ИНФОРМАЦИОННЫЕ ВОЙНЫ США

К ОПРЕДЕЛЕНИЮ НАЦИОНАЛЬНОЙ КИБЕРСТРАТЕГИИ

ЕЛЕНА БАТУЕВА
МГИМО (У) МИД России, Москва, Россия

Резюме

Вопросы информационной безопасности приобретают все большее значение в связи с постоянно возрастающим потенциалом информационно-коммуникационных технологий и возможностью их использования государствами в качестве эффективного оружия. Соединенные Штаты – родина Интернета и одна из наиболее технологически развитых стран – с середины 1980-х годов проводят трансформацию вооруженных сил и адаптируют их к новым вызовам и угрозам, активно интегрируя киберкомпонент. На вооружении американской армии находится самое передовое информационное оружие. Особый интерес представляет рассмотрение киберстратегии США, развитие которой во многом предопределяет глобальные тенденции использования ИКТ в военно-политических целях. Одна из ключевых задач для США – обеспечение возможности проведения не только оборонительных, но и наступательных операций против других государств как в военное, так и в мирное время, что, в свою очередь, ставит под угрозу международную безопасность и стабильность. Такая политика одного из лидеров на международной арене стимулирует гонку информационных вооружений и подталкивает другие страны к принятию военных кибердоктрин. Отсутствие общепринятых международных норм и правил поведения государств, регулирующих информационное противоборство, создает правовой вакуум. Сегодня международное сообщество стоит перед выбором пути формирования правового режима использования государствами ИКТ военно-политической направленности. В качестве основных альтернатив можно выделить американский подход, суть которого сводится к поиску общепринятых трактовок действующих норм и принципов обычного международного права, и российский подход, согласно которому, необходимо вести дело к разработке нового комплексного, юридически обязывающего документа, в котором были бы учтены все аспекты использования ИКТ в целях, несовместимых с задачами обеспечения мира и стабильности. При этом, несмотря на различия в позициях двух ключевых участников переговорного процесса по вопросам международной информационной безопасности, существующая зона компромисса, над расширением которой активно работают Россия и США, позволяет развивать двустороннее сотрудничество в области информационной безопасности, что в свою очередь обеспечивает важные договоренности на международном уровне.

Ключевые слова:

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

Использование информационно-коммуникационных технологий (ИКТ) в военно-политических целях становится неотъемлемой составляющей государственной политики технологически развитых стран. Борьба, ведущаяся за обладание ин-

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

формацией, достижение и удержание информационного превосходства, сегодня занимает значительное место в междержавной конкуренции. При этом технологически развитые страны имеют несравнимо более широкие возможности в информационном пространстве и зачастую используют свое преимущество в ущерб интересам остальных участников международных процессов, включая вмешательство во внутренние дела государств в нарушение принципа суверенитета. В виртуальном мире государства могут позволить себе то, что считалось бы слишком провокационным в мире реальном, считая допустимым эскалацию он-лайн конфликтов при внешне спокойной офлайн-обстановке [Шмидт, Коэн 2013: 123].

Американский ученый Т. Рона, который, как принято считать, впервые ввел в оборот термин «информационная война», изначально исходил из того, что концепция информационной войны может быть реализована как на политическом уровне, так и в качестве составляющей действий вооруженных сил государства [Rona 1976].

На политическом уровне информационное противоборство может осуществляться посредством воздействия «мягкой силой» [Nye 2004], направленной на оказание информационного влияния на конкурирующие государства, политическую, экономическую и социальную сферы жизни общества, в целях обеспечения собственного доминирования. Оно включает в себя и политическую пропаганду, и психологическую обработку населения. Так, например, волна протестов, охватившая страны арабского мира в 2010–2011 годах, известная как «арабская весна», для целого ряда исследователей стала наглядным свидетельством того взрывоопасного потенциала политико-технологической манипуляции, в том числе из-за рубежа, посредством которой в считанные дни, а то и часы можно поднять массовые волнения и дестабилизировать ситуацию не только в масштабе страны, но и целого региона.

