Олег Демидов

ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РОССИЙСКИЕ НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ

За последние два года вопросы, связанные с информационным пространством, окончательно перешли в разряд высших приоритетов международной безопасности. Свидетельствами этого стали сразу несколько событий и процессов, которые выглядят дистанцированными друг от друга, но уходят корнями в одну и ту же проблематику.

Во-первых, революционные события так называемой *Арабской весны* в мировом экспертном, медийном и политическом дискурсе оказались неразрывно связаны с ролью информационно-коммуникационных технологий (ИКТ). Несмотря на обильную спекулятивную составляющую и склонность преувеличивать роль социальных сетей и других инструментов Web 2.0 в революционных событиях на Ближнем Востоке и за его пределами, этот дискурс не был полностью лишен оснований. Беспрецедентная скорость распространения информации через интернет (в основном через социальные сети) сыграла против режимов, стремившихся скрыть свои репрессивные акции от международного сообщества и не владевших адекватными навыками ведения информационной борьбы. В то же время обилие непроверенной информации и попытки манипулирования ей привели к искажению глобальной информационной картины событий, которые происходили в Ливии, Сирии и других государствах Ближнего Востока.

Во-вторых, в США были приняты сразу два весьма значимых доктринальных документа, затрагивающих проблематику безопасности киберпространства. Международная стратегия по действиям в киберпространстве была опубликована 16 мая 2011 г. Ее логическим развитием в военной плоскости стала Стратегия Министерства обороны по действиям в киберпространстве, частично рассекреченная и опубликованная в июне 2011 г. В обоих документах киберпространство признается *средой действий*, то есть пространством проведения операций американских вооруженных сил наряду с землей, морем, воздухом и космосом[1]. Безопасность киберпространства впервые оказалась де-факто приравнена по своему значению к военной безопасности — и сделала это единственная в мире военная сверхдержава.

Последним по хронологии, но не по значимости событием в этом ряду стали инициативы России и представителей Шанхайской организации сотрудничества (ШОС), направленные на формирование глобального режима обеспечения безопасности информационного пространства. Речь идет прежде всего о концепции Конвенции ООН «Об обеспечении международной информационной безопасности». Концепция была презентована международному сообществу в ноябре 2011 г. на конференции по киберпространству в Лондоне. Чуть менее резонансной, но столь же масштабной по своим целям инициативой стал проект Правил поведения в области обеспечения международной информационной безопасности, направлен-

ный Генеральному секретарю ООН 12 сентября 2011 г. письмом от четырех государств — членов ШОС.

Наибольший интерес с международно-политической точки зрения вызывает концепция Конвенции об обеспечении МИБ. Представленный проект документа обладает несколькими характеристиками, которые позволяют назвать его не имеющим аналогов в международно-правовой практике регулирования информационного пространства. Так, в числе прочего проект документа:

- претендует на всеобъемлющий характер и полное урегулирование проблематики МИБ;
- должен через механизм ООН получить глобальный охват, распространившись на все международное сообщество;
- предполагает юридически обязывающий характер, не ограничиваясь декларативными заявлениями и формулированием общих принципов поведения государств в информационном пространстве;
- позиционируется как почти завершенный механизм, который, с точки зрения его авторов и сторонников, после соответствующей доработки может превратиться в действующий международно-правовой инструмент ООН уже в ближайшие годы.

С учетом этого российская инициатива в случае ее реализации станет значимой новацией для международного права в сфере ИКТ. Кроме того, превращение российских инициатив в механизмы ООН также будет иметь глобальные политические и военно-стратегические последствия. Поэтому концепция Конвенции, а также проект Правил поведения в области обеспечения МИБ (пусть и меньшей степени) напрямую затрагивают не только национальные интересы РФ, но и интересы ее ключевых зарубежных партнеров.

В связи с этим в настоящей статье инициативы Москвы и ее партнеров по ШОС в области обеспечения МИБ рассматриваются одновременно под углом российских национальных интересов и в то же время приоритетов мирового сообщества и его отдельных представителей, чьи позиции создают преграду продвижению российских проектов.

В рамках статьи предполагается осветить следующие вопросы:

1. Насколько недавние инициативы РФ и ее партнеров отвечают национальным российским интересам и интересам наших зарубежных партнеров и имеют шансы на реализацию в изначально задуманном формате?
2. Как рассматриваемые инициативы отразятся на политике России в области международного сотрудничества по борьбе с киберпреступностью? Необходимо ли России присоединяться к существующим механизмам в этой области или предлагать международному сообществу собственные решения, и какими они могут быть?
3. Какие меры может предпринять российское руководство для того, чтобы сблизить подходы и преодолеть наиболее острые противоречия с зарубежными партнерами и перевести строительство международного режима обеспечения МИБ из сферы дискуссий в практическое русло на компромиссной основе, но не отказываясь при этом от своих инициатив и их основополагающих принципов?

В *Таблице 1* представлены некоторые документы, затрагивающие вопросы обеспечения МИБ, включая действующие механизмы международного права (Екатеринбургское соглашение ШОС от 16 июня 2009 г.) и неофициальные проекты международно-правовых актов. К числу последних относится проект Глобального договора о кибербезопасности и киберпреступности авторства норвежского киберюриста Штайна Шольберга. В приведенной таблице все инициативы, включая

правительственные и неофициальные, упорядочены в рамках простейшей классификации по двум критериям:

а) уровень регулирования (от национального до глобального);

б) направления угроз, противодействие которым является приоритетом для того или иного документа.

Таблица 1. **Соотношение ключевых нормативно-правовых актов по сферам и уровням регулирования информационной безопасности**

Тип угроз/уровень регулирования	Кибер-преступность (*Citizens vs. Citizens*)	Кибер-шпионаж	Агрессивные действия государств в информационном пространстве		Информационный терроризм (*Citizens vs. States*)
			против государств (*States vs. Citizens*)	против граждан (*States vs. States*)	
Глобальный	КОНВЕНЦИЯ О МИБ ДОГОВОР ШОЛЬБЕРГА КОНВЕНЦИЯ СЕ ПРАВИЛА ПОВЕДЕНИЯ (ШОС)	КОНВЕНЦИЯ О МИБ ДОГОВОР ШОЛЬБЕРГА ПРАВИЛА ПОВЕДЕНИЯ (ШОС)	КОНВЕНЦИЯ О МИБ ДОГОВОР ШОЛЬБЕРГА (только кибер-пространство) ПРАВИЛА ПОВЕДЕНИЯ (ШОС)	?	КОНВЕНЦИЯ О МИБ ДОГОВОР ШОЛЬБЕРГА (только кибер-терроризм) ПРАВИЛА ПОВЕДЕНИЯ (ШОС)
Регио-нальный	СОГЛАШЕНИЕ ШОС 2009 КОНВЕНЦИЯ СЕ	СОГЛАШЕНИЕ ШОС 2009	СОГЛАШЕНИЕ ШОС 2009		СОГЛАШЕНИЕ ШОС 2009
Нацио-нальный	НАЦИОНАЛЬНАЯ СТРАТЕГИЯ КИБЕР-/ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				

Условные обозначения:
КОНВЕНЦИЯ О МИБ — российская концепция Конвенции об обеспечении международной информационной безопасности ООН, презентованная в ноябре 2011 г.
ДОГОВОР ШОЛЬБЕРГА — неофициальный проект Глобального договора о кибербезопасности и киберпреступности ООН Штайна Шольберга и Соланж Гернутти-Эли.
ПРАВИЛА ПОВЕДЕНИЯ (ШОС) — проект Правил поведения государств в области обеспечения международной информационной безопасности, выдвинутый странами — членами ШОС, включая Россию, в сентябре 2011 г.
СОГЛАШЕНИЕ ШОС 2009 — Межправительственное соглашение государств — членов ШОС о сотрудничестве в области обеспечения МИБ от 16 июня 2009 г.
КОНВЕНЦИЯ СЕ — Конвенция Совета Европы «О киберпреступности», открытая для подписания 23 ноября 2001 г.

Кроме того, в таблице фигурирует национальная стратегия информационной безопасности (или, как альтернатива, стратегия кибербезопасности), которая замыкает на себя вопросы обеспечения безопасности в области использования ИКТ как часть национальной государственной политики. Вопрос о том, нуждается ли Россия в выработке и принятии подобной стратегии, призванной дополнить и раз-

вить существующую Доктрину информационной безопасности от 2000 г., является дискуссионным и требует отдельного исследования, выходящего за рамки данной статьи. Также за рамки настоящей работы вынесен вопрос относительно того, какими механизмами должно регулироваться противодействие агрессивному поведению в киберпространстве государств и действующих в их интересах посредников в отношении частного сектора, гражданского общества и отдельных пользователей. Пока эта проблема остается нерешенной как на национальном, так и на международном уровнях.

ИСТОРИЯ РОССИЙСКИХ ИНИЦИАТИВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МИБ И МЕЖДУНАРОДНАЯ РЕАКЦИЯ НА НИХ

РФ в течение долгого времени уделяла значительное внимание продвижению тематики международного взаимодействия в сфере обеспечения МИБ через каналы ООН. Подробный обзор участия Российской Федерации в выработке механизмов регулирования безопасности информационного пространства приводит в своих работах и выступлениях А. В. Крутских. С весны 2012 г. г-н Крутских занимает должность специального координатора по вопросам использования ИКТ в политических целях в МИД России[2]. Начиная с первой половины *нулевых* годов именно он возглавлял российские делегации и группы правительственных экспертов ООН, которые создавались в рамках инициатив по изучению возможностей международного сотрудничества для борьбы с угрозами МИБ.

Как отмечает г-н Крутских, «с 1998 г. Россия продвигает идею налаживания международного сотрудничества по укреплению МИБ», при этом с самого начала «работа по согласованию конкретных мер в интересах упрочения МИБ проводилась главным образом через механизм ООН»[3]. Действительно, ежегодно в течение ряда лет российской стороной на рассмотрение Генассамблеи ООН вносились проекты резолюций «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». В проектах резолюций содержались призывы к рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных мер по ограничению угроз, возникающих в этой сфере.

Первая из этих резолюций (A/RES/53/70) от 4 декабря 1998 г. была принята Генеральной Ассамблей без голосования, консенсусом[4]. Однако принятый текст резолюции не соответствовал изначальному варианту, который был направлен Генеральному Секретарю ООН в письме от 23 сентября 1998 г. от постоянного представителя РФ при ООН, российского министра иностранных дел И. С. Иванова. Уже на тот момент в приложенном к письму проекте резолюции были сформулированы ключевые цели, которые отечественная дипломатия пытается решить сегодня в рамках концепции Конвенции об обеспечении МИБ. В частности, в проекте резолюции всем государствам — членам ООН предлагалось информировать Генерального Секретаря о своих взглядах на:

- использование информационных технологий в военных целях;
- определение понятий «информационное оружие» и «информационная война»;
- целесообразность строительства международно-правовых режимов с целью запрещения разработки особо опасных форм информационного оружия[5].

Однако в итоговом варианте резолюции эти проблемы не были отражены. Несмотря на это, вносимые Российской Федерацией резолюции принимались Генеральной Ассамблеей консенсусом в последующие годы, вплоть до 2005 г.

Еще одним направлением, на котором российская дипломатия активизировала свои усилия для обсуждения вопросов обеспечения МИБ, стало двустороннее

российско-американское обсуждение этой проблематики, также начатое в 1998 г. Итогом такого обсуждения стало *Совместное российско-американское заявление об общих вызовах безопасности на рубеже XXI в.*, которое президенты РФ и США подписали 2 сентября 1998 г. На том этапе, однако, существенных успехов в плане продвижения своего понимания МИБ российской стороне добиться не удалось. В тексте совместного заявления «ослабление действия негативных аспектов информационной технологии» признавалось «серьезной задачей в деле обеспечения стратегических интересов безопасности наших двух стран в будущем»[6]. Однако никакой системы международного сотрудничества документ не предлагал, а в части конкретики уделял внимание взаимодействию по совместному преодолению актуальной на тот момент «проблемы–2000», связанной со сменой компьютерных кодировок с наступлением новой календарной даты. Вместе с тем сам факт появления совместного заявления стал существенным шагом для двух стран в плане признания проблематики МИБ как важной составляющей двусторонних отношений. Кроме того, практика двустороннего российско-американского взаимодействия и совместных заявлений получила развитие в дальнейшем, спустя многие годы. 28 июня 2011 г. было опубликовано совместное заявление заместителя секретаря Совета Безопасности Российской Федерации Н. В. Климашина и (на тот момент) координатора Белого дома по кибербезопасности Говарда Шмидта.

Помимо двусторонних обсуждений и внесения проектов резолюций на сессиях Генассамблеи ООН Российская Федерация активно использовала механизм Групп правительственных экспертов (ГПЭ) ООН для продвижения повестки дня в области МИБ. Впервые ГПЭ ООН была учреждена 8 декабря 2003 г. во исполнение резолюции ГА ООН A/RES/56/19 от 29 ноября 2001 г. Целью Группы была активизация международного рассмотрения существующих и потенциальных угроз в сфере информационной безопасности, возможных мер по ограничению таких угроз, возникающих в этой сфере, и изучение международных стратегий, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем[7]. Первый проект доклада по итогам работы Группы был подготовлен в 2004 г., однако в изначальном виде не был принят консенсусом из-за серьезных разногласий между членами Группы и, в частности, противодействия российскому подходу со стороны представителей США. В результате в 2005 г. удалось принять лишь процедурный доклад A/60/202, в котором констатировалось, что «с учетом сложного характера вопросов, о которых идет речь, не было достигнуто консенсуса относительно подготовки окончательного доклада»[8].

Противоречия между участниками ГПЭ касались прежде всего двух вопросов, имевших политическое значение. Первый из них, принципиально важный для представителей РФ, касался военно-политических аспектов ИКТ и влияния этих технологий на национальную безопасность и международный военно-политический баланс. Несмотря на общее признание важности этих вопросов членами ГПЭ, им не удалось прийти к общему мнению относительно того, стоит ли включать в текст доклада формулировки, которые смещали бы общий акцент на угрозы, обусловленные использованием ИКТ в военно-политических целях государствами. Второе противоречие касалось вопроса о том, должны ли быть предметом рассмотрения Группы вопросы, связанные с содержательным наполнением распространяемой информации — *контентом*, или рассматривать следует лишь те вопросы, которые связаны с безопасностью информационной инфраструктуры. Первую точку зрения можно с некоторыми оговорками назвать *российской*, вторую — *американской*. Один из конкретных вопросов в этой связи касался того, следует ли рассматривать передачу и распространение трансграничной информации через ИКТ-сети в качестве вопроса национальной безопасности и обеспечивать соответствующий контроль над ними[9].

Призыв к созданию следующей ГПЭ прозвучал, вновь по инициативе России, уже 8 декабря 2005 г., когда была принята очередная резолюция «Достижения в сфере информатизации...» (A/RES/60/45)[10]. Как отмечает А. В. Крутских, возглавивший вторую ГПЭ, «несмотря на давление американской делегации [...] россий-

ские предложения по вопросам МИБ поддержали Япония, Израиль, Южная Корея, Австралия и Канада»[11]. Группа из 15 экспертов–представителей различных стран была сформирована в 2009 г. и завершила свою деятельность в 2010 г. после серии из четырех сессий. В отличие от предыдущей ГПЭ, итогом работы второй Группы стал принятый консенсусом и представленный на 65-й сессии Генеральной ассамблеи в июле 2010 г. доклад, который отразил некоторые ключевые вопросы и озабоченности российской стороны по поводу применения ИКТ в военно-политических целях. В частности, в докладе отмечается, что ИКТ могут «использоваться в целях создания угрозы международному миру и национальной безопасности». Кроме того, впервые в рамках ООН в документе была прямо отмечена угроза, связанная с тем, что «государства разрабатывают ИКТ в качестве инструментов ведения войны и разведки и для применения в политических целях». Наконец, в число итоговых рекомендаций в докладе было включено «принятие мер по укреплению доверия, обеспечению стабильности и уменьшению рисков в связи с последствиями государственного использования ИКТ, включая обмен мнениями стран по вопросу об использовании ИКТ в конфликтах»[12]. С учетом таких формулировок деятельность второй ГПЭ стала *прорывом* для России, сумевшей существенно продвинуть повестку дня в сфере ИКТ с учетом тех аспектов, которые являлись — и до сих пор являются — для нее центральными.

Последняя, третья ГПЭ была учреждена резолюцией Генассамблеи ООН A/RES/66/24, принятой без голосования 2 декабря 2011 г., чтобы продолжить изучение существующих и потенциальных угроз в сфере информационной безопасности, а также возможных стратегий по рассмотрению таких угроз. Деятельность группы, в которую, как и в предыдущие ГПЭ, входят российские представители, включает три встречи недельной продолжительности. Первая из встреч Группы прошла 6–10 августа 2012 г. в Нью-Йорке, последняя состоится там же в июне 2013 г.

