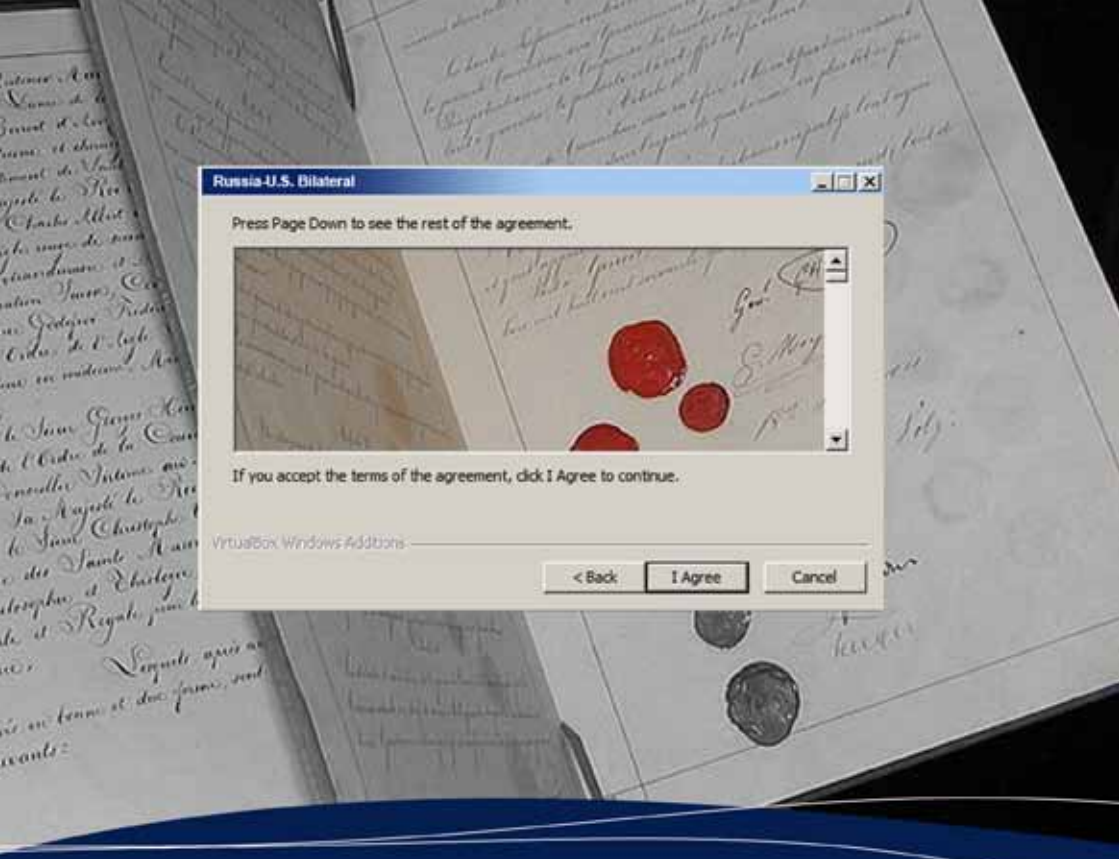


РОССИЙСКО-АМЕРИКАНСКАЯ ПРОГРАММА ПО ЗАЩИТЕ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

К ВЫРАБОТКЕ ПРАВИЛ ПОВЕДЕНИЯ В КИБЕРКОНФЛИКТАХ:

Женевские и Гаагские конвенции в информационном пространстве

Карл Фредерик Раушер и Андрей Коротков

EastWest Institute
Forging Collective Action for a Safer and Better World
30 YEARS

Институт Восток-Запад (ИВЗ) был основан в 1980 году как международная экспертная организация, ориентированная на практические действия. ИВЗ содействует разрешению наиболее сложных международных проблем, используя такие инструменты, как:

ПРОВЕДЕНИЕ конфиденциальных встреч и дискуссий между представителями общественных институтов и государств, испытывающих затруднения для нормального сотрудничества друг с другом. При этом ИВЗ выступает в качестве глобальной площадки для доверительного взаимодействия по линии неофициальной дипломатии, а также в роли организатора публичного обмена мнениями по вопросам мира и безопасности;

ПЕРЕФОРМАТИРОВАНИЕ ПОСТАНОВКИ вопросов, позволяющее найти взаимовыгодные решения проблемных ситуаций, – опираясь на сложившиеся у нас особые отношения с Россией, Китаем, США, Европой, другими державами и объединениями государств. ИВЗ сближает непримиримые позиции и взгляды, что способствует совместному движению к позитивным изменениям;

МОБИЛИЗАЦИЯ многоуровневой сети связей с ключевыми фигурами как в государственном, так и в частном секторе. ИВЗ использует свои контакты с лидерами экспертного, политического и бизнес-сообществ во всем мире в целях сглаживания существующих и предотвращения назревающих конфликтов.

Корпоративный лозунг ИВЗ (Forging Collective Action for a Safer and Better World), входящий в логотип Института, можно перевести так: «К совместным действиям за более безопасный и совершенный мир». Институт Восток-Запад является политически независимой некоммерческой организацией с офисами в Нью-Йорке, Брюсселе и Москве. ИВЗ придает большое значение сохранению своей независимости, что обеспечивается диверсифицированным составом как совета директоров, так и спонсоров.

Центр ИВЗ в Брюсселе
59-61 Rue de Trèves
1040 Brussels
Belgium
32-2-743-4610

Центр ИВЗ в Москве
7/5 Bolshaya Dmitrovka Str
Bldg. 1, 6th Floor
Moscow 125009
Russia, 7 495 234 7797

Центр ИВЗ в Нью-Йорке
11 East 26th Street
20th Floor
New York, NY 10010
U.S.A. 1-212-824-4100

www.ewi.info

РОССИЙСКО-АМЕРИКАНСКАЯ ПРОГРАММА ПО ЗАЩИТЕ
КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

К выработке правил поведения в киберконфликтах: Женевские и Гаагские конвенции в информационном пространстве

Карл Фредерик Раушер и Андрей Коротков

Январь 2011 года

EastWest Institute
Forging Collective Action for a Safer and Better World
30 YEARS

Dedication

To those whose suffering was the impetus for the Conventions.
May future generations have wisdom absent such impetus.

Посвящение

Посвящается тем, чьи страдания стали побуждающим мотивом принятия конвенций о законах, обычаях и защите жертв войны.
Пусть же у будущих поколений хватит мудрости не допустить подобных страданий.
.

Содержание

ВСТУПИТЕЛЬНОЕ СЛОВО

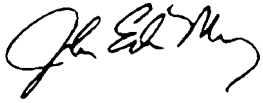
За последние три десятилетия стратегический диалог между Россией и Соединенными Штатами стал существенной частью усилий всего человечества в направлении создания более безопасного и лучшего мира. Достижение целого ряда соглашений в области ядерных вооружений, среди которых и последний договор СНВ-3, представляют собой веское свидетельство достигнутого в этом направлении прогресса.

Кибербезопасность - это новый вызов для развивающегося сотрудничества между Россией и США, а также для всего международного сообщества. Это область, где уровень доверия ничтожно мал, и где отсутствуют реально согласованные нормы поведения. Одновременно во многих странах мира нарастает обеспокоенность в отношении намерений и возможностей, которые имеются у негосударственных игроков. При этом пользователи сети, представители бизнеса и политики продолжают верить, что некая сложная система, механизм которой они не понимают, будет и дальше исправно функционировать. В настоящее время мировая экономика полностью зависит от цифровых технологий, что означает ее возрастающую уязвимость перед деструктивными действиями государственных или негосударственных структур. Это опасная ситуация. Крайне необходимо развитие международного сотрудничества по этой проблеме, имеющей в высшей степени стратегическое значение. Если мы потерпим неудачу в решении этой задачи, то возникшая угроза для глобальной стабильности может оказаться сравнимой с угрозой ядерного противостояния.

В течение тридцати лет Институт Восток-Запад служит интеллектуальной площадкой, объединяющей усилия для решения наиболее значимых стратегических вызовов, которые стоят перед нашим миром. В рамках своей программы «Всемирная инициатива по кибербезопасности» Институт создал группу Cyber 40*, цель которой - подготовка совместных докладов, помогающих сформировать доверие и способствующих построению фундамента для новых международных соглашений.

Российско-американское сотрудничество, результатом которого является настоящий совместный доклад, бросает вызов стереотипному представлению о том, что вопросы кибербезопасности слишком сложны и деликатны для достижения по ним международных договоренностей. Мы выражаем благодарность экспертам по вопросам технологий, бизнеса и политики, которые подготовили настоящий доклад, за их высокоэффективную и трудную работу. Их успех в проведении данного исследования и сделанные рекомендации показывают, чего можно достичь, если есть политическая и личная воля. Мы призываем представителей бизнеса и государственного сектора со стороны России и США проявить упорство в дальнейших усилиях по продвижению рекомендаций, согласованных в результате данного опыта сотрудничества в вопросах кибербезопасности. Мы также с нетерпением ждем заинтересованной реакции наших читателей. Институт Восток-Запад планирует продолжить работу, исходя из результатов данного исследования, и будет рад расширить круг участников. Мы верим, что эта работа поможет ускорить развитие международного диалога по кибербезопасности, в результате чего эффективное международное сотрудничество в этой сфере станет реальностью.

ГАРРИ Д. РАДИГИ, МЛ.
Почетный председатель Всемирного саммита по кибербезопасности Института Восток-Запад, бывший директор управления связи министерства обороны США, управляющий национальной системой связи, генерал-лейтенант (в отст.), ВВС США



ДЖОН ЭДВИН МРОЗ
Президент и главный исполнительный директор Института Восток-Запад

ПРЕДИСЛОВИЕ

В настоящем докладе представлены пять совместных рекомендаций для частного сектора и правительств. Некоторые являются довольно смелыми. Каждая требует принятия практических мер и, будучи реализована, обеспечит решительный шаг вперед в области международной политики регулирования киберконфликтов. Мы считаем, что, рассмотрение представленных здесь методологических принципов должно быть сделано безотлагательно с учетом потенциальных последствий современного развития ситуации.

Мы представляем этот доклад как документ по очень серьезной проблеме, с которой столкнулось человечество в век информации. Женевские и Гаагские конвенции о законах и обычаях войны определили меры по защите гражданского населения в условиях, когда все иные защитные механизмы разрушены. Сохранение жизнеспособности и осуществимости принципов, зафиксированных в Конвенциях, имеет важнейшее значение для миллиардов людей, как живущих сейчас, так и тех, кто появится позже. Поскольку наш мир быстро обрастает новыми сетевыми связями и интегрируется с киберпространством, сохранение имеющихся механизмов защиты не является ни автоматическим, ни прямолинейным. Киберпространство уже стало неотъемлемой частью нашей личной жизни во всех ее проявлениях, функционирования частного бизнеса и государственного управления. Фактически, информационно-коммуникационные технологии в корне преобразовали природу критической инфраструктуры и характер ее защиты, а также характер войны и методов ее ведения. Кибербезопасность становится опорой нашей взаимной сохранности, стабильности и безопасности. В этой ситуации не может не бросаться в глаза отсутствие “правил игры”, или хотя бы каких-то норм поведения в условиях киберконфликта.

Настоящий совместный анализ был проведен экспертами мирового класса из наших двух стран с целью достижения ощутимого прогресса на международной арене. Мы выражаем глубокую признательность нашим коллегам, фамилии которых перечислены на следующей странице. Участники проекта представляют самые разнообразные области знаний и компетенций, которые требовались для осуществления данного проекта; их совместный стаж работы по соответствующим темам превышает, в общей сложности, пятьсот лет. Личный вклад и приверженность каждого из соавторов общему делу в рамках интенсивного интерактивного процесса, служившего движущей силой нашего исследования, заслуживают признания и благодарности.

Меры гуманитарной защиты, предусмотренные Конвенциями, – это трудная награда, завоеванная нашей цивилизацией. Они священны и неоспоримы для всех. Давайте все вместе докажем, что мы станем достойными продолжателями того прогресса, который был достигнут предыдущими поколениями.

КАРЛ ФРЕДЕРИК РАУШЕР

Руководитель группы экспертов от США, директор по технологиям и почетный консультант, Институт Восток-Запад, президент Группы чрезвычайного реагирования по беспроводным технологиям, консультант компании Bell Labs, Нью-Йорк, США

АНДРЕЙ КОРОТКОВ

Руководитель группы экспертов от России, профессор Московского государственного института международных отношений МИД РФ, первый заместитель министра, министерство телекоммуникаций и информатизации России (2002 - 2004 гг.) Москва, Россия

СОАВТОРЫ-УЧАСТНИКИ ЭКСПЕРТНОЙ ГРУППЫ

Российская Федерация

Артем Аджемов, Московский технический университет связи и информатики
Владимир Иванов, Институт Восток-Запад
Виктор Минин, Межрегиональная общественная организация «Ассоциация защиты информации»
Борис Славин, Российский союз ИТ-директоров
Леонид Тодоров, Координационный центр национального домена сети Интернет RU
Елена Зиновьева, Московский государственный институт Международных отношений МИД РФ

Соединенные Штаты Америки

Чарльз (Чак) Бери, Университет национальной оборо-
ны (Charles (Chuck) Barry, National Defense University)
Джон С.Эдвардс, Диджиком, Инк. (John S. Edwards, Digicom, Inc.)
Дж.Б. (Джиб) Годвин, контр-адмирал (отст.), Нортроп Грумман
(J. B. (Gib) Godwin, RADM (ret.), Northrop Grumman)
Стюарт Голдман, консультант (отст.) Белл Лэбс (Stuart Goldman, Bell Labs Fellow (ret.))
Пол Николас, Корпорация Майкрософт (Paul Nicholas, Microsoft Corporation)
Джеймс Брет Майкл, Школа последипломного образования ВМФ
США (James Bret Michael, U.S. Naval Postgraduate School)
Джек Ослунд, Университет Джоджа Вашингтона (отст.) (Jack
Oslund, George Washington University (ret.))
Томас С.Уингфилд, Европейский центр исследований по безопасности им. Маршалла
(Thomas C. Wingfield, George C. Marshall European Center for Security Studies)

РЕЦЕНЗЕНТЫ

Рамзес Мартинес, ВериСайн Дженерал (отст.) (Ramses Martinez, VeriSign General (ret.))
Т. Майкл Мосли, ВВС США, почетный консультант им. Перо, Институт Восток-
Запад (T. Michael Moseley, USAF; Perot Distinguished Fellow, EWI)

ВЫРАЖЕНИЕ БЛАГОДАРНОСТИ

Особое признание и высокая оценка выражаются:

Вольфгангу Ишингеру - за включение настоящего документа в повестку дня Мюнхенской конференции по безопасности 2011 года.

Вартану Саркисяну и Владимиру Иванову - за их проницательность и настойчивость в обеспечении условий для реализации данного проекта
Францу Штефан-Гади - за его вклад в управление проектом и активный анализ политики государств в сфере кибербезопасности

Эндрю Нагорскому, Трейси Ларсен, Драгану Стояновскому и Абигейл Рабинович - за их контроль качества издания и обеспечение процессов коммуникации

Тэрри Моргану и Грэгу Остину - за их прочную непрерывную поддержку и содействие в отношении двусторонней российско-американской программы по кибербезопасности

Анатолию Сафонову, Владиславу Шерстюку, Андрею Крутских, Сергею Кисляку, Уильяму Бернсу, Майклу Макфолу, Джону Байерли и Джону Эдвину Мрозу - за их инновационные предложения, поддержку и перспективное мышление.

и наконец, широкому сообществу наших единомышленников в городах Москве и Вашингтоне, живой интерес которых к инновационным подходам в рамках общественной дипломатии служит залогом долговременной ценности подобных инициатив.

1. Основные положения

В духе «перезагрузки» отношений между Москвой и Вашингтоном, российские и американские эксперты по безопасности и ИТ-технологиям решили создать модель новых форм сотрудничества по наиболее острой теме с точки зрения безопасности – безопасности в киберпространстве. Общепринятое мнение состоит в том, что согласование “правил игры” для киберконфликта будет очень кропотливым и чрезвычайно трудным делом. Предприняв первую удачную попытку совместного исследования, российско-американская группа экспертов доказала, что прогресс в этой области возможен и реально достижим. Настоящий документ представляет пять совместных рекомендаций, которые могут быть реализованы незамедлительно, и, в случае осуществления, станут эффективным инструментом сохранения ключевых гуманитарных принципов так называемого «права войны». Продемонстрированный здесь успех может служить катализатором для дальнейшего продвижения по пути достижения поставленной цели.

Настоящий совместный документ представляет собой совместно согласованное заключение российских и американских экспертов по внедрению в киберпространство принципов Женевских и Гаагских конвенций о законах, обычаях и защите жертв войны. Данная работа является продуктом двусторонней программы общественной дипломатии, цель которой - открыть диалог, построить устойчивое доверие и оказывать положительное воздействие на самые трудные, критически важные области международной безопасности.

В новейшей истории Россия и Соединенные Штаты Америки оказывали и продолжают оказывать очень большое влияние на состояние международной ситуации. Когда эти две страны договариваются об общем подходе к решению какой-либо конкретной проблемы, то другие страны проявляют большую готовность к серьезному диалогу. Именно поэтому высококлассные эксперты из России и США согласились вместе заняться проблемой кибербезопасности в рамках подготовки настоящего доклада. Выражаем надежду, что другие страны также будут участвовать в этом процессе.

Одно из наиболее высоко оцениваемых достижений широкого сообщества государств, достигнутое полтора столетия назад, состояло в их сотрудничестве, которое привело к созданию Конвенций, защищающих достоинство и уважение человеческой жизни. Решения, принятые в Гааге и Женеве, нашли отражение в важных строках, которые гласят: «В битве ради достижения какой-либо цели или в организации обороны вам дозволено

дойти до определенных, четко обозначенных границ, переходить которые запрещено». Хотя эти принципы, по общему признанию, отражают только самые базовые аспекты гуманности, они, тем не менее, стоят в ряду наиболее значимых достижений цивилизации. В мире открытых столкновений между идеями, в том числе с использованием силы, они поддерживают в нас уверенность в том, что есть вещи, «о которых мы можем договориться».

Право не является предметом нашего доклада. Если мы и анализируем высокочтимые общие принципы Женевских и Гаагских конвенций, то только в качестве отправной точки проекта. Понятно, что современные информационно-коммуникационные технологии (далее - ИКТ) кардинально преобразовали мир, в котором мы живем. А это значит, что практическое приложение некоторых принципов Конвенций больше не является столь же прямолинейным, как это было когда-то.

Уникальные особенности работы

Вопросы применимости Женевских и Гаагских конвенций к киберпространству одно время вызывали широкий интерес. Этой теме было посвящено значительное количество аналитических исследований. По этим вопросам было высказано немало мнений. Основное внимание при этом уделялось юридическим вопросам, политическому значению или вероятным экстремальным сценариям развития киберконфликта. Наше исследование отличается тем, что фокусируется на тех направлениях деятельности, в которых возможно достижение стратегического согласия на базе ключевых принципов Конвенций, для чего применяются передовые технические методы и формулируются рекомендации практического характера.

Уникальность этого совместного доклада обусловливается, среди прочего, тем обстоятельством, что он является продуктом двусторонней программы сотрудничества двух кибернетических сверхдержав. Отличительными особенностями являются также следующие: интегрирование разнообразных базовых компетенций, необходимых для анализа предмета (Раздел 3), комбинированный подход к оценке сложного проблемного поля, использование передовых технических методов анализа (в частности, методологии под названием «восемь составляющих (8i)» и анализа факторов внутренней уязвимости) (Раздел 3), а самое главное – представление конкретных, реализуемых консенсусных рекомендаций, которые в случае успешного претворения в жизнь позволят эффективно сохранить сформулированные в Конвенциях гуманитарные принципы

защиты критической инфраструктуры (Раздел 4).

Совместные рекомендации

Ниже следуют рекомендации, которые далее в докладе приводятся в контексте иной существенной информации, призванной облегчить их практическое воплощение. Такой контекст включает важные справочные данные, предложения по распределению обязательств ключевых игроков, оценку выгод от реализации предложенной инициативы, анализ возможных альтернативных подходов и их последствий, а также характеристику критериев успеха. Каждая из рекомендаций более подробно описана в Разделе 4.

“Труднее всего объяснить то, что ослепительно очевидно, но что все решили не замечать.»

- Эйн Рэнд, американский писатель русского происхождения.

“Образование состоит главным образом из того, чему мы разучились.”

- Марк Твен, американский писатель.

“Знания не имеют ценности, если вы не пользуетесь ими в жизни”

- Антон Чехов, русский драматург и мастер короткого рассказа.

РЕКОМЕНДАЦИЯ 1. Выделение охраняемых объектов в киберпространстве.

Женевские конвенции обеспечивают некоторую степень защиты для объектов чисто гуманитарного назначения и обслуживающего их персонала, при определенных условиях, в военное время. Однако в киберпространстве защищенные и незащищенные объекты часто настолько переплетены, что это подвергает защищенные объекты опасности. До сих пор эта тема подвергалась анализу, в основном, в связи с обсуждением проблем национальной безопасности внутри отдельных государств. Данная рекомендация выводит ее на межгосударственный уровень, создавая импульс для совместной работы, сначала в контексте двустороннего взаимодействия, а в последующем – на многосторонней основе.

России и США, наряду с другими заинтересованными сторонами, следует проанализировать, в какой степени защищенные критические инфраструктуры гуманитарного назначения в настоящее время переплетены с незащищенными инфраструктурами, с тем, чтобы определить, являются ли имеющиеся в Конвенциях и Протоколах формулировки достаточными, и возможно ли на практике осуществить

выделение критических гуманитарных инфраструктурных объектов.

Результатом практического применения этой рекомендации будет выработка двустороннего или многостороннего заключения о том, являются ли предусмотренные Конвенциями средства защиты гуманитарных объектов по-прежнему действенными, либо потерявшими существенную долю своей эффективности, с возможностью восстановления таковой или безвозвратно, исходя из существующих тенденций в киберпространстве. Это заключение будет способствовать сохранению зафиксированных в Конвенциях принципов, которые охраняют жизненно важные гуманитарные инфраструктуры и гражданское население. Эффективное применение вышеизложенной рекомендации потребует от компаний частного сектора обеих стран поделиться своими техническими знаниями и деловым опытом. Кроме того, необходимым условием успеха является поддержка такого сотрудничества со стороны российских и американских правительственных кругов, в частности, путем направления своих соответствующих экспертов. Предполагается, что международные неправительственные организации, занимающиеся гуманитарной помощью, также внесут свой вклад.

РЕКОМЕНДАЦИЯ 2. Применение в киберпространстве женевской концепции опознавательной эмблематики.