Государства стремятся максимально интегрировать передовые технологии в деятельность вооруженных сил, адаптируя их к ведению информационных войн и информационных операций. В XXI веке ИКТ становятся «идеальным» средством ведения боевых действий, позволяя странам достигать больших результатов, чем традиционные вооружения или разведывательные операции, благодаря мощному потенциалу и возможности проведения кибератак при сохранении анонимности. Как следствие, особую актуальность приобретают вопросы обеспечения национальной и международной информационной безопасности (МИБ).

В настоящее время на международном уровне не выработано общепринятого определения **«информационной войны»**. Можно выделить два ключевых подхода к данному термину. Первый – подход России и ее союзников, которые рассматривают инфовойны в их широком понимании как *противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны*[1].

Второй – американский подход. США в настоящее время используют термин *«кибервойна», под которым понимаются действия государств или международных организаций, направленные на проведение атак против компьютерных систем и сетей другого государства в целях их искажения или разрушения* [Arquilla, Ronfeld 1997: 30]. Другими

[1]Соглашение между правительствами государств–членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. [Электронный ресурс]. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=INT;n=51984;dst=100107 (дата обращения: 10.12.2013)

словами, данный термин включает в себя исключительно технологические аспекты.

Как представляется, Соединенные Штаты заинтересованы в установлении ограничений границами «кибер», так как информационно-коммуникационная составляющая политики США является важным внешнеполитическим инструментом и в связи с этим не должна рассматриваться в военных категориях, в частности, приравниваться к «применению силы».

1

В США последствия информатизации в военной области воплотились в концепции «революции в военном деле». Соединенные Штаты первыми с середины 1980-х годов начали трансформацию вооруженных сил и разработку стратегий ведения информационных войн и информационных операций, признав киберпространство критически важным для проведения военных операций наравне с землей, морем, воздухом и космосом [Lynn 2010].

Основа военной кибердоктрины США была заложена Директивой министра обороны США TS 3600.1 «Информационная война» от 21 декабря 1992 года, в которой информационная война определялась как самостоятельное направление оперативной деятельности вооруженных сил и включала в себя пять ключевых элементов: психологические операции, противодействие разведывательной деятельности противника и обеспечение безопасности военных операций, дезинформирование противника, радиоэлектронная борьба и уничтожение пунктов управления и систем связи.

Изначально концепция информационной войны охватывала исключительно действия вооруженных сил во время кризиса или конфликта, однако позднее свое развитие получили элементы информационной борьбы в мирное время, в связи с чем министерство обороны (МО) США отказалось от дальнейшего использования термина «информационная война», заменив его на «информационные операции», что отражено в директивах минобороны США «Информационные операции» 1996 и 2006 годов.

Информационные операции (ИО) представляют собой меры по воздействию на информацию и информационные системы противника при обеспечении защиты собственной информации и информационных систем[2]. Сегодня в арсенале Минобороны США пять ключевых видов информационных операций: *электронная борьба, сетевые компьютерные операции, военные операции информационной поддержки (психологические операции), дезинформация противника и безопасность операций*[3].

Важно отметить, что информационные операции могут быть как наступательными, так и оборонительными, а их проведение возможно в военное и мирное время. В мирное время ИО обеспечивают военно-политические цели государства посредством воздействия на взгляды и механизмы принятия решений противника. В период кризиса ИО могут быть использованы как гибкий сдерживающий механизм демонстрации намерений, информирования о национальных интересах с целью воздействия на механизмы принятия решений противника. Во время конфликта ИО могут применяться для достижения как физических, так и психологических результатов в целях обеспечения военных задач. В постконфликтный период ИО продолжают обеспечивать национальные военно-политические цели и воздействовать на видение ситуации противника[4]. Иными словами, США ведут информационное противоборство на постоянной основе, и главной задачей является обеспечение стратегического превосходства в киберпространстве для сохранения свободы действий и недопущения аналогичного условия для противников.

