предотвращающее ядерное возмездие, или передача данных, которые могут привести к запуску). Вредоносное ПО обнаруживается кибервойсками Б, и руководство страны приказывает принять следующие меры: публичное заявление о повышении боеготовности своих ядерных сил; подготовка к кибернаступлению; требование разъяснений от А по вопросу инцидента с использованием «горячих линий» связи, либо публично. Маловероятно, что в качестве следующего шага А признает ответственность за операцию, но, возможно, предпримет некоторые меры по предоставлению гарантий отсутствия злонамеренных и деструктивных намерений и действий. При этом есть вероятность, что кибервоздействие было осуществлено каким-то другим актором. В этом случае худшим вариантом будет уверенность стороны А в том, что это изначально был план стороны Б, поскольку в Б повышена боеготовность ядерных сил и готовится (или была осуществлена) ответная кибероперация. Таким образом, возможные встречные действия страны А могут приблизить обе стороны к ядерному порогу. Наиболее критическая ситуация возникнет в случае принятия решения о нанесении удара первыми, так называемого, «удара отчаяния».

Также возможен и более «простой» сценарий, приближенный к реальности сегодняшнего дня[11]. Страна А наращивает интенсивность патрулирования своей дальней авиации в воздушном пространстве в непосредственной близости от территории страны Б, в том числе, с отработкой ударных действий. Если у страны Б, в отличии от страны А, недостаточное количество тяжелых бомбардировщиков и самолетов-заправщиков для симметричного ответа, но в наличии квалифицированные кибервойска, то Б может принять решение об операции смешанного характера: воздействуя на командные центры контроля воздушно-космического пространства страны А, а также публично доступные средства мониторинга воздушного движения[12] с помощью ИКТ-средств при одновременной отправке ограниченного количества своих тяжелых бомбардировщиков в сторону противника, вводит в заблуждение военно-политическое руководство противника в отношении своего реального потенциала. Страна А поднимает истребители на перехват, обнаруживает несколько настоящих бомбардировщиков, но датчики ее системы показывают значительно более массированную авиационную атаку. В кризисной ситуации это может быть воспринято как начало агрессии с применением стратегических вооружений, и, следовательно, привести к реальным боевым действиям, в т.ч. с использованием ЯО.

Таким образом, рост вероятности катастрофических последствий реализации киберугроз в области ЯО говорит о необходимости активизации действий по формированию и согласованию на международном уровне перечней критической инфраструктуры, связанной с военными, в том числе, с ядерными объектами, воздействие на которую с применением ИКТ будет расцениваться как попытка обезоруживающего либо обезглавливающего удара с соответствующими последствиями для атакующей стороны. В этом смысле появление соответствующих положений в российских и американских официальных документах[13] предоставляет некоторое пространство для возможного сотрудничества. Кроме того, чрезвычайно актуальной задачей является выработка общего понимания в отношении элементов системы АСБУ СЯС, любых типов кибернетического, электронного или кинетического воздействия, которые должны оставаться за рамками межгосударственного противоборства во избежание ядерной эскалации. Параллельно целесообразно вести работу по внедрению и поддержке строгих и эффективно работающих протоколов двусторонней связи в случае киберинцидентов (в первую очередь, развивая систему взаимодействия «Национальных центров по уменьшению ядерной угрозы»), включая процесс атрибуции. К сожалению, в настоящее время данная система связи между Россией

9 Указ Президента Российской Федерации от 2 июня 2020 г. № 355 «Об Основах государственной политики Российской Федерации в области ядерного сдерживания».

10 Либо другим государственным или негосударственным субъектом, который хочет, чтобы в Б посчитали, что А несет ответственность.

11 Главнокомандующий ВКС провел брифинг для военных атташе иностранных государств, 11.09.2020 // https://function.mil.ru/news_page/country/more.htm?id=12313777@egNews.