Способность воюющей стороны распознавать заявленный охраняемый объект имеет основополагающее значение для соблюдения Конвенций. Женевские и Гаагские конвенции предписывают, что охраняемые объекты, персонал и транспортные средства должны быть маркированы четким для визуального восприятия способом, позволяющим их отличать. Кроме того, Конвенции определяют стандартные виды опознавательных эмблем (например, Красный Крест, Красный Полумесяц), содержат инструкции по их применению и оговаривают последствия несанкционированного применения таких эмблем. *Однако в киберпространстве не существует четких опознавательных знаков (маркеров), которые могли бы применяться для обозначения охраняемых объектов, персонала или соответствующего имущества.* Без таких обозначений гуманитарные интересы, подпадающие под защиту Конвенций согласно намерениям составителей, находятся в опасности. Сформулированная ниже рекомендация предлагает разработать систему аналогичных маркеров для киберпространства с тем, чтобы обозначить защищенные объекты, персонал и прочие активы.

России и США, наряду с другими заинтересованными сторонами, следует провести совместную оценку преимуществ и возможностей применения специальных опознавательных знаков в киберпространстве, которые могли бы быть использованы для обозначения гуманитарных интересов, находящихся под защитой Конвенций и Протоколов о войне.

Практическая польза от применения этой рекомендации состоит в том, что она позволит четко опознавать защищенные объекты, людей или активы в киберпространстве. Способность воюющей стороны отличать такие защищенные объекты совершенно необходима для сохранения действенности Конвенций, посвященных защите гуманитарных интересов. Эффективное применение этой рекомендации потребует от частного бизнеса поделиться своим опытом и знаниями; от российских и американских правительственных кругов, поддерживающих сотрудничество, - предоставить соответствующих экспертов, а от организаций, выполняющих функции регулирования в Интернете и поддерживающих реализацию соответствующих мер, - ввести в действие механизм соблюдения принципа отличительной эмблематики в киберпространстве.

РЕКОМЕНДАЦИЯ 3. Признание растущего влияния роли негосударственных игроков и пользователей сети.

Цифровая революция создала киберпространство, представляющее собой по сути новую «территорию». Поскольку исторически конечной целью соперничества между вовлеченными в войну этническими группами и политическими силами являлся захват и установление контроля над территориями, лицами, поставившими свои подписи под Конвенциями, были государства, представлявшие конкретные нации. Цифровая революция коренным образом преобразила ситуацию: на арену в массовом порядке вышли негосударственные игроки и просто физические лица, которые получили возможность оккупировать, ставить под контроль и осуществлять управление кибертерриториями. Это нарушает симметрию сил в результате наращивания ударного потенциала новых участников процесса, которым ничто не мешает нарушать принципы Конвенций, причем в массовом порядке.

России, США и другим заинтересованным сторонам следует определить, как лучше всего согласовать принципы Конвенций с новой действительностью, в которой участниками киберконфликта могут стать негосударственные игроки.

Совместное изучение этого вопроса поможет выработать общее понимание новой динамики процессов в киберпространстве и связанных с ними растущих рисков. Кроме того, в рамках такого исследования можно спрогнозировать потребности различных групп, формирующих киберсообщество, в получении информации и овладении практическими навыками применения концепций защиты гражданских лиц и жизненно важных гражданских инфраструктур, заложенных в основу Женевских и Гаагских конвенций. Для достижения реальных положительных сдвигов необходимо, чтобы правительства были открыты для восприятия новых парадигм, основанных на принципах уважения, диалога, сотрудничества и доверия во взаимоотношениях с негосударственными игроками, в частности, с такими как неправительственные организации (НПО) и транснациональные компании (ТНК). Кроме того, как правительствам, так и значительной части негосударственным игрокам и пользователям. следует продемонстрировать готовность к сотрудничеству в киберпространстве на некотором новом, хотя бы минимальном уровне, который предстоит уточнить в дальнейшем.

РЕКОМЕНДАЦИЯ 4. Анализ принципов Женевского протокола применительно к кибернетическому оружию.

По мере увеличения зависимости современной цивилизации от ИКТ и киберпространства, растет беспокойство относительно потенциальных последствий распространения кибероружия, которое порождает новые виды агрессии, вызывает многоуровневые каскадные поражения и социально-экономическое опустошение. Кибернетическое оружие способно в мгновение ока распространять бесконтрольные волны вирусов, которые легко воспроизводятся и переносятся, не утруждаясь распознаванием цели. Эти свойства, в сочетании с агрессивными намерениями распространителей, вызывают понятное беспокойство. Самое лучшее в такой ситуации – воспользоваться Конвенциями как прецедентом наложения запрета на определенные виды оружия из гуманитарных соображений.

Военные, которым поручено обеспечивать решающее преимущество на поле боя, осознают стратегическое значение секретности и стремятся любыми способами избегать раскрытия информации. Вместе с тем, их оправданная обеспокоенность вопросами безопасности не могла не застопорить продвижение по пути международного сотрудничества в области анализа вооружений. Инновационность на-

шего подхода состоит в том, что мы предлагает сосредоточить внимание на факторах внутренней уязвимости ИКТ, признанных и исследованных в открытых источниках, что значительно смягчает озабоченности военных.

России, США и другим заинтересованным сторонам рекомендуется предпринять совместный анализ характеристик кибернетического оружия с тем, чтобы определить возможность проведения аналогий с теми видами вооружений, которые были ранее запрещены Женевским протоколом.

Результатом такого анализа, в случае успеха, могла бы стать «ломка льда» в отношениях между кибердержавами, что открыло бы новые возможности для обсуждения механизмов сдерживания конфликта, создало бы условия для понимания специфики кибероружия в международном масштабе и для ограничения распространения средств, применение которых может иметь разрушительные последствия для гражданского населения и критически важных гражданских инфраструктурных объектов. Успешное выполнение этой рекомендации потребует от экспертов максимальной открытости в ходе обсуждения различных видов кибероружия на базе открытой информации. Российское и американское правительства должны быть готовы признать, что некоторые виды вооружений могут быть сочтены недопустимыми по своим характеристикам, поскольку нарушают «принципы человечности и императивы общественной морали». [1]

РЕКОМЕНДАЦИЯ 5. Изучение «третьего» («иного, чем война») состояния международных отношений.

На международном уровне отсутствует ясное и согласованное определение того, что следует называть кибервойной. По этому вопросу наблюдается значительная путаница. Зачастую даже руководители одной и той же страны не могут согласиться друг с другом относительно того, ведется ли кибервойна в настоящее время, насколько ее проявления реальны и каковы могут быть их последствия в будущем. Существующая неоднозначность толкования препятствует разработке политики на государственном уровне и осложняет применение требований Конвенций в том виде, в каком они сформулированы и существуют на сегодняшний день. Возможно, черно-белая парадигма «либо мир, либо война» действительно не работает в чрезвычайно сложных условиях эпохи Интернета. Приведенная ниже рекомендация совместной экспертной группы предлагает иной подход, по-

1 Дополнительный протокол I, 1949, Статья 1. Женевские конвенции от 12 августа 1949 г. Международный комитет Красного Креста, Женева. http://www.icrc. org/eng/war-and-law/treaties-customary-law/geneva-conventions/index. jsp

зволяющий наметить направление работы на будущее.

России и США, наряду с другими заинтересованными сторонами, было бы целесообразно проанализировать возможность признания «третьего» («иного, чем война») состояния международных отношений для того, чтобы внести ясность в вопрос о применении существующих Конвенций и Протоколов.

Изучение вопроса о признании «третьей» модальности имело бы большую ценность, так как внесло бы необходимую прозрачность и структурированность в чрезвычайно сложную и запутанную дискуссию на эту тему. Даже в случае принятия решения об отказе от признания «третьего» состояния в международно-правовых отношениях, проделанная серьезная работа принесла бы большую пользу: она позволила бы понять причины, заставившие отдать предпочтение двум традиционным модальностям, а также определить границы и критерии отнесения к таковым. Эффективная реализация настоящей рекомендации потребует от заинтересованных кругов, отвечающих за национальную безопасность в России и США, признать, что нынешняя неопределенность в определении кибернетической войны недопустима. Кроме того, Россия, США и другие заинтересованные стороны должны исследовать новые концептуальные подходы к классификации конфликтов и проявить готовность к открытому рассмотрению новых вариантов управления поведенческими нормами в киберпространстве.

НЕМНОГО СТАТИСТИКИ

Приведем несколько цифр, которые характеризуют наше совместное исследование:

5	Разработано пять совместных рекомендаций, направленных на сохранение принципов Женевских и Гаагских конвенций
10	Сделано десять совместных выводов, касающихся законов ведения войны, мер гуманитарной защиты и правил поведения в киберпространстве.
16	Шестнадцать экспертов вошли в состав совместной российско-американской аналитической группы.
30	Для направления аналитической работы и разработки рекомендаций проведено тридцать рабочих совещаний.
79	Выявлено семьдесят девять внутренних факторов риска, связанных с функционированием киберпространства.
754	В ходе работы над проектом проанализировано семьсот пятьдесят четыре статьи из Женевских и Гаагских конвенций.

СОВМЕСТНЫЕ ВЫВОДЫ

Совместная группа сформулировала ряд выводов, в том числе десять основных. Основные выводы выделены особо с учетом их ключевой роли в обосновании совместных рекомендаций. Ниже приводятся краткие формулировки выводов, которые более подробно изложены в Разделе 3:

1. Защищенные и незащищенные объекты критической инфраструктуры тесно переплетены друг с другом в киберпространстве.
2. Обеспеченные защитой гуманитарные критические инфраструктуры не имеют опознавательных знаков, которые указывали бы на наличие у них статуса защищенного объекта.
3. Разграничение военных и гражданских объектов в киберпространстве затруднено.
4. ИКТ могут стать инструментом более полной реализации заложенных в Конвенциях принципов обеспечения гуманитарных нужд.
5. Негосударственные субъекты и индивидуальные пользователи могут стать более сильными игроками в киберпространстве.
6. Кибернетическое оружие имеет качественные отличия по сравнению с обычным, которые не могли быть приняты во внимание при разработке признанных в настоящее время законов ведения военных действий.
7. Военные будут заинтересованы в том, чтобы сохранять кибернетическое оружие в секрете.
8. Сложная структура ИКТ и киберпространства порождает таинственность в представлениях об их природе и возможностях.
9. Кибероперация может быть проведена незаметно, а выявление скрывающегося за ней игрока является проблематичным.
10. Неоднозначность в толковании термина «кибернетическая война» побуждает к поискам нового подхода.

ДАЛЬНЕЙШИЕ ШАГИ

Дальнейшие шаги, предлагаемые для реализации каждой рекомендации, подробно описаны непосредственно после ее изложения (Раздел 4, подраздел «Дальнейшие шаги»).

Предполагается, что такие шаги должны включать привлечение к дискуссии широкого круга заинтересованных сторон и организаций. Институт Восток-Запад, реализующий соответствующие программы, играет и продолжит играть роль стратегической

площадки для формирования между Россией и США доверия по вопросам кибербезопасности. Кроме того, одним из приоритетных направлений деятельности Института является Всемирная инициатива по кибербезопасности (Worldwide Cybersecurity Initiative, сокращенно - WCI). В рамках этой инициативы партнерами ИВЗ являются лидирующие на мировой арене аналитические центры, компании, неправительственные организации и правительства, усилия которых направлены на разработку системы международных соглашений, стандартов, политики и правил (Agreements, Standards, Policies and Regulations, сокращенно - ASPR).

2. Введение

В настоящем разделе излагаются предпосылки, определяется значимость проекта, формулируются задачи, описываются предмет и методология совместного исследования.

2.1 Значение

Анализ последствий принятия международных конвенций о ведении военных действий в киберпространстве с точки зрения защиты критической инфраструктуры имеет чрезвычайно важное значение. Несмотря на то, что определение «критическая» по отношению к инфраструктуре само по себе подчеркивает значимость таковой, в данной публикации приводится краткое обоснование тезиса о важности защиты критической инфраструктуры.

Поддержание *критических инфраструктур* имеет решающее значение для общественного порядка, экономической стабильности и национальной безопасности России, Соединенных Штатов и других развитых стран. Функционирование этих систем необходимо для обеспечения гражданского населения основными средствами к существованию, пригодным для проживания жильем и базовыми социальными услугами. То же самое можно сказать и об обычном деловом обороте, хозяйственной деятельности частных компаний и защите интересов национальной безопасности отдельных государств, - все это немыслимо без опоры на критические инфраструктуры. Определенная подгруппа объектов критической инфраструктуры признана имеющей чисто гуманитарное назначение (см. Таблицу 1).

Следует отметить, что *защита* критической инфраструктуры, будучи важнейшим обязательством со стороны государств, является также делом основополагающей важности для частного сектора, который во многих случаях выступает как собственник инфраструктурных объектов. Существуют две основные причины, объясняющие, почему вопросы защиты критической инфраструктуры

вызывают растущую озабоченность. Во-первых, это резко выросший масштаб последствий любого сбоя в работе инфраструктурных объектов, связанный с постоянно увеличивающейся нагрузкой на таковые со стороны общества.[2] Во-вторых, это стремительное нарастание сложности и мощи инфраструктурных систем, которое затрудняет управление ими и делает их более уязвимыми для рисков, связанных с нарушением нормального функционирования или выходом из строя.[3]

Женевские и Гаагские конвенции о законах и обычаях войны предусматривают крайние меры защиты гражданского населения на случай, когда все другие средства перестанут действовать. Сохранение действенности и применимости принципов, лежащих в основе этих конвенций, имеет огромное значение как для миллиардов людей, ныне живущих на Земле, так и для будущих поколений. Поскольку наш мир переживает крупномасштабный переход к эпохе кибертехнологий, сохранение указанных принципов не произойдет автоматически или путем прямого заимствования. Киберпространство уже сейчас является неотъемлемой частью и важнейшим фактором, оказывающим влияние на все аспекты частной жизни людей, функционирования частного бизнеса и управленческой деятельности государственных органов. В результате упомянутого перехода произошли радикальные и глубокие изменения как в характере самой критической инфраструктуры, так и в приемах и способах ведения войны.

Наконец, тот факт, что данный проект реализован благодаря *сотрудничеству российских и американских экспертов*, придает дополнительный вес сформулированным по его итогам заключениям. Россия и США являются двумя реальными «титанами» в глобальном киберпространстве и при этом имеют общепризнанные различия в культуре, идеологии и интересах. Именно поэтому договоренности, до-

---

2 "Политика Соединенных Штатов направлена на обеспечение того, чтобы (1) любой выход из строя критических инфраструктур США по причине физического повреждения или компьютерного сбоя был явлением как можно более редким, краткосрочным, географически ограниченным по действию, управляемым и минимально пагубным для экономики, сферы социального обслуживания и оказания государственных услуг, равно как и для национальной безопасности Соединенных Штатов." Закон о критической инфраструктуре 2001 г., Закон США о патриотизме, Раздел 1016 (c), 2001. http://www.fincen.gov/statutes_regs/patriot/.

3 "Конгресс делает следующие констатации: (1) Информационная революция трансформировала ведение бизнеса и деятельность правительства, а также инфраструктуру, на которую Соединенные Штаты опираются в целях обеспечения своей обороны и национальной безопасности. (2) Частный бизнес, государство и аппарат, отвечающий за национальную безопасность, находятся в растущей зависимости от тесно связанных друг с другом материальных и информационных компонентов критических инфраструктурных сетей, включая телекоммуникации, энергетику, финансовые услуги, водоснабжение и транспорт." Там же, Раздел 1016 (b).

стигнутые между представляющими эти страны экспертами и практиками, имеют исключительно важное значение.

2.2 Задачи

Перед двусторонней рабочей группой стояли три задачи. Первая предполагала *начало открытого и честного диалога* между экспертами и практиками из обеих стран. Вторая задача, являясь продолжением первой, задумывалась как *углубление понимания* позиций друг друга. Наконец, третья задача состояла в том, чтобы достичь консенсуса по наиболее важным вопросам, что позволило бы в дальнейшем перейти к стадии официальных двусторонних межгосударственных договоренностей, которые могли бы послужить прецедентом для других государств.[4] Из содержания настоящего доклада ясно, что первые две из сформулированных выше задач выполнены. Для выполнения третьей задачи требуется время.[5]

2.3 Предмет

Рамки настоящего исследования лучше всего определяются четырьмя параметрами: i) *стороны – участники проекта*; ii) *охраняемая инфраструктура*; iii) *конкретные международные договоры*; и iv) *средства защиты*.

Стороны – участницы проекта

Исследование было осуществлено экспертами из России и США. Каждый из экспертов является гражданином представляемой им страны и имеет профессиональный опыт, непосредственно связанный с тем или иным аспектом, относящимся к интересам национальной безопасности.

В период реализации проекта, носившего характер общественной инициативы (Track 2), никто из экспертов не являлся действующим сотрудником официальных государственных структур. Руководители обеих экспертных групп периодически информировали о ходе работы соответствующих участников проекта как в Москве, так и в Вашингтоне, округ Колумбия.

Коллективный опыт задействованных в проекте экспертов с многолетней квалификацией включал широкий спектр областей, необходимых для анализа предмета исследования. Это естественные науки, инженерное искусство, военное дело, гуманитарная помощь, право, разработка международной политики, проектирование,

---

4 Речь идет о договорном процессе в рамках официального диалога на межгосударственном уровне (Track 1).

5 На момент публикации настоящего доклада прорабатываются различные планы продолжения диалога и реализации предложенных в нем рекомендаций.

эксплуатация и защита объектов критической инфраструктуры. Важно добавить, что участники в их нынешних ролях представляют интересы как частного сектора, так и государственных институтов, включая военные структуры.

Помимо экспертов, активную роль в осуществлении проекта играли сотрудники Института Восток-Запад, которые выступали в роли доверенных организаторов, нейтральных координаторов, архитекторов рабочего процесса и мобилизаторов ресурсов.[6] Обычный порядок работы ИВЗ по такого рода программам предполагает последующую передачу инициативы официальным государственным каналам и использование достигнутых результатов и наработок в рамках многостороннего процесса, с учетом конкретной специфики.

Охраняемая инфраструктура

Инфраструктура – это имущество, системы, персонал и процедуры, играющие существенную роль в обеспечении общего функционирования общества. Предмет настоящего исследования включает объекты инфраструктуры, имеющие жизненно важное, или *критическое*, значение, носящие *общенациональный* характер и *отвечающие требованиям* Конвенций в отношении особой защиты.

Критическая инфраструктура

Объекты критической инфраструктуры отличаются от других инфраструктурных объектов тем, что их непрерывное функционирование имеет существенное значение для поддержания жизнедеятельности общества, экономической стабильности и устойчивости государственного управления, включая обеспечение национальной безопасности. Несмотря на попытки осуществить международную стандартизацию объектов критической инфраструктуры, существует немало разнообразных перечней, которые зачастую отличаются в разных странах.

Различия между странами могут объясняться как несовпадением концептуальных представлений о критической инфраструктуре, так и страновыми особенностями и традициями. Отнесение того или иного сектора к критической инфраструктуре определяется социально-политическими факторами, а также

6 Персонал ИВЗ выполнял функции нейтральных фасилитаторов. В проекте были задействованы пять сотрудников Института – граждане Армении, Австрии, Австралии, России и США.

Таблица 1. Критические инфраструктуры в России[10] [11] [12] и США[13] [14] [15] [16] [17] [18] [19]

КРИТИЧЕСКИЕ ИНФРАСТРУКТУРЫ		
Российская Федерация	Соединенные Штаты Америки	Примечания
Здравоохранение	Здравоохранение	Гуманитарное назначение
-	Службы экстренной помощи	Гуманитарное назначение
-	Национальные памятники и предметы искусства	Гуманитарное назначение
Сельское хозяйство	Сельское хозяйство и пищевая промышленность	Двойное назначение
Водоснабжение	Водное хозяйство	Двойное назначение
Государственные органы управления	Государственные органы управления	Двойное назначение
Крупнейшие информационные системы	-	Двойное назначение
Информация и телекоммуникации	Информация и телекоммуникации	Двойное назначение
Энергетика	Энергетика	Двойное назначение
Коммунальные услуги, включая системы отопления	-	Двойное назначение
Финансовая и банковская система	Банковское дело и финансы	Двойное назначение
-	Транспорт и перевозка грузов	Двойное назначение
Транспортные системы	-	Двойное назначение
Промышленность	Химическая промышленность, производство, транспортировка и хранение опасных веществ	Двойное назначение
-	Производство жизненно необходимых товаров	Двойное назначение
-	Почта	Двойное назначение
Муниципальные услуги	-	Двойное назначение
Гражданская оборона	-	Двойное назначение
-	Промышленная база оборонных отраслей	Целевая отрасль
Оборона	-	Целевая отрасль

географическими и историческими предпосылками.[7]

В Соединенных Штатах Америки Закон о патриотизме (Patriot Act) 2001 года определил критическую инфраструктуру следующим образом:

> . . . системы и активы, как материальные, так и виртуальные, имеющие жизненно важное значение для США, выход

7 Elgin M. Brunner and Manual Suter, International CIIP Handbook, An Inventory Of 25 National And 7 International Critical Information Infrastructure Protection Policies, Center for Security Studies (CSS) (Zurich:Center For Security Studies,2009). p.529.

> из строя или уничтожение которых имели бы негативные последствия для безопасности, национальной экономической безопасности, состояния здоровья или жизнедеятельности населения, либо для сочетания указанных состояний.[8]

В России не существует аналогичного формализованного определения критической инфраструктуры или защиты критической инфраструктуры, хотя в официальных документах приводятся ссылки на важность определенных российских систем, имеющих важнейшее значение для национальной безопасности, экономической стабильности, системы государственной и социальной защиты населения.[9]

В Таблице 1 приводится список отраслей, отнесенных к критической инфраструктуре в России и в США. Обратите внимание на то, что некоторые обозначенные отрасли используются исключительно в гуманитарных целях, другие – как в гуманитарных, так и в военных целях, но при этом подавляющее большинство секторов имеет двойное назначение.

---

8 Закон США о патриотизме (USA Patriot Act), Раздел 1016 (e), октябрь 2001 г.

9 Brunner, CIIP Handbook, pp. 527-528.

10 Национальная безопасность России. Документы, относящиеся к различным аспектам национальной безопасности России. http://www.scrf.gov.ru/documents/sections/3/.

11 Закон Российской Федерации от 5 марта 1992 г. № 2446-I «О безопасности», с учетом изменений за 1992 – 2007 гг. http://www.scrf.gov.ru/documents/20.html.

12 Стратегия национальной безопасности Российской Федерации до 2020 года, утверждена Приказом Президента Российской Федерации от 12 мая 2009 г. № 537. http://www.scrf.gov.ru/documents/99.html.

13 Указ Президента США от 17 июня 1996 г. № 13010 «О защите критической инфраструктуры» / Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138.