[2]Joint Doctrine for Information Operations. Joint Publication 3–13. Joint Chiefs of Staff. [Электронный ресурс]. October 9, 1998. p. vii. URL: http://www.c4i.org/jp3_13.pdf

[3]Information Operations. Directive TS 3600.1 Washington D.C.: U.S. Department of Defense [Электронный ресурс]. August 14, 2006. URL: https://www.fas.org/irp/doddir/dod/info_ops.pdf

[4]Там же.

В 2011 г. была принята «Международная стратегия для киберпространства», которая определяет американское видение развития киберпространства и основные приоритеты киберполитики США. Как подчеркивается в документе, главной задачей США является достижение лидерства в киберпространстве посредством участия во всех международных процессах, связанных с киберпространством: экономические аспекты, вопросы безопасности сетей, работа над законодательной базой, военно-политическое сотрудничество, разработка механизмов управления Интернетом.

Стоит отметить, что в случае враждебных действий в киберпространстве США зарезервировали за собой право использовать все необходимые средства: дипломатические, информационные, военные и экономические – в качестве самообороны, защиты союзников, партнеров и интересов государства[5].

Существенную ясность в планы действующей Администрации внесла Директива Президента PPD-20 «Политика США в области кибероперациий» 2012 года. В документе разграничены два направления: обеспечение защиты компьютерных сетей и ведение кибероперациий. Документ предписывает проводить более агрессивные действия для предотвращения кибератак на национальные сети, включая правительственные и частные, и предусматривает проведение наступательных кибероперациий в целях манипулирования, снижения работоспособности, блокирования или разрушения физических и виртуальных компьютерных систем противника. При этом отмечается, что такого рода операции обеспечат США возможность достигать военно-политические цели за пределами своей территории при минимальном времени предупреждения противников или же без предупреждения вообще и с потенциальным эффектом от незначительного ущерба до полного разрушения[6].

Таким образом, США последовательно, начиная с администрации У. Клинтона, разрабатывают стратегию ведения информационных операций, стремясь максимально использовать их потенциал, в том числе в комплексе с традиционными военными операциями. При этом особое внимание уделяется наступательной компоненте, которая позволяет обеспечивать стратегическое преимущество в ходе военных операций, а также достигать поставленных целей, не переходя в стадию открытого военного конфликта.

2

Впервые методы ведения информационной войны США опробовали в 1991 г. при проведении операции «Буря в пустыне». Информационные технологии, использованные силами коалиции в качестве оружия, а также в целях координирования действий, проведения разведывательных мероприятий, анализа ситуации и тылового обеспечения позволили сократить потери [Campen 1992].

Во всех последующих военных операциях США активно прибегали к проведению информационных операций: в Косове в 1999 г. (кибератаки на сербские военные системы), в Афганистане с 2001 г. (операции в информационных сетях противника, атаки на системы командования и контроля), в Ираке с 2003 г. (атаки на правительственные и военные информационные системы).

В 2010 г. в структуре Стратегического командования было создано Киберкомандование США (Киберком) под руководством генерала Кейта Александера, в сферу ответственности которого вошло: противодействие кибератакам и другим действиям в киберпространстве, представляющим угрозу национальной безо-

[5]International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. Washington D.C.: The White House [Электронный ресурс]. May 2011. p.14. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[6]Presidential Policy Directive/ PPD–20. U.S. Cyber Operations Policy [Электронный документ]. URL: http://www.fas.org/irp/offdocs/ppd/ppd–20.pdf

пасности, защита сетей МО США и поддержка региональных и функциональных боевых командований. Основными операциями Киберкомандования США стали: сетевые операции МО, оборонительные и наступательные кибероперации [Pellerin 2013]. В состав Киберкомандования входят 13 команд для ведения наступательной кибервойны, которые, в свою очередь, взаимодействуют с 27 командами ведения кибервойн в рамках стандартных боевых командований[7]. К 2015 г. в рамках киберкомандования планируется сформировать около 100 команд, которые будут осуществлять наступательные и оборонительные действия в киберпространстве, а также обеспечивать безопасность военных сетей [Nakashima 2012].