12 Например, FlightRadar24

13 Указ Президента Российской Федерации от 2 июня 2020 г. № 355 «Об Основах государственной политики Российской Федерации в области ядерного сдерживания»; Nuclear Posture Review, February 2018.

и США фактически не работает из-за проблемы отсутствия доверия к контрагенту.

Заключение

Наиболее серьезными киберугрозами международной безопасности и стабильности являются применение ИКТ-оружия в военно-политических целях для осуществления враждебных действий и актов агрессии; деструктивное кибервоздействие на объекты критически важной государственной инфраструктуры; вмешательство во внутренние дела суверенного государства, снижение общественной стабильности, разжигание межэтнической, межнациональной розни посредством ИКТ. Международное нормативно-правовое управление в этой области пока отсутствует. При этом ситуация, связанная с обеспечением необходимого и достаточного уровня стратегической стабильности сегодня может оцениваться как кризисная. В условиях существующих дестабилизирующих факторов, отсутствия переговоров по ограничению и сокращению ЯО, а также ускоренного развития разрушительных ИКТ существующих механизмов международного управления и контроля в этой области недостаточно. Следовательно, создание таких новых международных инструментов, направленных на создание международно-правового режима контроля над вредоносными ИКТ, является одной из важнейших проблем.

В контексте обеспечения стратегической стабильности особого внимания требует кибербезопасность ракетно-ядерных вооружений. Все ядерные державы модернизируют их, стремясь внедрять новые компьютерные технологии. Все больше компонентов военной ядерной инфраструктуры – от боеголовок и средств их доставки до систем управления и наведения, систем связи, командования и контроля стратегических ядерных сил – зависят от сложного программного обеспечения, что делает их потенциальными мишенями для кибератак. При этом в дополнение или вместо принципа сдерживания за счет неминуемого ответного удара, растет интерес к сдерживанию путем предотвращения использования наступательных средств (блокирование пуска, *left of launch*) с помощью ИКТ. Следовательно, защита стратегических вооружений, СПРН, систем противовоздушной и противоракетной обороны, управления, связи, командования и контроля над ядерными вооружениями от вредоносных ИКТ являются актуальными глобальными проблемами современности.

Снижение уровня стратегической стабильности обусловлено влиянием вредоносных ИКТ на рост вероятности ошибочного санкционированного запуска БР, получения ложной информации от СПРН о запуске баллистических ракет со стороны противника, повреждения или разрушения каналов коммуникаций, создания помех в системе управления, связи, командования и контроля вооруженными силами, а также снижения уверенности военных, принимающих решения, в работоспособности систем управления, связи, командования и контроля ВС и восприятия каких-то действий в качестве начального этапа перехода к условиям гарантированного взаимного уничтожения.

В этих условиях целесообразны международные действия с участием России в ответ на актуальные глобальные вызовы международной безопасности и стратегической стабильности:

- разработка и внедрение новых ИКТ России, совершенствование соответствующих специальных гражданских и военных структур для обеспечения глобального баланса сил и средств;
- возобновление переговоров РФ-США по ограничению и сокращению стратегических ракетно-ядерных вооружений; привлечение других ядерных держав к режиму ограничения и сокращения СЯС;
- включение вопросов обеспечения информационной безопасности в обсуждения и переговоры по ядерным вооружениям и стратегической стабильности на двусторонней (РФ-США) и многосторонней основе с участием России;
- разработка на международном военно-политическом уровне конкретных мер по укреплению доверия, в частности, обмен данными об информационных угрозах, практическое межгосударственное сотрудничество и др. на многосторонней основе, в первую очередь, между РФ и США с целью выхода на подписание документа о безопасности военной деятельности в информационном пространстве;
- активизация работы в государствах – обладателях ЯО по более эффективной подготовке персонала и защите программно-аппаратных средств военной инфраструктуры от различных ИКТ-нападений (в частности: унификация; территориальное распределение; дублирование обработки данных; создание «воздушной прослойки», т.е. отсутствие пересечения внутренних сетей критически важных объектов с глобальной информационной сетью; узкая специализация программного обеспечения и др.) для обеспечения как национальной, так и международной безопасности;
- для более эффективного решения последней задачи активизация усилий по созданию многонациональной исследовательской программы по ИКТ-стабильности военной сферы экспертами из стран-обладателей ЯО;
- расширение научных исследований в России по разработке теоретических и методологических подходов к понятию стратегической стабильности на современном этапе, международных критериев оценки и практических методов обеспечения ее необходимого и достаточного уровня в изменившейся системе международных военно-политических отношений с учетом новых дестабилизирующих факторов, среди которых, несомненно, уже находятся угрозы информационной безопасности;
- выработка и фиксация общего для РФ и США понимания критериев стратегической стабильности;
- выработка и фиксация общего для РФ и США понимания опасности ИКТ-угроз для международной безопасности и стабильности;