14 Политика Администрации Клинтона по защите критической инфраструктуры: Президентская директива № 63 / White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No.63.

15 Указ Президента США от 8 октября 2001 г. № 13228 «Об учреждении управления внутренней безопасности и совета по внутренней безопасности» / Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, , Federal Register, Vol. 66, No. 196, (October 8, 2001).

16 Закон США о патриотизме 2001 г. (USA PATRIOT Act, 2001). В Законе о внутренней безопасности 2002 г. (Homeland Security Act of 2002) повторяется определение, данное в Законе о патриотизме.

17 Управление внутренней безопасности США. Национальная стратегия внутренней безопасности от 16 июля 2002 г. / U.S. Department of Homeland Security, The National Strategy for Homeland Security, July 16, 2002.

18 Белый дом, Канцелярия Президента США. Национальная стратегия физической защиты критической инфраструктуры и основных активов (февраль 2003 г.) / White House, Executive Office of the President,The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (February, 2003).

Политика на уровне отдельных государств

Предпринятое двусторонней рабочей группой исследование проблем защиты критической инфраструктуры началось с обсуждения двух вариантов подхода: что следует проанализировать прежде всего - влияние политики на уровне отдельного государства на критические инфраструктуры в международном масштабе или влияние международной политики на критические инфраструктуры национального уровня. Первостепенное внимание было уделено международным инфраструктурам, которые были поставлены в центр дискуссии. Этот подход предполагал исследование таких международных инфраструктурных компонентов как сервер доменных имен (DNS) всемирной «паутины», телекоммуникационные спутники, Глобальная инфраструктура подводных коммуникационных кабельных сетей (GUCCI) и других. Проблемы, связанные с GUCCI, были частично решены путем практической реализации рекомендаций, сформулированных в докладе Института инженеров по электротехнике и электронике (IEEE).[20] После продолжительной дискуссии фокус внимания был перенесен на обсуждение влияния международной политики на критические инфраструктуры национального уровня, с учетом, прежде всего, следующих соображений: (a) движение за принятие общепризнанной международной конвенции имело сильные стартовые позиции, (b) ощутимый прогресс в данном направлении отсутствует, и (c) обе стороны понимают необходимость срочно сдвинуть процесс с мертвой точки.[21] Другие области и проблемы остаются потенциальным предметом для последующего совместного анализа.

Установленные критерии

Термин «критическая инфраструктура» в Конвенциях не употребляется. В то же время концепция жизненной важности определенных объектов и

19 Директива Президента США о внутренней безопасности № 7, HSPD-7, от декабря 2003 г. / Homeland Security Presidential Directive 7, HSPD-7, December, 2003.

20 Karl F. Rauscher, Reliability of Global Undersea Communications Cable Infrastructure-The Report, Institute of Electrical and Electronics Engineers (April, 2010), www.ieee-rogucci.org.

21 «Договор о правилах ведения кибернетической войны нужен незамедлительно, иначе будет слишком поздно» - таков ответ 71% участников Всемирного саммита по кибербезопасности, проведенного в Далласе (США) Институтом Восток-Запад 6 мая 2010 г. / A 'Treaty on Cyber Warfare' is needed now or is overdue" – response of 71% of participants, Participant Summary Results, Proceedings of the First Worldwide Cybersecurity Summit, Dallas, EWI,(May 6,2010).

персонала для решения гражданских и гуманитарных задач прослеживается в целом ряде статей. Исторически сложилось так, что Конвенциями были предусмотрены строгие критерии, которым должны соответствовать объекты и персонал для того, чтобы подпадать под охрану, а именно:[22]

- «составлять лишь небольшую части территории…»;
- «по сравнению с количеством населения, которое они могут вместить, они должны быть слабо заселены»;
- «находиться вдали от всяких военных объектов и каких бы то ни было крупных промышленных или административных учреждений»;
- «не должны находиться в районах, которые, по всей вероятности, смогут иметь значение для ведения войны»;
- «пути сообщения и транспортные средства… не должны быть использованы для перевозки войск или военных материалов»;
- «ни при каких обстоятельствах их не будут защищать военными средствами»;
- должны быть «обозначены красным крестом (красным полумесяцем, красным львом и солнцем)…»;
- «должны быть приняты все необходимые меры к тому, чтобы щадить… храмы, здания, служащие целям науки, искусств и благотворительности, исторические памятники, госпитали и места, где собраны больные и раненые, под условием, чтобы таковые здания и места не служили одновременно военным целям»;
- «подводные кабели, соединяющие занятую территорию с территорией нейтральной...».

Более подробный анализ соответствия инфраструктур установленным критериям приводится в Разделе 3 «Системный анализ».

Международные соглашения

Из общего числа существующих договоров, конвенций и соглашений, составляющих в совокупности так называемое «право войны», был отобран ряд документов, которые составили предмет более детального анализа. Критерием отбора являлось наличие в том или ином документе положений о защите гражданского населения и гражданских объектов. Совместная рабочая группа ввела и использует в настоящем докладе термин «Конвенции»

22 См., например: Женевская конвенция от 12 августа 1949 года о защите гражданского населения во время войны (Женевская конвенция IV), Приложение I, Статьи 1-13, Гаагская конвенция о законах и обычаях войны 1907 г. (Гаагская конвенция IV), Статьи 27-28, 54.

Таблица 2. Краткая характеристика Женевских и Гаагских конвенций

Документ	Название	Дата	Кол-во статей	Кол-во слов (англ. яз.)
Женевская конвенция	Об улучшении участи раненых на поле боя	1864 г.	10	660
Гаагская конференция II	О законах и обычаях сухопутной войны	1899 г.	60 (55 в прилож.)	3 960
Гаагская конференция IV	О законах и обычаях сухопутной войны	1907 г.	64 (56 в прилож.)	4 330
Женевский протокол	О запрещении применения на войне удушливых, ядовитых и иных подобных газов и бактериологических средств	1925 г.	-	400
Женевская конвенция I	Об улучшении участи раненых и больных в действующих армиях	1864 г., н.ред. - 1949 г.	77 (13 в прилож.)	8 600
Женевская конвенция II	Об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из составе вооруженных сил на море	1949 г.	63	6 795
Женевская конвенция III	Об обращении с военнопленными	1929 г., н.ред. – 1949 г.	143	20 246
Женевская конвенция IV	О защите гражданского населения во время войны	1949 г.	180 (21 в прилож.)	21 373
Женевская конвенция	О запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении	1975 г.	15	1 700
Протокол I	Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов	1977 г.	102	21 779
Протокол II	Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв вооруженных конфликтов немеждународного характера	1977 г.	28	3 376
Протокол III	Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся принятия дополнительной отличительной эмблемы	2005 г.	17	1 934

применительно к упомянутым отобранным документам. Предмет коллективного анализа включает статьи из Женевских и Гаагских конвенций, которые перечислены ниже:

- Женевская конвенция (1864 г.)
- Гаагская конвенция II (1899 г.)
- Гаагская конвенция IV (1907 г.)
- Женевский протокол (1925 г.)
- Женевская конвенция I (1949 г.)

- Женевская конвенция II (1949 г.)
- Женевская конвенция III (1949 г.)
- Женевская конвенция IV (1949 г.)
- Конвенция о биологическом оружии (1975 г.)[23]
- Дополнительный протокол I (1977 г.)
- Дополнительный протокол II (1977 г.)
- Дополнительный протокол III (2005 г.)

Некоторые из указанных конвенций были включены в предмет анализа постольку, поскольку они посвящены запрещенным видам оружия, которые могли бы пагубно повлиять на человеческую составляющую критической гуманитарной инфраструктуры (например, Женевские конвенции/протоколы 1925 и 1975 гг.).

Четвертая Женевская конвенция 1949 г. («Женевская конвенция IV») устанавливает особые требования к обращению с гражданскими лицами во время войны. В основном, речь идет о конкретных классах гражданских лиц, однако предусматривается определенный объем защиты и в отношении гражданского населения в целом. Дополнительный протокол № I 1977 г. («Дополнительный протокол № I») к Женевским конвенциям содержит более широкий спектр мер по защите гражданских лиц, включая детально проработанные положения о запрете нанесения ударов по гражданскому населению. Женевская конвенция IV и Дополнительный протокол № I были ратифицированы многими странами мира и применимы ко «всем случаям объявленной войны или любых других вооруженных конфликтов, которые могут возникнуть между двумя или большим числом Высоких договаривающихся сторон, даже в том случае, если состояние войны не признается одной из них».

Статья 51(4) Дополнительного протокола I запрещает сторонам конфликта наносить удары без выбора цели, то есть удары, которые: не нацелены на конкретные военные объекты; наносятся методом или с использованием боевых средств, которые

23 Полное название: Конвенция о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении.

Таблица 3. Перечень основных статей Конвенций о защите гражданского населения и гуманитарных ценностей

Документ	Номера статей	Кол-во статей
Женевская конвенция 1864 г.	10	10
Гаагская конференция II 1899 г.	27-28, 55-56	4
Гаагская конференция IV 1907 г.	27-28, 54-56	5
Женевский протокол 1925 г.	-	-
Женевская конвенция I 1949 г.	19 – 44, 1 – 13 в Приложении I	58
Женевская конвенция II 1949 г.	22 - 45	44
Женевская конвенция III 1949 г.	-	0
Женевская конвенция IV 1949 г.	1 – 26, в Приложении: 1 – 8	34
Женевская конвенция 1975 г.	15	15
Протокол I 1977 г.	1 – 34, 48 - 79	70
Протокол II 1977 г.	1 - 28	28
Протокол III 2005 г.	1 - 17	17

не позволяют нанести целенаправленный удар по конкретному военному объекту; либо наносятся методом или с использованием боевых средств, последствия применения которых не могут быть ограничены, как то требуется Дополнительным протоколом № I, и которые, следовательно, относятся к категории поражающих военные цели, гражданское население и гражданские объекты без разграничения. Статья 51(4) может быть сочтена резервным средством защиты, поскольку нанесение нецеленаправленных ударов, согласно определению, скорее всего приведет к нарушению других правил, установленных Дополнительным протоколом № I.[24]

Конвенции, о которых идет речь, включают 759 статей чрезвычайно насыщенного содержания, для передачи которого использовано всего лишь немногим более 93 200 слов. Многие статьи повторяют друг друга, излагая

24 Tania Voon, “Pointing The Finger: Civilian Casualties Of NATO Bombing In The Kosovo Conflict”, American University International Law Review, , Vol. 16, No.4, April, 2001, pp. 1091- 1095.

одни и те же принципы, но в разном контексте.

Эксперты в составе рабочей группы согласились с тем, что, выражаясь самым простым и понятным языком, критериями отнесения определенных видов инфраструктуры к «критическим», или жизненно важным, является их существенная роль в обеспечении сохранения жизни людей, экономической стабильности и национальной безопасности, с акцентом на сохранность человеческих жизней как на первоочередной приоритет. Хотя в Женевских и Гаагских конвенциях не используется термин «защита критической инфраструктуры», в них прямо говорится о безопасности человеческой жизни, в частности, в тех разделах Женевских конвенций, в которых речь идет об обращении с лицами, не участвующими в боевых действиях, т.е. с гражданским населением.[25]

В Таблице 3 приводится перечень статей из Конвенций, общим числом 295, которые были использованы как первоисточники при проведении настоящего исследования.

Средства защиты

В ходе нашего исследования была проанализирована типология средств защиты, предоставляемых Конвенциями как в настоящее время, так и потенциально в будущем. Положения Конвенций требуют исключения охраняемых лиц и инфраструктуры из «объектов нападения» и предусматривают, что они «будут во всякое время пользоваться уважением и покровительством».[26] Существуют также положения о предоставлении «соответствующего предупреждения» в случае, если предполагается, что покровительство перестанет действовать.[27] Транспортным средствам, отвечающим определенным критериям, должно предоставляться право «свободного пропуска».[28]

Средства защиты, предусмотренные для определенных категорий персонала и объектов, перестают действовать в том случае, если действие или использование таковых выходит за рамки строго установленных параметров.[29]

Несмотря на то,
что международное

25 См.: Женевская конвенция от 12 августа 1949 года о защите гражданского населения во время войны. (Женевская конвенция IV). Женева. 1949. http://www.un.org/ru/documents/decl_conv/conventions/geneva_civilian.shtml / Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 1949. http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp.

26 Женевская конвенция от 12 августа 1949 года о защите гражданского населения во время войны (Женевская конвенция IV), Статьи 18, 22.

27 Там же. Статья 19.

28 Там же. Статья 23.

29 Женевская конвенция 1864 года, Статьи 1-3, 27; Гаагская конвенция IV 1907 года, Статьи 27-28, 54; Женевская конвенция IV 1949 года, Статьи 15, 19.

гуманитарное право требует защиты гражданских лиц от прямого нападения, «за исключением тех случаев и периодов, когда они принимают непосредственное участие в военных действиях», ни Женевские конвенции, ни Дополнительные протоколы к ним не указывают, какая именно деятельность представляет собой прямое участие в военных действиях. Для исправления этой ситуации и защиты гражданского населения от ошибочных или случайных ударов, Международный комитет Красного Креста предпринял ряд неформальных исследований и консультаций с целью выяснения трех ключевых вопросов: (1) Кто считается гражданским лицом с точки зрения ведения военных действий? (2) Какая деятельность приравнивается к прямому участию в военных действиях? (3) В каких ситуациях с гражданских лиц может быть снята защита от прямого удара?[30]

Здесь следует заметить, что термин «защита критической инфраструктуры» часто используется правительствами, владельцами предприятий в частном секторе и операторами для обозначения проводимых ими мероприятий. Такого рода меры защиты обычно реализуются проектировщиками инфраструктурных объектов и поставщиками инфраструктурных услуг для местных государственных органов.

2.4 Принципы, положенные в основу исследования

Ниже перечисляется ряд важнейших принципов, которые были положены в основу совместного исследования.

Единая команда

Российские и американские участники совместного проекта составляли единую команду, перед которой стояла задача найти ответы на существую-

30 Nils Melzer, “Clarifying The Notion of Direct Participation in Hostilities- Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law”, Geneva, ICRC Legal Reference Document, June, 2009. http://www.icrc.org/eng/resources/documents/feature/direct-participation-ihl-feature-020609.htm.

щие в киберпространстве вызовы, связанные с внедрением новейших технических разработок. Стремясь к достижению единства в позициях как основы для консенсуса, эксперты-участники совместной группы в ряде случаев сочли наиболее оптимальным сформулировать и обосновать различия в своих позициях.

Неформальный характер диалога

Инициированный нами диалог во имя сотрудничества направляется и поддерживается неправительственными организациями. Основным местом работы большинства экспертов является либо компания частного сектора, либо академическое учреждение. Обе стороны периодически информировали заинтересованных лиц – представителей государственных структур как в Москве, так и в Вашингтоне, округ Колумбия.

Четыре комбинации

В результате совместного исследования были выделены четыре различные комбинации, которые требуют одновременного управления в процессе применения Конвенций на современном этапе. Эти комбинации более подробно проанализированы в Разделе 3 (Схема 1). Речь идет о:

- традиционных видах вооружений, нацеленных на критические объекты традиционной инфраструктуры;
- традиционных видах вооружений, нацеленных на сетевые критические инфраструктуры;
- кибернетическом оружии, нацеленном на критические объекты традиционной инфраструктуры;
- кибернетическом оружии, нацеленном на сетевые критические инфраструктуры.

Передовые методы анализа

Оценка поля и потенциала киберпространства и определение направления и возможностей будущего сотрудничества потребовали применения передовых технических методов анализа. Эти методы включают использование так называемой «восьмикомпонентной модели» (8i Framework) применительно к информационно-коммуникационным технологиям (ИКТ) и подхода, основанного на идентификации факторов внутренней уязвимости (Intrinsic Vulnerability).

3. Системный анализ

В этом разделе представлены заключения, к которым пришла российско-американская группа экспертов в результате совместного исследования. Предпринятый анализ предполагал изучение последствий применения в условиях киберпространства зафиксированных в Женевских и Гаагских конвенциях принципов защиты гуманитарных ценностей и людей в соответствии с установленными критериями с целью: (a) понять, ведет ли и, если да, то к каким проблемам ведет сохранение старых, высоко почитаемых гуманитарных принципов, лежащих в основе так называемого «права войны»; (b) выделить те аспекты ИКТ, которые потенциально могли бы способствовать продвижению принципов Женевских конвенций; и (c) определить вопросы, требующие дополнительного анализа.

Экспертная группа выделила четыре различные комбинации, которые требуют одновременного управления в процессе применения на современном этапе принципов, заложенных

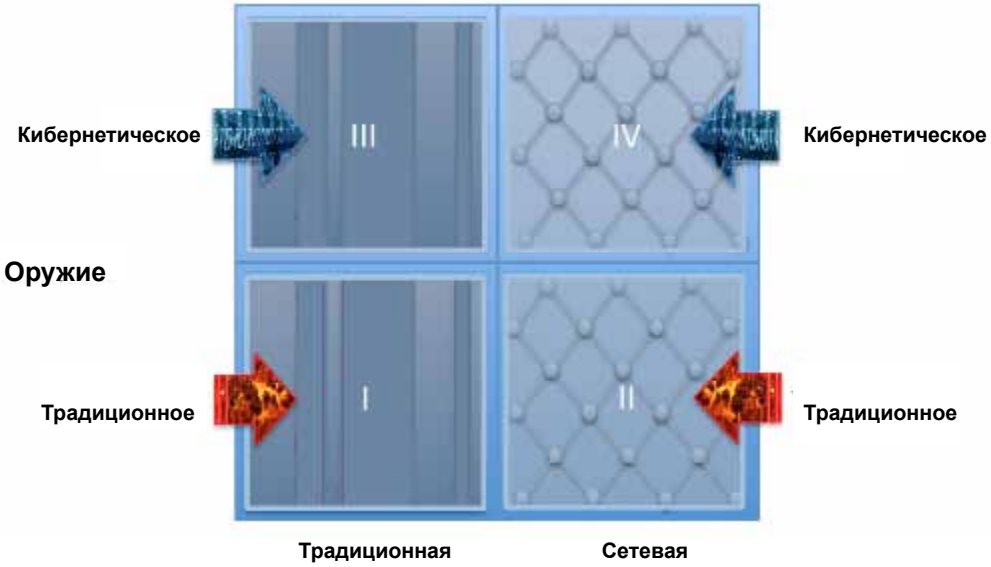


Схема 1. Четыре комбинации, описывающие варианты применения «права войны» в киберпространстве

Конвенциями.[31] В основе этих четырех комбинаций лежат два параметра – *тип инфраструктуры* и *тип оружия*. Ниже приведена Схема 1, отражающая в наглядном виде различные сочетания указанных параметров.

Приведенная выше схема призвана облегчить понимание и управление четырьмя различными комбинациями, а именно:

I. *традиционные* виды вооружений, нацеленные на критические объекты *традиционной* инфраструктуры;

II. *традиционные* виды вооружений, нацеленные на *сетевые* критические инфраструктуры;

III. *кибернетическое* оружие, нацеленное на критические объекты *традиционной* инфраструктуры;

IV. *кибернетическое* оружие, нацеленное на *сетевые* критические инфраструктуры.

Типологизация инфраструктур

В целях настоящего анализа примем, что две предложенные категории инфраструктуры взаимно исключают друг друга. Хотя различия представляют собой, главным образом, дифференциацию между сменяющими друг друга поколениями, существуют специфические характеристики, характерные и для того, и для другого типа. Традиционные инфраструктуры существовали до возникновения Интернета и продолжают существовать в виде широко распространенной матрицы разветвленных связующих каналов, а сетевые инфраструктуры олицетворяют собой нынешнее состояние современных систем. Переход от одной стадии к другой проходил постепенно, однако с точки зрения настоящего исследования детализация этого процесса не представляется необходимой.[32] Мы признаем, что в сегодняшнем мире сосуществуют оба типа инфраструктур, но при этом констатируем, что доминирующая глобальная тенденция заключается в том, что экономическое развитие сопровождается активным внедрением сетевых инфраструктур.

Основные отличительные характеристики двух типов инфраструктур перечислены ниже. Кроме того, для каждого типа приводится несколько примеров, которые служат иллюстрациями.

---

31 Термин «комбинация» (“dispensation”) используется в настоящем докладе, потому что он означает категорию, которая, имея четкие отличия, одновременно несет в себе идею смежности, а также потому что для такой категории характерен особый свод правил, которыми она должна регулироваться.

32 Авторы признают чрезвычайную сложность процесса смены генераций. Тем не менее, обсуждение деталей этого процесса выходит за рамки настоящей дискуссии. Характерные для переходного периода гибриды могут быть усовершенствованы и доведены до уровня соответствия критериям нового поколения технических средств.

- *Традиционные критические инфраструктуры* характеризуются тем, что:
  - наблюдение и контроль за ними в ходе эксплуатации осуществляются людьми;
  - люди управляют связями между различными инфраструктурными объектами;
  - масштабы применения таковых сокращаются.

Примерами традиционных критических инфраструктур могут служить электростанции и распределительные сети, управляемые, главным образом, на основании прогнозов, больницы, в которых документация ведется в бумажном виде, а возможности оказания квалифицированной медицинской помощи ограничиваются имеющимся на месте персоналом, основанные на приблизительных оценках логистические системы управления грузоперевозками, финансовые рынки, оперирующие с бумажными документами, авиадиспетчерские службы, осуществляющие ручную координацию движения на базе радиосвязи и получаемой с радаров информации.

- *Сетевые критические инфраструктуры* характеризуются следующими параметрами:
  - контроль за операционной деятельностью осуществляется с помощью программного обеспечения в режиме реального времени (например, с применением систем искусственного интеллекта);
  - связи между различными инфраструктурными объектами носят чрезвычайно взаимозависимый и сложный характер;
  - масштабы применения таковых возрастают;
  - играют более значимую роль в жизнеобеспечении гражданского населения, особенно на территориях городов.

В качестве примеров сетевых критических инфраструктур можно привести энергосистемы, управляемые в режиме реального времени интеллектуальными устройствами с обратной связью, больницы, использующие электронные медицинские карты с неограниченными возможностями доступа к базам данным и консультациям специалистов на расстоянии, управление товарно-материальными запасами в синхронном режиме посредством радиочастотной идентификации (RFID) упаковок, электронные системы, позволяющие осуществлять финансовые расчеты день в день, а также различные автоматизированные системы управления воздушным движением.

Здесь уместен следующий вопрос: *«Лучше или хуже сетевые критические инфраструктуры в сравнении с*

Схема 2. Восьмикомпонентная модель (8i) [36]

традиционными системами, на смену которым они пришли?». С точки зрения повседневного опыта, наиболее доступного каждому из нас (повседневная жизнь, бизнес-операции, государственное управление и т.д.), ответ однозначный: *«лучше!»*. Сетевые инфраструктуры помогают нам делать больше и при этом тратить меньше времени и усилий.