Параллельно с министерством обороны активную деятельность в киберпространстве проводит Агентство национальной безопасности (АНБ). АНБ совместно с Киберкомом проводят многочисленные операции по вмешательству в иностранные компьютерные сети с целью установления контроля над компьютерами и получения доступа к данным. Только в 2011 г. данными ведомствами была проведена 231 операция, которые включали в себя, в частности, шпионаж, манипулирование данными, а также воздействие на инфраструктуру [Gellman, Nakashima 2013].

В июне 2011 г. Пентагон объявил о разработке секретного списка кибероружия и киберинструментов, включая вирусы, посредством которых может быть проведена диверсия против критических сетей противника. Летом 2012 г. Агентство передовых оборонных исследовательских проектов при Министерстве обороны США (Defense Advanced Research Projects Agency, DARPA) анонсировало пятилетний проект с бюджетом в 110 млн. долларов США – «План X», в рамках которого планируется создание: самообновляемой передовой карты киберпространства, включающей информацию о всех компьютерах и других устройствах, что позволит военному командованию определить цели в киберпространстве и вывести их из строя при помощи компьютерного кода через Интернет или другими средствами; а также устойчивой операционной системы, посредством которой можно будет осуществлять кибератаки, при возможности отражать контратаки противника[8].

3

Операция «Олимпийские игры» по предотвращению получения Ираном обогащенного урана, проведенная полностью в киберпространстве, открыла новую перспективу использования киберметодов и средств в мирное время, не переходя к фазе открытого военного конфликта. Компьютерный червь «Стакснет» (Stuxnet) стал первым специально разработанным военным оружием, которое когда-либо было направлено против другого государства [Sanger 2012].

Атака «Стакснет» наглядно продемонстрировала ряд характерных для киберпространства особенностей. **Первое** – *сложность идентификации источника* агрессии или угрозы (вирус был внедрен в компьютерные сети ядерного объекта Натанц в общей сложности в течение двух лет; первоначально анализ данной атаки позволил исследователям сделать лишь предположительные выводы об источнике). **Второе** – *непредсказуемость результатов кибератаки* (несмотря на то что «Стакснет» был направлен на конкретные объекты инфраструктуры Ирана, в различной степени также пострадали технологические системы сразу нескольких стран – Австралии, Великобритании, Германии, Индонезии, Индии, Китая, Пакистана, США) [Kerr и др. 2010].

[7]Statement of General Keith B. Alexander Before the Senate Committee on Armed Servises. March 12, 2013. p. 1. [Электронный ресурс]. URL: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-091.pdf (дата обращения 12.12.2013 г.)

[8]Plan X. Program Information. DARPA [Электронный ресурс].URL: http://www.darpa.mil/Our_Work/I2O/Programs/Plan_X.aspx (дата обращения: 12.12.2013)

Принимая во внимание данные особенности киберпространства, потенциально кибератака против какого-либо государства может спровоцировать масштабный международный конфликт, в том числе в физическом пространстве, так как, *с одной стороны*, в условиях глобальной взаимосвязи информационных инфраструктур государств крайне сложно рассчитать масштаб и последствия такой атаки, *с другой* – ответные меры пострадавшей стороны могут быть непропорциональными в связи со сложностью определения источника и вероятностью ошибочной оценки ситуации.

4

Учитывая тот факт, что более 30 государств уже приняли военные доктрины, предполагающие вероятность ведения кибервойн, а всего более 120 государств прибегают к использованию ИКТ в военно-политических целях [Carr 2010: 1], назрела потребность в формировании международной политико-правовой базы, регулирующей действия государств в информационном пространстве, включая использование ИКТ в целях, несовместимых с задачами обеспечения международного мира и стабильности.

На международном уровне по-прежнему сохраняется правовой вакуум, связанный с отсутствием специально разработанных норм и принципов, регулирующих конфликты в киберпространстве. Представляется, что такая ситуация играет на руку США, которые активно работают над развитием национальной стратегии в киберпространстве и заинтересованы в возможности широкого толкования таких ключевых принципов международного права, как «право на самооборону» и «пропорциональность ответа» на кибератаки, а также в отсрочке принятия запрещающих норм в отношении проведения наступательных кибероперации и кибератак.