DOI:10.21681/2311-3456-2020-05-77-86

- выработка общих подходов к оценке вероятности непреднамеренных и преднамеренных ИКТ-атак на СЯС;
- четкая фиксация вероятного ответа в случае обнаружения ИКТ-атак на СЯС в целях обеспечения сдерживания в применении ИКТ-вооружений.

Эти меры могут заложить основу для создания политики сдерживания в ИКТ-среде так, как это было сделано в период биполярности в отношении ядерных вооружений, стать фундаментом для более широких двусторонних и многосторонних соглашений о контроле над вооружениями в так называемом информационно-ядерном пространстве в будущем. При этом работа по оценке ИКТ-угроз находится на одном из первых этапов, и логично полагать, что деятельность экспертного сообщества сегодня может быть исключительно полезной для структур, принимающих государственные решения.

Параллельно целесообразно работать над созданием режима контроля над ИКТ-вооружениями, который мог бы включать:

- запрет на ИКТ-атаки на конкретные объекты, в первую очередь, в военной сфере (заявления, обязательства, соглашения, договоры) [24];
- ограничение и/или отказ от наступательных ИКТ-возможностей;
- меры контроля за распространением ИКТ-вооружений;
- международные нормы в отношении средств и методов предотвращения и устранения киберконфликтов;
- разработку конвенции о запрещении вредоносного использования ИКТ в сфере ЯО.