К счастью, принципы, сформулированные в конвенциях о войне, не затрагивают большинство из нас напрямую. Использование ИКТ может способствовать более строгому соблюдению конвенций,[33] но при этом возникают новые проблемы, которые необходимо решать.

Каждая из различных характеристик, сформулированных выше, является прямым или косвенным результатом внедрения ИКТ. Здесь уместно рассмотреть «восьмикомпонентную модель», которая позволяет представить полную картину, включающую как ИКТ, так и менее технически продвинутые элементы киберпространства (Схема 2). «Восьмикомпонентная модель» может использоваться для систематизированного анализа имманентных факторов уязвимости, или рисков, связанных с каждым из включенных в нее элементов.[34] В отличие от уравнения с таким количеством переменных факторов, которое делает ряд их возможных пермутаций практически бесконечным, количество рисков, присущих каждому из восьми упомянутых компонентов, а следовательно и всей киберпространственной системе сетевых критических инфраструктур в целом, является конечным.[35]

33 См. Раздел 3.5, Совместный вывод 4.

34 Karl F. Rauscher et al. Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security, Bell Labs Technical Journal Homeland Security Special Issue, Vol. 9, No. 2, April, 2006.

35 См.: Appendix G, Next Generation Networks Report, The President's National Security Telecommunications Advisory Committee (NSTAC),(March, 28, 2006),

36 ATIS Telecom Glossary; Bernando Rancho, *Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop*,; Karl F. Rauscher., *Protecting Communications Infrastructure*, Bell Labs Technical Journal, Special Issue: Homeland, Security, Vol. 9, No. 2, July, 2004; *Next Generation Networks Task Force Report,* The President's National Security Telecommunications Advisory Committee,(March 28, 2006), Background and Charge*; Annual Report 2002*, ATIS Network Reliability Steering Committee (NRSC).

Типологизация вооружений

В целях настоящего анализа примем, что две используемые нами в этом тексте категории взаимно исключают друг друга. Первая относится к вооружениям, существовавшим на момент написания конвенций, а вторая обозначает новейшие типы вооружений, которые появляются сегодня и в которых применяются ИКТ. Как и в случае с трансформацией инфраструктур, переход от одной стадии к другой не был дискретным. Хотя в настоящее время существуют оба типа вооружений, основное внимание уделяется разработкам, представляющим собой последнее слово науки и техники, которые являются либо усовершенствованными вариантами традиционных видов оружия, либо совершенно новыми моделями, основанными на использовании кибернетических возможностей.[37]

Ниже приводятся основные характеристики, отличающие два обозначенных выше типа вооружений, а также служащие иллюстрациями примеры.

- *Традиционные вооружения* характеризуются следующими параметрами:[38]
  - использование физической силы (включая кинетическую энергию, энергию электромагнитных полей и ядерную энергию), боевых биологических средств или химических отравляющих веществ;
  - непосредственная цель – физический объект;
  - спроектированы, как правило, для использования в вооруженном конфликте;
  - доступ к новейшим разработкам чрезвычайно ограничен;
  - наиболее распространенные базовые модели относительно недороги, а

37 « Киберкомандование США (USCYBERCOM) планирует, координирует, интегрирует, синхронизирует и осуществляет деятельность по управлению работой и защите определенных информационных сетей министерства обороны, готовит и, в случае поступления приказа, проводит полномасштабные военные кибероперации в целях обеспечения США и их союзникам свободы действий в киберпространстве и возможности проводить операции во всех областях, а также лишения такой возможности наших противников.» Министерство обороны США. Информационный бюллетень Киберкомандования США (25 мая 2010 г.) / U.S. Department of Defense U.S. Cyber Command Fact Sheet, (May, 25 2010).

38 Важно отметить, что традиционные виды вооружений в настоящее время активно совершенствуются с применением ИКТ, что позволяет переводить их на дистанционное управление и в автоматизированный режим, внедрять системы поддержки принятия решений, повышать точность, наращивать функциональные возможности и т.д. Существующие гибридные системы по своим характеристикам могут быть приближены к разработкам новейшего поколения.

самые современные стоят чрезвычайно дорого.

Примерами традиционных вооружений являются огнестрельное оружие, гранаты, бомбы, артиллерия, ядерные ракеты и т.п.

- Отличительные черты *кибернетического оружия*:
  - использование логических схем;
  - цель – информация или контроль;
  - системы часто имеют приложения гражданского назначения;
  - порог доступа низкий и продолжает снижаться;
  - может быть относительно дешевым.[39]

К кибернетическому оружию, используемому для нанесения ударов в киберпространстве, могут быть отнесены компьютерные «черви», вирусы, системы ручного дистанционного контроля и программы для перехвата вводимой с клавиатуры информации. Примерами традиционных видов вооружений, которые могут быть усилены с помощью ИКТ, могут служить системы наведения на базе GPS, летательные аппараты с дистанционным управлением, сетевые системы, включающие солдат и боевую технику.

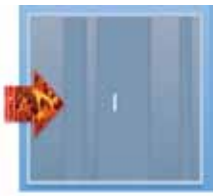
Для того чтобы быть эффективным, кибероружие должно быть способным находить и использовать в своих целях присущие информационно-коммуникационным технологиям уязвимые стороны. В этом контексте может быть снова конструктивно применена «восьмикомпонентная модель», поскольку она предлагает систематизированный подход к анализу факторов внутренней уязвимости, используемых кибероружием для нанесения поражающего удара (Схема 2). Полный спектр кибернетического оружия включает все виды оружия, способные использовать факторы внутренней уязвимости.

3.1 Комбинация I. Традиционные виды вооружений и традиционные инфраструктуры

Эта комбинация соответствует ситуации, существовавшей в период подготовки нового варианта конвенции 1949 года, которая именно тогда была в последний раз существенным образом обновлена. Архитектура критических инфраструктурных связей, характер взаимозависимостей и опора

39 «Однако есть одна большая разница между [ядерным и кибернетическим оружием]. Кибернетическое оружие очень дешево, почти бесплатно». Владислав Шерстюк. Цит. в переводе с английского языка по: David Talbot, Russia's Cyber Security Plans, MIT Technology Review Blog, http://www.technologyreview.com/blog/editors/25050/, (posted April 16, 2010).

на ручное управление указывают на то, что речь идет о системах прошлого поколения. Следует также обратить внимание на то, что включенные в данную комбинацию вооружения основаны на принципе передаче энергии для импульсного толчка.



Примерами разрушающих воздействий внутри данной комбинации могут служить следующие:

- движущаяся бронированная машина (например, танк) обстреливает снарядами большого калибра нефтеперерабатывающий завод;
- с подводной лодки производится пуск торпеды для потопления корабля;
- реактивный бомбардировщик наносит удар по взлетно-посадочной полосе аэродрома.

Совместная группа экспертов пришла к выводу, что Женевские и Гаагские конвенции напрямую применимы к Комбинации I в том виде, в каком они были задуманы первоначально. В данном случае положения указанных конвенций могут служить непосредственной основой для решения вопросов, вызывающих обеспокоенность в связи с защитой критической инфраструктуры.

3.2 Комбинация II. Традиционные виды вооружений и сетевые инфраструктуры

Данная комбинация напоминает ситуацию 1949 года с точки зрения типов вооружений, которые в нее входят, но отличается тем, что включенные в нее критические инфраструктуры объединены в сеть, то есть характеризуются интенсивной взаимозависимостью, автоматизированным контролем и высокой степенью сложности.

Примеры использования оружия в рамках рассматриваемой комбинации:

- реактивный гранатомет обстреливает снарядами большого калибра антенную мачту, передающую сигналы мобильной связи;
- десантный корабль-амфибия с экипажем штурмует и уничтожает подводную станцию по укладке кабеля с использованием стрелкового оружия и взрывчатки;

- реактивный бомбардировщик наносит удар по узлу «интеллектуальной» связи.

Сетевая инфраструктура включает все физические компоненты традиционной инфраструктуры, плюс такие новейшие продукты как программное обеспечение. Следует подчеркнуть, что кибернетические составляющие, которые могут поражаться традиционными видами оружия, представляют собой не отдельные элементы, а *среду*, включающую сетевое оборудование, силовые агрегаты и распределительное оборудование, электронные устройства и комплексы, сами сети и обслуживающий персонал. Программное обеспечение, информационное наполнение, договоры, стандарты, принципы и правила не являются физическими целями и, следовательно, если и могут быть повреждены традиционными видами оружия, то скорее косвенно, а не напрямую.

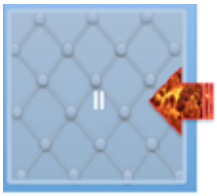
С точки зрения эффективного управления такой средой нельзя не признать, что последствия выведения из строя критической инфраструктуры в настоящее время гораздо сильнее влияют на другие системы, приводя к их каскадному отключению, с большей вероятностью наносят вред гражданскому населению и приводят к хаосу.[40]

40 Существуют и другие факторы риска, которые могут еще более осложнить работу системы, например, в случае отсутствия доступа к другим системам.

Можно сказать, что из-за сложного характера взаимодействия между компонентами критических инфраструктур возрастает вероятность того, что некоторые виды аварий, повреждений или их последствия могут быть неизвестны даже тем обществам, которые наиболее далеко продвинулись по пути планирования.

При всех многочисленных разговорах о кибероружии, *не следует* забывать о существующем арсенале обычных вооружений. Нет сомнения в том, что запасы вооружений будут пускаться в ход и пополняться. На сегодняшний день обычное оружие, особенно адресно направленное, имеет более широкий спектр целей.

Совместные выводы 1 – 4 имеют ключевое значение с точки зрения управления указанной комбинацией (Раздел 3.5). В первых трех речь идет о возможности отличить защищенные объекты от незащищенных. Четвертый вывод констатирует наличие многочисленных преимуществ использования ИКТ в связи с практической реализацией принципов, заложенных в Конвенциях.



3.3 Комбинация III. Кибернетическое оружие и критические объекты традиционной инфраструктуры

Комбинация III схожа с ситуацией 1949 года с точки зрения типов инфраструктур, являющихся объектом нападения, но *отличается* от нее использованием кибернетического оружия. Отметим, что поскольку мишенью в этой схеме является традиционная, а не интегрированная в киберпространстве инфраструктура, мы имеем здесь дело, в основном, с оружием, *приводимым в действие с помощью ИКТ*.

Примеры операций, совершаемых в рамках данной комбинации:

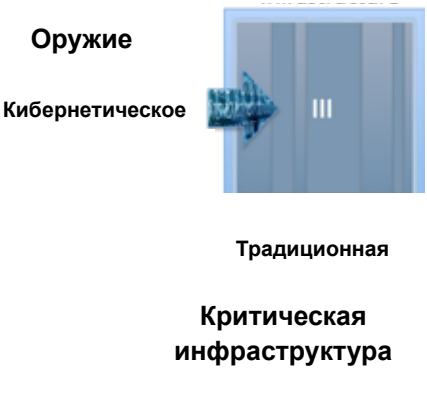
- ракета, направляемая с помощью глобальной навигационной системы GPS, наносит удар по транспортному узлу;
- боевой солдат, оснащенный оборудованием сетевого доступа, атакует двигающуюся цель при помощи передаваемого через спутник видеосигнала;
- телепилотируемый летательный аппарат (беспилотный самолет) передает морской артиллерии координаты боевой машины пехоты для нанесения удара.

Обратите внимание на то, что инфраструктурные компоненты традиционных информационно-коммуникационных систем не включают такие новейшие продукты, как, например, программное обеспечение. Такие системы могут быть физически поражены традиционными видами оружия, усиленными с помощью ИКТ. Это связано с тем, что упомянутые виды оружия работают, главным образом, на кинетическом принципе. Мишенью является *среда*, которая включает *сетевое оборудование*, оборудование для *выработки и распределения* электроэнергии, *электронную аппаратуру*, *сети* и операционный *персонал*. Вместе с тем, любое усиленное с помощью ИКТ оружие уязвимо со стороны каждого из восьми компонентов.

Однако при умелом управлении такой средой эффективность, объемы и операционная сложность арсенала вооружений могут быть значительно увеличены. В случае поступления команды о нанесении «хирургического» удара, значительно увеличивается точность попадания в цель.

Совместные выводы 4 – 6 и 10 имеют ключевое значение для управления указанной комбинацией (Раздел 3.5). Четвертый вывод признает, что использование ИКТ позволяет более эффективно применять принципы Конвенций. Так, например, результаты анализа свидетельствуют о наличии реального потенциала повышения ответственности за правильное приня-

тие и исполнение решений благодаря совершенно новым возможностям отличать разрешенные и запрещенные цели. Пятый вывод акцентирует внимание на усилении статусной защиты физических лиц и некоторых организаций. Логично было бы предположить, что доступность новейших видов оружия, усиленных за счет ИКТ, будет возрастать. В выводах 6 и 7 речь идет о том, что хотя специфические виды новейшего оружия могут быть засекречены на законных основаниях, все параметры, делающие их эффективными, основываются на точной научной информации из открытых источников. Наконец, в выводе 10 сформулировано важное замечание о том, что введение оружия, использующего ИКТ, осложнило историческое понимание вооруженного конфликта. Это соображение более подробно развито в разделе, посвященном Комбинации IV.



3.4 Комбинация IV. Кибернетическое оружие и сетевые критические инфраструктуры

Предмет анализа в данном разделе представляет собой область пересечения кибернетического оружия и кибернетических целей. Это почва для создания многих новых видов оружия, появление которых в настоящее время можно только предполагать. Аналогичным образом, судя по очевидной тенденции усиления роли ИКТ в обществе, бизнесе, государственном управлении и армии, количество целей будет увеличиваться экспоненциально. Контроль над этой сферой представляется жизненно важным для тех государств, которые стремятся к сохранению своего военного превосходства.

Примеры разрушающих взаимодействий в рамках Комбинации IV:

- небольшая международная группа, действующая в интересах определенных лиц, применяет вредоносное пакетированное программное приложение с целью искажения данных в компьютерной сети, используемой правительством;
- государство, в котором зарегистрирован широко известный поставщик сетевого коммуникационного оборудования, активирует скрытые

программные возможности, что приводит к сбою и многодневной нестабильности в работе оборудования в стране, являющейся объектом удара;

- тщательно подготовленное, невыявляемое вторжение в системы управления боевой операцией приводит к хаотичному изменению координат и данных о местонахождении персонала, в результате чего огонь обрушивается на свои или дружественные подразделения.

В рамках Комбинации IV все восемь компонентов киберпространства уязвимы для кибероружия, которое, в свою очередь, может быть поражено каждым из упомянутых восьми компонентов.

Помимо других вопросов, вызывающих обеспокоенность, участвующие в управлении этой средой профессионалы признают, что данная область, имеющая колоссальное коммерческое и стратегическое значение, находится в стадии формирования и нуждается в выработке «правил игры», а также то, что критические инфраструктуры подвергаются все большему риску по мере распространения кибернетических видов оружия и роста зависимости общества от ИКТ как источника многочисленных благ.

Для понимания Комбинации IV и управления ею важны все десять Совместных выводов. Здесь более подробно анализируются те выводы, которые ранее не обсуждались в разделах 3.1 – 3.3. Вывод 3 отражает общую обеспокоенность сторон в связи с трудностями различения целей, подпадающих под защиту Конвенций, и целей, по которым разрешается наносить легитимные удары. В выводе 8 констатируется, что, несмотря на высокую степень сложности, быстроту изменений и наличие других факторов, которые делают киберпространство недоступным для всеобъемлющего понимания, существуют также фундаментальные научные, инженерные и математические ограничители и правила, которые могут быть более активно использованы для управления этой средой. Наконец, вывод 9 обращает внимание на то, что киберсобытие может произойти таким образом, что пострадавшая сторона не узнает о нем в момент происшествия, а, возможно, и вообще никогда не узнает.

3.5 Совместные выводы

Следующие десять выводов были выбраны из общего числа выводов, сделанных по итогам исследования. Они были сформулированы в результате анализа статей законов о ведении военных действий и различий между описанными выше комбинациями.

Совместный вывод 1: Защищенные и незащищенные объекты критической инфраструктуры тесно переплетены друг с другом в киберпространстве.

Принятие этого вывода является важным шагом для сохранения заложенных Конвенциями принципов о защите гражданского населения. Объекты, пользующиеся защитой, окажутся лишенными таковой, если пострадают в результате нанесения удара по незащищенным объектам. Речь идет о сопряженном ущербе как одном из последствий военных действий, относительно которого имеется давно сложившееся понимание. Однако масштаб сопряженного ущерба (включающего функциональные сбои в работе оборудования) в настоящее время может оказаться значительно больше.

В первую очередь, необходимо сказать о принципе защиты в том виде, в каком он заложен в Конвенциях. Предусмотрены, по крайней мере, четыре различные области защиты гражданского населения и критической инфраструктуры гражданского назначения:[41]

Защита населения: Конвенции устанавливают принцип защиты «всего населения находящихся в конфликте стран…»[42]

Защита отдельных территорий: Конвенции обеспечивают сторонам возможность создавать «на своей собственной территории, а в случае необходимости на оккупированных территориях санитарные и безопасные зоны и местности, организованные таким образом, чтобы оградить от действий войны [далее перечислены категории гражданского населения, пользующиеся покровительством, – прим. пер.]…».[43] «Гражданские больницы… не могут ни при каких обстоятельствах быть объектом нападения, но будут во всякое время пользоваться уважением и покровительством...».[44]

---

41 Хотя это следует из контекста, Конвенции тем не менее разъясняют, что «... военные объекты, крупные промышленные или административные учреждения» являются легитимными целями. Женевская конвенция об улучшении участи раненых и больных в действующих армиях (Женевская конвенция I). Приложение 1, Статья 4.

42 Женевская конвенция IV О защите гражданского населения во время войны.. Статья 13.

43 Женевская конвенция IV. Статья 14.

44 Женевская конвенция IV. Статья 18.

Таблица 4. Краткое изложение совместных выводов

Совместный вывод	Комбинация				Компонент							
	I	II	III	IV	Окруж. среда	Энергия	Тех. средства	Программ. обеспеч-е	Сеть	Контент	Человек	ASPR
1. Защищенные и незащищенные объекты критической инфраструктуры тесно переплетены друг с другом в киберпространстве.		II		IV								
2. Обеспеченные защитой гуманитарные критические инфраструктуры не имеют опознавательных знаков, которые указывали бы на наличие у них статуса защищенного объекта.		II		IV								
3. Разграничение военных и гражданских объектов в киберпространстве затруднено.				IV								
4. ИКТ могут стать инструментом более полной реализации заложенных в Конвенциях принципов обеспечения гуманитарных нужд.	I	II	III	IV								
5. Негосударственные субъекты и индивидуальные пользователи могут стать более сильными игроками в киберпространстве.			III	IV								
6. Кибернетическое оружие имеет качественные отличия по сравнению с обычным, которые не могли быть приняты во внимание при разработке признанных в настоящее время законов ведения военных действий.			III	IV								
7. Военные будут заинтересованы в том, чтобы сохранять кибернетическое оружие в секрете.			III	IV								
8. Сложная структура ИКТ и киберпространства порождает таинственность в представлениях об их природе и возможностях.		II		IV								
9. Кибероперация может быть проведена незаметно, а выявление скрывающегося за ней игрока является проблематичным.				IV								
10. Неоднозначность в толковании термина «кибернетическая война» побуждает к поискам нового подхода.												

Защита персонала: Конвенции предусматривают защиту для «лиц, занимающихся систематически и исключительно обслуживанием и администрацией гражданских больниц …».[45]

Защита инфраструктур: Конвенции требуют «уважения и покровительства»[46] в отношении различных транспортных средств, используемых в гуманитарных целях. «Запрещается наносить

45 Женевская конвенция IV. Статья 20.

46 Женевская конвенция IV. Статьи 21, 22.

> удары, уничтожать, перемещать или выводить из строя объекты, без которых невозможно выживание гражданского населения, в частности, объекты, обеспечивающие население продуктами питания, сельскохозяйственные районы, где производятся продукты питания, выращиваются зерновые культуры и скот, сооружения, снабжающие население питьевой водой, запасы питьевой воды, ирригационные сооружения, с конкретной целью лишить возможности пользоваться таковыми, по причине их существенного значения для жизнеобеспечения, гражданское население или сторону противника, независимо от мотивации, как в целях принуждения населения к голоданию или к перемещению с занимаемой территории, так и в любых других целях».[47]

Во-вторых, мы видим, что Конвенции налагают на участников обязательство по разграничению объектов. В контексте 1949 года речь шла о физическом разграничении.

> **Разграничение**: Конвенции предписывают, чтобы пользующиеся покровительством объекты «располагались по возможности дальше...» от потенциальных военных целей.[48]

Существует огромное количество комментариев относительно толкования и применения процитированных выше статей. Однако здесь важно не углубляться в детали, а констатировать наличие определенных мер защиты, установленных в законодательном порядке.

Для осуществления своих базовых функций современные жизненно важные инфраструктуры, отличающиеся чрезвычайно высокой степенью *взаимо*зависимости, требуют снабжения электричеством и наличия работающих коммуникационных сетей. Современные общества утратили способность выживать без указанных ресурсов. Проблема стоит особо остро для урбанизированных районов, которые отличаются в этом смысле повышенной уязвимостью. Положение еще более усложняется в связи с распространением системы управления материальными запасами в режиме реального времени.

Современные больницы представляют собой учреждения с высокой степенью сетевой интеграции, зависящие от телемедицины и непрерывного получения из географически удаленных мест информации, которая в большинстве случаев хранится в

47 Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов (Протокол I), ст. 54.

48 Женевская конвенция IV. Статья 18.

информационных центрах, концентрирующих также данные, относящиеся к промышленности и управлению, а, возможно, и к оборонной отрасли. Поддержание работоспособности такого учреждения требует защиты информации и коммуникационных инфраструктурных связей. В этих условиях сфера действия запрета на нанесение удара существенно расширяется (этому способствуют распределенная система обработки и хранения данных, совмещение и другие факторы), что значительно усложняет соблюдение требований Конвенций.[49] Введение разграничений оказалось бы, по всей вероятности, чрезвычайно затратным, а, кроме того, шло бы вразрез с нынешними тенденциями развития инфраструктурной архитектуры, которые предполагают использование распределенных емкостей памяти и циклов компьютерной обработки данных, в зависимости от наличия свободных мощностей на тот или иной момент времени.[50]

Рекомендация 1 содержит предложение относительно пути решения этой проблемы (Раздел 4).

Совместный вывод 2: Охраняемые гуманитарные критические инфраструктуры не имеют опознавательных знаков, которые указывали бы на наличие у них статуса защищенного объекта.