Существует два пути выработки принципов и норм международного права в отношении киберпространства. *С одной стороны*, это путь выработки общего подхода к применению действующих норм международного обычного права, а также принципов гуманитарного права, регулирующих применение силы в киберпространстве – вариант предлагаемый и отстаиваемый США[9]. Стоит отметить, что данная работа ведется на экспертном уровне уже не первый год, однако до сих пор не удалось прийти к консенсусу по ключевым определениям.

В марте 2013 г. Центром передового опыта в области кибероборонны при НАТО было опубликовано исследование – «Таллиннское руководство по международному праву, применимому к кибервойне» (Tallinn Manual on the International Law Applicable to Cyber Warfare)[10]. Результаты работы международной группы экспертов показали, что киберпространство обладает целым рядом уникальных характеристик, требующих дальнейшей проработки ключевых понятий, таких как «агрессия» и «применение силы», в контексте кибербезопасности.

В 2014 г. Группа правительственных экспертов ООН по международной информационной безопасности (ГПЭ ООН по МИБ) проведет работу по вопросам применения международного права к действиям государств в информационном пространстве.[11] Данное исследование пред-

[9]Developments in the Field of Information and Telecommunications in the Context of International Security.

Report of the Secretary-General. Document A/66/152. 15 July 2011. p. 18. [Электронный ресурс]. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=E (дата обращения: 16.12.2013)

[10]Tallinn Manual. NATO Cooperative Cyber Defense Centre of Excellence. [Электронный ресурс]. URL: http://www.ccdcoe.org/249.html (дата обращения: 16.12.2013)

[11]Резолюция Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 27 декабря 2013 г. Документ A/RES/68/243 [Электронный ресурс]. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/454/05/PDF/N1345405.pdf?OpenElement (дата обращения: 16.12.2013)

ставляется крайне своевременным и будет способствовать выработке общего понимания политико-правовых аспектов информационной безопасности, а также принятию дальнейших решений на международном уровне.

С другой стороны, альтернативным вариантом, который не исключает американского подхода, а, скорее, включает его, является разработка и принятие нового комплексного, юридически обязывающего документа, который бы регулировал все аспекты использования ИКТ в целях, несовместимых с задачами обеспечения международного мира и стабильности, включая военно-политические аспекты, угрозы криминального и террористического характера. Первая концепция конвенции ООН «Об обеспечении международной информационной безопасности» была разработана и представлена Российской Федерацией и ее союзниками – странами Шанхайской организации сотрудничества в 2011 году. Учитывая отсутствие общего понимания по ключевым определениям, работа над конвенцией потребует дополнительных усилий от международного сообщества, направленных на поиск компромиссных формулировок. В случае успешной работы ГПЭ ООН по МИБ, достигнутые результаты будут способствовать продвижению к выработке международного режима в области информационной безопасности.

Сложность и деликатность вопросов, связанных с информационной безопасностью государств, обусловливает необходимость в поэтапном развитии политико-правовой базы, начиная с укрепления мер доверия в киберпространстве, выработки общепринятых правил поведения и достижения двух- и многосторонних договоренностей о сотрудничестве по отдельным аспектам кибербезопасности.

В июне 2013 г. на полях саммита «группы восьми» *Россия и США* совершили прорыв, подписав впервые за всю историю многосторонних и двусторонних отношений соглашения, формирующие комплексную систему мер доверия в киберпространстве. Принятые документы предполагают организацию каналов прямой связи между: группами оперативного реагирования на компьютерные инциденты в целях создания механизма обмена информацией для обеспечения более эффективной защиты критически важных информационных систем; центрами по уменьшению ядерной опасности для содействия обмену срочными сообщениями, которые могут снизить риск недопонимания, эскалации и конфликта; а также должностными лицами высокого уровня по вопросам урегулирования потенциально опасных ситуаций, вызываемых событиями, которые могут создавать угрозы безопасности в сфере использования ИКТ и самим ИКТ[12].