Литература

1. Schwab K. The fourth industrial revolution: What It Means and How to Respond? //Foreign Affairs. December 12, 2015. // https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.
2. Information Security Threats during Crisis and Conflicts of the XXI Century / Eds.: N.P. Romashkina, A.V. Zagorskii. Moscow: IMEMO, 2016. 134 p. // https://www.imemo.ru/files/File/en/publ/2016/2016_001.pdf.
3. Nye J. S. Controlling Cyber Conflict // Project Syndicate. Aug. 8, 2017 // https://www.project-syndicate.org/commentary/new-norms-to-prevent-cyber-conflict-by-joseph-s--nye-2017-08/russian.
4. Проблемы информационной безопасности в международных военно-политических отношениях / Под ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН, 2016. 183 с. // https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf.
5. Гареев М.А., Турко Н.И. Война: современное толкование теории и реалии практики // Вестник Академии военных наук. 2017. № 1 (58). С.4-10.
6. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1(1). С.28-36.
7. Ромашкина Н.П. Вооружения без контроля: современные угрозы международной информационной безопасности // Пути к миру и безопасности. 2018. № 2(55). С. 64-83.
8. Ромашкина Н.П., Пересыпкина О.В. Информационно-психологическое воздействие в период кризиса на Украине: уроки для России // Информационные войны. 2016. № 1 (37). С. 42-54.
9. Марков А.С., Шеремет И.А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник академии военных наук. 2019. № 2 (67). С. 82-90.
10. Шеремет И.А. Угрозы техносфере России и противодействие им в современных условиях // Вестник академии военных наук. 2014. № 1. С. 27-34.
11. Кравцов Д.Н. Информационно-психологическое оружие как средство обеспечения защиты национальных интересов государства // Коммуникология. 2017. № 3. С. 78-89.
12. Барсенков А.С., Веселов В.А., Есин В.И., Шеремет И.А. Вопросы обеспечения стратегической стабильности в советско-американских и российско-американских отношениях: теоретические и прикладные аспекты // Сер. Политико-военные проблемы современных международных отношений. – М.: Изд-во МГУ им. М.В. Ломоносова, 2019. 144 С.
13. Ромашкина Н.П. Стратегическая стабильность в современной системе международных отношений. М.: Научная книга, 2008. 288 С.
14. Stoutland P., Pitts-Kiefer S., Nuclear Weapons in the New Cyber Age // Nuclear Threat Initiative, September 2018. 32 P. // https://media.nti.org/documents/Cyber_report_finalsmall.pdf.
15. Futter A. Cyber Threats and Nuclear Weapons New Questions for Command and Control // Security and Strategy. London: Royal United Services Institute for Defence and Security Studies, 2016. // https://rusi.org/sites/default/fi les/cyber_threats_and_nuclear_combined.1.pdf.
16. Panda A., North Korea, US 'Left of Launch' Cyber Capabilities, and Deterrence // The Diplomat, December 06, 2018. // https://thediplomat.com/2018/12/north-korea-us-left-of-launch-cyber-capabilities-and-deterrence/.
17. Балыбин В.А., Высторобский С.Г., Ельцов О.Н., Сырбу И.А. Роботизированные комплексы РЭБ: перспективы создания и применения // Радиоэлектронная борьба в Вооруженных Силах Российской Федерации – 2018. Материалы от войск радиоэлектронной борьбы ВС РФ. 2018. 31 С. // https://reb.informost.ru/2018/pdf/1-5.pdf.
18. Стефанович Д.В. Искусственный интеллект и ядерное оружие // Российский совет по международным делам. 6 мая 2019 // https://russiancouncil.ru/analytics-and-comments/analytics/iskusstvennyy-intellekt-i-yadernoe-oruzhie/.

19. Stefanovich D. Artificial intelligence advances in Russian strategic, The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, vol. III, South Asian Perspectives, SIPRI: Stockholm, April 2020. // https://www.sipri.org/publications/2020/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-iii-south-asian.
20. Втюрина А. Г., Елисеев В. Л., Жиляев А. Е., Николаева А. С., Сергеев В. Н., Уривский А. В. Реализация средства криптографической защиты информации, использующего квантовое распределение ключей // Доклады ТУСУР. 2018. № 2. С. 15-21.
21. Горбачев Ю.Е. Радиоэлектронная борьба в сложной электромагнитной обстановке. // Радиоэлектронная борьба в Вооруженных Силах Российской Федерации. 2017. / http://reb.informost.ru/2017/pdf/1-3.pdf.
22. Ромашкина Н. П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. №. 1 (29). С. 2-9, DOI: 10.21681/2311-3456-2019-1-2-9.
23. Раков Ю. А., Шелест А. Б., Непочатых А. А. Противоспутниковое оружие: кибернетические системы // Научная мысль. 2019. Т. 9. №. 3. С. 98-102.
24. Stefanovich D., Russia's Basic Principles and the Cyber-Nuclear Nexus // European Leadership Network, July 14, 2020 // https://www.europeanleadershipnetwork.org/commentary/russias-basic-principles-and-the-cyber-nuclear-nexus/.

STRATEGIC RISKS AND PROBLEMS OF CYBER SECURITY

Romashkina N.P.[14], Stefanovich D.V.[15]

Abstract.