Конвенции устанавливают, что пользующиеся покровительством *объекты* «будут обозначаться эмблемой...»[51] и что отличительные эмблемы должны быть «отчетливо видны».[52] Кроме того, предусматривается, что обеспеченный защитой *персонал* будет отличаться ношением повязки, которая «будет снабжена эмблемой, предусмотренной [далее приводится ссылка на соответствующую статью Женевской конвенции 1949 года об улучшении участи раненых и больных в действующих армиях – прим. пер.]».[53] Наконец, Конвенции определяют, что различные транспортные средства должны «быть обозначены отличительной эмблемой …".[54]

Современная медицинская информация зачастую создается в электронной форме и хранится, либо

49 Обратим внимание в этой связи на следующее требование Статьи 4 Приложения 1 к Женевской конвенции I: «Санитарные и безопасные зоны должны отвечать следующим условиям: (c) они должны находиться вдали от всяких военных объектов и каких бы то ни было крупных промышленных или административных учреждений». [Выделение авторов доклада].

50 Такая система обработки и хранения сетевой информации по-английски называется 'cloud computing' («облачные компьютерные технологии»).

51 Женевская конвенция IV. Статья 18.

52 Там же. Статья 18.

53 Там же. Статья 20.

54 Там же. Статьи 21, 22.

передается через киберпространство. Такая информация включает медицинские карты пациентов, источники, используемые в исследовательской и аналитической работе, средства и системы контроля и данные по счетам. Указанные ресурсы, хотя и носят гуманитарный характер, редко отделяются от других, незащищенных инфраструктурных компонентов. Может быть выдвинут резонный аргумент о том, что защита обеспечивается только в связи с оказанием базовой медицинской помощи, а настаивать на расширении покровительства для всей современной медицины было бы чрезмерным требованием, выходящим за границы Конвенций. Однако подход, положенный в основу Конвенций, признает «растущие требования цивилизации» и «постоянно развивающиеся требования цивилизации».[55] [56]

Предложение по совместной работе в этой связи сформулировано в Рекомендации 2 (Раздел 4).

Совместный вывод 3: Разграничение военных и гражданских объектов в киберпространстве затруднено.

Эта констатация базируется на Совместных выводах 1 и 2. Она имеет существенное значение, поскольку избирательность и различение цели является важным обязательством атакующей стороны.[57] «Одно из существующих ограничений Международного гуманитарного права (МГП), которое можно считать применимым к киберпространству, относится к обязанности атакующей стороны обнаруживать военные цели».[58]

> Для обеспечения уважения и защиты гражданского населения и гражданских объектов, Стороны, находящиеся в конфликте, должны всегда проводить различие между гражданским населением и комбатантами, а также между гражданскими объектами и военными целями и соответственно направлять свои действия только против военных целей.[59]

55 Гаагская конвенция II 1899 года. Преамбула.

56 Гаагская конвенция IV 1907 года. Преамбула.

57 На принятие решения о нападении влияют четыре фактора, а именно: различение цели, необходимость, пропорциональность и отвага. См.: part III.Thomas C. Wingfield, The Law of Information Conflict: National Security Law in Cyberspace (Falls Church: Aegis Research, 2000).

58 Дополнительные правила включают, среди прочего, запрет на нанесение ударов без выбора цели и требование минимизации сопряженного ущерба для гражданского населения и объектов. Knut Durmann, “Computer Network Attack and International Humanitarian Law”, 19-05-2001 Cambridge Review of International Affairs “Internet, State and Security Forum”,Cambridge, May, 2001.

59 Дополнительный протокол I к Женевским конвенциям от 12 августа 1949 года. Женева, 1977 год. Статья 48.

Конвенциями предусматривается, что владелец того или иного объекта или имущества обязан маркировать свою собственность. Это положение учтено в Рекомендациях 1 и 2 (Раздел 4).

Совместный вывод 4: ИКТ могут стать инструментом более полной реализации заложенных в Конвенциях принципов обеспечения гуманитарных нужд.

ИКТ могут также помочь в практической реализации различных требований, сформулированных в Конвенциях. Примерами служит использование ИКТ для поиска и обнаружения людей, поддержания коммуникации между членами семьи, обеспечения базовых культурных, образовательных и духовных потребностей людей.

> Находящиеся в конфликте стороны будут принимать необходимые меры, чтобы дети до 15 лет, осиротевшие или разлученные со своими семьями вследствие войны, не были предоставлены самим себе, и чтобы облегчить при всех обстоятельствах их содержание, выполнение обязанностей, связанных с их религией, и их воспитание. Их воспитание, если это возможно, будет поручено людям тех же культурных традиций.[60]
>
> Кроме того, они будут стараться принимать необходимые меры, чтобы личность всех детей до 12 лет могла быть установлена путем ношения опознавательного медальона или любым другим способом.[61]
>
> Каждое лицо, находящееся на территории состоящей в конфликте стороны или на оккупированной ею территории, сможет сообщать членам своей семьи, где бы они ни находились, а также получать от них сведения чисто семейного характера. Эта переписка должна будет пересылаться быстро и без промедления, не вызываемого необходимостью.[62]

Другие преимущества включают предоставленные военнопленным права на удовлетворение духовных потребностей и поддержание связей с семьей. Положительными сторонами

60 Женевская конвенция IV от 12 августа 1949 года. Статья 24.

61 Там же.

62 Там же. Статья 25.

применения ИКТ в гуманитарных критических инфраструктурах, равно как и в других областях, являются эффективность, скорость, повышение степени контроля за соблюдением правовых норм, более высокое качество предлагаемых продуктов и услуг. Появление школ, работающих в режиме «он-лайн», демонстрирует новые возможности удовлетворения образовательных потребностей молодежи благодаря виртуальной коммуникации через Интернет.

Совместный вывод 5: Негосударственные субъекты и индивидуальные пользователи могут стать более сильными игроками в киберпространстве.

Уровень технической квалификации и финансового обеспечения, необходимый для обладания новейшим арсеналом традиционных вооружений, очень высок. Способность достичь этого уровня отчасти определяла и продолжает определять принадлежность к сверхдержавам. Однако сегодня прежняя, основанная на силе глобальная архитектура, как и многие другие сферы, претерпевает революционные изменения под воздействием ИКТ. Дело в том, что в настоящее время «источником киберугроз является широкий диапазон различных групп и индивидов с различными навыками, мотивами и целями».[63] «Мы сталкиваемся с государствами, террористическими сетями, организованными преступными группами, физическими лицами и другими участниками киберпространства, обладающими различными возможностями доступа, техническими знаниями и квалификацией, и имеющими различные намерения».[64] Суровая реальность, на которую правительства не могут закрывать глаза, состоит в том, что негосударственные игроки, или участники киберпроцесса (Non-State Actors), и даже обычные люди получили возможность использовать компьютеры, созданные для применения в невоенных целях, против государств.[65]

Новая ситуация породила серьезные и разнообразные по своему характеру вызовы. К их числу относятся, в частности, следующие: проблема отсутствия опознавательных знаков, делающая невозможным отличить участников боевых действий в форме от комбатантов, не одетых в форму; отсутствие необходимой компьютерной подготовки для населения в целом; огромное, исчисляемое миллиардами,

63 Robert, S. Mueller, III, Federal Bureau of Investigation (FBI) Director Statement Before the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, DC, (March 17, 2010).

64 Dennis C. Blair, Director of National Intelligence Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, Washington DC, (February 2, 2010).

количество компьютеров и их «онлайн» пользователей; асимметричный характер отношений между участниками конфликта применительно к масштабам грозящих сторонам потерь.

На основе анализа этих вызовов сформулирована Рекомендация 3.

Совместный вывод 6: Кибернетическое оружие имеет качественные отличия по сравнению с обычным, которые не могли быть приняты во внимание при разработке признанных в настоящее время законов ведения военных действий.

Кибернетическое оружие нацелено, главным образом, на информацию, логические связи и контроль. В сравнении с традиционными видами вооружений, кибероружие может показаться экстремальным по своим характеристикам, поскольку оно: (a) может быть за считанные секунды доставлено в любую точку планеты; (b) распространяется подобно вирусам; (c) обладает искусственным интеллектом, позволяющим носителям обучаться и адаптироваться; (d) может быть произведено достаточно дешевым способом; и (e) может быть копировано и передано. Когда речь идет о средствах нанесения удара, все эти характеристики представляются чем-то фантастическим, но это не более чем поверхностное впечатление. Те же самые технические свойства ИКТ и коммуникационных сетей используются нами ежедневно как в частной

65 Никаких общепринятых в международном сообществе определений негосударственных субъектов (Non-State Actors) или неправительственных организаций (Non-Governmental Organizations) не существует. В результате любая организация, не являющаяся межправительственной (Intergovernmental Organization), считается негосударственным субъектом. Вместе с тем, Комитет по негосударственным субъектам в международном праве Ассоциации международного права разработал рабочее определение, позволяющее структурировать различные виды таких субъектов. (The Hague Conference: First Report of the Committee on Non-State Actors in International Law: Aims, Approach and Scope of Project and Legal Issues, International Law Association, The Hague, 2010.) Были установлены три критерия, позволяющие судить о возможности или невозможности отнесения того или иного лица к числу негосударственных субъектов: (1) структуры, состоящие из представителей государств, управляемые или контролируемые государствами или группами государств, такие как межправительственные организации или объединения государств типа Группы 7, были исключены из определения негосударственных субъектов; (2) было констатировано, что отнесение к негосударственным субъектам может быть осуществлено только на основании анализа фактически осуществляемой ими деятельности и их поведения; и (3) было предложено считать негосударственными субъектами международного права те лица, деятельность которых на международной арене имеет реальное или потенциальное влияние на международное право. Из числа негосударственных субъектов были прямо исключены мафия, Аль-Каида и пиратские сообщества по причине преступного характера деятельности всех этих группировок.

жизни, так и на работе. Все дело в разнице целеполагания. Направленность на уничтожение делает ИКТ инструментом ведения боевых действий.

Конвенции уже давно создали прецедент законодательного запрета в отношении оружия массового поражения. В частности, примерами средств поражения, объявленных вне закона, являются химическое и биологическое оружие. Они были «справедливо осуждены цивилизованным миром» и запрещены международным правом.[66] [67] Совместная группа экспертов пришла к выводу о том, что исследование характеристик кибернетического оружия было бы чрезвычайно полезной работой.

Рекомендация 4 основана на вышеизложенном выводе.

Совместный вывод 7. Военные будут заинтересованы в том, чтобы сохранять кибернетическое оружие в секрете.

Видовое разнообразие кибероружия, по всей вероятности, значительно вырастет в ближайшем будущем. Государства, разрабатывающие самые современные средства поражения, чрезвычайно заинтересованы в защите информации, относящейся к таким техническим средствам. Это дает им такие преимущества, как способность нанести внезапный удар по противнику, которому ничего неизвестно о таких возможностях, либо скрыть источник или замаскировать фактический характер нападения, либо своевременно укрепить собственную оборону исходя из понимания сути возможной атаки.

Рекомендация 4 сформулирована с учетом данной проблематики.

Совместный вывод 8: Сложная структура ИКТ и киберпространства порождает таинственность и домыслы в представлениях об их природе и возможностях.

ИКТ-системы настолько сложны, что это делает их непрозрачными во всех практических смыслах. Кроме того, подлинное овладение этими технологиями требует очень серьезного профессионального образования в области физики, электротехники, математики и компьютерного программирования. Среди высшей государственной элиты, отвечающей за принятие политических решений, слишком мало людей, обладающих такими специальными знаниями, что порождает дискуссии относительно

66 Женевский протокол О запрещении применения на войне удушливых, ядовитых и иных подобных газов и бактериологических средств , 1925 г.

67 Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении (Конвенция о запрещении химического оружия), 1992 г.

непонятных аспектов или озабоченность из-за невозможности опираться на известные базовые установки. У нас сформировалось представление о компьютерах как о «магических черных ящиках», которые содержат внутри себя нечто нам неведомое и при этом непонятным способом выдают определенный продукт после введения в них конкретных данных. Внимание средств массовой информации, разведки, военных и даже бизнес-сообщества сфокусировано, в основном, на связанных с ИКТ угрозах. В результате учащаются случаи, когда разрабатываются и принимаются такие влияющие на киберпространство политические решения, которые основаны на рецикруляции фактов и далеко не первичной информации. Научное и инженерное сообщество обладает тем преимуществом, что понимает, из чего состоит критическая инфраструктура и как устроены ее компоненты, и, следовательно, может видеть, в чем состоит внутренняя уязвимость отдельных частей.[68] Для продвижения в этом направлении важно объединить знания и квалификацию экспертов в самых разных областях, имеющих отношение к ИКТ.

68 Karl F. Rauscher et al. Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security, Bell Labs Technical Journal Homeland Security Special Issue, Vol. 9, No. 2, April, 2006.

Этот вывод включен в Рекомендацию 4.

Совместный вывод 9: Кибероперация может быть проведена незаметно, а выявление скрывающегося за ней игрока является проблематичным.

Как Вы узнаете о том, что замеченное Вами действие является кибероперацией? Атаки или другие манипуляции в киберпространстве могут осуществляться незаметно. Понимание того, что произошло, может прийти с опозданием или вообще никогда не прийти. К тому же, последствия кибероперациий могут развиваться по каскадному сценарию, с приобретением значимости на второй или третьей стадии, причем взаимосвязь между событиями первого и последующего порядков может быть неизвестна.

Аналогичным образом, встает вопрос о том, как узнать, кто инициировал нападение. Вариабельность заголовков сообщений, способность маскировать источники информации и ряд других факторов делают фундаментально проблематичным до-

стижение абсолютной уверенности в происхождении нанесенного удара.[69]

Совместный вывод 10: Неоднозначность в толковании термина «кибернетическая война» побуждает к поискам нового подхода.

Очень важно внести ясность в вопрос об условиях применения Конвенций к киберконфликту. В настоящее время существует широкая палитра мнений относительно того, что считать кибервойной. Примерами двойственного понимания одних и тех же реальностей служат приведенные ниже цитаты.

Еще одним пунктом разногласий, помимо острой дискуссии по вопросу о реальности или нереальности кибервойны в настоящее время и в будущем, является тема последствий кибератаки.[70] [71] [72] Анализ этих противоречий может быть полезен для выработки первоначальных определений и формирования понимания в отношении наиболее адекватного способа оценки новой формы агрессии и оружия.

> Кибернетическая война никогда не имела четкого определения и никогда не подпадала ни под какие взаимно согласованные между государствами международные

69 Для государств, находящихся под подозрением, применяются разные градации степени ответственности и возможности контроля со стороны государства. Shackelford, Scott, J., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, Conference on Cyber Conflict Proceedings, Tallinn, 2010.

70 «В США и ряде стран Запада сегодня бытует мнение, что угроза «информационных войн», а главное, масштабность и последствия применения «информационного оружия» ... сильно преувеличиваются.». - И.Н.Дылевский, С.А. Комов, С.В.Коротков, С.Н,Родионов, А.В.Федоров. Военная политика Российской Федерации в области обеспечения международной информационной безопасности. (2006) // Международная информационная безопасность: дипломатия мира. Сборник материалов. / Под общ.ред. д.в.н., проф. С.А. Комова. - Москва, 2009, стр. 42

71 «Кибервойна – это реальность. То, что мы пока что видим, не сопоставимо с тем, что можно было бы сделать». Ричард Кларк (Richard Clarke). Cyber War – The Next Threat to National Security and What to do about it, (New York: Harper Collins Publishers, 2010), p. 21.

72 «Именно тема ведения военных действий, тема кибервойны, должна быть поставлена в центр нашего самого пристального внимания, поскольку она несет в себе разрушительный потенциал». Адмирал Майк Маллен (Mike Mullen), председатель Объединенного комитета начальников штабов США. Цит. по: Lalit Kha Jha, “Cyberwarfare has devastating potential: Mullen”, MSN News (January 13, 2011), http://news.in.msn.com/international/article.aspx?cp-documentid=4797248.

Схема 3. Контрасты между взглядами на кибервойну*

* На схеме представлены выдержки из следующих цитат:

[вверху слева] Продолжение цитаты: «. . . Я думаю, что это жуткая метафора, и полагаю, что это убийственная идея. В этой среде нет победителей». Говард Шмидт (Howard Schmidt), цит. по: Ryan Singel, “White House Cyber Czar: There is no Cyber War”, Wired Magazine, March 4 2009. http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/.

[вверху справа] Продолжение цитаты: «… и мы проигрываем. Все очень просто. Являясь самой продвинутой страной на Земле с точки зрения сетевых коммуникаций, мы ассоциируемся с большей частью значимых целей. При этом наши средства кибернетической обороны удручающе неразвиты». Майк МакКоннел (Mike McConnell), бывший директор национального разведывательного управления. Washington Post, 28 февраля 2010 г.

[внизу слева] Peter Sommer and Ian Brown, “Reducing Systemic Cybersecurity Risk”, OECD-IFP Project on “Future Global Shocks”, (January 14, 2011). http://www.oecd.org/dataoecd/57/44/46889922.pdf

[внизу справа] Продолжение цитаты: «… которое может буквально парализовать всю страну». Леон Панетта (Leon Panetta), директор ЦРУ. Цит. по: The New New Internet – The Cyber Frontier, (April 21, 2010), http://www.thenewnewinternet.com/2010/04/21/panetta-warns-cyber-attack-could-be-next-pearl-harbor/. Ниже приводится еще одна цитата на ту же тему, принадлежащая Шону Генри (Shawn Henry), помощнику директора киберуправления ФБР: «Помимо угрозы, связанной с применением ядерного устройства или иного разрушительного оружия, самая критическая угроза, с которой мы столкнулись, - это угроза всей нашей инфраструктуре, нашей информации, нашей компьютерной сети». «Террористические группы работают над созданием виртуальной катастрофы, аналогичной 11 сентября, которая повлекла бы за собой такой же ущерб для нашей страны, для всех стран, для всех наших сетей, как и таран зданий самолетами». Цит. по: Homeland Security Newswire,(January 6, 2009). http://homelandsecuritynewswire.com/fbi-us-facing-cybergeddon.

конвенции. Между тем, кибервойна, неся в себе громадный побудительный потенциал, может стать причиной колоссального ущерба для вовлеченных государств. Отношение к нападающей стороне зачастую бывает снисходительным по причине отсутствия международного сотрудничества и юрисдикции. Примером может служить история с «титановым дождем».[73]

73 Maya Tao,”Law Brief on Cyberwarfare”, The Maya Tao Blog, http://mayatao.com/wp-content/uploads/2010/11/Law-Brief-on-Cyber-Warfare.pdf, (accessed, January 21, 2011).

Эксперт по международному праву из Международного комитета Красного креста указал на то, что «если атаки на компьютерные сети используются против противника с целью нанесения ущерба, вряд ли можно оспаривать тот факт, что такие атаки являются по сути способом ведения военных действий».[74] Возможно, существующие парадигмы мира, войны, саботажа, терроризма и преступления следовало бы расширить.

Рекомендация 5 представляет собой совместную рекомендацию экспертной группы на эту тему.

74 Knut Dörmann, "Computer Network Attack and International Humanitarian Law", 19-05-2001 Cambridge Review of International Affairs "Internet, State and Security Forum",Cambridge.May, 2001.

4. Совместные рекомендации

В настоящем докладе сформулированы пять совместных рекомендаций. Каждая из них имеет решающее значение для сохранения принципов охраны критической инфраструктуры гуманитарного назначения, которые лежат в основе Конвенций. Каждая рекомендация носит практический характер и, в случае реализации, будет эффективно способствовать преодолению ныне существующих препятствий. Эксперты, представляющие обе стороны, настаивают на скорейшем рассмотрении и принятии мер на основании каждой из сформулированных рекомендаций.

«Законы о войне» неоднократно пересматривались с течением времени. К сожалению, история свидетельствует о том, что таким изменениям предшествовали вероломные действия народов друг против друга. За осуждением подобных действий со стороны «общественного мнения цивилизованного мира» последовало введение положения о необходимости «сообразовываться с постоянно развивающиеся требованиями цивилизации».[75] [76] Каждая из предлагаемых нами рекомендаций направлена на то, чтобы согласовать концепции развития современной сетевой критической

75 Женевский протокол *О запрещении применения на войне удушливых, ядовитых и иных подобных газов и бактериологических средств*, 1925 г.

76 Гаагская конвенция II, 1899 г., Преамбула.

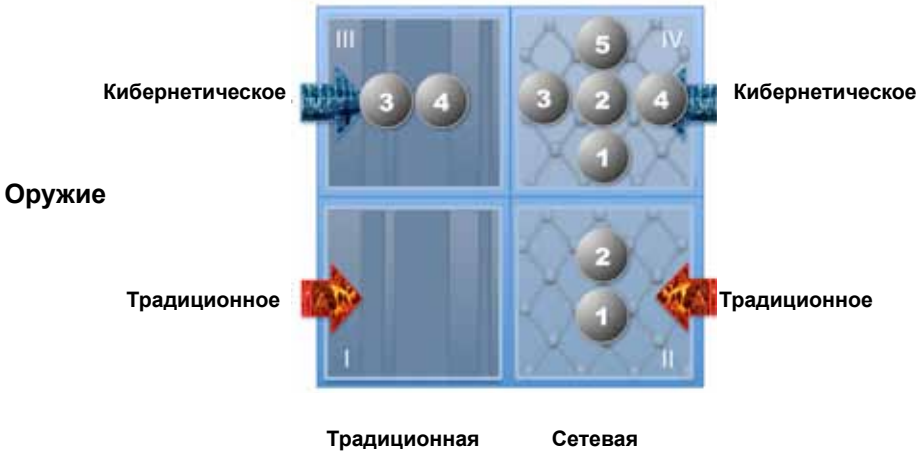


Схема 4. Применение рекомендаций

инфраструктуры с принципами, заявленными в Женевских и Гаагских конвенциях и Протоколах.

Рекомендации, более подробно изложенные ниже, применимы к четырем комбинациям, как показано на Схеме 4. Каждая из рекомендаций предлагает решение конкретных проблем, вызывающих наибольшую обеспокоенность в рамках проанализированных комбинаций.

Практическое применение наших рекомендаций потребует лидирующей роли и содействия со стороны государства, частного сектора и неправительственных организаций (НПО). Таблица 5 отражает объем и распределение потребностей в поддержке со стороны руководящих государственных структур и в источниках экспертных знаний. Следует заметить, что во многих случаях первостепенные роли принадлежат не государству, а частному бизнесу и НПО, что может вызвать удивление у тех, кто привык считать выполнение правительствами руководящих функций делом естественным и само собой разумеющимся. В данном случае речь идет о частно-государственном партнерстве при лидиру-

ющей роли частного сектора.[77] Это важный акцент, на который следует обратить внимание ввиду концентрации в частных компаниях новейших экспертных и операционных знаний, а также собственности на ИКТ и ИКТ-инфраструктуры.