Достигнутые российско-американские договоренности, в свою очередь, послужили основой для разработки первоначального *перечня мер укрепления доверия с целью снижения рисков возникновения конфликтов в результате использования ИКТ*, принятого в рамках ОБСЕ в декабре 2012 г. Это, безусловно, важный шаг международного сообщества в сторону повышения транспарентности, предсказуемости и стабильности в киберпространстве.

Следующим шагом является *разработка правил поведения государств в киберпространстве*. Достигнутое общее видение норм и принципов будет определять вектор дальнейшего движения международного сообщества в области информационной безопасности. Российская Федерация вместе с партнерами по ШОС – Китаем, Казахстаном и Узбекистаном уже выступили с проектом «Правил поведения в области обеспечения МИБ» в 2011 году. Одиннадцать норм охватывают основные аспекты обеспечения информационной безопасности и, в частности, обязуют государства не

[12]Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия от 17 июня 2013 г. [Электронный документ]. URL: http://news.kremlin.ru/ref_notes/1479 (дата обращения: 13.12. 2013)

использовать ИКТ для осуществления враждебных действий, актов агрессии, создания угроз международному миру и безопасности или распространения информационного оружия; сотрудничать в борьбе с преступной или террористической деятельностью с использованием ИКТ[13].

Однако США не готовы вести работу по данному проекту, ссылаясь на подмену существующих норм международного права, регулирующих вопросы применения силы и отношения между государствами во время вооруженных конфликтов, новыми, не в полной мере определенными правилами[14]. При этом выработка международных правил поведения государств в киберпространстве является одним из приоритетов Соединенных Штатов в области кибербезопасности[15], что говорит об их намерении продолжать работу над приемлемыми для всех государств правилами поведения.

Несмотря на то что Соединенные Штаты на данном этапе блокируют российские инициативы, направленные на формирование глобального режима информационной безопасности, анализ позиции США позволяет выделить ряд зон совпадения интересов, работа по которым может быть продолжена в формате двусторонних и многосторонних переговоров.

Так, руководство США демонстрирует понимание необходимости введения ограничений на проведение кибератак против объектов критической инфраструктуры, от безопасности которых зависит не только национальная, но и международная безопасность, а также против гражданской инфраструктуры[16]. В этой связи на международном уровне было бы крайне полезно составить официальный список таких «неприкасаемых объектов» и заложить его в соглашения двустороннего и многостороннего уровней.

Кроме того, США считают необходимым проведение юридического обзора вооружений с киберпотенциалом на предмет его соответствия ключевым принципам гуманитарного права – гуманности и пропорциональности[17]. Данную идею можно было бы рассмотреть в контексте включения в правила поведения положений об ограничении использования кибероружия. Представляется важным рассмотреть возможность составления международного реестра таких вооружений, который бы обновлялся на постоянной основе.

Несмотря на то что США не готовы обсуждать нормы, направленные на полный запрет кибероружия, идея о выработке режима по ограничению возможности его применения, а также ведения кибервойн (в частности, по примеру договоренностей по ядерному оружию), находит поддержку в американском истеблишменте [Clark, Knake 2010: 268–270]. В перспективе данный вопрос мог бы также стать одним из пунктов повестки дня по вопросам международной информационной безопасности.

* * *

Киберстратегия США, направленная на достижение информационного превосходства, вполне может стать дестабилизирующим фактором, так как подталкивает другие страны к принятию наступательных

[13]Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря. Документ A/66/359 [Электронный ресурс]. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement (дата обращения: 12.12.2013)

[14]Statement by the Delegation of the United States of America in the First Committee of the Sixty-seven Session of the United Nations General Assembly. November 1, 2012. [Электронный ресурс]. URL: http://geneva.usmission.gov/2012/11/23/us-first-committee/ (дата обращения 12.12.2013)

[15]Schneider D. Cyber Security Keynote Address. U.S. Department of State. 9 June 2010. [Электронный ресурс]. URL: http://www.osce.org/fsc/68524 (дата обращения: 12.12.2013)

[16]Koh H. Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace. September 18, 2012. [Электронный ресурс]. URL: http://www.state.gov/s/l/releases/remarks/197924.htm (дата обращения: 12.12.2013)

[17]Там же.