Purpose: *To identify the current strategic stability problems associated with the destructive impact of information and communication technologies (ICT) on the basis of analysis and systematization according to various parameters of cyber risks and threats to international security and global stability that can reduce the level of strategic stability and to develop relevant proposals that can lay the foundation for creation of a deterrence policy in the ICT domain.*

Research method: *analysis, synthesis and scientific forecasting, expert assessment, comparative analysis of the cyber domain within the framework of a systematic approach.*

Result: *the article presents analysis and systematization risks and threats to international security and global stability emanating from the cyber sphere according to various parameters. The article proves the impact of the accelerated development of information and communication technologies (ICT) on strategic stability, and that ensuring the cybersecurity of nuclear weapons requires special attention. The global problems of strategic stability at the current stage are posed and the conclusions are that the protection of strategic weapons, early warning systems, air and missile defense, communications, command and control over nuclear weapons from harmful ICTs are the pressing global problems of our time. Specific scenarios of cyber threats leading to a decrease in the level of strategic stability below the necessary and sufficient level have been elaborated, and proposals have been formulated to minimize the corresponding escalation threats. Proposed measures can become a basis for a deterrence policy in the ICT domain, as it was done during the period of bipolarity with regard to nuclear weapons, and become the foundation for broader international agreements on arms control in the so-called nuclear information space of the future.*

Keywords: *Information and communication technology (ICT), information space, cyber weapon, informational threat, cyber threat, cyberattack, strategic stability, command and control system, nuclear weapon, critical national infrastructure (CI).*

References

1. Schwab K. The fourth industrial revolution: What It Means and How to Respond? //Foreign Affairs. December 12, 2015. // https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.
2. Information Security Threats during Crisis and Conflicts of the XXI Century / Eds.: N.P. Romashkina, A.V. Zagorskii. Moscow: IMEMO, 2016. // https://www.imemo.ru/files/File/en/publ/2016/2016_001.pdf.
3. Nye J. S. Controlling Cyber Conflict // Project Syndicate. Aug. 8, 2017 // https://www.project-syndicate.org/commentary/new-norms-to-prevent-cyber-conflict-by-joseph-s--nye-2017-08/russian.

14 Nataliya Romashkina, Ph.D., Head of the Informational Security Problems Group of the Primakov National Research Institute of World Economy and International Relations (IMEMO) of the Russian Academy of Sciences, Moscow, Russia. E-mail: Romachkinan@yandex.ru

15 Dmitry Stefanovich, Research Fellow at the Center for International Security, Primakov National Research Institute of World Economy and International Relations (IMEMO) of the Russian Academy of Sciences, Moscow, Russia. E- mail: stefanovich@imemo.ru, ORCID 0000-0002-8694-8040