Каждая рекомендация представлена в сжатой форме и направлена на то, чтобы поддержать процесс принятия принципиальных решений, сохранить импульс, возникший при работе над докладом, и мобилизовать ресурсы для конкретных действий. План изложения каждой рекомендации структурирован следующим образом:

- **Титульная формулировка** приводится в целях идентификации, как и краткое резюме.
- **Общая информация** позволяет понять основные элементы контекста обсуждаемого вопроса.
- **Рекомендация** определяет, кому и что именно следует делать.
- **Раздел «Что нужно сделать»** в общем виде очерчивает, какие обязательства должны быть взяты на себя основными участниками для достижения успеха.
- **Практическая польза** характеризует значение и ценность применения рекомендации на практике.
- **Альтернативы и их последствия** содержат описание других вариантов и вероятных последствий их осуществления.
- **Дальнейшие шаги** излагают предложения по поддержанию заданного импульса и фокусировки.
- **Критерии успеха** описывают механизм объективной оценки результативности.

77 Термин обозначается английской аббревиатурой PPP и используется для смыслового выделения лидерских позиций частного сектора. Впервые был введен автором в оборот в программном докладе, подготовленном для Конференции министров Европейского Союза по вопросам защиты критической информационной инфраструктуры, Таллин, 27-28 апреля 2009 г. (the European Union Ministerial Conference on Critical Information Infrastructure Protection).

Таблица 5. Источники лидерских компетенций и экспертной поддержки для реализации рекомендаций

	Лидерство			Экспертиза		
Рекомендация	Государство	Частный сектор	НПО	Государство	Частный сектор	НПО
1. Выяснение степени переплетения защищенных и незащищенных критических инфраструктур в киберпространстве	Роль поддержки	Основная роль	Основная роль	Роль поддержки	Основная роль	Основная роль
2. Применение в киберпространстве женевской концепции опознавательной эмблематики	Основная роль	Роль поддержки	Основная роль	Роль поддержки	Основная роль	Основная роль
3. Признание роли негосударственных игроков и пользователей сети	Основная роль	Роль поддержки	Основная роль	Основная роль	Основная роль	Основная роль
4. Анализ принципов Женевского протокола применительно к кибернетическому оружию	Основная роль	Роль поддержки	Роль поддержки	Основная роль	Основная роль	Роль поддержки
5. Изучение «третьего» («иного, чем война») состояния международных отношений.	Основная роль	Роль поддержки	Основная роль	Основная роль	Основная роль	Роль поддержки

Основная роль | Роль поддержки

4.1 Выделение охраняемых объектов в киберпространстве

Общая информация

Женевские конвенции предусматривают определенные меры защиты для объектов чисто гуманитарного назначения и обслуживающего их персонала, при определенных условиях, в военное время.[78] Однако в киберпространстве защищенные и незащищенные объекты часто настолько переплетены, что это подвергает защищенные объекты опасности.[79]

Ситуация с охраняемыми объектами достаточно понятна. Преимущества применения ИКТ носят конкретный,

78 Женевская конвенция от 12 августа 1949 года о защите гражданского населения во время войны (Женевская конвенция IV), Статьи 13, 14, 18, 20-22, 54.

79 См.: Совместный вывод 1 (Защищенные и незащищенные объекты критической инфраструктуры тесно переплетены друг с другом в киберпространстве), Раздел 3.2. Существует огромное количество комментариев относительно применения тех статей Конвенций, на которые приведена ссылка. Наша задача в этой связи заключается не в том, чтобы делать какие-либо заключения, а в том, чтобы установить, что Конвенциями предусмотрены определенные меры защиты.

материальный характер. Они включают значительное расширение возможностей, повышение эффективности и снижение затрат. В условиях, когда в общественном сознании господствует мировоззрение мира, происходит быстрое развитие технологий, а среда отличается высокой степенью конкуренции, неудивительно наблюдать отсутствие целенаправленного планирования мер по обеспечению эквивалентной защиты, соответствующей требованиям «права войны».

До настоящего времени эта тема подвергалась анализу, в основном, в связи с обсуждением проблем национальной безопасности внутри отдельных государств. Данная рекомендация выводит ее на межгосударственный уровень, создавая импульс для совместной работы, сначала в контексте двустороннего взаимодействия, а в последующем – на многосторонней основе.

Рекомендация 1 прямо ставит вопрос о наличии взаимозависимостей и сложных переплетений в киберпространстве как о характерном свойстве как Комбинации II, так и Комбинации IV (Раздел 3, Схема 1).

Рекомендация 1

России и США, наряду с другими заинтересованными сторонами, следует проанализировать, в какой степени защищенные критические инфраструктуры гуманитарного назначения в настоящее время переплетены с незащищенными инфраструктурами, с тем, чтобы определить, являются ли имеющиеся в Конвенциях и Протоколах формулировки достаточными, и возможно ли на практике осуществить выделение критических гуманитарных инфраструктурных объектов.

Что нужно сделать

Для эффективного выполнения данной рекомендации необходимо следующее:

- Компании частного сектора из обеих стран должны поделиться своими техническими знаниями и деловым опытом.
- Российские и американские государственные структуры должны поддержать сотрудничество, выделив для

участия в нем соответствующих экспертов.[80] [81]

- Международные неправительственные организации, занимающиеся гуманитарной помощью, должны внести свой концептуальный вклад в совместную работу.
- Каждая из указанных сторон должна проявить готовность к объективному анализу и исследованию имеющихся вариантов.

Альтернативы и их последствия

Альтернативами предложенному подходу могут быть следующие:

- Ничего не делать . . . В этом случае уровень защиты для гражданского населения, предусмотренный Женевскими и Гаагскими конвенциями, будет снижаться.
- Сознательно ждать, пока пройдет время и мы чему-либо научимся на уроках первых произошедших трагедий. Затем принять на себя ответственность за полученный результат, который может включать неприемлемые потери человеческих жизней и нанесение непоправимого вреда имуществу.
- Признать невозможность перенесения принципов Конвенций в киберпространство, что будет означать отсутствие гуманитарной защиты в период конфликта.

Практическая польза

Позитивным результатом осуществления этой рекомендации будет выработка двустороннего или многостороннего заключения о том, являются ли предусмотренные Конвенциями

---

80 "Основными задачами военной политики в области обеспечения международной информационной безопасности будут следующие: ... создание условий для равноправного и безопасного международного информационного обмена на основе общепризнанных норм и принципов международного права ... " - И.Н.Дылевский, С.А. Комов, С.В.Коротков, С.Н,Родионов, А.В.Федоров. Военная политика Российской Федерации в области обеспечения международной информационной безопасности. (2006) // Международная информационная безопасность: дипломатия мира. Сборник материалов. / Под общ.ред. д.в.н., проф. С.А. Комова. - Москва, 2009. (стр. 43).

81 "… укрепить наши международные партнерские отношения с целью создания инициатив, покрывающих весь спектр видов деятельности, политики и возможностей, связанных с кибербезопасностью." – Пункт 7 Краткосрочного плана действий, Белый Дом, Исполнительный аппарат Президента США, Обзор политики в области кибербезопасности – Обеспечение пользующейся доверием и жизнеспособной информационно-коммуникационной инфраструктуры (29 мая 2009 г.) (Point 7 of Near-Term Action Plan, White House, Executive Office of the President, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure (May 29, 2009)),http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

средства защиты гуманитарных объектов по-прежнему действенными, либо потерявшими существенную долю своей эффективности, с возможностью восстановления таковой или безвозвратно, исходя из существующих тенденций в киберпространстве. Это заключение будет способствовать сохранению зафиксированных в Конвенциях принципов, которые охраняют жизненно важные гуманитарные интересы, в том числе пользующееся защитой гражданское население и имущество, и, следовательно, являются важнейшей частью критической инфраструктуры. Наконец, сохранение в силе способности отличать охраняемые территории может иметь неоценимое значение хотя бы потому, что невозможно в количественных параметрах измерить ценность человеческой жизни. Кроме того, поставленные задачи включают охрану других гуманитарных интересов.

Дальнейшие шаги

Предлагаются следующие шаги по созданию и поддержанию импульса, необходимого для реализации данной рекомендации:

- 1.1 Собрать экспертов из России, США и других стран, которые проявит желание участвовать в работе, для того, чтобы определить, допустимы ли существующие уровни переплетенности инфраструктурных объектов, и вероятные последствия.
- 1.2 Подготовить краткое изложение выводов на основании предпринятого анализа, упомянутого в предыдущем пункте.
- 1.3 Если результатом осуществления действий, предусмотренных предыдущими пунктами, станет выработка какого-либо значимого методического руководства, - провести совместное тестирование с целью оценки реализуемости предложения.
- 1.4 На основании предусмотренных выше действий сформулировать соответствующие рекомендации.

Критерии успеха

Об успехе реализации данной рекомендации можно будет судить по следующим критериям:

- Достижение двустороннего, а затем многостороннего консенсуса по вопросу о допустимости нынешнего состояния переплетенности инфраструктурных объектов.
- Успешное проведение тестирования предложенных рекомендаций.
- Выделение охраняемых объектов критической гума-

нитарной инфраструктуры или расширение предмета защиты за счет включения в него отдельных переплетенных инфраструктур, отвечающих определенным критериям.

4.2 Применение в киберпространстве концепции опознавательной эмблематики

Общая информация

Женевские и Гаагские конвенции предписывают, что охраняемые объекты, персонал и транспортные средства должны быть маркированы четким для визуального восприятия способом, позволяющим их отличать.[82] Кроме того, Конвенции определяют стандартные виды опознавательных эмблем, содержат инструкции по их применению и оговаривают последствия несанкционированного применения таких эмблем.[83] Способность воюющей стороны распознавать заявленные охраняемые объекты имеет решающее значение с точки зрения соблюдения Конвенций. Без строжайшего соблюдения правил использования опознавательных знаков невозможно реализовать принципы защиты. Вместе с тем, на сегодняшний день критическая инфраструктура гуманитарного назначения в значительной степени переведена на ИКТ и полностью интегрирована в киберпространство. В результате сложилась ситуация, когда в киберпространстве не существует четких опознавательных знаков (маркеров), которые могли бы применяться для обозначения охраняемых объектов, персонала или соответствующего имущества. Без таких обозначений гуманитарные интересы, подпадающие под защиту Конвенций согласно намерениям составителей, находятся в опасности.[84]

Совместная экспертная группа предлагает рассмотреть вопрос о введении опознавательных знаков (маркеров) в киберпространстве для обозначения охраняемых объектов, персонала и имущества. Одним из возможных вариантов было бы введение доменного расширения, например, «.med» или «.+++» или «.nsz» (сокращение от английского «no strike zone» («зона, свободная от ударов»),

82 Совместный вывод 2: Охраняемые гуманитарные критические инфраструктуры не имеют опознавательных знаков, которые указывали бы на наличие у них статуса защищенного объекта. Раздел 3.2.

83 Женевская конвенция I, Статьи 38-44, 53, Приложение I Статья 6; Женевская конвенция IV, Статьи 18, 20, 21, Приложение I Статья 6.

84 В киберпространстве, точно так же, как и в физическом мире, непредусмотренным последствием обозначения охраняемых объектов может быть их идентификация атакующей стороной, например, террористом.

по аналогии с «.com» или «.org.»[85] Необходимо проявить максимальную осторожность с тем, чтобы избежать конфликта с существующим доменом какой-либо страны или организации. Данная рекомендация предлагает прямое решение проблемы отсутствия опознавательных знаков в киберпространстве, которая является особенно значимой в случае с Комбинацией II и Комбинацией IV (Раздел 3, Схема 1).[86]

Сформулированная ниже рекомендация предлагает разработать систему аналогичных маркеров для киберпространства с тем, чтобы обозначить защищенные объекты, персонал и прочие активы.

России и США, наряду с другими заинтересованными сторонами, следует провести совместную оценку преимуществ и возможностей применения специальных опознавательных знаков в киберпространстве, которые могли бы быть использованы для обозначения гуманитарных интересов, находящихся под защитой Конвенций и Протоколов о войне.

Практическая польза от применения этой рекомендации состоит в том, что она позволит четко опознавать защищенные объекты, людей или активы в киберпространстве. Способность воюющей стороны отличать такие защищенные объекты совершенно необходима для сохранения действенности Конвенций, посвященных защите гуманитарных интересов. Эффективное применение этой рекомендации потребует от частного бизнеса поделиться своим опытом и знаниями; от российских и американских правительственных кругов, поддерживающих сотрудничество, - предоставить соответствующих экспертов, а от организаций, выполняющих функции регулирования в Интернете и поддерживающих реализацию соответствующих мер, - ввести в действие механизм соблюдения принципа отличительной эмблематики в киберпространстве.

Здесь следует заметить, что существующие сопутствующие принципы, в частности, такие как обязательство собственника имущества аккуратно и надлежащим образом обозначать свою собственность, с соблюдением единства маркировки, также должны быть включены в предлагаемое решение.[87]

Рекомендация 2

России и США, наряду с другими заинтересованными сторонами, следует провести совместную оценку преимуществ и возможностей применения специальных опознавательных знаков в киберпространстве, которые могли бы быть ис-

85 Может быть одна или несколько опознавательных эмблем, но каждая из них должна признаваться во всех без исключения системах.

86 Применительно к Комбинации II речь идет о проблеме распознавания.

87 Женевская Конвенция IV, Статья 18.

пользованы для обозначения гуманитарных интересов, находящихся под защитой Конвенций и Протоколов о войне.

Что нужно сделать

Для эффективного выполнения данной рекомендации необходимо следующее:

- Компании частного сектора должны поделиться своим экспертным пониманием возможных вариантов введения опознавательной эмблематики в киберпространстве.
- Российские и американские государственные структуры должны поддержать сотрудничество, выделив для участия в нем соответствующих экспертов.
- Организации, регулирующие функционирование Интернета, должны поддержать меры по введению принципа четкой опознавательной эмблематики в киберпространстве.

Альтернативы и их последствия

У предложенного подхода могут быть следующие альтернативы:

- Ничего не делать . . . Продолжать опираться на Конвенции в их нынешнем виде, что потенциально приведет к росту уязвимости охраняемых объектов, повышению риска их непреднамеренного уничтожения или к неуверенности в способности распознавать охраняемые объекты, персонал и имущество в киберпространстве.
- Сознательно ждать, пока пройдет время и мы чему-либо научимся на уроках первых произошедших трагедий. Затем принять на себя ответственность за полученный результат, который может включать неприемлемые потери человеческих жизней и нанесение непоправимого вреда имуществу.
- Признать невозможность перенесения принципов Конвенций в киберпространство, что будет означать отсутствие гуманитарной защиты в период конфликта.

Практическая польза

Сильной стороной этой рекомендации, в случае ее выполнения, будет введение четкого, общепризнанного обозначения охраняемых объектов, лиц и имущества в киберпространстве. Способность участвующей в военных действиях атакующей стороны идентифицировать охраняемый статус имеет решающее значение для сохранения в силе Конвенций, предус-

матривающих защиту гуманитарных интересов. Уже на следующий день после учреждения гарантирующего защиту домена, организации с охраняемым статусом смогут пользоваться преимуществами своей однозначно определяемой идентификации.

Дальнейшие шаги

Предлагаются следующие шаги по созданию и поддержанию импульса, необходимого для реализации данной рекомендации:

- 2.1 Представителям России, США и других заинтересованных сторон следует собраться и разработать цели и задачи, которым должно отвечать предложение по применению принципа опознавательной эмблематики в киберпространстве, а также само предложение.
- 2.2 Форум, упомянутый выше в параграфе (2-1), поручит избранным на нем участникам представить предложение в соответствующие организации по разработке международных стандартов (standards development organizations, сокращенно – SDO).[88]
- 2.3 Основываясь на результатах предыдущих этапов, пользующаяся доверием нейтральная организация проанализирует и подготовит политические и финансовые соглашения, необходимые для обеспечения практической реализации достигнутой договоренности.

Критерии успеха

Об успехе реализации данной рекомендации можно будет судить по следующим критериям:

- Достижение двустороннего консенсуса по предложению о применении принципа опознавательной эмблематики, заложенного Женевскими и Гаагскими конвенциями.
- Утверждение и поддержка опознавательных знаков (эмблем) для обозначения охраняемых объектов, персонала и имущества в киберпространстве.

---

88 Например, речь может идти о неформальных собраниях экспертов “Birds of a Feather” (BOF) в рамках Рабочей группы по Интернет-инжинирингу (Internet Engineering Task Force (IETF)), к которой может быть обращена просьба предоставить комментарии (RFC).

- Обеспечение возможности четкой идентификации охраняемых объектов, персонала и имущества в киберпространстве атакующей стороной.[89]

4.3 Признание растущего влияния роли негосударственных игроков и пользователей сети

Общая информация

Одним из наиболее фундаментальных, глубинных условий достижения договоренностей по «законам о войне» является наличие у держав-подписантов достаточных полномочий на проставление подписей.[90] В исторической перспективе войны происходили между этническими группами или государственными образованиями (например, между нациями или королевствами). При этом основным инструментом разрешения спора являлась оккупация и установление контроля над территорией. Понятие «кибер***пространства***» вводит новое представление о «территории».[91] [92] Еще одна новая реальность связана с тем, что кибернетическое оружие предоставляет своим пользователям совершенно революционные возможности. Оно позволяет негосударственным игрокам и сетевым пользователям аккумулировать в своих руках огромную власть.[93] Следует очень внимательно отнестись к формированию этой новой, ассиметричной структуры распределения власти.[94] Налицо ситуация, когда неправительственные организации и негосударственные игроки, включая физических лиц, потенциально могут обладать возможностями, позволяющими им оказывать разрушающее воздействие на

89 Важным компонентом этого достижения должна быть способность систем осуществлять автоматическое распознавание.

90 См. подписи под Женевскими и Гаагскими конвенциями.

91 Mary Ann Davidson, The Monroe Doctrine in Cyberspace, Testimony of Oracle Chief Security Officer before the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, March, 2009.

92 Эта новая реальность играет ключевую роль с точки зрения управления Комбинациями II и IV.

93 Эта реальность является одним из факторов управления Комбинациями III и IV.

94 См. Совместный вывод 5 («Негосударственные субъекты и индивидуальные пользователи могут стать более сильными игроками в киберпространстве»), Раздел 3.3.

общественную, экономическую или национальную безопасность.[95]

Усилия по гармонизации принципов Конвенций о защите гражданского населения и критической инфраструктуры с новой реальностью не могут быть продуктивны без решения широкого спектра очевидных задач. Одна из них состоит в том, чтобы повысить уровень информированности гражданских лиц, а в данном случае лучше сказать – обычных пользователей сетей, о требованиях Конвенций. Женевская конвенция о защите гражданского населения во время войны устанавливает, что «Высокие Договаривающиеся Стороны обязуются как в мирное, так и в военное время распространять возможно шире текст настоящей конвенции в своих странах и, в частности, включить ее изучение в учебные программы военного и, если возможно, гражданского образования, с тем, чтобы с ее принципами было ознакомлено все население в целом» (Статья 144). Таким образом, принцип приоритета информирования граждан (получающих таким образом возможность играть активную роль) в целях практической реализации Конвенций не является чем-то новым.

Рекомендация 3

России, США и другим заинтересованным сторонам следует определить, как лучше всего согласовать принципы Конвенций с новой действительностью, в которой участниками киберконфликта могут стать негосударственные игроки.

Что нужно сделать

Для эффективного выполнения данной рекомендации необходимо следующее:

- Правительства должны быть открыты для восприятия новых парадигм уважения, диалога, сотрудничества и доверия во взаимоотношениях с негосударственными игроками.
- Неправительственные организации (НПО) и транснациональные компании (ТНК) должны предложить свои концептуальные подходы и видение для выработки практически реализуемых решений.
- Как правительствам, так и значительной части негосударственных игроков и

95 Существующее международное право признает три категории участников конфликта: вооруженные силы государства, состоящие из одетых в форму комбатантов, организованные вооруженные группы и подразделения, гражданские лица. Каждая из этих категорий может быть объектом нападения при различных обстоятельствах. Правовые режимы, регулирующие принудительное исполнение и сохранение в тайне конфиденциальной информации, предполагают использование особых критериев и механизмов, которые могут быть полезны для определения «плохих игроков» в киберпространстве.

пользователей следует продемонстрировать сотрудничество в киберпространстве на некотором новом, минимальном уровне, конкретные параметры которого предстоит уточнить.

Альтернативы и их последствия

У предложенного подхода могут быть следующие альтернативы:

- Ничего не делать . . . В этом случае отчуждение новой формирующейся силы в киберпространстве еще более усилится.
- Проявить несдержанность и, не дожидаясь результатов совместной оценки, поставить негосударственных игроков и пользователей в равное положение с государствами – участниками киберпроцессов. Результатом такого подхода была бы ситуация хаоса из-за появления огромного количества неуправляемых игроков и неквалифицированных ресурсов.
- Непродуманно отказаться от дальнейшего обсуждения, что ускорит отчуждение негосударственных игроков.

Практическая польза

Практическая польза от осуществления данного проекта заключается в расширении и углублении понимания динамики быстро развивающихся процессов, формировании состояния готовности к дополнительным рискам, связанным с выходом на сцену ранее неизвестной силы, получении информации, позволяющей прогнозировать потребности нового сообщества в обучении и тренинге на предмет предусмотренных Женевскими и Гаагскими конвенциями механизмов защиты для гражданского населения и объектов критической инфраструктуры гражданского назначения.

Дальнейшие шаги

Предлагаются следующие шаги по созданию и поддержанию импульса, необходимого для реализации данной рекомендации:

- 3.1 Российские и американские эксперты определяют и договариваются по структуре и целям совместной оценки.
- 3.2 Российские и американские эксперты аккумулируют данные, необходимые для совместной оценки, с привлечением к аналитической работе других заинтересованных сторон, в особенности негосударственных игроков.
- 3.3 Совместная экспертная группа готовит доклад по итогам оценки и представляет его на рассмотрение

ключевых международных межправительственных и отраслевых форумов.[96]

Критерии успеха

Об успехе реализации данной рекомендации можно будет судить по следующим критериям:

- Будет лучше понята роль негосударственных игроков в сохранении и реализации положений Конвенций.
- Конвенции признаются эффективными с точки зрения учета роли негосударственных игроков и сетевых пользователей, либо корректируются с учетом новой реальности.

96 Примерами таковых могут служить Организация Объединенных Наций (ООН), Кибер40, Институт инженеров по электротехнике и радиоэлектронике (IEEE), Международная Торговая Палата (МТП).