В общем и целом деятельность ГПЭ внесла большой вклад в продвижение проблематики ИКТ в контексте МИБ, и в том числе российского видения этих вопросов. Любопытно, что с течением времени даже США перестали отрицать важность проблемы использования ИКТ государствами в военно-политических целях. В докладе Генерального секретаря ООН от 15 июля 2011 г. (A/66/152) в ответе, полученном от правительства США, среди мотивов деятельности, создающей угрозы работе глобальной сети и критических инфраструктур, упоминается «перенесение традиционных форм государственного конфликта в киберпространство»[13], а в число субъектов, создающих такие угрозы, включены государства. В том же докладе отмечается, что «в ряде обстоятельств подрывная деятельность в киберпространстве может представлять собой вооруженное нападение»[14]. Вместе с тем Вашингтон по-прежнему отстаивает приоритет вопросов инфраструктуры и не желает рассматривать проблему содержания трансграничных информационных потоков в плоскости международной безопасности.

Кроме того, в контексте настоящей статьи немаловажно то, что дискуссии в ходе деятельности ГПЭ и обсуждения проектов вышеназванных резолюций позволили выработать некий вариант *нейтральной терминологии*. В тексте резолюций рассматриваемая проблематика формулируется вне рамок западной лексики кибербезопасности и, по большей части, не в терминах «обеспечения МИБ». Поиски участниками ГПЭ взаимоприемлемых формулировок с целью нахождения компромисса привели к тому, что тексты резолюций обращены к проблематике «ИКТ в контексте международной безопасности», что корректно и нейтрально, хотя и достаточно размыто, характеризует суть затрагиваемых вопросов. Потенциал использования официальной терминологии резолюций Генассамблеи ООН для сближения подходов РФ и ее зарубежных партнеров в настоящее время будет рассматриваться ниже.

Сегодня можно говорить о том что, несмотря на впечатляющую активность России в продвижении проблематики обеспечения МИБ за последние 15 лет, с разработкой концепции Конвенции в 2011 г. усилия российской дипломатии вышли

на принципиально новый уровень. Полноценная презентация документа прошла 1 ноября 2011 г. в Лондоне, на Конференции по вопросам киберпространства. С речью, посвященной преимущественно концепции Конвенции, выступил И. О. Щеголев, на тот момент глава Министерства связи и массовых коммуникаций РФ. Незадолго до этого, 22 сентября 2011 г. документ был представлен главам спецслужб и силовых ведомств 52 стран на встрече в Екатеринбурге[15]. Чуть ранее, 12 сентября 2011 г. Генеральному секретарю ООН было направлено письмо от Постоянных Представителей в ООН четырех государств ШОС — России, Китая, Узбекистана и Таджикистана. К письму прилагался проект Правил поведения в области обеспечения международной информационной безопасности. В отличие от концепции Конвенции, Правила не носят юридически обязывающего характера, но в целом воспроизводят проблематику концепции Конвенции, хотя и без столь явного упора на военно-политическую составляющую информационной безопасности.

Международная реакция на инициативы Москвы в большинстве случаев характеризуется довольно острым интересом, который, однако, до настоящего времени не выливался в конкретные встречные инициативы. В Азиатско-Тихоокеанском регионе, где Россия пыталась последовательно наращивать активность в преддверии Саммита АТЭС в августе 2012 г., идеи Конвенции и Правил поведения были встречены противоречиво. В рамках Азиатско-Тихоокеанского совета сотрудничества по безопасности (АТССБ), *трека два*, объединяющего 22 страны региона, включая Индию, США, Японию, Китай и Россию, инициативы РФ и ШОС были встречены с интересом, но также с недоверием и определенным скепсисом. Наибольший интерес к ним проявляет Индия, претендующая на роль одной из ведущих IT-держав и в то же время все более опасающаяся киберугроз, исходящих от Китая, своего основного соперника в Азии. В апреле 2012 г., в Гармиш-Партенкирхене (ФРГ) прошел шестой международный форум[16], посвященный в основном вопросам МИБ. В ходе форума впервые публично обсуждалась российская концепция Конвенции. В поддержку документа высказался заместитель главы организации оборонных исследований Минобороны Индии Амит Шарма, призвав дополнить российский проект определениями из области кибербезопасности, в частности понятиями *национального киберпространства* и *враждебных действий государств в киберпространстве*. В целом, в восточноазиатском регионе для России в плане обсуждения вопросов международной безопасности интересны прежде всего Восточно-Азиатские саммиты, АСЕАН и Региональный форум АСЕАН — АРФ, а также упомянутый *трек* АТССБ. На данный момент, спустя год после презентации концепции Конвенции, в рамках этих форматов не было принято конкретных решений о поддержке российских инициатив. Однако привлечение на сторону российского подхода Индии представляется весьма важной задачей. Россия вместе с КНР — лишь две крупные державы, отстаивающие собственное понимание роли ИКТ в контексте международной безопасности. С Индией речь идет уже о половине человечества, включая «крупнейшую в мире демократию».

Одна из ключевых причин осторожного отношения к российским инициативам состоит в том, что проблематика военно-политического использования ИКТ по-прежнему остается чувствительной для ряда государств и не всегда включается в повестку дня многостороннего международного взаимодействия. К примеру, на встрече Рабочей группы по кибербезопасности АТССБ в Бенгалуру в октябре 2011 г. реакция на инициативу эксперта ПИР-Центра о внесении в повестку дня вопросов агрессивного поведения государств в киберпространстве сводилась к тезису о том, что этот вопрос не укладывается в формат деятельности группы. При этом — и такой подход характерен отнюдь не только для формата АТССБ — вопрос военно-политических аспектов применения ИКТ позиционируется как фактор, который политизирует повестку дня и подразумевает необходимость «дружбы против третьего». Подобное понимание сути и цели проблем, которые поднимает российская сторона, довольно далеко от действительности. Однако его широкое распространение говорит, в том числе, о том, что сама концепция Конвенции

и родственные ей инициативы в нынешнем виде звучат недостаточно внятно и четко и оставляют пространство для интерпретации их задач и приоритетов.

Кроме того, для части российских партнеров, прежде всего для ЕС и США, объектом критики выступают нормы концепции Конвенции, предполагающие запрет на распространение информации, «которая вдохновляет терроризм, сепаратизм, экстремизм или подрывает политическую, экономическую и социальную стабильность других стран». В данных положениях зарубежные партнеры РФ усматривают скрытый потенциал для интернет-цензуры и контроля над национальными сегментами глобальной Сети. Так, после ноябрьской конференции 2011 г. в Лондоне заместитель госсекретаря США Майкл Познер назвал проект Правил поведения в области обеспечения МИБ неприемлемым решением, за счет которого интернет превращается «из пространства, управляемого множеством людей и заинтересованных сторон», в систему, «подконтрольную центральным правительствам»[17]. С момента презентации концепции Конвенции и Правил поведения целый ряд аналогичных заявлений был озвучен высокопоставленными чиновниками и дипломатами США, СЕ и стран Европы. Тональность высказываний западных дипломатов не претерпела существенных изменений и год спустя, на очередной конференции по вопросам киберпространства в Будапеште 4–5 октября 2012 г. Как заявил в своем выступлении на конференции глава британского МИД Уильям Хейг, прозрачно намекая на российскую концепцию Конвенции, Лондон «не призывает к новому межправительственному договору [по вопросам кибербезопасности], который был бы обременителен в плане согласования, трудновыполним и слишком узок по своему охвату»[18].

При анализе критической реакции зарубежных партнеров России на инициативы в области МИБ следует прежде всего учитывать то, что на Западе и в ряде других стран распространен фундаментально иной подход к вопросам регулирования информационного обмена. Этот подход предполагает принципиально меньший по сравнению с российскими инициативами объем контроля государства над информационными потоками и их содержанием, в том числе применительно к трансграничному информационному обмену. В результате многие вопросы и проблемы, которые затрагивают концепция Конвенции и Правила поведения, наши партнеры вообще не считают уместными для обсуждения и регулирования в категориях международного права.

Подобная точка зрения распространяется на экспансию и доминирование в глобальном информационном пространстве, принуждение государств к принятию решений в чужих интересах и ряд подобных им угроз, которые упоминаются в концепции Конвенции. Прежде всего существование ряда угроз из этого перечня вообще не всегда признается нашими партнерами. Кроме того, большинство акторов, обеспечивающих формирование *контента* в глобальном информационном пространстве, в западных странах не находятся под прямым государственным контролем и зачастую имеют транснациональную природу. Подчинение их нормам межправительственного соглашения, по мнению наших партнеров, не соотносится с логикой *децентрализованного* информационного пространства. Наконец, те виды деятельности (психологическая война), наличие и важность которых не оспариваются, являются приоритетом спецслужб и не подлежат согласованию в рамках международного диалога.

В свою очередь, в основе подхода, который сегодня является концептуальной альтернативой российским инициативам в области обеспечения МИБ, лежит иное определение сферы рассматриваемых проблем и угроз безопасности — через понятие *кибербезопасности*. Соответственно, рассматривается и совсем другая среда — *киберпространство* вместо информационного пространства. Подробный анализ западного подхода выходит за рамки задач настоящей статьи, но в целом необходимо отметить, что парадигматика кибербезопасности включает прежде всего упор на безопасность инфраструктуры компьютерных сетей. Вопросы влияния информационных потоков на социополитические и иные процессы в проблематику кибербезопасности практически не включаются — и это один из основных

идейных разломов с концепцией МИБ. Проблематика кибербезопасности ограничивается спектром цифровых технологий, в отличие от МИБ. В основном границы проблематики кибербезопасности определяются через совокупность информационных систем, функционирующих на основе *двоичного кода*.

Для согласования подходов России и западных государств и лучшего понимания парадигматики кибербезопасности был даже выработан специальный глоссарий с переводом ключевых терминов западного происхождения. В совместном исследовании Института Запад–Восток (East–West Institute) и Института проблем информационной безопасности (ИПИБ) МГУ имени М. В. Ломоносова («*Российско-американский базовый перечень критических понятий в области кибербезопасности*») выработана согласованная русско-английская понятийная база по ключевым военно-политическим вопросам кибербезопасности. В итоговый доклад были включены определения основных 20 терминов, включая кибервойны, киберконфликты и собственно киберпространство[19]. Однако на текущий момент лучшее понимание не способствует сближению двух подходов. Напротив, конкуренция России и ее союзников (КНР и другие государства ШОС) с западными государствами в части утверждения на глобальном уровне того или иного понимания роли ИКТ в контексте международной безопасности приобретает черты идеологического противостояния.

Так или иначе, сущностное рассмотрение концепции Конвенции невозможно без более подробного анализа терминологии, на которой она основана и которая несет в себе принципиальные черты российского подхода к вопросам МИБ, глубоко отличающегося от западных концепций.

ТЕРМИНОЛОГИЯ РОССИЙСКИХ ИНИЦИАТИВ: КОНЦЕПТУАЛЬНЫЕ ВЫЗОВЫ И УЯЗВИМЫЕ МЕСТА

Первой ключевой характеристикой, в равной степени присущей проекту Правил поведения, концепции Конвенции и Екатеринбургскому соглашению ШОС, является опора на понятия информационной безопасности и информационного пространства, которые используются почти в той же форме, в которой они существуют в национальном законодательстве РФ. Ведущая роль российской стороны как теоретика и идеолога названных международных документов и инициатив обусловила тот факт, что именно российский подход лег в основу их терминологической базы. В результате бо́льшая часть понятий и определений, в частности в концепции Конвенции, преемственны либо близко родственны по отношению к российским доктринальным документам.

Однако концептуальные и терминологические противоречия возникают в тех случаях, когда Россия пытается предложить новые для международного права определения, особенно в части регулирования поведения государств в информационном пространстве. Одним из примеров является определение *информационной войны*, которое представляет собой одно из ключевых понятий в рамках российского подхода к обеспечению МИБ. В концепции Конвенции это определение также заимствовано. В рамках законодательства России понятие информационной войны впервые фигурировало в Доктрине ИБ от 2000 г., однако в документе не содержалось соответствующего определения.

С 2009 г. такое определение появилось, причем сразу на уровне действующего международного договора. Понятие и определение информационной войны было зафиксировано в межправительственном соглашении государств — членов ШОС о сотрудничестве в области обеспечения МИБ, которое было подписано 16 июня 2009 г. в Екатеринбурге во время шестого саммита организации (далее по тексту — Екатеринбургское соглашение ШОС). В документе под информационной войной понимается «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва поли-

тической, экономической, социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»[20].

Следует выделить несколько особенностей приведенного определения, которые важны для понимания сути доктринального видения, частью которого оно выступает.

Во-первых, в рамках определения (как и, по большей части, в концепции Конвенции в целом) не упоминается и не рассматривается возможность участия в информационных войнах разного рода *негосударственных акторов*. Между тем государствоцентричное понимание конфликтов в информационном пространстве прямо противоречит реально наблюдаемой картине. Во-первых, если взять в качестве примеров кибератаки в Грузии в 2008 г., в Эстонии в 2007 г., а также атаки на иранские или американские сети в последние годы, за ними всегда стоят некие субъекты, чьи действия могут осуществляться в интересах тех или иных государств, но прямую связь при этом проследить затруднительно или невозможно. Иногда речь действительно идет о лицах и группах, являющихся частью государственных силовых структур и спецслужб. Однако зачастую эти субъекты представляют собой либо группы, действующие автономно из патриотических или иных побуждений, либо *посредников*, которые действуют в интересах и/или по заказу государственных структур, либо иным косвенным образом связаны с ними. Проблема посредников неотделима от вопросов информационных войн, так как одним из ключевых препятствий к использованию механизмов международного права в сфере обеспечения МИБ является нерешенность проблемы атрибуции — определения авторства деструктивных действий в информационном пространстве и ответственности за их осуществление. Как отмечается в исследовании ПИР-Центра, единственным способом, позволяющим достоверно установить связь субъектов, осуществляющих деструктивную деятельность в киберпространстве, с государственными структурами, остается агентурная работа спецслужб. Однако ни одна из национальных разведок в обозримом будущем не будет располагать ресурсами, позволяющими системно решать задачи по выявлению такого рода связи в случае каждой политически мотивированной кибератаки[21].

Другая субстантивная сложность, связанная с определением информационной войны в концепции конвенции и Екатеринбургском соглашении ШОС связана с тем, что оно описывает сразу несколько различных явлений и процессов, между которыми на практике далеко не всегда присутствует взаимосвязь. С одной стороны, под информационной войной фактически понимаются кибератаки на ИКТ-сети и инфраструктуру, с другой же стороны, речь идет о классической *психологической войне* в западном понимании. По этой логике, применение *Stuxnet, Duqu, Flame* и *Gauss* против информационной инфраструктуры в государствах Ближнего Востока, атаки на сервера госучреждений и компаний частного сектора в Эстонии в 2007 г. и в Грузии в 2008 г., а также программы вещания финского телевидения на территорию СССР в 1980-х гг. следует считать эпизодами информационной войны. Вопрос состоит в том, что общего у этих событий и как объединение их в единую категорию угроз помогает выработать дифференцированные подходы к их отражению.

Кроме того, определение информационной войны в концепции Конвенции не совсем корректно идентифицирует цели тех действий и процессов, которые оно в себя включает. В частности, встает вопрос об эффективности определения как рабочего инструмента классификации угроз МИБ применительно к проблеме кибершпионажа, который также может быть составляющей информационной войны. Следует оговориться, что речь не идет о коммерческом кибершпионаже, практикуемом с целью кражи ноу-хау, клиентских баз, карт месторождений и рыночных исследований организаций частного сектора. Ближневосточные сложные вирусы, в частности *Duqu* и *Flame*, являют собой пример кибершпионажа иного уровня и масштаба. Имеется в виду сбор данных о критических объектах, программах,

а также связанных с ними персоналиях, для последующих действий в отношении данных *целевых объектов*. В иранских сетях до сих пор действуют высококлассные инструменты, адаптированные под конкретные учреждения (*Duqu*), а иногда и под конкретных людей, имеющих отношение к ядерной и ракетной программам Тегерана. При этом до последнего времени параллельно функционировало целое семейство программ, по всей вероятности, созданных киберспециалистами из числа американских военных и разведки. На данный момент выявлено, как минимум, четыре беспрецедентно сложных программы (*Stuxnet, Duqu, Flame, Gauss*), не считая серии их модификаций; ведется поиск и других программ (*Wiper*). *Лабораторией Касперского* также выявлены три неиспользованных *заготовки* вирусов с кодом, родственным коду *Flame*[22].