4. Problemy informacionnoj bezopasnosti v mezhdunarodnyh voenno-politicheskih otnosheniyah / Pod red. A.V. Zagorskogo, N.P. Romashkinoj. M.: IMEMO RAN, 2016. // https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf.
5. Gareev M.A., Turko N.I. Vojna: sovremennoe tolkovanie teorii i realii praktiki // Vestnik Akademii voennyh nauk. 2017. № 1 (58), p.4-10.
6. Markov A.S., Fadin A.A. Organizacionno-tekhnicheskie problemy zashchity ot celevyh vredonosnyh programm tipa Stuxnet // Voprosy kiberbezopasnosti. 2013. № 1(1), p. 28-36.
7. Romashkina N.P. Vooruzheniya bez kontrolya: sovremennye ugrozy mezhdunarodnoj informacionnoj bezopasnosti // Puti k miru i bezopasnosti. 2018. № 2(55), p. 64-83.
8. Romashkina N.P., Peresypkina O.V. Informacionno-psihologicheskoe vozdejstvie v period krizisa na Ukraine: uroki dlya Rossii // Informacionnye vojny. 2016. № 1 (37), p. 42-54.
9. Markov A.S., SHeremet I.A. Bezopasnost' programmnogo obespecheniya v kontekste strategicheskoj stabil'nosti // Vestnik akademii voennyh nauk. 2019. - № 2 (67), p. 82-90.
10. SHeremet I.A. Ugrozy tekhnosfere Rossii i protivodejstvie im v sovremennyh usloviyah // Vestnik akademii voennyh nauk. 2014. № 1., p. 27-34.
11. Kravcov D.N. Informacionno-psihologicheskoe oruzhie kak sredstvo obespecheniya zashchity nacional'nyh interesov gosudarstva // Kommunikologiya. 2017. № 3., p. 78-89.
12. Barsenkov A.S., Veselov V.A., Esin V.I., SHeremet I.A. Voprosy obespecheniya strategicheskoj stabil'nosti v sovetsko-amerikanskih i rossijsko-amerikanskih otnosheniyah: teoreticheskie i prikladnye aspekty // Ser. Politiko-voennye problemy sovremennyh mezhdunarodnyh otnoshenij. – M.: Izd-vo MGU im. M.V. Lomonosova, 2019, 144 p.
13. Romashkina N.P. Strategicheskaya stabil'nost' v sovremennoj sisteme mezhdunarodnyh otnoshenij. M.: Nauchnaya kniga, 2008, 288 p.
14. Stoutland P., Pitts-Kiefer S., Nuclear Weapons in the New Cyber Age // Nuclear Threat Initiative, September 2018. // https://media.nti.org/documents/Cyber_report_finalsmall.pdf.
15. Futter A. Cyber Threats and Nuclear Weapons New Questions for Command and Control // Security and Strategy. London: Royal United Services Institute for Defence and Security Studies, 2016. // https://rusi.org/sites/default/fi les/cyber_threats_and_nuclear_combined.1.pdf.
16. Panda A., North Korea, US 'Left of Launch' Cyber Capabilities, and Deterrence // The Diplomat, December 06, 2018 // https://thediplomat.com/2018/12/north-korea-us-left-of-launch-cyber-capabilities-and-deterrence/.
17. Balybin V.A., Vystorobskij S.G., El'cov O.N., Syrbu I.A. Robotizirovannye kompleksy REB: perspektivy sozdaniya i primeneniya // Radioelektronnaya bor'ba v Vooruzhennyh Silah Rossijskoj Federacii – 2018, 31 p Materialy ot vojsk radioelektronnoj bor'by VS RF. 2018. // https://reb.informost.ru/2018/pdf/1-5.pdf.
18. Stefanovich D.V. Iskusstvennyj intellekt i yadernoe oruzhie // Rossijskij sovet po mezhdunarodnym delam. 6 maya 2019 // https://russiancouncil.ru/analytics-and-comments/analytics/iskusstvennyy-intellekt-i-yadernoe-oruzhie/.
19. Stefanovich, D. Artificial intelligence advances in Russian strategic, The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, vol. III, South Asian Perspectives, SIPRI: Stockholm, April 2020. // https://www.sipri.org/publications/2020/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-iii-south-asian.
20. Vtyurina A. G., Eliseev V. L., ZHilyaev A. E., Nikolaeva A. S., Sergeev V. N., Urivskij A. V. Realizaciya sredstva kriptograficheskoj zashchity informacii, ispol'zuyushchego kvantovoe raspredelenie klyuchej // Doklady TUSUR. 2018. № 2, p. 15-21.
21. Gorbachev YU.E. Radioelektronnaya bor'ba v slozhnoj elektromagnitnoj obstanovke. // Radioelektronnaya bor'ba v Vooruzhennyh Silah Rossijskoj Federacii. 2017.
22. Romashkina N. P. Global'nye voenno-politicheskie problemy mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy, perspektivy //Voprosy kiberbezopasnosti. 2019. №. 1 (29)., p.2-9, DOI: 10.21681/2311-3456-2019-1-2-9.
23. Rakov YU. A., SHelest A. B., Nepochatyh A. A. Protivosputnikovoe oruzhie: kiberneticheskie sistemy //Nauchnaya mysl'. 2019. T. 9. №. 3., p. 98-102.
24. Stefanovich D., Russia's Basic Principles and the Cyber-Nuclear Nexus // European Leadership Network, July 14, 2020 // https://www.europeanleadershipnetwork.org/commentary/russias-basic-principles-and-the-cyber-nuclear-nexus/.