4.4 Анализ принципов Женевского протокола применительно к кибернетическому оружию

Общая информация

Одним из наиболее важных успехов «права войны» является достижение согласия относительно запрета на «применение на войне удушливых, ядовитых и иных подобных газов и бактериологических средств».[97] Указанные средства ведения войны были «справедливо осуждены цивилизованным миром».[98] Но можно ли назвать полным перечень видов оружия, оскорбляющих «совесть» наций?[99] Предложения о включении в него таких средств из ставшего традиционным арсенала, как ядерное оружие, кластерные бомбы и фугасные мины, высказывались неоднократно. В последнее время возник вопрос о том, что делать с возникшим арсеналом кибернетического оружия.

Увеличение зависимости современной цивилизации от ИКТ и киберпространства приводит к усилению беспокойства относительно потенциальных последствий распространения кибероружия, которое может порож-

97 Женевский протокол 1925 г.

98 Там же.

99 Там же.

дать новые виды агрессии, оказывать пагубное воздействие и вызывать опустошение. Кибернетическое оружие способно привнести новые характеристики и свойства в уже имеющийся арсенал вооружений. Речь идет, в частности, о потенциальной способности воспроизводить вирусы, которые не утруждаются распознаванием целей и распространяются с компьютерными скоростями. Эти свойства, в сочетании с агрессивными намерениями распространителей, вызывают понятное беспокойство.

С другой стороны, использование новейшего супероружия может сыграть решающую роль на поле боя при проведении военной операции, особенно в случае, если такое оружие неизвестно противнику и, следовательно, не может быть адекватно нейтрализовано.[100] Обеспокоенность военных в связи с возможными последствиями раскрытия информации столь чувствительного характера совершенно оправдана. Однако она мешает обсуждению новейших средств ведения войны с участием представителей разных стран. С учетом существующих ограничений, становится понятным, почему пробуксовывают усилия по налаживанию международной кооперации в этой области.

Инновационный подход, в значительной степени учитывающий упомянутые выше озабоченности, заключается в том, чтобы: (a) избежать нарушения режима секретности в отношении информации военного характера об определенных свойствах новейших вооружений, и (b) вести диалог в рамках существующих принципов Конвенций, причем исключительно по тем техническим характеристикам, которые достаточно подробно описаны в документах, имеющихся в открытом доступе.[101] Рекомендация 4 отвечает критериям такого подхода. Эта рекомендация прямо учитывает необходимость предвосхищать возникающие изменения, характерную как для Комбинации III, так и для Комбинации IV (Раздел 3, схема 1).

Рекомендация 4

России, США и другим заинтересованным сторонам рекомендуется предпринять со-

100 Информация в публичном доступе включает широко публикуемые материалы о принципах физики, сведения о программировании электротехнических средств и компьютеров, исторические данные о ранее применявшихся «зловредных» кодах. Методология «восьми составляющих (8i)» и подход, предполагающий анализ факторов внутренней уязвимости, также уместны в этой ситуации.

101 Предложение о применении к киберпространству принципов запрета определенных видов оружия не ново. Однако в большинстве случаев речь идет не о запрете вообще, а о запрете применения по отношению к тому или иному конкретному объекту (что может быть проверено, например, путем проведения инспекции). См., напр., Kenneth Geers, , Cyber Weapons Convention, Naval Criminal Investigative Service (NCIS), Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, Estonia, 2010.

вместный анализ характеристик кибернетического оружия с тем, чтобы определить возможность проведения аналогий с теми видами вооружений, которые были ранее запрещены Женевским протоколом.

Что нужно сделать

Для эффективного выполнения данной рекомендации необходимо следующее:

- Российским и американским экспертам следует проявить открытость при обсуждении видов вооружений на основании информации, имеющейся в общественном доступе.
- Правительства России и США не должны исключать возможность того, что некоторые виды вооружений по своим характеристикам могут быть признаны неприемлемыми, поскольку они нарушают «принципы человечности и императивы общественной морали».”[102]

Альтернативы и их последствия

У предложенного подхода могут быть следующие альтернативы:

- Ничего не делать . . . В этом случае возникает риск развязывания гонки кибервооружений или бесконтрольного использования кибероружия с пагубными последствиями, либо будет утерян шанс применить уроки, полученные в прошлом и нашедшие отражение в существующих Конвенциях.
- Реагировать путем введения чересчур жестких норм регулирования и ограничений в области технологий, что приведет к созданию препятствий для инноваций и «выдавит» передовые научные исследования и разработки в подпольную сферу.
- Ввести ограничения на обсуждение технических характеристик кибероружия, в результате чего в будущем мы неожиданно окажемся лицом к лицу с новым видом оружия, которое потребует незамедлительной реакции.

Практическая польза

Практическая польза от успешного завершения российско-американской совместной оценки принципов Женевского протокола применительно к кибервооружениям будет включать «ломку льда» в отношениях между кибердержавами, что открыло бы новые возможности для обсуждения

102 Дополнительный протокол I, 1949 г., Статья 1.

механизмов сдерживания конфликтов, создало бы условия для лучшего понимания специфики кибероружия в международном масштабе и для предотвращения его применения, которое может иметь разрушительные последствия для гражданского населения и критически важных инфраструктурных объектов гражданского назначения.

Дальнейшие шаги

Предлагаются следующие шаги по созданию и поддержанию импульса, необходимого для реализации данной рекомендации:

- 4.1 Российские и американские эксперты совместно разрабатывают цели и методологию исследования кибероружия в свете принципов, заложенных в Женевском протоколе.
- 4.2 Российские и американские эксперты приступают к совместному анализу как принципов Женевского протокола в отношении вооружений, так и характеристик кибероружия на базе информации, имеющейся в публичном доступе.
- 4.3 Совместная экспертная группа готовит доклад по итогам работы и представляет свои заключения на рассмотрение соответствующих государственных структур и ключевых международных форумов, сообразуясь с принципом целесообразности.

Критерии успеха

Об успехе реализации данной рекомендации можно будет судить по следующим критериям:

- Разрабатывается совместный российско-американский механизм для лучшего понимания сформулированных в Женевском протоколе принципов запрета определенных типов оружия.
- Российские и американские эксперты предпринимают совместный анализ характеристик вооружений, основанных на использовании ИКТ.
- Созданный по итогам работы совместный российско-американский доклад используется для определения того, какие виды кибернетического оружия могут быть сочтены по своим характеристикам аналогичными тем типам оружия, которые были запрещены Женевским протоколом 1925 года.

4.5 Изучение «третьего» («иного, чем война») состояния международных отношений

Общая информация

Критические инфраструктуры становятся все более уязвимыми для киберугроз, которые, будучи реализованы, могут привести к серьезным потерям как человеческих жизней, так и материальных средств. Конвенции предусматривают меры защиты для гражданского населения и критически важных гуманитарных объектов, которые отвечают строго установленным критериям.[103] [104] Вместе с тем, оговаривается, что эти меры защиты могут использоваться, главным образом, во время войны.[105] На международном уровне отсутствует ясное и согласованное определение того, что следует считать кибервойной. По этому вопросу наблюдается значительная путаница во взглядах.[106] Схема 3 наглядно демонстрирует, что зачастую даже руководители одной и той же страны не могут прийти к согласию относительно того, *действительно* ли ведется кибервойна в настоящее время и насколько она *реальна*.[107]

Общепринятое понимание различных состояний конфликта можно представить в виде горизонтальной линии, на одном конце которой условно помещается мир, а на другом – война. Между ними расположены различные уровни конфликта.[108] [109]

---

103 Первая Женевская конвенция, Статьи 19 – 44, а также Статьи 1 – 13 Приложения I; Вторая Женевская конвенция, Статьи 22 – 45; Четвертая Женевская конвенция, Статьи 1 – 26, а также Статьи 1 – 8 Приложения; Протокол I, Статьи 1 – 34, 48 – 79; Протокол II, Статьи 1 – 28; Протокол III, Статьи 1 – 17.

104 Участники рабочей группы заметили, что авторы Конвенций понимали «войну» не просто как объявленное состояние отношений между народами, а скорее как состояние конфликта, включающее использование силы.

105 См., напр., Женевская конвенция IV, Преамбула и Статьи 1-3.

106 Для того, чтобы в этом убедиться, достаточно просмотреть газетные заголовки на предмет кибернетической войны.

107 Совместный вывод 10, Раздел 3.5.

108 Существующие правовые механизмы предусматривают применение различных ответных мер, включая принудительное исполнение, разведывательные и военные операции. Каждый из этих режимов использует собственные, отличающиеся критерии оценки угроз. При этом любой инцидент, имеющий место в киберпространстве, может быть охарактеризован как подпадающий под применение двух, а то и всех трех режимов, в зависимости от ситуации. Например, при выявлении факта внедрения в чужие системы расследование правовых аспектов нарушения и организация преследования в судебном порядке отнюдь не исключают, в случае необходимости, принятия незамедлительных (и, возможно, силовых) мер со стороны военных, а также действий разведслужб по приказу исполнительных органов, если их привлечение целесообразно и оправданно.

109 Устав ООН, Статья 39.

[110] В настоящее время киберсобытия рассматриваются именно сквозь эту призму в целях приведения их в соответствие с существующими представлениями о пороговых характеристиках и системах координат.[111] Однако применение существующих стандартов к качественно новому явлению чревато некоторыми фундаментальными проблемами. Например, нельзя забывать о том, что кибератаки могут не поддаваться непосредственному наблюдению и могут исходить из источника, однозначная или высокоточная идентификация которого чрезвычайно затруднена.[112] Констатировав существующие на данный момент сложности в приведении двух различных явлений к единому знаменателю, совместная группа экспертов высказалась в пользу продолжения двусторонних усилий, направленных на переоценку основополагающих потребностей и возможностей в этой сфере.[113]

Рекомендация 5

России и США, наряду с другими заинтересованными сторонами, было бы целесообразно проанализировать возможность признания «третьего» («иного, чем война») состояния международных отношений для того, чтобы внести ясность в вопрос о применении существующих Конвенций и Протоколов.

Что нужно сделать

Для эффективного выполнения данной рекомендации необходимо следующее:

- Органы, отвечающие за национальную безопасность в России и США, должны признать, что существующая нечеткость определения войны в киберпространстве неприемлема, и проявить готовность к поиску четкой формулировки.
- Представителям России, США и других заинтересованных сторон следует собраться для того, чтобы совместно

110 Дополнительный протокол I, 1949 г., Статья 1.

111 Киберсобытия могут представлять собой: (a) действия в рамках «международного мира и безопасности», т.е. законные действия; (b) использование силы, являющееся само по себе незаконным, но не создающее возможностей для ответного применения силы; (c) вооруженное нападение, являющееся основанием для односторонней силовой реакции на конкретный инцидент; и (d) войну, т.е. распространенное состояние враждебных действий, при котором все вооруженные силы одного государства могут быть законным образом нацелены на все вооруженные силы другого государства. Существуют также критерии и методы перехода с более низкого на более высокий уровень в рамках этой градации.

112 Совместный вывод 9, Раздел 3.5.

113 Эта рекомендация является попыткой ответить на вопрос, характерный для Комбинаций II, III и IV. Особенно остро он стоит для Комбинации IV (см. Раздел 3, Схема 1).

выработать новые критерии классификации конфликтов.

- Все заинтересованные стороны должны быть максимально готовы к открытому анализу и рассмотрению новых, альтернативных норм управленческого поведения в киберпространстве.[114]

Альтернативы и их последствия

У предложенного подхода могут быть следующие альтернативы:

- Ничего не делать . . . Что приведет к сохранению неразберихи и разногласий относительно того, что считать приемлемым поведением, соответствующим нормам мирного времени, а что – состоянием войны в киберпространстве.
- Сходу отказаться от концепции «третьего состояния», что приведет к ограничению предмета дискуссии и поиска альтернатив нынешней бинарной классификации, основанной на противопоставлении войны и мира.

Практическая польза

Практическая польза рассмотрения вопроса о «третьем состоянии» будет состоять в инициировании дискуссии, которая привнесет столь необходимую четкость и структурированность в нынешние сумбурные представления об этом сложном сюжете. Отказ от концепции «третьего состояния» был бы не менее продуктивным, чем ее признание, так как способствовал бы формированию более ясного понимания того, почему следует предпочесть именно две ныне существующие модели, и какие параметры имеют решающее значение с точки зрения их определения.

Дальнейшие шаги

Предлагаются следующие шаги по созданию и поддержанию импульса, необходимого для реализации данной рекомендации:

- 5.1 Россия, США и другие заинтересованные стороны осуществляют детальный разбор нынешней ситуации с точки зрения фундаментальных принципов и возвращаются к рассмотрению возможных опций и характеристик моделей «иного, чем война» состояния.
- 5.2 Озабоченности всех участников процесса относительно реальной ценности и при-

114 Очень важно, чтобы этот анализ опирался на фундаментальные научные и инженерные знания и компетенции.

менимости новой конструкции суммируются, с последующей разработкой по каждому спорному вопросу пробных критериев, которые удовлетворяли бы интересы всех сторон.

- 5.3 Совместная экспертная группа осуществляет анализ новой модели, основываясь на разработанных критериях оценки, и готовит совместный доклад с изложением своих выводов.

Критерии успеха

Об успехе реализации данной рекомендации можно будет судить по следующим критериям:

- Достигается двусторонний или многосторонний консенсус относительно преимуществ международного признания «иного, чем война» состояния конфликта.
- Предпринимаются необходимые последующие действия для того, чтобы: i) либо внедрить такую «третью» модель в практику международных отношений, либо ii) полностью отказаться от ее дальнейшего обсуждения с приведением окончательных выводов.

5. Заключение

В настоящем докладе описаны первые шаги в рамках двустороннего российско-американского процесса, направленные на укрепление позиций обеих стран по вопросу о защите критической гуманитарной инфраструктуры в киберпространстве. Совместная аналитическая группа строила свою работу на прочном фундаменте, обеспечивавшем согласие среди экспертов, а именно на высокочтимых и общепризнанных принципах Женевских и Гаагских конвенций, которые предусматривают меры по защите гуманитарных интересов. Для более эффективного управления сложным и динамичным комплексом проблем была введена система четырех комбинаций. Анализ упомянутых комбинаций позволил сформулировать и поставить в центр дискуссии основные Совместные выводы относительно применимости к киберпространству принципов, заложенных Конвенциями. Затем вопросы, вытекающие из этих выводов, были положены в основу пяти совместных рекомендаций, которые, будучи реализованы, могли бы внести существенный вклад в сохранение критической гуманитарной инфраструктуры в киберпространстве.

Двусторонняя российско-американская группа готова продолжить начатый диалог по вопросам защиты критической инфраструктуры, который имеет чрезвычайно важное значение. Последующие усилия будут направлены на поддержку реализации представленных в настоящем докладе рекомендаций, превращение двустороннего диалога в многосторонний развивающийся процесс, расширение тематики дискуссий за счет включения в нее новых, важных для обеих стран областей, связанных с кибербезопасностью.

БИОГРАФИИ

Об авторах

Карл Фредерик Раушер

Карл Фредерик Раушер (Karl Frederick Rauscher) является директором по программам в области технологий и ведущим научным сотрудником Института Восток-Запад. Ранее он работал исполнительным директором управления надежности и безопасности Alcatel-Lucent – сетевой структуры лабораторий Bell Labs и по-прежнему является научным сотрудником Bell Labs. Карл Раушер консультировал высшее руководство государственных и отраслевых структур на пяти континентах, включая вице-председателя Консультативного комитета по национальной безопасности в области телекоммуникаций при Президенте США (NSTAC), и был руководителем исследования по вопросам доступности и эксплуатационной надежности электронных коммуникационных инфраструктур (ARECI), которое спонсировалось Европейской Комиссией.

В числе последних публикаций – доклад о надежности глобальной инфраструктуры подводных коммуникационных кабельных сетей (ROGUCCI) Института инженеров по электротехнике и электронике (IEEE).

Карл Раушер является почетным председателем консультативного совета по качеству и надежности коммуникаций IEEE, а также учредителем и президентом некоммерческой Группы реагирования на чрезвычайные ситуации в сфере беспроводной связи (WERT). Автор многочисленных изобретений, имеющий более 50 патентов/заявок на патенты в таких областях, как искусственный интеллект, защита критической инфраструктуры, аварийная связь, энергосбережение, телемедицина. Лично обнаружил более 1000 программных «жучков» в работающих сетях. Участвовал в разработке более 600 программных документов, отражающих наилучшие стандарты отраслевой практики на базе консенсуса между экспертами.

Андрей Коротков

Андрей Коротков – один из российских технологических лидеров, эксперт по системам управления бизнес-процессами, информационного общества, искусственного интеллекта, математических проблем в биологии. Доктор экономических наук, заведующий кафедрами Московского государственного института международных отношений (МГИМО (У)) и Российской академии народного хозяйства и государственной службы (РАНХ и ГС).

Занимал руководящие должности в аппарате правительства и администрации Президента РФ (1997-2002гг.) Первый заместитель министра Российской Федерации по связи и информатизации (2002-2004), один из идеологов ФЦП «Электронная Россия 2002-2010 гг».

Лауреат национальной премии «ИТ-лидер» 2005, 2009 гг.

Главный редактор журнала «Системы управления бизнес-процессами»

Автор монографий, учебно-методических пособий, научно-популярных книг, журнальных и газетных публикаций по проблемам информационного общества.

Эксперты-соавторы исследования:

Артем Аджемов

Артем Аджемов – ректор и профессор Московского технического университета связи и информатики. Преподает информатику и связь. Является экспертом в области телекоммуникаций. Автор 60 научных книг и учебных пособий. Член Международной академии связи и Международной академии открытого образования.

Чарльз (Чак) Бэрри (Charles (Chuck) Barry)

Чарльз Бэрри является ведущим научным сотрудником Института национальных стратегических исследований при Университете национальной обороны США. Офицер в отставке с обширным опытом практической и руководящей работы. В течение более чем 30 лет Ч.Бэрри исследовал проблемы трансатлантических отношений, военной политики, системы оперативного контроля и управления, которым были посвящены его многочисленные публикации. Член Национального почетного общества Pi Alpha Alpha по направлению «государственное управление» и Фонда Вудро Вильсона. Имеет степень доктора в области государственного управления (управления информацией), полученную в Университете Балтимора.

Джон С. Эдвардс (John S. Edwards)

Джон С. Эдвардс более 51 года работал в области телекоммуникаций, занимаясь проектированием, анализом и бизнес-планированием. Он основал и успешно управлял несколькими проектными группами, а также учредил три компании, одна из которых в дальнейшем была приобретена более крупной корпорацией за миллиард долларов. Занимал высшие руководящие посты в ряде компаний, в течение 25 лет представлял Nortel Networks в Отраслевом исполнительном подкомитете Консультативного комитета по национальной безопасности при Президенте США, возглавлял различные рабочие группы, организованные комитетом. В настоящее время является Президентом Digicom, Inc. и членом технического консультативного комитета по информационным системам министерства торговли США.

Дж. Б. (Гиб) Годвин (J. B. (Gib) Godwin), контр-адмирал (в отставке)

Контр-адмирал (в отставке) Гиб Годвин в настоящее время является вице-президентом по кибербезопасности и интеграции систем компании Northrop Grumman Information Systems и использует свой многолетний опыт в области систем обнаружения целей и сбора военной информации для концептуальной разработки инновационных подходов к обеспечению кибербезопасности. Г-н Годвин более 15 лет служил в Командовании военно-морскими авиационными системами и в Командовании космическими и военно-морскими боевыми системами. Ему был присвоен ранг контр-адмирала ВМФ США. В качестве программного исполнительного директора по информационным системам на предприятиях, г-н Годвин выполнял роль координатора ВМФ по взаимодействию со всеми сетевыми системами наземного базирования.

Стюарт Голдмэн (Stuart Goldman)

Стюарт Голдмэн внес большой вклад в развитие компьютерной и телекоммуникационной отраслей, которым он посвятил 45 лет напряженной работы до выхода на пенсию. Г-н Голдмэн спроектировал ряд коммуникационных систем и активно участвовал в работе нескольких национальных и международных органов, занимающихся вопросами стандартизации, выполняя различные руководящие роли. Имеет 25 патентов, а также 53 заявки на патенты в стадии рассмотрения. Научный сотрудник Bell Labs (в отставке).

Владимир Иванов

Владимир Иванов является директором филиала Института Восток-Запад (ИВЗ) в России (Москва). Ранее руководил в Институте программой «Открытые финансы», в том числе изданием серии работ, посвященных межбюджетным отношениям в Российской Федерации. В 2006-2009 годах играл ведущую роль в организации сотрудничества ИВЗ с Россией по вопросам развития международных частно-государственных партнерств по борьбе с терроризмом в таких областях, как кибербезопасность, защита критической инфраструктуры и противодействие незаконному обороту драгоценных металлов и камней.

В настоящее время В.Иванов вовлечен во все проекты ИВЗ, так или иначе связанные с Россией, в частности российско-американский диалог по кибербезопасности и программу по Евро-Атлантической безопасности. Обладает профессиональным опытом в сферах социальных наук, деловой журналистики и связей с общественностью. Является автором многочисленных публикаций на экономические темы в газетах Русский Телеграф и Время Новостей. Имеет диплом МГИМО о высшем образовании в области международной журналистики и степень кандидата исторических наук. Владеет английским и французским языками.

Джеймс Брет Майкл (James Bret Michael)

Джеймс Брет Майкл – профессор компьютерных наук и электромашиностроения в Школе последипломного образования ВМФ США. Эксперт в области распределенных систем и обеспечения надежности и достоверности вычислительных процессов. Д-р Майкл является ведущим техническим консультантом группы экспертов, объединивших свои усилия в рамках «таллинского» проекта создания учебного пособия по правовым вопросам вооруженного конфликта в киберпространстве. Член Института инженеров по электротехнике и электронике (IEEE), которому был присужден Приз года как лучшему инженеру IEEE по системам безопасности. Докторскую степень в области информационных технологий получил в Университете Джорджа Мейсона.

Виктор Минин

Виктор Минин является экспертом в области автоматики, телемеханики и социальной психологии. Имеет 29-летний опыт работы в сфере информационной безопасности. В частности, находясь на военной службе, Виктор Минин отвечал за вопросы информационной безопасности в особом подразделении по информационно-коммуникационной работе Федеральной службы безопасности РФ. В настоящее время член Координационного совета государств-участников СНГ по информатизации при Региональном содружестве в области связи, председатель Общественного консультативного совета по научно-технологическим вопросам информационной безопасности.

Пол Николас (Paul Nicholas)

Дж. Пол Николас возглавляет Группу по вопросам стратегии глобальной безопасности и дипломатии корпорации Microsoft, которая видит свою основную задачу в том, чтобы способствовать стратегическим изменениям, направленным на повышение уровня безопасности и жизнеспособности инфраструктур, как внутри Microsoft, так и вовне. Г-н Николас имеет более чем десятилетний опыт работы по глобальным проблемам, связанным с управлением рисками, реагированием на события, организацией связи в условиях чрезвычайных ситуаций и обменом информацией. Работал директором по кибербезопасности и защите критической инфраструктуры в Белом Доме, заместителем директора управления учета в Правительстве США, старшим сотрудником аппарата Сената, аналитиком министерства обороны. Степень бакалавра получил в Университете штата Индиана, а степень магистра – в Университете Джорджтауна. Сертифицированный специалист в области безопасности информационных систем.