Понятийный аппарат концепции Конвенции не позволяет уверенно ответить на вопрос о том, как квалифицировать подобную деятельность на международном уровне и бороться с ней. Еще одно противоречие здесь заключается в том, что многие эксперты как на Западе, так и в РФ (например, Евгений Касперский[23]) называют *Flame, Gauss, Duqu* и другие шпионские программы, выявленные в иранских сетях, *кибероружием* и характеризуют их применение как эпизод информационной войны. Но в концепции Конвенции об обеспечении МИБ термин «информационное оружие» замкнут на понятие информационной войны и определяется как «информационные технологии, средства и методы», предназначенные для ее ведения. В результате акты кибершпионажа как бы выпадают из понятийного аппарата документа, так как не наносят ущерба информационным системам, критическим структурам и не ведут к психологической обработке населения. Важно подчеркнуть, что *Stuxnet* в данном случае стоит особняком, представляя собой орудие *киберсаботажа*, то есть, несомненно, информационное оружие. А вот как классифицировать *Flame*, который «устанавливает профессиональную систему слежения с четко обозначенными целями»[24], но сам ничему не вредит, из концепции Конвенции неясно.

Представляется, что проект документа должен быть дополнен отдельной статьей, в рамках которой рассматривались бы вопросы кибершпионажа, а также вводилось бы соответствующее определение. Более того, особого пункта и определения *заслуживает кибершпионаж с целью сбора критических знаний и дальнейшего использования в военно-стратегических целях,* который должен рассматриваться не как правонарушение, а как акт международной агрессии. Подобное разделение важно, так как именно подобные программы и средства кибершпионажа сегодня называют кибероружием — без соответствующих юридических оснований.

Спорные моменты в терминологии концепции Конвенции не исчерпываются определением информационной войны. Несколько противоречиво выглядит определение информационного *пространства* как «*сферы деятельности*». Дело в том, что подобная дефиниция затрудняет дальнейшее развитие стратегий и направлений практической деятельности госорганов и иных структур в этой области. Так, во второй половине 2011 г. в Минобороны РФ был подготовлен первый в своем роде документ, который был опубликован в январе 2012 г. под названием *Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве*[25]. Терминология документа полностью идентична понятийному аппарату концепции Конвенции, в том числе в части использования понятия информационного пространства. Однако в этом случае возникает вопрос с частичной рекурсивностью понятия *деятельности ВС в информационном пространстве* — исходя из терминологии обоих документов речь идет о *деятельности в сфере деятельности*. В результате определение не становится некорректным, но страдает размытостью; исходя из него к ведению вооруженных сил должна относиться вся деятельность по формированию, созданию, преобразованию, передаче, использованию, хранению информации. Из этого спектра нельзя выделить задачи, *специфически* присущие вооруженным силам и не присущие СМИ, дипломатии, политическим и негосударственным структурам.

Характерно, что авторы документа Минобороны в результате идут другим путем и определяют деятельность ВС в информационном пространстве как «*использова-*

ние вооруженными силами информационных ресурсов для решения задач обороны и безопасности». Само понятие информационного пространства как отдельного термина из концепции Конвенции и документа Минобороны здесь не используется, а определение формируется на основе другого понятия — информационных ресурсов. Таким образом, нарушается логическая целостность определения и концептуальная стройность документа.

При этом содержание ключевых определений дублируется и воспроизводится в других определениях и статьях документа, в которых содержатся отсылки на них. Так, рассмотренное понятие *информационной войны* в тексте концепции Конвенции фигурирует еще в одном определении и трех статьях. Схожая ситуация наблюдается и с Правилами поведения в области обеспечения МИБ, в которых используется по большей части та же самая терминологическая база.

Специфика подхода к МИБ России и ее единомышленников по ШОС, отраженная в концепции Конвенции, не исчерпывается ее ключевыми определениями. Более принципиальной особенностью документа является видение в национальных государствах ключевых участников глобального информационного обмена, обладающих полным контролем над трансграничными информационными потоками. В рамках этой логики информационное пространство, хотя и является *общечеловеческим достоянием,* тем не менее делится на информационные пространства государств, к которым в полной мере применим принцип государственного суверенитета. Наиболее четко эта идея формулируется в пункте 5 статьи 5 концепции Конвенции, гласящем, что «каждое государство-участник вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством». Суверенитет государства в информационном пространстве подразумевается и пунктом 7 упомянутой статьи, согласно которому «каждое государство-участник имеет право свободно осуществлять без вмешательства извне развитие своего информационного пространства».

Особо важен тот факт, что из подобного подхода напрямую следует государствоцентричность не только информационного пространства, но и самого информационного обмена. Иными словами, подразумевается, что государства в полной мере контролируют *содержание* трансграничных информационных потоков и несут за это содержание ответственность. Такой подход, в частности, постулируется шестым основным принципом обеспечения МИБ концепции Конвенции, который предполагает ответственность государств «за собственное информационное пространство, в том числе за его безопасность и за содержание размещаемой в нем информации». При этом негосударственные участники мирового информационного обмена в документе в основном не упоминаются. В результате логика концепции Конвенции не позволяет документу охватить субъектов, которые в общем-то наполняют мировую систему коммуникаций содержанием и без которых информационный обмен невозможен:

- *Частный сектор.* Организации частного сектора выступают ключевыми субъектами в вопросах, связанных с кибербезопасностью. На частные компании приходится весьма значительная доля кибератак, причем зачастую политически мотивированных. В сетях частных структур ведется основная масса операций кибершпионажа, однако они же выступают абсолютными лидерами в области разработки средств и технологий защиты от киберугроз как рядовых юзеров, так и стратегических компаний и госструктур. Сверхсекретная сеть Пентагона *JWICS (Джейвикс)* не была бы создана без технологий частного сектора; созданием защищенных информационных систем и средств их защиты для российского Минобороны сегодня также занимаются частные компании. В США, КНР, России и других *кибердержавах* ведется активное взаимодействие между военными структурами и сообществами хакеров. Наконец, нельзя обойти тот факт, что частный сектор в лице частных провайдеров, телекоммуникационных корпораций и ИТ-компаний обеспечивает технологическое функционирование и развитие системы глобального обмена информацией. Частный

сектор во многом обеспечивает информационный обмен, предоставление доступа к информации основной массе пользователей, эффективную защиту от угроз в информационном пространстве.

- Отдельного упоминания заслуживают *глобальные СМИ*, которые по большей части также имеют негосударственную природу. От них зависит формирование наполнения, содержания мирового информационного обмена — и они не могут однозначно ассоциироваться с теми или иными государствами. *BBC, CNN, Al Jazeera* зачастую вносят вклад в искажение глобальных информационных потоков — события августа 2008 г. в Грузии, 2011 г. в Ливии, 2012 г. в Сирии и многие другие эпизоды служат тому примерами, но ответственность за их действия не может автоматически возлагаться на Великобританию, США, Катар или любое другое государство. С учетом того, что критерии информации, представляющей угрозу для МИБ, в концепции Конвенции отсутствуют, встает вопрос об имплементации упомянутого принципа ответственности государств за содержание информации в национальных сегментах информационного пространства. Понятия и критерии противозаконной информации существенно варьируются в различных государствах, не говоря уже о том, что львиная доля информации, представляющей угрозы для МИБ в рамках изложенного в концепции Конвенции видения, может вообще не подпадать под правовые санкции в национальных законодательствах. Даже принцип территориальной ответственности государств за *кибер*угрозы, предлагаемый рядом американских экспертов, весьма трудно воплотим на практике, хотя охватывает куда более узкую проблематику. По крайней мере, пока не решена проблема атрибуции в отношении кибератак. Возложение ответственности за действия медиа-акторов на государственные субъекты в рамках принципа территориальной ответственности — тот пункт, который России будет особенно трудно сдвинуть с мертвой точки. Без адекватного юридического обоснования он рискует быть воспринят как норма, подрывающая устои частного сектора и легитимирующая цензуру в СМИ и информационном пространстве в целом. В приведенной формулировке и в отсутствие более подробного ее разъяснения данное положение скорее выглядит контрпродуктивным и рискует вызвать возражения у большинства зарубежных партнеров РФ.

- Не менее важны *интернет-сообщества,* которые играют все большую роль в глобальном информационном обмене в интернете, где отсутствуют иерархия, правовая система, а зачастую и идентификация. Прежде всего существует проблема анонимности, которая делает идею ответственности государств за содержание информационного обмена в Сети достаточно условной. На сегодняшний день в мире не выработаны единые, официально согласованные стандарты и подходы к глобальной интернет-идентификации и аутентификации; простых решений в этой сфере не просматривается[26]. При этом преодоление анонимности участников информационного обмена в Сети сталкивается прежде всего не с техническими проблемами, а с вопросом о том, как быть, если анонимность признается правом? Концепция Конвенции не предлагает решений проблемы анонимности — однако в таком случае принципы, постулируемые в ней, не могут быть эффективно имплементированы. Россия не может нести ответственность за свое информационное пространство, если ее госорганы не имеют права устанавливать личность участников интернет-коммуникаций (пользователей анонимного видеохостинга, чата, блога), пока размещаемая ими информация не нарушает национальное законодательство. При этом тот факт, что информация, создающая угрозу МИБ, автоматически будет носить противоправный характер, далеко не очевиден. Загрузка видео на *YouTube* с недостоверной информацией о событиях в Сирии или Ливии не является правона-

рушением. Однако загрузка сотен тысяч таких видеозаписей в рамках скоординированной кампании — именно то, что положения концепции Конвенции позволяют расценивать как угрозу МИБ.

Помимо проблемы анонимности встает вопрос с трансграничными сервисами, такими как социальные сети. Какое государство должно нести ответственность за мои действия, если в российской сети *ВКонтакте* я, находясь в ФРГ и являясь гражданином США, оставляю на стене пользователя из Польши *перепост* видео пользователя из Украины с призывом к джихаду? И вообще, ответственность лежит на пользователях или на самой социальной сети, допустившей загрузку таких материалов? Вопросы упираются в сетецентричную природу интернета и не имеют легкого и однозначного решения, а в концепции Конвенции этот вопрос и вовсе не рассматривается.

Кроме того, на практике тезис о государствоцентричности информационного пространства оказывается неверен, по крайней мере, для большинства развитых стран, в части государственного контроля над критической информационной инфраструктурой. Не затрагивая тривиальный пример с корневыми серверами системы DNS, которые управляются международной неправительственной и некоммерческой организацией ICANN, мы имеем массу свидетельств подобного рода как в США, где в частной собственности находится до 90% критической инфраструктуры, так и других странах.

В США государство напрямую не контролирует работу информационной системы Нью-йоркской фондовой биржи, капитализация рынка акций которой на ноябрь 2010 г. составляла 13,39 трлн долларов, или около 50% суммарной капитализации мирового фондового рынка[27]. Сама *New York Stock Exchange LLC* по своему правовому статусу близка к российскому понятию общества с ограниченной ответственностью (ООО), что исключает прямой государственный контроль над ее информационной системой. Подтверждением независимого статуса NYSE стали события 11 сентября 2001 г., когда деятельность биржи, расположенной в сравнительной близости от Всемирного торгового центра, оказалась нарушена. Несмотря на то что действия руководства биржи по обеспечению сохранности, безопасности и бесперебойного функционирования ее информационной системы координировались с представителями Комиссии по ценным бумагам и биржам, а также Казначейством США на экстренном совещании, прямого перехвата контроля госорганами не произошло даже в тех чрезвычайных условиях[28, 29].

Важно подчеркнуть, что приведенный пример не может считаться значимым лишь для США уже в силу того, что крупнейшие фондовые биржи являются элементами *глобальной* критической инфраструктуры. Нью-Йоркская биржа обеспечивает стабильность мировой финансовой системы, элементом которой является и финансовая система РФ. То же применимо к информационным системам крупных промышленных объектов, таких как ГЭС, АЭС, газопроводы, трансграничные энергосети, операторами которых в развитых странах чаще всего являются структуры частного сектора. Согласно исследованию компании *Symantec* за октябрь 2010 г., 85% всей критической инфраструктуры США, подключенной к информационным сетям, находится под контролем частных операторов, включая энергетические сети, промышленную, транспортную, финансовую инфраструктуру[30]. В большинстве случаев работу объектов критической инфраструктуры обеспечивают частные информационные сети, атака на которые способна привести к последствиям, далеко выходящим за рамки национальных границ или отдельно взятого региона.

Вообще, делегируя государствам право выступать на мировой арене от имени всех участников глобального информационного обмена, концепция Конвенции рискует столкнуться с проблемой фундаментального характера. Несколько десятилетий назад проблема регулирования деятельности трансграничных акторов рассматривалась в контексте Кодекса ООН для транснациональных корпораций (ТНК). Проект такого кодекса в разных вариантах прорабатывался с 1972 по 1992 г. и в итоге был отклонен, так как делегаты ООН сочли консенсус по его проек-

ту невозможным[31]. За 20 лет работы над Кодексом так и не удалось согласовать правовой механизм, который обеспечивал бы юридически обязывающий характер кодекса, предлагал реальные варианты имплементации прописанных в нем норм и не ущемлял бы интересы самих ТНК. Причина неудачи заключалась в том, что государства сегодня неспособны самостоятельно, без участия других субъектов и посредников регулировать те институты, процессы и явления, которые развиваются преимущественно вне национальных границ и систем нормативно-правового регулирования. А в случае с глобальным информационным пространством процесс преимущественно протекает вообще вне рамок государственного административного контроля.

Установление такого контроля сегодня — весьма сложная задача, особенно в части верификации исполнения тех норм, которые предлагает российская концепция Конвенции. В частности неясно, как обеспечить верификацию в части отказа от создания кибероружия. Возможностями по созданию таких средств сегодня обладает абсолютное большинство государств мира, при том, что такие возможности доступны и негосударственным акторам. По оценке российских дипломатов, эксперименты «в области ведения информационных или кибервойн» сегодня ведут не менее 120 государств[32]. Отследить разработки кибероружия той или иной группой субъектов на ранних этапах до его применения пока практически невозможно, в отличие от ОМУ и космического оружия, — для их создания требуется минимальный объем общедоступной технической инфраструктуры. Несколько упрощая, для этого достаточно ПК и *флэшки.* Что касается средств ведения информационной войны *за рамками* ее кибернетических аспектов, то здесь оружием может выступать каждое СМИ, блог и аккаунт отдельного пользователя Сети.

Названные факторы наряду с трансграничным характером глобальных медиа и минимальным контролем над интернет-пользователями во многих странах мира вызывают серьезные сомнения в эффективности механизмов контроля, которые могут быть предложены на данном этапе с технической и правовой точек зрения. Это отнюдь не означает неэффективности мер раннего предупреждения и выявления угроз, а также международного взаимодействия в области пресечения их распространения. Но в концепции Конвенции прописан *отказ от разработки* информационного оружия, что потребует качественно иных возможностей верификации — увы, отсутствующих на сегодня и в ближайшей обозримой перспективе. Принятие Конвенции, не обеспеченной надлежащими механизмами верификации ее норм, чревато лишь девальвацией ценности идеи, заложенной в основу документа.

Суммируя сказанное, следует признать, что концепция Конвенции и Правила поведения, изначально преследуя весьма масштабные цели, на сегодняшнем этапе сталкиваются с рядом трудностей и вызовов концептуального характера. Во-первых, терминология концепции Конвенции имеет ряд уязвимых мест и нуждается в значительной доработке, в частности в выработке более строгих и однозначных определений ключевых понятий, а также *закрытии брешей*, таких как не затронутая в документе проблема кибершпионажа. Что еще более важно, российские инициативы страдают избыточным упором на роль государства, что ведет к *выпадению* из текста документов других участников информационного обмена — частного сектора, глобальных СМИ, интернет-пользователей, а также посредников, выполняющих волю государств в информационном пространстве. Идеи и принципы контроля государств над сегментами информационного пространства и их ответственности за содержание информационных потоков не подкрепляются решениями правовых и технологических проблем, которые при этом возникают. России необходимо обозначить свой подход к проблемам анонимности в интернете, а также вопросу ответственности за информационные потоки в трансграничной Сети — без этого имплементация принципов концепции Конвенции едва ли возможна. Прописанные в концепции Конвенции задачи по недопущению использования ИКТ в военно-политических целях в ряде случаев опережают нынешние реалии с технологической, международно-правовой и международно-политической точек зрения. Для более успешного продвижения российской идеи на мировой арене целесообраз-

но сужение спектра ее задач в той части, где принципы международного поведения, прописанные в концепции Конвенции, не обеспечиваются работоспособными механизмами контроля верификации. Имеются в виду контроль над содержанием трансграничных информационных потоков, отказ от создания информационного оружия, а также принцип ответственности государств за содержание информации, размещаемой в их информационном пространстве.