военных кибердоктрин и разработке информационных средств борьбы. Результатом этого процесса становится гонка информационных вооружений, возрастает потенциал возникновения дву- и многосторонних киберконфликтов с трудно прогнозируемыми последствиями и масштабом. Столкновения в информационной сфере могут перерасти в открытые военные конфликты с применением традиционных видов вооружений. Кроме того, использование преимуществ в информационном пространстве в ущерб национальным интересам других стран подрывает доверие между государствами и может непосредственно сказаться на политическом и экономическом партнерстве стран.

Важной задачей для международного сообщества является выработка международных договоренностей и новых норм международного права для киберпространства. Очевидно, процесс не будет быстрым. Однако первые шаги в данном направлении свидетельствуют о том, что международное сообщество будет продолжать двигаться по пути формирования глобального режима обеспечения международной информационной безопасности.

Список литературы

Шмидт Э., Коэн Дж. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств / пер. С.Филин. – Манн, Иванов и Фербер, 2013. 368 с.

Campen A. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Afcea Intl Pr, 1992. 195 p.

Carr J. Inside Cyber Warfare. O'Reilly Media, Inc, 2010. 212 p.

Clapper J. US Intelligence Community Worldwide Threat Assessment. Statement for the record. Office of the Director of National Intelligence, 2013. 30 p. URL: http://www.intelligence.senate.gov/130312/clapper.pdf (дата обращения: 14.12.2013)

Clarke R., Knake R. Cyber War: The Next Threat to National Security and What to do about it. HarperCollins Publishers. 2010. 290 p.

Gellman B., Nakashima E. U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011 // The Washington Post. August 30, 2013. URL: http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration (дата обращения: 12.12.2013)

Kaminski P. and others. 2013 Task Force Report: Resilient Military Systems and the Advanced Cyber Threat // Department of Defense. Defense Science Board.138 p. URL: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf (дата обращения: 15.12.2013)

Kerr P., Rollins J., Theohary C. The Stuxnet Computer Worm: Harbtinger of an Emerging Warfare Capability. Congressional Research Service. December 9, 2010. 9 p. URL: https://www.fas.org/sgp/crs/natsec/R41524.pdf (дата обращения: 16.12.2013)

Lynn W. III. Defending a New Domain. The Pentagon's Cyberstrategy. U.S. Department of Defense, 2010. URL: http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx (дата обращения: 16.12.2013)

Lynn W. III. The Pentagon's Cyberstrategy, One Year Later. // Foreign Affairs. September 28, 2011. URL: http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later (дата обращения: 16.12.2013)

Nakashima E. Pentagon proposes more robust role for its cyber-specialists // The Washington Post [Электронный ресурс]. August 10, 2012. URL: http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story_1.html (дата обращения 16.12.2013)

Nye J. Soft Power: The Means to Success in World Politics. New York: Public Affairs, 2004. 208 p.

Pellerin C. Cyber Command Adapts to Understand Cyber Battlespace // U.S. Department of Defense News. March 7, 2013. URL: http://www.defense.gov/news/newsarticle.aspx?id=119470 (дата обращения: 14.12.2013)

Rona T. Weapons Systems and Information War. Boeing Aerospace Company. Seattle, Washington 98124, 1976. 71 p. URL: http://www.dod.mil/pubs/foi/homeland_defense/missile_defense_agency/09-F-0070WeaponSystems_and_Information_War.pdf (дата обращения: 12.12.2013)

Sanger D. Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power. New York: Broadway Paperbacks, 2012. 485 p.