Джек Осланд (Jack Oslund)

Джек Осланд более 40 лет проработал в государственных структурах, промышленности и науке в области национальной безопасности и международных коммуникаций. Преподавал в Колледже разведывательной информации по национальной обороне, был сотрудником международного отдела Управления телекоммуникационной политики Белого Дома, занимал руководящие посты в Communications Satellite Corporation. Кроме того, г-н Осланд участвовал в работе Консультативного комитета по национальной безопасности в области телекоммуникаций (NSTAC) и вел учебные занятия в качестве адъюнкт-профессора в Университете имени Джорджа Вашингтона. В настоящее время является ведущим научным сотрудником Института политики внутренней безопасности Университета имени Джорджа Вашингтона.

Борис Славин

Борис Славин с 2008 года является председателем правления Союза ИТ-директоров Российской Федерации. Получил степень кандидата физико-математических наук в МГУ им. Ломоносова. Автор ряда публикаций по вопросам ИТ-управления и по теории информационного общества. Имеет большой практический опыт в области информационных технологий. Работал директором по ИТ в крупных российских компаниях.

Леонид Тодоров

Леонид Тодоров получил степень бакалавра в области управления в Университете Копенгагена и степень магистра в области лингвистики в Московском государственном педагогическом университете. После начала российских реформ более десятилетия являлся руководителем аппарата премьер-министра Егора Гайдара. Затем работал в горнодобывающей компании и в PR-компании в Москве. В 2008 году поступил на работу в Координационный центр национального домена сети Интернет. В настоящее время занимает должность заместителя директора по связям с государственными органами Координационного центра. Занимается вопросами ИТ-управления, IDNs, международного сотрудничества и кибербезопасности. Автор или соавтор целого ряда публикаций по названным темам. Неоднократно выступал с докладами на различных национальных и международных форумах.

Томас К. Уингфилд (Thomas C. Wingfield)

Томас К. Уингфилд – профессор международного права Европейского центра исследований в области безопасности имени Джорджа Маршалла в Гармиш-Партенкирхене, Германия, где он читает лекции по таким дисциплинам, как верховенство закона, права человека и право войны. Являясь научным сотрудником Центра НАТО по повышению квалификации в области совместной кибероборонь в г. Таллине, Эстония, разрабатывает, в качестве соавтора, учебное пособие по правовым вопросам вооруженного конфликта в киберпространстве. В центре научных интересов г-на Уингфилда – разработка правовых стандартов, которые характеризуют использование силы и вооруженного нападения в киберпространстве.

Елена Зиновьева

Имеет научные степени кандидата юридических наук и магистра права, присвоенные Центром правоведения Университета Джорджтауна. Завершает работу над докторской диссертацией по юриспруденции в Школе права Университета Вирджинии. Бывший председатель Комитета по международному уголовному праву Американской ассоциации адвокатов. Автор книги «Право информационного конфликта: законодательство о национальной безопасности в киберпространстве» (The Law of Information Conflict: National Security Law in Cyberspace).

Е.С.Зиновьева с отличием окончила Санкт-Петербургский государственный университет, факультет международных отношений, по специальности «Прикладная информатика в гуманитарной сфере (область применения: международные отношения)». Она также обучалась на факультете филологии и искусств Санкт-Петербургского государственного университета и на факультете журналистики и политических наук Варшавского университета. В 2009 г. Е.С.Зиновьева завершила обучение в очной аспирантуре МГИМО (У) МИД России, защитив диссертацию на соискание ученой степени кандидата политических наук на тему «Роль международных организаций и институтов в формировании режима управления интернетом». С 2010 г. преподает в МГИМО (У) МИД России на кафедре мировых политических процессов факультета политологии. Зиновьевой Е.С. были опубликованы работы по вопросам регулирования интернета, политических аспектов развития информационных технологий, а также научно-техническим проблемам международных отношений.

СОКРАЩЕНИЯ

8i	Eight Ingredient (Framework of ICT Infrastructure) (Восьмикомпонентная модель инфраструктуры ИКТ)
ASPR	Agreements, Standards, Policies and Regulations (Система международных соглашений, стандартов, политики и правил)
ATIS	Alliance for Telecommunications Industry Solutions (Объединение за поиск решений для индустрии телекоммуникаций)
BOF	Birds of a Feather (буквально – «из одного теста», термин используется в информатике для обозначения неформальных встреч участников для обсуждения общих интересующих их вопросов)
CCD	Cooperative Cyber Defense (Коллективная кибероборона)
CIIP	Critical Infrastructure Information Protection (Защита информации о критических инфраструктурах)
CIP	Critical Infrastructure Protection (Защита критической инфраструктуры)
CNA	Computer Network Attacks (Атаки на компьютерные сети)
COE	Counsel of Europe (Совет Европы)
DoS	Denial of Service (Отказ в обслуживании)
DDoS	Distributed Denial of Service (Распределенный отказ в обслуживании)
DNS	Domain Name Server (Сервер доменных имен)
EWI	EastWest Institute (Институт Восток-Запад)
FBI	Federal Bureau of Investigation (Федеральное бюро расследований)
GPS	Global Positioning System (Глобальная система позиционирования)
GUCCI	Global Undersea Communications Cable Infrastructure (Глобальная инфраструктура подводных коммуникационных кабельных сетей)
ICRC	International Committee of the Red Cross (Международный комитет Красного Креста)
ICT	Information and Communications Technology (Информационно-коммуникационные технологии – ИКТ)
IEEE	Institute of Electrical and Electronics Engineers (Институт инженеров по электротехнике и электронике)

IETF	Internet Engineering Task Force (Рабочая группа по Интернет-инжинирингу)
IGO	Intergovernmental Organization (Межправительственная организация)
IHL	International Humanitarian Law (Международное гуманитарное право)
ISP	Internet Service Provider (Провайдер Интернет-сервиса)
ITU	International Telecommunications Union (Международный телекоммуникационный союз)
LoW	Laws of War («право войны», или законы ведения военных действий)
MED	Символ, предложенный для маркировки охраняемых объектов в киберпространстве (Рекомендация 2)
MNC	Multi-National Corporations (Транснациональные корпорации)
NATO	North Atlantic Treaty Organization (Организация Североатлантического договора)
NGO	Non-Government Organizations (Неправительственные организации)
NSA	Non-State Actors (Негосударственные игроки, организации и активисты)
NSTAC	National Security Telecommunications Advisory Committee, The President's (Консультативный комитет по национальной безопасности в области телекоммуникаций при Президенте США)
NSZ	No Strike Zone («зона, свободная от ударов»)
OECD	Organization for Economic Co-Operation and Development (Организация экономического сотрудничества и развития)
PC	Personal Computer (Персональный компьютер – ПК)
PPP	Private-Public Partnership (Частно-государственное партнерство)
PPP	Public-Private Partnership (Государственно-частное партнерство)
RFC	Request for Comment (Просьба предоставить комментарии)
RFID	Radio Frequency Identification (Радиочастотная идентификация)
RPG	Rocket-Propelled Grenade (Реактивная граната)
ROI	Return on Investment (Доходность инвестированного капитала)

SCADA	Supervisory Control and Data Acquisition (Система оперативного диспетчерского управления и сбора данных)
TLD	Top-Level Domain (Домен верхнего уровня)
UAV	Unmanned Aerial Vehicle (Беспилотный летательный аппарат)
UN	United Nations (Организация Объединенных Наций – ООН)
URW	UnRestricted Warfare (Неограниченные военные действия)
U.S.	United States (of America) (Соединенные Штаты Америки)
VNSA	Violent Non-State Actors (Экстремистские негосударственные игроки)
WCI	Worldwide Cybersecurity Initiative (Всемирная инициатива по кибербезопасности)
WWW	World Wide Web (Всемирная «паутина»)
+++	Символ, предложенный для маркировки охраняемых объектов в киберпространстве (Рекомендация 2)

Источники и литература

Avalon Project, Yale University, avalon.yale.edu.

ATIS Network Reliability Steering Committee (NRSC) 2002 Annual Report, www.atis.org/nrsc .

ATIS Telecom Glossary, www.atis.org, 2007.

Blair, Dennis, C., *Director of National Intelligence Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, Washington, DC.* February 2, 2010.

Brenner, Susan W., Clarke, Leo L., "*Civilians in Cyberwarfare: Conscripts," Vanderbilt Journal of Transnational Law* 43.

Brunner, Elgin, M. and Manuel Suter, "International CIIP Handbook: An Inventory Of 25 National And 7 International Critical Information Infrastructure Protection Policies." *International CIP Handbook 2008/2009.* Zurich, Switzerland: Center for Security Studies (CSS), 2008.

Charter of the United Nations, The, 1973.

Civil Defense in International Law, Advisory Service on International Humanitarian Law, International Committee of the Red Cross, June 2001.

"Confusion on the Cyber-Battlefield – The World Needs Rules of Cyberwar," *Science Daily,* October 2010.

"Clarifying the notion of direct participation in hostilities," ICRC, 2009.

Presidential Decision Directive No. 63, *"Clinton Administration's Policy on Critical Infrastructure Protection."* White Paper, May 22, 1998.

Executive Order 13,010, "*Critical Infrastructure Protection*," *Federal Register* 61, No. 138. July 17, 1996.

"Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," White House, 2009.

Davidson, Mary Ann, *The Monroe Doctrine in Cyberspace,* Testimony of Oracle Chief Security Officer before the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, March 2009.

Definition of Aggression, UN General Assembly Resolution 3314 (XXIX), 1974.

Dion, Maeve, "*When Cyber Incidents Threaten National or International Security: What is the Law?" The CIP Report, Legal Insights* 9 No. 7, January 2011.

Dörmann, Knut, "*Computer Network Attack and International Humanitarian Law*," *Cambridge Review of International Affairs. (*May 2001).

Dylevsky, I.N., et al., *Russian Federation Military Policy in the Area of International Information Security: Regional Aspects,* Moscow Military Thought 31*,* July 2009.

Establishing the Office of Homeland Security and the Homeland Security Council, Executive Order 13228, Federal Register, Vol. 66, No. 196, October 8, 2001.

Fedorov, Alexander V., *Terrorism and International Information Security*, Yaderny Kontrol, December 2001.

Fulghum, David A., *Cyber Attacks No Longer Non-Kinetic*, A Defense Technology Bog, September 2010.

Geneva Convention, The, *The Geneva Conventions of 1949 and their Additional Protocols*, Geneva.

Geneva Protocol, The; *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*, Geneva, 1925.

Hague Convention, *The Hague Convention of 1899 and 1907* The Hague.

Homeland Security Physical Security Focus Group Final Report, Network Reliability and Interoperability Council (NRIC) VI Issue 3, December 2003.

Homeland Security Presidential Directive 7, HSPD-7, December, 2003.

Hughes, Rex, Towards a Global Regime for Cyber Warfare, Cyber Security Project, Chatham House, London.

International Information Security: the Diplomacy of Peace. Moscow, 2009.

Komov, Sergey A., Korotkov, Sergey, V, Dylevsky, Igor N., *Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law*.

Lorents, Peeter and Ottis, Rain, *Knowledge Based Framework for Cyber Weapons and Conflict*, Proceedings of Conference on Cyber Conflict, CCD COE Publications, Tallinn, Estonia, 2010.

Michael, James Bret, *On the Response Policy of Software Decoys: Conducting*

Software-based Deception in the Cyber Battlespace, IEEE Proceedings of the 26th Annual International Computer Software and Applications Conference (COMPSAC'0), 2002.

Michael, James Bret, Tikk, Eneken, Wahlgrn, Wingfield, Thomas C., *"From Chaos to Collective Defense,"* IEEE Computer Society, August, 2010.

Michael, James B., Wingfield, Thomas C., Wijesekera, Duminda, *Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System,* Proceedings of the IEEE Computer Society (27th) Annual International Computer Software and Applications Conference, 2003.

Moteff, John and Parfomak, Paul, *Critical Infrastructure and Key Assets: Definition and Identification,* CSR Report, October 2004.

Mueller, Robert, S. III, *Federal Bureau of Investigation (FBI) Director Statement Before the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies*, Washington, DC, March 17, 2010.

National Security of Russia, The. http://www.scrf.gov.ru/documents/sections/3/.

National Strategy for Homeland Security, The, U.S. Office of Homeland Security, July 16, 2002.

National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, The, Office of the President, February, 2003.

Next Generation Networks Task Force Report, NSTAC, March 28, 2006.

Nonstate Actors: Impact on International Relations and Implications for the United States, National Intelligence Council, August, 2007.

NSTAC Report to the President on International Communications, The President's National Security Telecommunications Advisory Committee (NSTAC), August, 2007.

Our World. Views from the Field., International Committee of the Red Cross, 2009.

Public Data Network Reliability Focus Group Final Report, Issue 3, NRIC VII October 2005.

Participant Summary Results, Proceedings of the First Worldwide Cybersecurity Summit, Dallas, EWI 2010.

Protection of 'Critical Infrastructure' and the Role of Investment Policies

Relating To National Security, OECD, May 2008.

Rauscher, Karl Frederick, *Reliability of Global Undersea Communications Cable Infrastructure, The Report*, (ROGUCCI) IEEE, 2010. www.ieee-rogucci.org.

Rauscher, Karl F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal – Special Issue: Homeland Security, Volume 9, Issue 2, 2004.

Rauscher, Karl F., Krock, Richard E., Runyon, James P., *Eight ingredients of communications infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security*, Bell Labs Technical Journal, Volume 11, Issue 3, 2006.

Rauscher, Karl, F., European Commission-Sponsored, *Availability And Robustness Of Electronic Communications Infrastructures (ARECI) Report*, March 2007.

Rowe, Neil, C., U.S. Naval Postgraduate School , *Ethics of Cyberwar Attacks*, A chapter in Cyber War and Cyber Terrorism, ed. A. Colarik and L. Janczewski, Hershey, PA: The Idea Group, 2007.

Russia's Cyber Security Plans, MIT Technology Review, April 2010.

Saunders, Steven Chris, *Confusion on the Cyber-Battlefield – The World Needs Rules of Cyberwar,* North Carolina Journal of Law and Technology, February, 2010.

Sabadia, Aisha, Austin, Greg, PROTECT! Cilivians and civil Rights in Couner-Terrorism, EWI Policy Paper, 2007.

Scott, James Brown, ed. *The Hague Peace Conferences of 1899 and 1907, Vol. 1, The Conferences*, The Johns Hopkins Press ,1909.

Schmitt, Michael, N., Harrison Dinniss, Heather, A., Wingfield, Thomas C., *Computers And War: The Legal Battlespace,* Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge, June, 2004.

Security, Russian Federation Law on March 5, 1992, N 2446-I, as amended 1992 – 2007. http://www.scrf.gov.ru/documents/20.html.

Strategy of the National Security of the Russian Federation Until 2020, Presidential Decree No. 537, Russian Federation, May 12, 2009. http://www.scrf.gov.ru/documents/99.html.

Shanghai Cooperation Organization, The, http://www.sectsco.org/EN/

Shackelford, Scott, J., *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, Conference on Cyber Conflict Proceedings, Tallinn, 2010.

Sommer, Peter and Brown, Ian, *Reducing Systemic Cybersecurity Risk*, OECD Multi-Disciplinary Issues International Futures Program, January 2011.

Suter, Manuel, *A Generic National Framework For Critical Information Infrastructure Protection (CIIP)*, Center for Security Studies, ETH Zurich, August 2007.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), 107th United States Congress, October 2001.

U.S. Army Cyber Operations and Cyber Terrorism Handbook, 1.02, US Army Training and Doctrine Command, Fort Leavenworth, Kansas 2005.

U.S. Cyber Command Fact Sheet, U.S. Department of Defense, May 2010.

Voon, Tania, *Pointing The Finger: Civilian Casualties Of NATO Bombing In The Kosovo Conflict*, 2001.

Wingfield, Thomas C ., "The Law of Information Conflict : National Security Law in Cyberspace," Aegis Research, 2000.

Wingfield, Thomas, C., Michael, James B., *An Introduction to Legal Aspects of Operations in Cyberspace*
Naval Postgradute School, The, Monterey, California, April 2004.

Wireless Network Reliability Focus Group Final Report, NRIC, VII Issue 3, October 2005.

EWI Board of Directors

OFFICE OF THE CHAIRMEN

Francis Finlay (U.K.)
EWI Co-Chairman
Former Chairman,
Clay Finlay LLC

Ross Perot, Jr. (U.S.)
EWI Co-Chairman
Chairman, Hillwood;
Member of Board of Directors, Dell, Inc.

Armen Sarkissian (Armenia)
EWI Vice-Chairman
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President and CEO
EastWest Institute

R. William Ide III (U.S.)
Counsel and Secretary
Partner, McKenna Long & Aldridge LLP

Mark Maletz (U.S.)
Chair of the Executive Committee of EWI Board of Directors
Senior Fellow, Harvard Business School

Leo Schenker (U.S.)
EWI Treasurer
Senior Executive Vice President, Central National-Gottesmann, Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former President of Finland

Jerald T. Baldridge (U.S.)
Chairman
Republic Energy Inc.

Sir Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Tewodros Ashenafi (Ethiopia)
Chairman & CEO
Southwest Energy (HK) Ltd.

Thor Bjorgolfsson (Iceland)
Chairman
Novator

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises, Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Mark Chandler (U.S.)
Chairman and CEO
Biophysical

Michael Chertoff (U.S.)
Co-founder and Managing Principal
Chertoff Group

Craig Cogut (U.S.)
Founder & Co-Managing Partner
Pegasus Capital Advisors

David Cohen (U.K.)
Chairman
F&C REIT Property Management

Joel Cowan (U.S.)
Professor
Georgia Institute of Technology

Addison Fischer (U.S.)
Chairman and Co-Founder
Planet Heritage Foundation

Adel Ghazzawi (U.A.E.)
Founder
CONEKTAS

Melissa Hathaway (U.S.)
President
Hathaway Global Strategies, LLC;
Former Acting Senior Director for Cyberspace
U.S. National Security Council

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Emil Hubinak (Slovak Republic)
Chairman and CEO
Logomotion

John Hurley (U.S.)
Managing Partner
Cavalry Asset Management

Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference

James L. Jones (U.S.)
Former United States
National Security Advisor

Haifa Al Kaylani (U.K.)
Founder & Chairperson
Arab International Women's Forum

Donald Kendall, Jr. (U.S.)
Chief Executive Officer
High Country Passage L.P.

Zuhal Kurt (Turkey)
CEO
Kurt Enterprises

Christine Loh (China)
Chief Executive Officer
Civic Exchange, Hong Kong

Ma Zhengang (China)
President
China Institute of International Studies

Michael Maples (U.S.)
Former Executive Vice President
Microsoft Corporation

F. Francis Najafi (U.S.)
Chief Executive Officer
Pivotal Group

Frank Neuman (U.S.)
President
AM-TAK International

Yousef Al Otaiba (U.A.E.)
Ambassador
Embassy of the United Arab Emirates in Washington D.C.

Sarah Perot (U.S.)
Director and Co-Chair for Development
Dallas Center for Performing Arts

Louise Richardson (U.S.)
Principal
University of St Andrews

John R. Robinson (U.S.)
Co-Founder
Natural Resources Defense Council

George F. Russell, Jr. (U.S.)
Chairman Emeritus
Russell Investment Group;
Founder, Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
Sanbar Development Corporation, S.A.

Ikram Sehgal (Pakistan)
Chairman
Security and Management Services

Kanwal Sibal (India)
Former Foreign Secretary of India

Henry J. Smith (U.S.)
Chief Executive Officer
Bud Smith Organization, Inc.

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., Ltd.

William Ury (U.S.)
Director
Global Negotiation Project at Harvard Law School

Pierre Vimont (France)
Ambassador
Embassy of the Republic of France in the United States

Alexander Voloshin (Russia)
Chairman of the Board of Directors
OJSC Uralkali

Charles F. Wald (U.S.)
DoD Director, Federal Government Services
Deloitte Services LLP

Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Marshall Bennett (U.S.)
President
Marshall Bennett Enterprises

John A. Roberts, Jr. (U.S.)
President and CEO
Chilmark Enterprises L.L.C.

J. Dickson Rogers (U.S.)
President
Dickson Partners, L.L.C.

Laurent Roux (U.S.)
Founder
Gallatin Wealth Management, LLC

George Sheer (U.S.)
President (retired)
Salamander USA & Canada
Founder & CEO
International Consulting Group, USA

Bengt Westergren (Sweden)
President (ret.)
AIG Central Europe & the Former Soviet Union

CHAIRMEN EMERITI

Berthold Beitz (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California at Los Angeles

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor and Minister of Foreign Affairs of Germany

Donald M. Kendall (U.S.)
Former Chairman & CEO
PepsiCo., Inc.

Whitney MacMillan (U.S.)
Former Chairman & CEO
Cargill, Inc.

Ira D. Wallach* (U.S.)
EWI Co-Founder

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
Chief Executive Officer
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
Institute for Regional Cooperation and Conflict Prevention
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, the OSCE and the United Nations in Vienna

William E. Murray* (U.S.)
Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates, Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
Former Minister of Foreign Affairs of Norway

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman of Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

Российско-американская программа по защите критически важной инфраструктуры

К выработке правил поведения в киберконфликтах: Женевские и Гаагские конвенции в информационном пространстве

Пилотный выпуск доклада был представлен на Мюнхенской конференции по безопасности 4-6 февраля 2011 года

Ведущие авторы:

Карл Фредерик Раушер, Институт Восток-Запад

Андрей Коротков, Московский государственный институт международных отношений министерства иностранных дел Российской Федерации

Перевод с английского языка на русский: Галина Чернакова

Редактор текста на русском языке: Владимир Иванов

Дизайн обложки и оформление: Драган Стояновски.

Институт Восток-Запад (ИВЗ), EastWest Institute (EWI) - международная, политически независимая, некоммерческая экспертная организация, специализирующаяся на противодействии критическим вызовам, создающим угрозу миру. ИВЗ был основан в 1980 году в целях содействия росту международного доверия, развития лидерства и поощрения сотрудничества ради прогресса. Институт имеет офисы в Нью-Йорке, Брюсселе и Москве. Контактные данные для получения дополнительной информации об Институте Восток-Запад или о настоящем документе:

The EastWest Institute 11 East 26th Street, 20th Floor New York, NY 10010 U.S.A. тел. +1-212-824-4100; эл.почта: communications@ewi.info. Для запросов по данному докладу обращайтесь к Францу Штефан-Гади или Эндрю Нагорскому. Адрес ИВЗ в Интернете: http://www.ewi.info