ТРАНСГРАНИЧНАЯ КИБЕРПРЕСТУПНОСТЬ И ПОЗИЦИЯ РОССИИ ПО БУДАПЕШТСКОЙ КОНВЕНЦИИ: ПРОБЛЕМА 32B

В европейских странах, США и Канаде одним из факторов, спровоцировавших критику в адрес российских инициатив по обеспечению МИБ, стало наличие в концепции Конвенции положений о международном сотрудничестве в сфере борьбы с трансграничной киберпреступностью. Противодействию этому виду противоправной деятельности в информационном пространстве посвящена глава 4 концепции Конвенции, которая включает в себя статью 10 (Основные меры противодействия правонарушениям в информационном пространстве) и статью 11 (Меры по организации уголовного процесса).

Как известно, Россия на данный момент не является участником ключевого международного механизма противодействия киберпреступности — Конвенции Совета Европы «О киберпреступности», открытой для подписания 23 ноября 2001 г. в Будапеште и вступившей в силу в 2004 г. Несмотря на то что документ носит открытый характер, Россия в конечном счете отказалась присоединиться к нему, в отличие от 37 государств, ратифицировавших Конвенцию по состоянию на 20 сентября 2012 г. Изначально присоединение России к Конвенции было санкционировано распоряжением российского президента от 15 ноября 2005 г. «О подписании Конвенции о киберпреступности» на условиях пересмотра положений статьи Конвенции 32, пункта b[33]. Однако 22 марта 2008 г. вступило в силу распоряжение Президента РФ, в соответствии с которым распоряжение от 15 ноября 2005 г. признано утратившим силу. С тех пор российская сторона не высказывала интереса к конвенции Совета Европы, сосредоточившись на продвижении собственных инициатив в области противодействия кибертерроризму. В ноябре 2010 г. начальник Юридического управления Росфинмониторинга П. В. Ливадный заявил, что «РФ продвигает подход, предусматривающий разработку глобальной конвенции по борьбе с преступлениями в информационной сфере»[34]. При этом характерно, что одна из задач перспективного российского подхода должна будет заключаться «в недопущении расследований [...] на чужой территории», без постановки в известность «правоохранительных органов соответствующего государства»[35].

В данном случае имеется в виду положение Будапештской конвенции, которые вызывает у российской стороны принципиальное несогласие и стало основным препятствием к присоединению России к ее механизму. Статья Конвенции 32, пункт b, предполагает санкционированный доступ уполномоченных органов одного государства-участника к компьютерным данным, хранящимся на территории другого государства, без предварительного получения согласия последнего. «Сторона может без согласия другой Стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему»[36].

Именно неприятие данного пункта и определяет ту *генеральную линию*, которую заняла Москва в отношении конвенции Совета Европы с 2010 г. и продолжает придерживаться в настоящее время. Представители правительства, МИД и силовых структур в своих работах и выступлениях всячески подчеркивают, что Конвенция была бы неплохим документом, если бы не 32b. По мере созревания российских инициатив по обеспечению МИБ было найдено решение — вырабатывать механизм глобальной борьбы с киберпреступностью собственными силами. Частично

этой цели отвечает концепция Конвенции об обеспечении МИБ, которая содержит ряд положений, затрагивающих вопросы борьбы с трансграничной киберпреступностью. Кроме того, до конца 2012 г. ожидается презентация российской стороной новых инициатив — нового отдельного проекта глобального договора, на этот раз сфокусированного прежде всего на вопросах киберпреступности, либо переработанного проекта Конвенции об обеспечении МИБ.

Критика Конвенции СЕ, которая ведется российскими представителями из числа сотрудников МИД и силовых структур, затрагивает прежде всего данный пункт документа. В частности, утверждается, что это положение Конвенции:

- препятствует эффективному межгосударственному сотрудничеству, обходя согласование с одной из сторон вопроса о трансграничном доступе в ее сети;
- подрывает дух доверительного и слаженного взаимодействия между ее участниками;
- служит формальным прикрытием действий, преследующих не столь дружественные и партнерские действия участников Конвенции.

В рамках последнего пункта предметом опасений представителей российской стороны является угроза разведывательной деятельности европейских и американских спецслужб в российских сетях под прикрытием следственных действий. Например, по словам предыдущего начальника Бюро специальных технических мероприятий МВД России Б. Н. Мирошникова, «лукавая 32-я статья преследует другие цели, а отнюдь не цели расследования компьютерных преступлений»[37].

Аналогичные мнения озвучивались и озвучиваются многими представителями ФСБ, МВД, Совета безопасности РФ и других структур.

Помимо угрозы кибершпионажа, неприемлемым пункт 32b, по версии РФ, делает нарушение государственного суверенитета за счет бесконтрольного вторжения третьей стороны в информационные сети национального государства. Как отмечает профессор МГИМО (У) МИД России А. Г. Волеводз, «в любой стране мира возможно найти конкретного провайдера», который имеет в распоряжении «законные технические механизмы доступа к компьютерным данным, хранящимся за границей», или самостоятельно хранит такие данные на физическом сервере[38]. В итоге, по мнению эксперта, применение статьи 32b к подобным провайдерам создает возможность де-факто бесконтрольного доступа к компьютерным данным в сетях иностранного государства.

Наконец, в последние годы усиливается критика Конвенции в целом как устаревшей и не отвечающей современным тенденциям и изменениям в области трансграничной киберпреступности. Прежде всего отмечается неспособность Конвенции охватить те виды и классы компьютерных преступлений, которые получили развитие за прошедшие 10 лет с момента ее подписания. В список таких киберпреступлений можно включить:

- фишинг;
- создание и использование ботнетов;
- усовершенствованные технологии спама;
- преступления, совершаемые в *виртуальных мирах,* — социальных онлайн-сообществах по типу *Second Life*;
- преступления с использованием социальных сетей — мошенничество, неправомерное завладение персональными данными, воровство аккаунтов (неправомерное присвоение виртуальной идентичности) и т. д.;
- кибертерроризм и использование киберпространства для пропаганды насилия, экстремизма, терроризма.

Некоторые эксперты также включают в этот список массированные организованные кибератаки на объекты критической информационной инфраструктуры, не выделяя их как отдельный феномен киберконфликта, выходящий за рамки киберпреступности[39].

Признавая, что вопрос о нарушении механизмом пункта 32b принципа государственного суверенитета и создании угроз национальной безопасности требует отдельного углубленного исследования, следует, тем не менее, отметить справедливость призывов к модернизации Конвенции СЕ. Необходимость внесения поправок и дополнений в документ действительно назрела. Темпы развития ИКТ и глобальной сети интернет делают невозможным эффективное выполнение своих задач инструментом, рассчитанным на противодействие технологическим вызовам рубежа тысячелетий. Вне механизма Конвенции остается вся совокупность правонарушений, совершаемых в трансграничных социальных сетях, а также преступлений с использованием современных технологий рассылки спама, взлом систем ДБО (дистанционное банковское обслуживание), распространение в интернете информации экстремистского и террористического характера.

Пока на направлении обновления Будапештской конвенции не наблюдается практической активности, что может свидетельствовать о том, что Совет Европы и его государства-участники пока не в полной мере осознали такую необходимость. Так или иначе, если в ближайшие два-три года в Конвенцию не будут привнесены необходимые новации, ее практическое значение как международного механизма противодействия киберпреступности начнет девальвироваться. В таком случае потенциальные инициативы России и ее партнеров могут оказаться более востребованными.

Еще одним слабым местом Будапештской конвенции считается ее *региональный характер* и несоответствие статусу подлинно глобального механизма, который эффективно охватывал бы все международное сообщество. Действительно, на сегодняшний день Конвенции не удалось охватить многие из государств, оказывающих наибольшее влияние на мировую киберпреступность, прежде всего Россию и Китай. Вне Конвенции пока остаются и другие страны, которые на сегодняшний день играют чуть меньшую роль в обеспечении МИБ, однако имеют колоссальный потенциал роста национального IT-сектора, а значит, и взрывного роста рынка киберпреступности. В числе таких стран стоит отметить Индию, Индонезию, Нигерию, Мексику, Вьетнам и другие густонаселенные развивающиеся страны с быстро растущим ИКТ-сектором. В то же время на превращении Конвенции СЕ в глобальный механизм особо настаивают США, которые обеспокоены попытками России выработать ему некие альтернативы.

Официальные лица США все чаще пытаются позиционировать Конвенцию СЕ как безальтернативный и универсальный механизм взаимодействия для стран в любых регионах, включая АТР, особо значимый в этом контексте. Роль развивающихся стран в глобальном информационном обмене, включая прежде всего представителей Восточной и Юго-Восточной Азии, быстро растет, и в будущем будет иметь ключевое значение для международного сообщества. С учетом этого выбор странами региона модели международного взаимодействия по вопросам кибербезопасности и киберпреступности весьма важен как для РФ, так и для США. Пока национальные и региональные подходы находятся в стадии формирования, однако именно страны АТР все чаще поднимают вопрос о модернизации либо замене Будапештской конвенции. Так, возможность разработки и принятия новой конвенции ООН с целью дополнения механизма Будапештской конвенции обсуждалась на Семинаре по акторам-*посредникам* в киберпространстве АРФ, который прошел во вьетнамском Хойане 14–15 марта 2012 г.[40]. Участники семинара не пришли к единому мнению, однако отметили необходимость обновления инструментария Будапештской конвенции.

Подобная ситуация предоставляет России *окно возможностей* по продвижению собственных инициатив и проектов в области глобального противодействия киберпреступности. Однако временные рамки этого окна невелики — процесс

изменения Будапештской конвенции запустить проще и быстрее, чем добиться принятия Конвенции ООН на основе концепции Конвенции об обеспечении МИБ. Кроме того, несмотря на критику и потребность в модернизации Конвенции, процесс присоединения новых членов к ее механизму набирает обороты. Только с начала 2012 г. Будапештскую конвенцию ратифицировали пять государств, включая Грузию и Японию[41], при том, что для Токио процесс ратификации растянулся на 10 лет. В марте 2012 г. было объявлено о запуске третьей фазы Глобального проекта по киберпреступности Совета Европы, целью которого является «содействие применению Будапештской конвенции в глобальном масштабе»[42]. Таким образом, Совет Европы и его ключевые члены, включая Великобританию, уже сейчас четко позиционируют Конвенцию как глобальный, а не региональный инструмент борьбы с киберпреступностью. В этой связи прилагаются соответствующие усилия, включая финансирование программы региональных и страновых семинаров с целью адаптации национальных законодательств к механизму Конвенции СЕ.

Кроме того, интерес к Конвенции проявляет один из главных союзников России по ШОС и ОДКБ — Республика Казахстан. Казахстан с 2011 г. изучает возможность присоединения к конвенции, хотя соответствующее политическое решение в подробностях не прорабатывалось. Учитывая, что Казахстан является вторым по значимости после Китая партнером России по ШОС, любая дискуссия относительно Будапештской конвенции будет воспринята Москвой довольно болезненно. Озабоченность российской стороны в данной области проявила себя в ходе переговоров министра иностранных дел России С. В. Лаврова с главой МИД Казахстана Е. Х. Казыхановым, которые прошли 21 ноября 2011 г. в Москве. Несмотря на то что противодействие новым угрозам фигурировало в повестке переговоров лишь вскользь, российская сторона затронула вопрос казахской позиции относительно противодействия киберпреступности. После этого руководство Казахстана приняло во внимание позицию российской стороны, настаивавшей на необходимости детально проработать возможные последствия присоединения Казахстана к Конвенции СЕ с учетом обязательств Республики перед партнерами по ШОС. На данный момент решение по-прежнему не принято, но сложно ожидать, что Казахстан полностью откажется от рассмотрения такого варианта, особенно в случае модернизации и дальнейшего расширения Будапештской конвенции.

Наконец, любопытна позиция Украины, которая ратифицировала Будапештскую конвенцию еще в 2005 г. с рядом оговорок и заявлений. В 2006 г. Верховная Рада также приняла закон о ратификации Дополнительного протокола к конвенции, однако с тех пор так и не адаптировала свое национальное законодательство к ее нормам. В свете активизации диалога между Киевом и Москвой в последние годы российские власти, вероятно, рано или поздно вернутся к обсуждению украинской позиции в отношении Будапештской конвенции. Что ответит Киев, совершенно неясно — по-видимому, четкое представление о дальнейшей работе по имплементации норм документа отсутствует и в самой Украине.

Еще одним неприятным для Москвы *поворотом сюжета* стала новость о том, что заявку о присоединении к Конвенции СЕ в мае 2012 г. подала Белоруссия[43]. На тему целесообразности присоединения к Конвенции белорусские чиновники высказывались еще в 2007 г.[44], однако нынешнее решение Минска оказалось неожиданностью для Москвы. Любопытно, что речь идет не только об одном из ключевых российских союзников в военно-политических вопросах, но и об элементе Союзного государства России и Белоруссии. Если Минск действительно запустит механизм присоединения к Конвенции, это станет серьезным ударом для Москвы, которой будет сложнее убедить партнеров из отдаленных регионов (АТР, Латинская Америка) в привлекательности своих подходов на фоне потери единомышленников в ключевой зоне влияния — СНГ.

Впрочем, серьезность намерений белорусского руководства по присоединению к Конвенции Совета Европы вызывает сомнения. Открытость и трансграничное сотрудничество, заложенные в основу ее механизма, плохо стыкуются с непрозрачностью системы силовых и правоохранительных органов Белоруссии и тра-

дициональным нежеланием Минска брать на себя какие-либо обязательства в части раскрытия информации, предоставления доступа к своим системам и инфраструктуре. Кроме того, неотъемлемой частью философии Конвенции СЕ является продвижение *неограниченной* свободы в интернете, что сложно связать с курсом белорусских властей, практикующих цензуру в глобальной сети и идентификацию интернет-пользователей по паспортам. Скорее, речь идет о конъюнктурном политическом маневре как части стратегии балансирования Минска между РФ и Евросоюзом, двумя центрами влияния и экономических потоков. Однако подобный торг ставит Россию в уязвимое положение, так как распространение ее среди других партнеров Москвы стало бы дополнительным препятствием к продвижению инициатив, альтернативных Будапештской конвенции.

Вместе с тем, в конечном счете, целесообразность присоединения тех или иных стран к Конвенции СЕ прежде всего определяется тем, насколько эффективно их собственные национальные правовые системы позволяют бороться с киберпреступностью. Этот тезис справедлив и в отношении России. Учитывая, что даже в случае трансформации российской инициативы в конвенцию о МИБ ООН уже в 2013 г. на практическую имплементацию ее механизмов уйдут годы, России в краткосрочной перспективе нужно рассчитывать либо на собственные законы, либо на Будапештскую конвенцию. Между тем на данный момент ситуация на российском рынке киберпреступности представляется тревожной и требующей оперативных изменений.

При этом объективные сложности противодействия киберпреступникам отнюдь не исчерпываются слабостью нормативной базы в РФ. Ключевым препятствием к успешному расследованию киберпреступлений является *трансграничность* преступных групп. Стандартной схемой для широкого ряда киберпреступлений является формирование сообщества, члены которого действуют одновременно с территории различных государств. Количественный и качественный рост банковского сектора и, соответственно, интернет-банкинга, распространение электронных платежных систем и терминалов, общий рост доходов населения РФ и бурное развитие частного сектора сделали достоянием прошлого те времена, когда криминальные атаки осуществлялись только *из* России *против* расположенных за рубежом организаций, объектов, систем. РФ превратилась в самостоятельный, крупный и привлекательный рынок, который с каждым годом привлекает все больше киберпреступников, в том числе из-за рубежа.

В результате российская киберпреступность демонстрирует впечатляющий рост, сдержать который правоохранительным органам в полной мере не удается. В 2010 г. объем средств, заработанных преступниками в российском сегменте интернета в 2010 г., оценивался в 2–2,5 млрд евро[45], а темп роста количества кибератак в том же году оценивался в 80%. Совокупный заработок *русских* киберпреступников в 2010 г. оценивается на уровне 2,5 млрд долл., при этом прогнозировался его рост до 3,7 млрд долл. в 2012 г. и 7,4 млрд долл. США в 2013 г.[46]. Иначе говоря, среднегодовой темп роста показателя приблизится к 100%, а через год доходы *русской* киберпреступности превысят совокупный оценочный доход мирового рынка киберпреступлений за 2010 г. (7 млрд долл. США).

Ситуацию с российским законодательством о спаме и распространении при помощи ИКТ детской порнографии хорошо иллюстрирует пример спамера *Leo Kuvayev* (также известен как *Bad Cow)*, в 2005–2010 гг. известного как «король спама». По словам экспертов[47], в течение нескольких лет Л. А. Куваев, выходец из РФ, проживая в основном в США, создал сложнейшую автоматизированную систему распространения спама, торговли порнографией и вредоносными программами через интернет. Система ежедневно в автоматическом режиме создавала для данной цели, а также для кибермошенничества до тысячи сайтов. Партнерские программы из спамерской сети Куваева *до сих пор* генерируют доход в размере около 30 млн долл. в год. После открытия уголовного дела в США в 2005 г. спамер вернулся в Россию, где оказался недосягаем для американского правосудия, включая Федеральное бюро расследований (ФБР), и продолжил вести свою деятельность,

пользуясь тем, что российские законы *не позволяли привлечь его к ответственности*. Потребовалось пять лет, прежде чем Л. А. Куваева арестовали в России, причем не за совершенные киберпреступления, а по *педофильской* статье 134 УК РФ[48]. Более того, 23 августа 2012 г. стало известно о том, что Верховный суд России снизил срок Куваеву вдвое, с 20 до 10 лет, с отбытием наказания в колонии общего режима[49]. Особенно интересно такое решение выглядит на фоне сегодняшней бурной кампании по борьбе с педофилией и детским порно в интернете.