THE US INFORMATION WARS
TOWARDS DEFINING A NATIONAL CYBER STRATEGY

ELENA BATUEVA
Moscow State Institute of International Affairs (MGIMO University),
Moscow, 119454, Russian Federation

Abstract

Cyber security issues are becoming critically important due to the growing potential of ICT and the possibility of using it as an effective weapon by states. The United States, as the motherland of the Internet and one of the most technically developed countries, has been transforming its military forces since the mid-1980s by integrating cyber components into all the activities of the Department of Defense and other agencies responsible for national security. As one of the American strategic goals is The domination of cyberspace, the United States is interested in retaining all the possibilities necessary to conduct defensive as well as offensive information operations during the periods of both war and peace.

However, such a policy puts the national security of other countries under risk and threatens international security and stability by motivating other nations to work on crafting offensive cyber strategies and thus provoking an information arms race. The lack of international norms regulating conflicts in cyberspace, as well as ofglobally accepted rules of conduct, creates a legal vacuum. The author provides an overview of severalalternative ways to further the development of an international legal regime for cyberspace, as well as thepotential fields for international cooperation on cyber security issues.

The United States and Russia stand for different approaches when it comes to the main driving forces of multilateral negotiations on information security issues. U.S. officials are convinced that existing principles of international law serve as the appropriate framework that should govern the use of cyberspace in connection with hostilities, while Russia promotes the idea of a new complex global convention that would set an international information security regime. Despite differences in their approaches, Russia and the United States are consistently working on practical bilateral agreements that create an important basis for the further development of cyber issues on the multilateral level.

Keywords:

ICT; information war; cyber war; information operations; international information security; USA; Russia.

References

Campen A. (1992) *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Afcea Intl Pr. 195 p.

Carr J. (2010) *Inside Cyber Warfare.* O'Reilly Media, Inc. 212 p.

Clapper J. (2013) US Intelligence Community Worldwide Threat Assessment. Statement for the record. *Office of the Director of National Intelligence*, 2013. 30 p. Available at: http://www.intelligence.senate.gov/130312/clapper.pdf (accessed 14.12.2013)

Clarke R., Knake R. (2010) *Cyber War: The Next Threat to National Security and What to do about it.* HarperCollins Publishers. 290 p.

Gellman B., Nakashima E. (2013) U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011 // *The Washington Post*. Available at: http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration (accessed 12.12.2013)

Kaminski P. and others. (2013) Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. *Department of Defense. Defense Science Board*. 138 p. Available ay: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf (accessed 15.12.2013)

Kerr P., Rollins J., Theohary C. (2010) The Stuxnet Computer Worm: Harbtinger of an Emerging Warfare Capability. *Congressional Research Service*. 9 p. Available at: https://www.fas.org/sgp/crs/natsec/R41524.pdf (accessed 16.12.2013)

Lynn W. III. (2010) Defending a New Domain. The Pentagon's Cyberstrategy. U.S. Department of Defense. Available at: http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx (accessed 05.03.2014)

Lynn W. III. (2011) The Pentagon's Cyberstrategy, One Year Later. *Foreign Affairs*. Available at: http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later (accessed 16.12.2013)

Nakashima E. (2012) Pentagon proposes more robust role for its cyber-specialists. *The Washington Post*. Available at: http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story_1.html (accessed 16.12.2013)

Nye J. 2004. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs, 2004. 208 p.

Pellerin C. (2013) Cyber Command Adapts to Understand Cyber Battlespace. U.S. *Department of Defense News*. Available at: http://www.defense.gov/news/newsarticle.aspx?id=119470 (accessed 14.12.2013)

Rona T. (1976) *Weapons Systems and Information War*. Boeing Aerospace Company. Seattle, Washington 98124. 71 p. Available at: http://www.dod.mil/pubs/foi/homeland_defense/missile_defense_agency/09-F-0070WeaponSystems_and_Information_War.pdf (accessed 12.12.2013)

Sanger D. (2012) *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power*. New York: Broadway Paperbacks. 485 p.

Schmidt E., Cohen J. (2013) *Novyi tsifrovoi mir. Kak tekhnologii meniaiut zhizn' liudei, modeli biznesa i poniatie gosudarstv. [The New Digital Age: Reshaping the Future of People, Nations and Business]*. Mann, Ivanov i Ferber. 368 p.