Не менее тревожной видится ситуация противодействия мошенничеству в интернете. В частности, РФ имеет скудный опыт успешного доведения до суда (не говоря об обвинительных приговорах) дел о мошенничестве в области ДБО. Кроме того, осужденные кибермошенники чаще всего получают наказание по статьям, не имеющим прямого отношения к киберпреступности. Ярким примером является случай хакера Евгения Аникина, который 8 февраля 2011 г. был признан судом виновным во взломе в 2008 г. платежной системы *RBS WorldPay* с нанесением ущерба в размере 10 млн долларов. Сообщники Аникина ранее были экстрадированы в США, где их обвинили в *мошенничестве с использованием электронных средств коммуникации*, за что им грозят тюремные сроки до 20 лет[50]. Сам же Аникин был осужден на условный срок в пять лет за *кражу, совершенную в особо крупном размере* по статье 158 УК РФ, пункт б, часть 4. Разница едва ли нуждается в комментариях. При этом количество преступлений в сфере ДБО в России выросло за 2011 г. в три раза; за одну атаку хакеры в среднем похищают от 600 тыс. до 2 млн рублей[51]. Российская правоохранительная система на данный момент позволяет доводить до суда лишь единицы уголовных дел по таким правонарушениям. Однако только в Москве *ежемесячно* происходит 10–20 *успешных* атак подобного рода, а общее число только зарегистрированных МВД преступлений в сфере информационной безопасности в 2009 г. превысило 15 тыс.[52]. Иными словами, обвинительные приговоры выносятся менее чем по 0,1% дел от числа уже зарегистрированных киберпреступлений.

Схожим образом складывается ситуация с борьбой с DOS и DDOS-атаками. В 2011 г. в РФ DDOS-атакам с использованием ботнетов часто подвергались социальные сервисы, сайты СМИ, интерактивные сообщества на базе платформы *Ushahidi.* Особую тревогу вызывает тот факт, что выбор объектов атаки и характер атак (выбор времени, одновременные мощные атаки на большое количество ресурсов) дает почву для предположений о политическом подтексте подобных акций. Накануне, во время и после выборов в Государственную Думу РФ 4 декабря 2011 г. мощным DDOS-атакам подверглись сайты ведущих СМИ, освещавших выборы (*Коммерсантъ*), *Карта нарушений* — интерактивная онлайн-платформа, позволявшая в режиме реального времени собирать информацию о нарушениях в выборном процессе, блоговый сервис *LiveJournal*, считающийся *цитаделью* российской либеральной оппозиции, и другие ресурсы. Весьма пассивная реакция правоохранительных органов на подобные инциденты отчасти объясняется слабостью российского законодательства в отношении DDoS-атак. Как отмечает эксперт ЦТТИ МГУ имени М. В. Ломоносова А. В. Лямин, «большинство статей [УК РФ], посвященных информационной безопасности, для DDoS *нерабочие*»[53], а виновные в них лица привлекаются к ответственности «исключительно по статье 273 УК РФ»[54]. В итоге слабость законодательных механизмов и пассивность госорганов создают для организаторов подобных атак обстановку безнаказанности.

Впрочем, подобная оценка российской нормативной базы в части борьбы с киберпреступлениями разделяется не всеми специалистами. По словам И. К. Сачкова, «в нашей стране используются те же правовые механизмы, что и на Западе»[55]. При этом «девять составов преступлений, которые в большинстве стран признаны как киберпреступления, у нас отражены в трех статьях главы 28 Уголовного кодекса РФ в совокупности с другими составами [преступлений]», что «дает российскому УК больше пространства для маневрирования» по сравнению с Будапештской конвенцией. По мнению эксперта, преимущество законодательства РФ обусловливается тем, что «в российском УК, в отличие от Будапештской конвенции, отсутствует жесткая привязка к конкретным составам преступлений»[56]. Кроме того, при оценке

темпов роста российского рынка киберпреступности следует принимать во внимание бурный рост интернет-сектора в РФ в целом. В определенной степени расширение масштаба рынка киберпреступности представляет собой естественный процесс, который развивается параллельно с многократным ростом объемов российской интернет-экономики за последнее десятилетие.

Однако данные оговорки не снимают остроты проблемы с киберпреступностью в РФ, равно как и не отменяют потребности в совершенствовании механизмов международного сотрудничества по данным вопросам. Вне зависимости от того, как скоро обновленные российские проекты глобальных механизмов борьбы с киберпреступлениями будут представлены международному сообществу, в ближайшие годы до их возможной практической имплементации Конвенция Совета Европы останется ключевым механизмом в этой области. Возможно, возвращение Москвы к рассмотрению вопроса о присоединении к Конвенции следует увязывать с прогрессом в модернизации последней и наращиванию в ее рамках норм, которые принимали бы во внимание сегодняшние криминальные вызовы в киберпространстве.

Вопрос о соотношении пользы и ущерба от Конвенции СЕ для национальной безопасности и экономики РФ сохраняет свою дискуссионность. Для его критичной и объективной оценки необходимо тщательное исследование, которое позволит оценить негативные и позитивные эффекты от присоединения к Конвенции в экономических категориях. Исследование должно ответить на вопрос, покроет ли потенциальное сокращение объемов потерь российской экономики от действий киберпреступников в результате присоединения к Конвенции возможные потери конфиденциальной информации и ущерб национальной безопасности в результате негативных эффектов применения пункта *32b*, в экономическом выражении. Подобная четкая постановка вопроса поможет развеять существующее в экспертном и деловом сообществах недопонимание позиции российского руководства и спецслужб в отношении Будапештской конвенции. В конце концов киберпреступность представляет такую же угрозу национальной безопасности, а отстаивание принципов государственного суверенитета в современном мире не является абсолютной ценностью, особенно когда речь идет об изначально едином и трансграничном киберпространстве. Конвенция СЕ при всех недостатках не воспринимается в качестве акта, ущемляющего суверенитет, 37 ее членами, включая Японию, Канаду, США и другие государства, которые не участвуют в процессах делегирования государственного суверенитета на наднациональный уровень в рамках Евросоюза. Аналогично, для России вопрос может заключаться не столько в отстаивании жестких принципов, сколько в точном и выверенном *cost-benefit анализе* Конвенции, который позволит более объективно оценить соответствие ее механизма нашим национальным интересам. Важен подход, в рамках которого ни тотальный отказ от Конвенции, ни присоединение к ней не будут рассматриваться в качестве самоцели. Конвенция СЕ могла бы выступать подспорьем для РФ ровно до того момента, когда будут выработаны другие международные нормы по борьбе с киберпреступностью. При этом шанс, что их поддержат зарубежные партнеры РФ, существует и определяется не столько политическими аспектами дискуссии о подходах к МИБ, сколько практической ценностью предлагаемых механизмов. Как отметил в интервью *Индексу Безопасности* директор по вопросам международной политики в киберпространстве британского МИД Джейми Сондерс, если речь будет идти о правовом механизме, «который предложит востребованные на сегодня нормы и более эффективные меры сотрудничества по сравнению с Будапештской конвенцией»[57], такой механизм вполне может быть поддержан Лондоном.

ПЕРСПЕКТИВЫ РОССИЙСКИХ ИНИЦИАТИВ И ВОЗМОЖНЫЕ ПРАКТИЧЕСКИЕ ШАГИ ПО ИХ РЕАЛИЗАЦИИ

Во-первых, официальные выступления представителей РФ на международных мероприятиях, данные о закрытых обсуждениях как внутри страны, так и с партнерами за рубежом позволяют говорить о разумной и гибкой позиции российских

госструктур в части продвижения концепции Конвенции на международной арене. В своем выступлении 1 ноября 2011 г. на Лондонской конференции по вопросам киберпространства глава Минкомсвязи России И. О. Щеголев выразил надежду на то, что российская концепция Конвенции «заложит основу для выработки универсальной конвенции под эгидой ООН»[58]. Таким образом, подача российской инициативы оставляет место для рассмотрения ее в качестве рабочей заготовки, гибкого проекта, который скорее служит базой для дальнейшего диалога по намеченным в нем вопросам, нежели предлагает нашим зарубежным партнерам готовые негибкие решения. В схожем ключе была выдержана речь специального представителя президента РФ по ШОС на Восьмой Генеральной конференции АТССБ — по сути, первая официальная презентация идей Правил поведения в области МИБ ШОС государствам АТР, которые РФ справедливо считает *целевой аудиторией* своих инициатив в сфере обеспечения МИБ[59].

Кроме того, российские государственные органы предпринимают практические усилия по доработке текста концепции Конвенции с учетом отзывов экспертов и наиболее веских пунктов критики со стороны зарубежных партнеров. Такая работа в настоящее время ведется по большей части на площадке российского Совета Безопасности. В частности, текст концепции Конвенции, перспективы его доработки и ключевые критические отзывы в адрес документа обсуждались 6–8 июня 2012 г. на Третьей международной встрече высоких представителей, курирующих вопросы безопасности в Санкт-Петербурге. По итогам встречи не было разработано какого-либо нового варианта текста, однако были учтены отдельные критические замечания и было принято решение продолжить работу в этом направлении. Любопытно, что в преддверии мероприятия секретарь Совбеза Н. П. Патрушев отметил, что задача РФ состоит в том, чтобы заложенные в концепции Конвенции правила стали приемлемы «для большинства государств на начальном этапе», а на конечном этапе распространились бы «в целом, в мире»[60]. Из подобных высказываний можно сделать вывод о том, что российское руководство на данный момент не ставит перед собой задачу максимально быстрого принятия конвенции в рамках ООН. Центр тяжести российских усилий перемещается в область формирования *коалиции поддержки* концепции конвенции, достаточно широкой, чтобы вопрос о принятии конвенции ООН звучал максимально легитимно, даже несмотря на возражения отдельных важных игроков на мировой арене. Не отказываясь от изначальной, весьма масштабной задачи, российский подход в части концепции Конвенции об обеспечении МИБ становится более реалистичным и гибким.

Во-вторых, международное право, на которое зачастую ссылаются западные партнеры Российской Федерации, предусматривает определенные ограничения на распространение информации, подрывающей общественную безопасность. Именно такие действия, по мнению политического руководства и экспертов из России и ряда других стран мира, имели место в 2011–2012 гг. в ходе событий *Арабской весны.* Так, согласно пункту 3 Статьи 19 Международного пакта о гражданских и политических правах, принятого резолюцией Генеральной Ассамблеи ООН от 16 декабря 1966 г., пользование свободой «искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору *налагает особые обязанности и особую ответственность*» и может быть «*сопряжено с некоторыми ограничениями*, которые, однако, должны быть установлены законом и являться необходимыми для:

a) уважения прав и репутации других лиц;

b) охраны государственной безопасности, общественного порядка, здоровья или нравственности населения»[61].

Безусловно, ссылка на норму одного из ключевых актов международного права в области прав и свобод человека придает убедительности позиции российского МИД и самой концепции Конвенции. Проблема, однако, заключается в том, что указанная статья представляет собой норму, которая пока по большому счету не при-

жилась в международной правоприменительной практике, в отличие, скажем, от статьи 51 Устава ООН. С момента принятия Пакта в 1966 г., случаи, когда государства обосновывали бы свои действия в сфере контроля над распространением информации ссылкой на данную норму, крайне редки. Характерно, что эта норма осталась также вне поля зрения правительств Хосни Мубарака, Бен Али, Каддафи, Башара Асада и А. Г. Лукашенко, которые в ходе событий *Арабской весны* активно искали способы ограничить активность оппозиционных движений в социальных сетях на относительно легитимных и понятных мировому сообществу основаниях. Тем не менее апелляция к этой статье вполне правомерна и может использоваться в качестве аргумента в диалоге с зарубежными партнерами РФ. Проблема скорее состоит в том, что положения Пакта, как и любых базовых документов международного права, имеют весьма общую формулировку и оставляют большое пространство для дискуссий. Например, британские власти могли бы считать апелляцию к Статье 19 оправданной для противодействия координации в социальных сетях беспорядков в Лондоне в 2011 г., но отрицать ее применимость к вопросам военно-политического использования ИКТ. Единожды зафиксированные правовые принципы сами по себе далеко не всегда способны переломить политическую волю международных коалиций или отдельных крупных игроков. В этом можно было еще раз убедиться на примере операции НАТО в Ливии в 2011 г., соответствие которой мандату Совета Безопасности ООН широко ставилось под сомнение в мире. Безусловно, данный момент следует учитывать российскому руководству в плане продвижения российских инициатив по обеспечению МИБ.

В-третьих, ошибочно полагать, что Россия одинока в своих подходах, а идея глобального международно-правового документа, охватывающего сразу все измерение информационной безопасности, маргинальна и больше никем не рассматривается. В 2010 и 2011 гг. были опубликованы два издания проекта *The UN Global Treaty on Cybersecurity and Cybercrime* за авторством крупнейшего норвежского киберюриста Штайна Шольберга и его швейцарской коллеги Соланж Гернутти-Эли. Профессор Шольберг в 2007–2008 гг. занимал пост председателя Группы экспертов высокого уровня по кибербезопасности (High Level Expert Group on Cybersecurity), которая была учреждена в 2007 г. для изучения возможностей координации усилий международного сообщества по обеспечению кибербезопасности[62]. Деятельность Группы экспертов должна была дополнять Глобальную программу кибербезопасности Международного союза электросвязи (МСЭ), которая начала действовать в том же 2007 г.[63]

Центральной идеей в проекте Договора является утверждение всеобъемлющего комплексного подхода к регулированию кибербезопасности в международном праве. В этом смысле данная инициатива полностью созвучна российским инициативам. Различие заключается в том, что европейские эксперты по понятным причинам не включают в список угроз распространение информации, которая угрожает подрывом социально-политической стабильности. Куда более явный акцент в проекте сделан на блоке, посвященном киберпреступности. Амбиция авторов состоит в том, чтобы предложить альтернативу определениям Будапештской конвенции и самой Конвенции как таковой. Вместе с тем, согласно комментарию одного из ведущих российских экспертов по киберправу, договор может представлять интерес в контексте отвлеченного теоретизирования и построения идеальных моделей, однако «не представляется перспективным с международно-правовой точки зрения». Подтверждением этой оценки служит тот факт, что с момента выхода проекта Договора в конце 2010 г. не последовало никакой практической реакции на него ни по каналам ООН, ни в рамках каких-либо других рабочих форматов. О самом существовании проекта до конца 2011 г. не было известно российскому МИД, весьма озабоченному поиском единомышленников для российских инициатив.

Кроме того, проекты глобальных норм и договоров в информационном пространстве сегодня прорабатывают многие структуры, в том числе ключевые и крупнейшие международные организации. Как отмечается в выводах программного доклада МСЭ от 2011 г. *В поисках кибермира,* для достижения *кибермира* госу-

дарствам и международным организациям необходимо стремиться к «разработке кодекса поведения в киберпространстве и правовой основы, поддерживающих и продвигающих геокиберстабильность»[64]. Упор в докладе делается прежде всего на декларативные документы и нормы мягкого права, подобные этическим кодексам. В качестве примера таких механизмов приводится Декларация Эриче о принципах киберстабильности и кибермира, принятая в 2009 г. Всемирной федерацией ученых[65]. Однако риторика и тезисы доклада оставляют место и для более традиционных международно-правовых механизмов, в том числе юридически обязывающих договоров и конвенций ООН.

Любопытно, что и сами США — частично под давлением активной российской позиции в области обеспечения МИБ — начинают понемногу играть на поле строительства глобального режима безопасности в сфере ИКТ. На конференции по вопросам киберпространства в Будапеште 4 октября 2012 г. госсекретарь США Хиллари Клинтон выступила с речью, в которой впервые анонсировала заинтересованность и практическую вовлеченность Белого дома в создание среды, где поведением государств в киберпространстве «движут нормы ответственного поведения» и «верховенство права»[66]. Конечно, следует сделать скидку на три принципиально важных момента, которые делают выступление госсекретаря весьма далеким от капитуляции перед российским подходом. Во-первых, речь идет о механизмах *мягкого права*, не имеющих обязательной юридической силы, либо фиксирующих общие обязательные принципы, но не конкретные нормы и механизмы взаимодействия. В этой части госпожа Клинтон скорее приближает постановку вопроса к инициативе Правил поведения в области обеспечения МИБ, но не к концепции Конвенции. Во-вторых, речь по-прежнему идет о киберпространстве, а не об информационном пространстве, а значит, о значительно более узком круге вопросов. Наконец, в выступлении госсекретаря вовсе не прозвучала ООН — единственная рабочая площадка для выработки *глобальных* норм и правил поведения. Вместе с тем были отмечены усилия Вашингтона по налаживанию двусторонних диалогов по вопросам кибербезопасности с Индией, Бразилией и ЮАР. Характерно, что данный перечень включает в себя именно те страны БРИКС, которые Россия активнее всего пытается *перетянуть на свою сторону* в плане подхода к обеспечению МИБ. С учетом этих нюансов следует скорее говорить о продолжении *битвы идей* между сторонниками двух подходов, хотя одна из сторон и пытается модифицировать риторику, частично воспроизводя самые сильные идеи оппонента, но оставаясь в рамках собственной концепции.

В-четвертых, невозможно пытаться отрицать наличие той проблемы, которую призвана решить концепция Конвенции об обеспечении МИБ. Даже если оставить в стороне требующий отдельного исследования вопрос об угрозе информационной войны как манипулировании информацией для подрыва социально-политического уклада в тех или иных государствах, обостряются проблемы киберугроз глобального масштаба, включая кибервойны и саботаж критической инфраструктуры программными средствами. Данная проблематика полностью подпадает под задачи и механизмы в рамках российских инициатив, хотя и составляет лишь их часть. Российский подход к МИБ, что следует особо подчеркнуть, не отметает вопросы кибербезопасности, а просто включает их в более широкую проблематику и не выделяет в качестве самостоятельной сферы регулирования.

Реальность угрозы кибервойн и киберконфликтов в полной мере осознают европейские государства, включая Германию. С 30 ноября по 1 декабря 2011 г. в ФРГ прошла операция *Luekex 2011*, которая представляла собой не что иное, как учебную кибервойну[67]. В рамках операции, в которой приняли участие не менее трех тысяч чиновников имитировались массированные атаки на сайты и информационные системы ряда федеральных и региональных госучреждений. Симуляция кибервойны осуществлялась под наблюдением Национального центра кибероборонны и спецслужб, а подготовка к ней заняла почти два года[68]. Эффективная кибероборона также была включена в число важнейших условий безопасности НАТО в новой Стратегической концепции Альянса от 2010 г.[69]. С 2007 г. после серии атак

на киберинфраструктуру эстонских госучреждений и частных компаний в Таллинне был создан Центр кибероборонь НАТО (CCD COE). В целом, активность государств в сфере военно-стратегического применения ИКТ характеризуется лавинообразным ростом. Если в 1998 г., на момент принятия первой резолюции Генассамблеи ООН по МИБ Генассамблеей ООН серьезными разработками в этой сфере занимались разве что РФ, США и Китай, то сегодня, как уже упоминалось, их ведут более сотни государств, не считая негосударственных субъектов.

Лучше всего о реальной остроте угроз глобальной кибербезопасности свидетельствует их признание той стороной, которая всячески настаивает на несостоятельности российских инициатив, — Вашингтоном. Именно США, согласно американским же экспертам, научным центрам и отчетам госструктур, больше всех страдают от *враждебных актов* в киберпространстве, за которыми якобы стоят государства. Только за последние два года доклады всевозможных американских аналитических центров и институтов приписывают китайским, российским и иранским хакерам систематические атаки на сети Пентагона, попытки кражи данных из сетей ряда федеральных министерств и ведомств, крупнейших оборонных, нефтяных, финансовых и энергетических компаний. В частности, в докладах Пентагона утверждается, что сети ведомства ежедневно выдерживают более шести миллионов попыток неправомерного доступа, в большинстве из которых стоит подозревать российских и китайских хакеров[70].

14 июля 2011 г. замминистра обороны США Уильям Линн III предал гласности данные о крупнейшей успешной атаке «иностранных агрессоров» на сети Пентагона, имевшей место в марте того же года. По словам замминистра, в результате атаки были похищены 24 неизвестными злоумышленниками 24 тыс. секретных и конфиденциальных файлов. Несмотря на отказ прямо назвать автора атаки, источники в Пентагоне весьма прозрачно намекнули на КНР[71]. В ноябре 2011 г. американцы заявили, что взломы геодезических спутников США, якобы имевшие место в 2007 и 2008 гг., «полностью укладываются в логику последних положений военной стратегии Китая»[72]. Тревожной выглядит ситуация с *политически мотивированными* кибератаками на сети частных компаний, обслуживающих объекты критической инфраструктуры. По данным компании *Symantec*, в США только за 2010 г. жертвами таких атак объявили себя 53% операторов объектов национальной критической инфраструктуры[73], практически в каждом втором случае авторство атак приписывается китайцам.

Однако, как можно убедиться на примере операции *Олимпийские игры*, Белый дом далеко не всегда оказывается в оборонительной позиции. По последним данным, разработка серии сложнейших вирусов и внедрение их в сети Ирана и других государств Ближнего Востока стали частью масштабной операции военных и спецслужб США, цель которой в максимальном замедлении иранской ядерной программы. Операция, получившая название *Олимпийские игры*, была спланирована и запущена еще администрацией Джорджа Буша-младшего в 2006 г., резко интенсифицирована после прихода к власти Барака Обамы в 2008 г. и частично продолжает действовать до сих пор[74]. Несмотря на отказ официально признать причастность Белого дома к этой программе и созданию *Stuxnet*, утекающую информацию почти не пытаются опровергать американские власти, так как ситуация выглядит достаточно однозначно.

Развитие военно-стратегического потенциала ИКТ ведется в США и по многим другим направлениям и задачам, зачастую не признаваемым публично. По утверждению Ричарда Кларка, бывшего Национального координатора по безопасности, защите инфраструктуры и контртерроризму США, еще в 2007 г. Израиль провел секретную операцию по уничтожению неопознанного атомного объекта в Сирии, использовав изощренную компьютерную программу для *ослепления* командных систем сирийских ПВО[75]. В результате сирийские силы ПВО были полностью *ослеплены* и не сумели помешать эскадрилье израильских бомбардировщиков, которые успешно разбомбили секретный объект в течение нескольких ночных часов. Данная операция получила в западных экспертных кругах неофициальное название *Фрук-*

товый сад. Г-н Кларк, равно как и другие западные эксперты, не распространяется о том, как Израиль смог разработать подобную программу. Однако, по словам российских технических экспертов в области кибербезопасности, создать такие инструменты без помощи США Израиль на тот момент был не в состоянии, а для операции были использованы наработки американского проекта *Сьютер* (*Suter*).

Оформление кибербезопасности как части *военно-политической* повестки дня происходит в США и на организационно-структурном уровне. Еще в 2009 г. в составе Вооруженных сил США было создано единое Киберкомандование США (USCYBERCOM), в чьи функции входит отражение угроз национальной кибербезопасности, включая *военные киберугрозы*. В результате наряду с тайными операциями превентивные *силовые* действия в киберпространстве получают все более активное развитие в официальных (или полуофициальных) задачах американских госструктур. Перед началом операции *Odyssey Dawn* по обеспечению бесполетной зоны в Ливии в марте 2011 г. американским военным командованием рассматривался вариант нанесения массированного кибердара по инфраструктуре режима Муаммара Каддафи[76]. Подобная опция, несмотря на несоответствие резолюции Совбеза ООН, санкционировавшей бесполетную зону, хорошо укладывается в видение киберпространства как *поля битвы,* которое оформилось в США с принятием Стратегии по действиям в киберпространстве. В ноябре 2011 г. Пентагон подтвердил закрепленное в стратегии право использовать «все необходимые средства», включая военные, «для защиты своей страны, наших союзников, партнеров и интересов»[77]. Таким образом, киберугрозы оказались приравнены к *традиционным* военным угрозам, а в мировой практике появился прецедент права реагировать на киберугрозы использованием обычных вооружений. В августе 2012 г. стало известно о том, что американское Агентство передовых военных разработок (DARPA), стоявшее у истоков создания интернета, объявило тендер на работы в рамках программы *Plan X*[78]. Программа предусматривает создание онлайн-карты киберинфраструктуры США и их потенциальных противников с указанием степеней защищенности и подробных схем стратегических и иных объектов, включая центры оперативного управления, военные базы и склады, объекты транспортной инфраструктуры и системы электроснабжения. Параллельно был объявлен тендер американских ВВС на разработку серии вредоносных программ для «вывода из строя, заражения и взлома операционных систем, серверов и иных сетевых устройств противника», а также «установления временного контроля над киберпространством».

Наконец, США проецируют военно-стратегическое измерение работы с ИКТ и на частный сектор. В августе 2012 г. министру обороны США Леону Панетте была направлена инициатива по расширению полномочий специалистов Пентагона за счет права в отдельных случаях бороться с киберугрозами в сетях других ведомств, а также в частных сетях[79]. А за две недели до этого, в конце июля 2012 г., глава Киберкомандования и директор Агентства национальной безопасности США Кит Александер в своей речи на хакерской конференции *Def Con* в Лас-Вегасе призвал лучших представителей хакерского сообщества идти на службу в возглавляемые им структуры[80].

Упомянутые факты свидетельствуют о том, что Белый дом до сих пор разделяет видение ИКТ, присущее администрации Джорджа Буша-младшего. Суть его сводится к тому, что кибертехнологии — это прежде всего стратегический *актив*, а не *уязвимость* в системе национальной безопасности США. Однако обладая наиболее развитой инфраструктурой ИКТ в мире, Соединенные Штаты оказываются уязвимы для кибератак в беспрецедентной для других стран степени. Дилемма выбора стратегии реагирования на подобную уязвимость долгое время полуспонтанно решалась в пользу укрепления *превентивно-наступательного* потенциала в киберпространстве. Причин было несколько — краткий момент униполярности мира во главе с Америкой в 1990-х гг., казавшийся огромным технологический отрыв США от других стран в сфере ИКТ, отсутствие по-настоящему серьезных киберугроз для самих США, наконец, крайне успешный опыт применения ИКТ для решения военных задач, таких как операция *Буря в пустыне* в 1991 г. в Ираке.

На сегодняшний день мир изменился, однако приоритеты американского подхода к военно-политическому использованию ИКТ остаются прежними, что создает весьма значимую угрозу безопасности глобального киберпространства.

Наращивание США ударного киберпотенциала вкупе с нежеланием обсуждать юридически обязывающие международно-правовые акты в рамках борьбы с киберугрозами тормозит выход мирового сообщества из латентного состояния *войны всех против всех* по Томасу Гоббсу, перенесенной в киберпространство. Государства мира предпочитают готовиться к кибервойнам, а не пытаться исключить их возможность. Эксперты и военные аналитики в Соединенных Штатах уже прогнозируют начало китайско-американской кибервойны на 2015–2017 гг. в связи с вероятным кризисом по поводу статуса Тайваня или спорных островов в Южно-Китайском море[81]. Однако возможные последствия подобного конфликта между государствами с развитыми национальными ИКТ-секторами доподлинно не известны. Поражение критической инфраструктуры в ходе кибервойны способно вызвать непредсказуемые последствия, особенно если речь идет об информационных сетях АЭС, ГЭС, крупных промышленных предприятий, нефте- и газопроводов, логистических узлов, объектов энергогенерации и энергораспределительных сетей. С учетом взаимосвязи элементов глобальной информационной системы, кибервойна в любом случае не может ограничиваться национальными границами изначального объекта агрессии — затронута в той или иной мере будет вся Сеть. Уже по этой причине предотвращение кибервойны является задачей каждого государства, включая как Россию, так и ее партнеров.

Упомянутые факты заставляют задаться закономерным вопросом: насколько уместно игнорировать инициативы по ограничению применения ИКТ в военно-политической плоскости? Как отмечалось выше, США и их западные союзники пока не готовы обсуждать вопросы, связанные с использованием содержания информационных потоков в качестве оружия или военно-стратегического инструмента. Даже если ограничиваться гораздо более узким кругом вопросов кибербезопасности, значительного прогресса не наблюдается и здесь, хотя времени остается все меньше.

Однако, несмотря на данные соображения, на сегодняшний день очевидно, что российская инициатива в той конкретной формулировке и подаче, которые имели место год назад, пока еще не приемлема для *критической массы* наших зарубежных партнеров. Если оставить в стороне рассмотренный ранее вопрос о причинах такой ситуации, на первый план выходит другой вопрос: что делать сейчас?

Менять магистральное направление российского курса в области МИБ, во-первых, вряд ли возможно, во-вторых, контрпродуктивно. Вместе с тем нужно учитывать тот факт, что без определенного сближения позиций и согласования подходов с зарубежными партнерами продвижение российских инициатив вряд ли будет осуществляться должными темпами. Вопрос заключается в том, как предложить ключевым партнерам РФ по диалогу в сфере МИБ приемлемые для них формулы, не отказываясь от конечной цели — построения всеобъемлющего глобального режима обеспечения МИБ. Представляется, что такая работа должна вестись поэтапно, начиная с разрешения наиболее острых противоречий с тем актором, который предлагает и продвигает глобальную альтернативу российскому подходу, то есть с Белым домом. В силу отмеченных выше особенностей доктринального видения США проблем безопасности в сфере ИКТ на нынешнем этапе трудно рассчитывать, что Вашингтон согласится рассматривать тот или иной проект, предполагающий полный запрет на разработку кибероружия и ведение кибервойн, не говоря уже об информационном противоборстве.

С другой стороны, даже среди американского истеблишмента крепнет понимание необходимости запрещения или хотя бы ограничения применения государствами кибероружия в *отдельных* сферах и против *отдельных* типов объектов. Речь, в частности, идет об объектах, имеющих критическое значение для международной безопасности и глобальной стабильности. Прежде всего имеется

в виду инфраструктура, обеспечивающая работу мировой финансовой системы, от которой в равной степени зависят США, Китай, Россия и прочие государства, за исключением нескольких государств вроде КНДР. Такая постановка вопроса, в принципе, отвечает национальным интересам России и всех стран, являющихся элементами глобальной финансовой системы. Вопрос о заключении соглашения о запрете применения кибероружия против информационной инфраструктуры мировой финансовой системы вполне может быть включен в повестку дня российско-американского диалога в дополнение к ведущемуся сотрудничеству по укреплению мер доверия в киберпространстве. Подобные нормы до некоторой степени могут являться развитием постулатов международного гуманитарного права XX в., в частности Гаагских, Женевских конвенций и Дополнительных протоколов к последним.

Безусловно, данным сегментом дальнейшие шаги по укреплению международного сотрудничества в противодействии информационным вызовам ограничиваться не должны. Использование изощренных вирусов, включая включая *Stuxnet, Duqu, Flame, Gauss*, против инфраструктуры Ирана, делает актуальной задачу выработки соглашения, которое запрещало бы целенаправленные кибератаки на информационные системы ОМУ, а также киберинфраструктуру мирной атомной отрасли и наиболее *чувствительных* производств и промышленных объектов. Белый дом едва ли охотно пойдет на обсуждение этого сюжета, по понятным и уже упомянутым причинам. Однако подобная инициатива, в том числе будучи озвученной РФ, оставляет своего автора в выигрышном положении. В данном случае отсутствует привычная почва для критики — размытость формулировок, скрытые возможности для цензуры интернета и прочие недостатки, которые озвучиваются в отношении концепции Конвенции об обеспечении МИБ. Кроме того, идея не просто уместна — она отвечает ключевым озабоченностям международного сообщества в отношении дальнейшего усугубления проблем киберсаботажа. *Stuxnet* всего лишь вывел из строя обогащавшие уран центрифуги, однако следующее поколение подобных программ вполне может быть адаптировано для саботажа на АЭС, химических заводах, хранилищах и системах транспортировки ядерных отходов и других объектах, нарушение нормальной работы которых чревато техногенными катастрофами. Перспектива, которую открывает бесконтрольное использование инструментов киберсаботажа уровня *Stuxnet* уже сегодня — инциденты с человеческими жертвами. В условиях отсутствия согласованного на международном уровне дипломатического и военного алгоритма реагирования и нерешенной проблемы атрибуции такие инциденты могут спровоцировать острейшие дипломатические кризисы и эскалацию конфликтов вплоть до начала военных действий.

Понимание опасности подобного развития событий широко присутствует среди экспертов и дипломатов во всем мире. Если Россия сумеет в правильном ключе подать эту инициативу на международной арене, Вашингтон, решившись ей оппонировать, рискует оказаться в явном меньшинстве и получить поддержку разве что от Израиля. Кроме того, отрицание конструктивного потенциала такой инициативы способно спровоцировать критику со стороны значительной части американского экспертного сообщества. Государства Европы ни *де-юре*, ни *де-факто* не воспринимают операции киберсаботажа по типу *Stuxnet* в качестве адекватных и допустимых инструментов обеспечения национальных интересов. Даже стратегия кибербезопасности Великобритании от 2011 г., в которой ощущается влияние американской парадигматики, отводит место ответным ударам по сетям киберагрессоров и активной обороне в киберпространстве, но никак не превентивному разрушению чужой атомной и промышленной инфраструктуры[82]. В похожем, преимущественно *реактивно-оборонительном* ключе кибервойна понимается и на европейском континенте. Представляется, что основным препятствием к успешному продвижению данной инициативы является скорее в целом настороженное отношение среди западных партнеров к российским инициативам в области МИБ, связанное с вышеупомянутыми спорными моментами в концепции Конвенции. Вместе с тем фундаментальных противоречий приоритетам развитых и развивающихся стран, а также международного сообщества в целом в данном

случае не прослеживается. То есть проблема не носит фундаментального характера, и российской дипломатии требуется лишь преодолеть недоверие наших партнеров при наличии всех *козырей* по сущностной стороне вопроса.

Однако успех этих шагов, в свою очередь, также во многом зависит от того, сумеет ли РФ предложить какие-либо решения применительно к проблеме атрибуции киберугроз и кибератак. Расследование применения *Stuxnet* и его модификаций, длившееся в общей сложности более двух лет, говорит о том, что сами государства без помощи ведущих частных компаний и лабораторий неспособны решать задачу атрибуции сложных и глобальных атак. На острие технического прогресса, хотя и по другую сторону от кибершпионов, киберпреступников и исполнителей актов киберсаботажа, находятся именно крупные частные структуры, которые способны отслеживать даже тщательно замаскированные источники атак. В связи с этим прослеживается еще один потенциальный сюжет, к которому может и должна активно подключиться Россия. Как показала практика, сложные вирусы на Ближнем Востоке изучаются, обнаруживаются и блокируются частными компаниями, которые далеко не всегда сотрудничают друг с другом, а также с государствами, кроме тех, кто сам зовет их на помощь. Ситуация стала понемногу меняться с 2011 г., когда был придан официальный статус сотрудничеству МСЭ с Международным многосторонним партнерством против киберугроз (ИМПАКТ). Только с начала 2012 г. сотрудничество МСЭ и ИМПАКТ позволило выявить несколько серьезных киберугроз — вирусы *Flame* и *Gauss*, а также не получивших практического применения родственников *Flame*. Можно утверждать, что с запуском механизма взаимодействия между ИМПАКТ и МСЭ сотрудничество международных организаций с частным сектором в сфере противодействия глобальным киберугрозам перестало быть спонтанным и начало осуществляться на более-менее системной основе.

Однако потенциал этого механизма пока раскрыт не на 100%, в частности для России, на которую до сих пор не распространяются услуги ИМПАКТ по обеспечению кибербезопасности, в отличие от 144 других государств. При этом в число ключевых участников ИМПАКТ наряду с *Symantec Corporation, F-Secure, Trend Micro, Microsoft* входит и российская *Лаборатория Касперского*, которая фактически стала мировым лидером в части обнаружения изощренных ближневосточных вирусов и противодействия им. Российским госструктурам, безусловно, необходимо в полной мере использовать государственно-частный потенциал (ГЧП) в сфере кибербезопасности, тем более если мы можем задействовать уникальный *центр компетенций — Лабораторию Касперского* — в рамках широкого международного формата.

Удачно проявляющий себя механизм ГЧП должен развиваться и далее, укрепляя свои позиции на площадке ООН. В этой связи перспективным решением представляется создание *Центра предотвращения киберугроз ООН*. Развиваясь на площадке ИМПАКТ, подобная структура может взять на себя функции глобальной площадки по выявлению наиболее серьезных киберугроз и борьбе с ними — ее прообразом уже является Глобальный центр реагирования (ГЦР), составляющий основу механизма ИМПАКТ. Помимо нынешних функций (раннее обнаружение и оповещение о киберугрозах, совместные расследования случаев применения кибероружия, консультации и экспертная помощь пострадавшим государствам) *Центр* может стать официальным разработчиком новых стандартов кибербезопасности, а также вносить вопросы борьбы с развитием кибероружия в повестку Генассамблеи ООН. Россия благодаря сильным позициям и традиционно активному участию в обсуждении вопросов информационной безопасности на площадке Объединенных Наций вполне может сыграть одну из ведущих ролей в укреплении подобного механизма, который отвечает нашим национальным интересам.

С учетом непрекращающегося выявления все новых сложных вредоносных программ в сетях ближневосточных стран опыт и компетенции *Лаборатории Касперского* и других российских структур частного сектора могут стать стратегическим активом РФ на Ближнем Востоке, да и за его пределами. Задача российских госу-

дарственных органов — более системно работать с такими активами, в том числе в рамках задачи формирования режима МИБ. В данном случае России не придется преодолевать сопротивление США, ЕС или других государств, так как ИМПАКТ и государственно-частное партнерство в сфере противодействия киберугрозам воспринимаются в качестве конструктивной и взаимовыгодной инициативы практически всеми странами и международными организациями.

Упомянутыми мерами *точки пересечения* интересов РФ и ее зарубежных партнеров, включая США, по вопросам обеспечения МИБ или безопасности киберпространства не исчерпываются. Их логическим развитием должно стать соглашение о всеобщем запрете на применение кибероружия против критической инфраструктуры невоенных объектов и информационных систем отдельных видов неядерных ударных вооружений. Эти меры являются частью работы по изучению возможностей адаптации и имплементации норм международного гуманитарного права в отношении киберпространства, которую активно ведет РФ. Развитие *Центра предотвращения киберугроз* в дальнейшем открывает возможности для создания *Центра предотвращения информационных угроз ООН,* деятельность которого уже будет распространяться за рамки проблематики *кибер*безопасности. Последняя, к слову, не является более важной, чем вопросы, которые пытается артикулировать Россия. Однако она легче поддается *фиксации* и практической проработке, она более *осязаема* в силу объективных сложностей, которые присущи концептуальным и теоретическим аспектам информационной безопасности в рамках российского подхода и которые рассматривались выше. А следовательно, в том, чтобы пока, *на сегодняшнем этапе* сосредоточиться на формировании международного режима кибербезопасности, нет ничего контрпродуктивного и противоречащего российским интересам. Важно продвигаться там, где это получается на данный момент, и российское руководство на самом деле хорошо это понимает, судя хотя бы по активным переговорам с США по вопросам обмена информацией о киберугрозах и мерах доверия в киберпространстве, которые считаются чисто американским *коньком*. Первым этапом взаимодействия по этой линии стало совместное заявление Климашина–Шмидта в июне 2011 г. и создании российско-американской линии оперативного взаимного информирования о киберинцидентах. Второй этап с подписанием соглашения сорвался в самом начале июня 2012 г., перед встречей двух президентов в Мексике. Однако новая серия обсуждений этих вопросов пройдет уже осенью 2012 г., и рано или поздно приведет к расширению каналов и повестки двустороннего взаимодействия.

Обобщая сказанное, уместно будет привести соображение общетеоретического характера. Суть его заключается в том, что *накрыть* всю проблематику МИБ единым международно-правовым актом в настоящее время едва ли возможно. Необходимо последовательное движение *снизу вверх* — от точечных, узких договоренностей к механизмам более широкого и универсального характера. На фоне стратегической важности задачи строительства режима обеспечения МИБ необходимо помнить о том, что в мировой истории практически неизвестны случаи, когда режимы в сфере разоружения и международной безопасности сразу начинали формироваться с всеобъемлющих глобальных соглашений. При этом также важно, что сфера военно-политического применения ИКТ, не говоря уже о киберпреступности и кибертерроризме, сегодня с трудом поддается эффективному контролю со стороны государств — в отличие от размещения оружия в космосе, вопросов химического и биологического ОМУ.

В данной связи полезен может быть опыт режима контроля над ядерными вооружениями (ЯВ), который в основном сложился за время холодной войны. Его формирование заняло несколько десятилетий, а в части проблематики увязки оборонительных и наступательных стратегических вооружений продолжается до сих пор. Режим контроля над ЯВ вырастал из ограниченных по масштабу и временному горизонту мер, таких как временный договор об ограничении стратегических наступательных вооружений (ОСВ-1) между СССР и США, а также договоров о запрещении испытаний ЯВ в отдельных пространствах. Сверхдержавы

*Пал **Дунай (Венгрия)**, руководитель программы по международной безопасности Женевского центра политики безопасности — по электронной почте из Будапешта:* Я не ожидаю презентации и обсуждения каких-либо «глобальных договоров и предложений по регулированию киберпространства» до конца 2012 г. Конечно, единственное исключение возможно в том случае, если с таким предложением выступят Россия и Китай, подобно тому, как они уже делали в прошлом году перед Конференцией по киберпространству в Лондоне и в ходе нее. На самом деле, мне неизвестно, планирует ли Россия представить какие-либо инициативы помимо тех, которые были изложены год назад в Лондоне и вновь обсуждались на конференции в Будапеште 4–5 октября 2012 г. США и страны Запада, во всей видимости, сейчас не слишком настроены обсуждать подобные идеи. Лондонская конференция, к слову, не считается такой уж успешной, несмотря даже на тот факт, что на ней присутствовали некоторые весьма высокопоставленные персоны, включая шведского министра иностранных дел. То же самое по большому счету можно сказать и в отношении недавней встречи в Будапеште. Возможно, эти конференции все же откроют дверь для более плодотворных обсуждений будущих шагов по укреплению международного сотрудничества в киберпространстве.

прошли через долгие годы изматывающей гонки стратегических ядерных арсеналов и Карибский кризис, прежде чем решились перейти от *выставления потолков* к сокращению запасов ЯВ. Еще недавно применение ЯВ рассматривалось в качестве крайней, но все-таки возможной меры, причем не только оборонительного характера — стоить вспомнить военные доктрины США 1950-х гг. Упомянутая *горячая линия* по киберинцидентам между США и РФ является аналогом канала оповещения об инцидентах с ядерным оружием, который был создан после Карибского кризиса в 1963 г. — за десятилетия до старта масштабного процесса разоружения двух сверхдержав, принятия ряда ключевых договоров в сфере контроля над вооружениями и запрещения ядерных испытаний. Следуя этой аналогии, мы находимся почти в самом начале пути. Сегодня, когда разрушительное оружие может быть создано в течение считанных месяцев и применено в любой точке глобального информационного пространства, десятилетий у нас в запасе нет. Однако законы строительства режимов в сфере международной безопасности действуют и применительно к информационному пространству. Именно поэтому необходимо начинать с соглашений — пусть ограниченных и даже точечных — по наиболее острым и одновременно поддающимся практической проработке вопросам.

ВЫВОДЫ И РЕКОМЕНДАЦИИ

1. До практической имплементации российских инициатив в области борьбы с киберпреступностью в рамках механизмов ООН, очевидно, пройдут годы, в течение которых российский рынок киберпреступности при сохранении *статус-кво* ждет мощный рост. Ситуация во многом обусловливается трансграничным характером киберпреступности, которая все больше ориентируется на Россию как на самостоятельный рынок. Неучастие России в Будапештской конвенции существенно обостряет эту проблему, однако в нынешнем виде Конвенция может нарушать принцип государственного суверенитета и использоваться для скрытого кибершпионажа против РФ. Кроме того, ее нормы устаревают и не покрывают бурно растущие новые сегменты глобальной киберпреступности.

Для критичной и объективной оценки целесообразности присоединения РФ к Конвенции СЕ необходим непредвзятый анализ, который позволит оценить и измерить негативные и позитивные эффекты такого решения в экономических категориях. Необходимо дать ответ на вопрос о том, покроет ли потенциальное сокращение объемов потерь российской экономики от киберпреступности в результате присоединения к Конвенции возможные потери конфиденциальной информации и ущерб национальной безопасности в результате негативных эффектов применения пункта *32b* в экономическом выражении. Подобная постановка вопроса поможет развеять существующее сегодня среди зарубежных партнеров и части российского экспертного сообщества недопонимание позиции российского руководства и спецслужб в отношении Будапештской конвенции. Кроме того, вопрос пересмотра РФ своей позиции в отношении Конвенции может быть увязан с ее обновлением и повышением эффективности ее механизма. Если такие изменения будут иметь место, целесообразен мог бы быть вариант присоединения России к Конвенции на тот срок, пока не будут приняты и имплементированы иные международные механизмы борьбы с киберпреступностью, более отвечающие российским национальным интересам.

2. На сегодняшний день инициативы России и ШОС, изначально преследуя весьма масштабные цели, сталкиваются с рядом концептуальных трудностей и вызовов. Во-первых, их терминология имеет ряд уязвимых мест и нуждается в значительной доработке, в частности выработке более строгих и однозначных определений, а также *закрытии брешей*, таких как проигнорированный вопрос кибершпионажа. Проекты документов страдают избыточным упором на роль государства, который ведет к *выпадению* из их поля зрения других участников информационного обмена, в том числе частного сектора, глобальных медиа, интернет-пользователей и посредников, выполняющих волю государств в информационном пространстве.

В концепции Конвенции и других документах необходимо обозначить подход к проблемам анонимности в интернете, а также вопросу ответственности за информационные потоки в трансграничной Сети, без чего имплементация их принципов едва ли возможна. Прописанные в концепции Конвенции задачи по недопущению использования ИКТ в военно-политических целях в ряде случаев опережают сегодняшние реалии. Для продвижения российских инициатив на мировой арене необходимо сузить спектр задач в той части, где их принципы не подкрепляются дееспособными механизмами контроля и верификации. Такими проблемными вопросами являются контроль над содержанием трансграничных информационных потоков, полный отказ от создания информационного оружия и ответственность государств за содержание информации, размещаемой в «его информационном пространстве».

3. Проблема, которую призвана решить концепция Конвенции об обеспечении МИБ и другие инициативы РФ, стоит весьма остро в глобальном масштабе. Помимо угрозы информационной войны как манипулирования информацией с целью подрыва социально-политического уклада, нарастают глобальные киберугрозы, включая кибервойны и разрушение критической инфраструктуры. Данная

ЛИСТАЯ СТАРЫЕ СТРАНИЦЫ

Современные информационные технологии могут использоваться в качестве оружия. Причем воздействие такого оружия качественно отличается от традиционного, и, соответственно, вопросы его дальнейшего развития, распространения и возможного применения должны стать предметом специальных норм международного права. Вся история развития новых видов оружия начиная от обычного и кончая ракетно-ядерным говорит о том, что международное сообщество в итоге находило разработку таких норм рациональной и необходимой. Проблема, однако, в том, что эти меры разрабатывались чаще всего уже после того, как новое оружие было изобретено и применено.

Международные вызовы информационной безопасности. М.: ПИР-Центр, 2001.

проблематика полностью подпадает под задачи и механизмы в рамках российских инициатив. Российский подход к обеспечению МИБ включает вопросы кибербезопасности в более широкую проблематику, не выделяя их в качестве самостоятельной сферы регулирования.

С учетом взаимосвязи элементов глобальной информационной сети, кибервойна в той или иной мере затронет ее всю. По этой причине предотвращение кибервойн является задачей каждого государства, включая Россию и ее западных партнеров. Однако сегодня международные усилия по формированию режима безопасности киберпространства явно недостаточны. Наращивание США ударного киберпотенциала вкупе с нежеланием обсуждать юридически обязывающие международно-правовые акты в рамках борьбы с киберугрозами тормозит выход мирового сообщества из латентного состояния *войны всех против всех* по Томасу Гоббсу, перенесенной в киберпространство. Государства мира предпочитают готовиться к кибервойнам, а не пытаться исключить их возможность.

4. Вместе с тем в мире крепнет понимание необходимости запрета или хотя бы ограничения применения кибероружия в *отдельных* сферах и против *отдельных* типов объектов. Речь идет об объектах, имеющих критическое значение для международной безопасности и глобальной стабильности. России в данный момент имеет смысл сосредоточить усилия на следующих вопросах:

- выработка и заключение многостороннего соглашения (при особой роли взаимодействия с США) о запрете кибератак на информационную инфраструктуру глобальной финансовой системы;
- заключение на площадке ООН договора/конвенции о запрете кибератак на инфраструктуру ОМУ, а также наиболее *чувствительных* производств и промышленных объектов, разрушение которых чревато техногенными катастрофами;
- присоединение к механизму ИМПАКТ и максимальное усиление своих позиций в рамках этого механизма, включая использование потенциала частных российских компаний (в том числе *Лаборатории Касперского*) в решении глобальных проблем кибербезопасности;
- развитие ИМПАКТ до официальной площадки ООН по противодействию угрозам МИБ — *Центра информационных угроз ООН*, структуры ГЧП, которая объединит крупнейших игроков индустрии кибербезопасности, а также масс медиа. Структура сможет стать официальным разработчиком новых стандартов кибербезопасности, а также вносить вопросы борьбы с разработкой и применением кибер- и информационного оружия в повестку дня Генассамблеи ООН, расследовать случаи применения такого оружия и информировать об информационных угрозах мировое сообщество.
- адаптация ключевых норм и принципов международного гуманитарного права, включая Гаагские конвенции, а также Женевские конвенции и Дополнительные протоколы к ним, к условиям конфликтов в кибер- и информационном пространстве. Это направление может включать выработку всеобщего запрета на применение кибероружия против критической инфраструктуры невоенных объектов.

Проблематика кибербезопасности не является фундаментально более важной, чем вопросы обеспечения МИБ, которые пытается артикулировать Россия. Однако на данном этапе вопросы кибербезопасности легче поддаются *фиксации* и практической проработке, они более *осязаемы* в силу объективных сложностей, присущих концептуальным и теоретическим аспектам информационной безопасности в рамках российского подхода. В силу этого *на сегодняшнем этапе* целесообразнее сосредоточиться на формировании международного режима безопасности киберпространства, что также в полной мере отвечает российским национальным интере-

сам. Представляется, что *охватить* всю проблематику МИБ единым международно-правовым актом на данный момент невозможно, и, следовательно, необходимо постепенное движение *снизу вверх* — от точечных, узких договоренностей к механизмам более широкого и универсального характера, которые на некотором этапе перерастут рамки проблематики кибербезопасности и вместят в себя те вопросы, которые Россия пытается выдвинуть в ранг глобальных приоритетов сегодня. Пока первостепенной задачей должно стать достижение конкретных соглашений в более узкой нише кибербезопасности как первый шаг в последовательном движении из состояния полной правовой неурегулированности ИКТ в контексте международной безопасности к всеобъемлющему режиму обеспечения МИБ.

5. Последнее соображение не вытекает из анализа напрямую и представляет собой развитие предыдущих выводов. Для продвижения инициатив в области обеспечения МИБ России, по всей видимости, необходимы определенные шаги на национальном уровне. Ключевым из них представляется разработка национальной стратегии информационной безопасности (или, возможно, кибербезопасности). Одной из задач такой стратегии должно стать обеспечение поддержки российским международным инициативам за счет формирования видения проблематики кибер- и информационной безопасности в рамках приоритетов национального уровня. Для обеспечения преемственности и единства подхода к вопросам информационной безопасности на национальном и международном уровне такой документ должен решать следующие задачи:

- определять пути совершенствования законодательной базы РФ в области противодействию киберпреступности, особенно в части международного сотрудничества;
- закреплять и обосновывать модель реагирования на агрессивные действия государств и их посредников в информационном пространстве с учетом *проблемы атрибуции*;
- выделять в отдельное направление и подробно регулировать вопросы, которые укладываются в проблематику кибербезопасности (защиту критической инфраструктуры, противодействие актам киберсаботажа, защиту национальных сетей от вредоносного кода и так далее);
- синхронизировать деятельность структур, отвечающих за обеспечение национальной безопасности РФ, по противодействию информационной агрессии, а также закреплять видение и принципы взаимодействия таких структур с российскими и глобальными медиа, частными организациями ИТ-сектора и интернет-сообществами.

В целом, новый стратегический документ должен стать тем *пропущенным звеном эволюции* между Доктриной информационной безопасности 2000 г. и конкретными законодательными актами, отсутствие которого мешает свести российскую государственную политику в сфере информационной безопасности в единый логически цельный комплекс ценностей, задач и средств их достижения. Международная составляющая такой политики от этого выиграет в первую очередь.

Примечания

[1] Department of Defense Strategy for Operating in Cyber Space. July 2011. http://www.defense.gov/news/d20110714cyber.pdf (последнее посещение — 4 октября 2012 г.).

[2] Крутских А. К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы*. http://www.intertrends.ru/thirteen/003.htm (последнее посещение — 4 октября 2012 г.).

[3] Там же.

[4] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей (по докладу Перво-

го комитета (A/53/576). Организация объединенных наций. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement (последнее посещение — 4 октября 2012 г.).

[5] Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. Fifty-third session. First Committee. Distr.: General. 30 September 1998. http://disarmament2.un.org/Library.nsf/1c90cfa42bbb0d6985257631004ff541/663e6453bdaa2e22852576500055027 7/$FILE/A-C1-53-3_russia.pdf (последнее посещение — 4 октября 2012 г.).

[6] Text: Common Security Challenges at Threshold of the 21st Century. USIS Washington File. 1998, September 02, http://www.fas.org/news/russia/1998/98090212_tpo.html (последнее посещение — 4 октября 2012 г.). Также см.: *Крутских А.* К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы. Журнал теории международных отношений и мировой политики.* http://www.intertrends.ru/thirteen/003.htm#2 (последнее посещение — 4 октября 2012 г.).

[7] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей [по докладу Первого комитета (A/56/533)]. A/RES/56/19. Генеральная Ассамблея. http://www.ifap.ru/ofdocs/un/5619.pdf (последнее посещение — 4 октября 2012 г.).

[8] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря. A/60/202. Генеральная Ассамблея. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/65/PDF/N0545365.pdf?OpenElement (последнее посещение — 4 октября 2012 г.).

[9] Fact Sheet. Developments In The Field Of Information And Telecommunications In The Context Of International Security. United Nations Office for Disarmament Affairs. http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf (последнее посещение — 4 октября 2012 г.).

[10] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/RES/60/45. Генеральная Ассамблея. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/490/32/PDF/N0549032.pdf?OpenElement (последнее посещение — 4 октября 2012 г.).

[11] *Крутских А.* К политико-правовым основаниям... http://www.intertrends.ru/thirteen/003.htm (последнее посещение — 4 октября 2012 г.).

[12] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря. A/65/201. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/469/59/PDF/N1046959.pdf?OpenElement (последнее посещение — 4 октября 2012 г.).

[13] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря. A/66/152. Генеральная Ассамблея. http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=R (последнее посещение — 4 октября 2012 г.).

[14] Там же.

[15] Черненко Е. Россия зашла на интернет-форум со своими правилами. *Газета «Коммерсантъ»*. 2011, 1 ноября, http://www.kommersant.ru/doc/1807713/print (последнее посещение — 4 октября 2012 г.).

[16] Шестой международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму», 23–26 апреля 2012 г. Институт проблем информационной безопасности (ИПИБ) МГУ имени М. В. Ломоносова. 2012, 25 апреля, http://www.iisi.msu.ru/news/news56/(последнее посещение — 4 октября 2012 г.).

[17] Там же.

[18] An open internet is the only way to support security and prosperity for all. Foreign Secretary speech at the Budapest Conference on Cyberspace. Foreign&Commonwealth Office. 2012,

October 4, http://www.fco.gov.uk/en/news/latest-news/?id=818554782&view=Speech (последнее посещение — 4 октября 2012 г.).

[19] Russia — U.S. Bilateral on Cybersecurity. Critical Terminology Foundations. Issue 1, 2011. EastWest Institute and the Information Security Institute of Moscow State University. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=130080 (последнее посещение — 4 октября 2012 г.).

[20] О ратификации Соглашения между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Закон Республики Казахстан от 01.06.2010 № 286-IV. http://e.gov.kz/wps/wcm/connect/62b81c00433164d5bac4be06acaf12a7/Z100000286_20100601.htm?MOD=AJPERES&CACHEID=62b81c00433164d5bac4be06acaf12a7&useDefaultText=0&useDefaultDesc=0 (последнее посещение — 4 октября 2012 г.).

[21] Подробнее см. статью в этом номере журнала *Индекс Безопасности*: Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности. *Индекс Безопасности*. 2013. Весна. № 1 (104). С. 78–80.

[22] Три брата Flame. Лаборатория Касперского. 2012,17 сентября, http://www.kaspersky.ru/news?id=207733844 (последнее посещение — 4 октября 2012 г.).

[23] «Лаборатория Касперского» и Международный союз электросвязи обнаружили новый вид кибероружия. Kaspersky Lab. 2012, 28 июня, http://www.kaspersky.ru/news?id=207733770 (последнее посещение — 4 октября 2012 г.).

[24] Вирусы-шпионы для кибервойны. Сделано в США, эффект гарантирован. *Радио Голос России.* 2012, 18 сентября, http://rus.ruvr.ru/2012_09_18/Flame-masshtab-jepidemii-besprecedenten/(последнее посещение — 4 октября 2012 г.).

[25] Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве Министерство обороны Российской Федерации (Минобороны России). http://www.ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (последнее посещение — 4 октября 2012 г.).

[26] Подробнее о проблемах глобальной идентификации в Сети см. статью в этом номере журнала Индекс Безопасности: Якушев М. Международно-политические проблемы идентификации в интернете. *Индекс Безопасности*. 2013. Весна. №1 (104) С. 87–102.

[27] World Federation of Exchanges. NYSE Euronext — NewYork. http://www.world-exchanges.org/member-exchanges (последнее посещение — 4 октября 2012 г.).

[28] NYSE Euronext. September 8, 2004: Testimony of Robert G. Britz, President and Co-COO, New York Stock Exchange, Inc. on «Protecting our Financial Infrastructure: Preparation and Vigilance». before the Committee on Financial Services U.S. House of Representatives Washington, DC.

[29] Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives. January 2003 CRITICAL INFRASTRUCTURE PROTECTION. Efforts of the Financial Services Sector to Address Cyber Threats. http://www.gao.gov/new.items/d03173.pdf (последнее посещение — 4 октября 2012 г.).

[30] Symantec 2010 Critical Infrastructure Protection Study. Symantec. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=CIP_survey (последнее посещение — 4 октября 2012 г.).

[31] *Hedley R. A.* Transnational Corporations and Their Regulation: Issues and Strategies. ABSTRACT. http://instructional1.calstatela.edu/tclim/S09_Courses/HEDLEY-tncs.pdf (последнее посещение — 4 октября 2012 г.).

[32] Черненко Е. Россия продвигает границы в интернет. *Газета «Коммерсантъ»*. 2012, 27 апреля, http://www.kommersant.ru/doc/1924818/print (последнее посещение — 4 октября 2012 г.).

[33] Council of Europe. Convention on Cybercrime, Budapest, 23.XI.2001. http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (последнее посещение — 4 октября 2012 г.).

[34] Россия отказалась ратифицировать конвенцию СЕ о киберпреступности. *Газета «Взгляд»*. 2010. 9 ноября. http://www.vz.ru/news/2010/11/9/445958.html (последнее посещение — 4 октября 2012 г.).

[35] Там же.

[36] European Treaty Series — No. 185. Convention on Cybercrime. Budapest, 23.XI.2001. http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (последнее посещение — 4 октября 2012 г.).

[37] Выступление начальника Бюро специальных технических мероприятий МВД России генерал-полковника милиции Бориса Мирошникова на конференции в рамках Проекта Международного сотрудничества по уголовным делам на тему: «Перспективы международного сотрудничества по уголовным делам, 1 марта 2007. Министерство внутренних дел Российской Федерации. http://www.mvd.ru/reform/interview/show_83370 (последнее посещение — 4 октября 2012 г.).

[38] Волеводз А. Конвенция о киберпреступности: новации правового регулирования. *Правовые вопросы связи*. 2007. № 2. С. 17–25. http://www.mgimo.ru/files/113908/113908.pdf (последнее посещение — 4 октября 2012 г.).

[39] Schjolberg S., Ghernaouti-Helie S. A Global Treaty on Cybersecurity and Cybercrime. Second edition, 2011. http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (последнее посещение — 4 октября 2012 г.).

[40] Co-Chairs' Summary Report. ARF Workshop On Proxy Actors In Cyberspace. Hoi An City, Quang, Nam Province, Viet Nam. ASEAN Regional Forum. 14–15 March 2012. http://aseanregionalforum.asean.org/files/library/ARF%20Chairman's%20Statements%20and%20Reports/The%20Nineteenth%20ASEAN%20Regional%20Forum,%202011-2012/10%20-%20Co-Chairs%20Summary%20Report%20-%20ARF%20Workshop%20on%20Proxy%20Actors%20in%20-Cyberspace,%20Quang%20Nam.pdf (последнее посещение — 4 октября 2012 г.).

[41] CYBERCRIME. Council of Europe. 2012, March 2, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (последнее посещение — 4 октября 2012 г.).

[42] UK supports the Global Project on Cybercrime. Council of Europe. 2012, March 2, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (последнее посещение — 4 октября 2012 г.).

[43] Черненко Е. Белоруссия выбрала интернет побезопаснее. *Газета Коммерсантъ*. 2012, 7 июня, http://www.kommersant.ru/doc/1953059 (последнее посещение — 4 октября 2012 г.).

[44] Киберпреступность не имеет границ. *Экономическая газета*. 2007, 29 мая, http://www.neg.by/publication/2007_05_29_8207.html?print=1 (последнее посещение — 4 октября 2012 г.).

[45] ESET: рынок киберпреступности в России. Итоги 2010 года. *ESET.* http://www.esetnod32.ru/.company/news/?id=35865&year=2011# (последнее посещение — 4 октября 2012 г.).

[46] «Русский» рынок компьютерных преступлений в 2010 году: состояние и тенденции. Москва, 2011. Group-IB. http://www.group-ib.ru/wp-content/uploads/2011/03/GIB-Issl-rynka_2010.pdf (последнее посещение — 4 октября 2012 г.).

[47] Сачков И. Правовые аспекты борьбы с киберпреступностью. Доклад в рамках Специальной программе RIW-2011: Неделя российского интернета, 18.10.2011. http://2011.russianinternetweek.ru/program/(последнее посещение — 4 октября 2012 г.).

[48] Половое сношение и иные действия сексуального характера с лицом, не достигшим шестнадцатилетнего возраста.

[49] Раскин А. Насильнику смягчили приговор. *Expert Online*. 2012, 23 августа, http://expert.ru/2012/08/23/nasilniku-smyagchili-prigovor/(последнее посещение — 4 октября 2012 г.).

[50] За кражу $10 млн российскому хакеру дали условный срок. *BFM.Ru.* 2011, 8 февраля, http://www.bfm.ru/articles/2011/02/08/za-krazhu-10-mln-rossijskomu-hakeru-dali-uslovnyj-srok.html (последнее посещение — 4 октября 2012 г.).

[51] Число преступлений в сфере интернет-банкинга за год выросло в три раза. *DIGIT. Проект РИА Новости*. 2011, 28 октября, http://digit.ru/internet/20111028/385602315.html (последнее посещение — 4 октября 2012 г.).

[52] Семинар Академии народного хозяйства при Правительстве РФ «Компьютерные преступления или что делать, если это случилось в твоей компании». 2011, 3 марта, http://www.globalcio.ru/theme-2011-03-first/(последнее посещение — 4 октября 2012 г.).

[53] Интернет-конференция «DDoS-атаки в России как способ нечестной конкурентной борьбы». *ИА Клерк.Ру*. 2010, 16 декабря, http://www.klerk.ru/buh/articles/205822/(последнее посещение — 4 октября 2012 г.).

[54] Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ. Уголовный Кодекс РФ от 13.06.1996 № 63-ФЗ (принят ГД ФС РФ 24.05.1996) (действующая редакция). http://www.consultant.ru/popular/ukrf/10_38.html#p4556 (последнее посещение — 4 октября 2012 г.).

[55] Сачков И. Интервью с автором. 2012, 27 сентября.

[56] Там же.

[57] Подробнее см. интервью в этом номере журнала *Индекс Безопасности*: Сондерс Джейми. Как избежать эскалации конфликтов в киберпространстве? *Индекс Безопасности*. 2013. Весна. № 1 (104). С. 11–16.

[58] Выступление Игоря Щёголева на конференции по вопросам киберпространства (The London Conference on Cyberspace), Лондон, 1 ноября. Минкомсвязь России. http://minsvyaz.ru/ru/speak/index.php?id_4=42975 (последнее посещение — 4 октября 2012 г.).

[59] Kirill Barsky, Special Representative of the President of the Russian Federation on the Shanghai Cooperation Organization. «The International Information Security as a Global Challenge: The Shanghai Cooperation Organization's Vision». Текст имеется в распоряжении ПИР-Центра.

[60] РФ представит Совбезу ООН конвенцию по IT-безопасности. Digit. Проект РИА Новости. 2012, 5 июня, http://www.digit.ru/state/20120605/392334876.html (последнее посещение — 4 октября 2012 г.).

[61] Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 г. Официальный вебсайт ООН. http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (последнее посещение — 4 октября 2012 г.).

[62] The High-Level Experts Group on Cybersecurity (HLEG). ITU Official Website. http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html (последнее посещение — 4 октября 2012 г.).

[63] *Schjolberg S., Ghernaouti-Helie S.*. A Global Treaty on Cybersecurity and Cybercrime. Second edition, 2011. http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (последнее посещение — 4 октября 2012 г.).

[64] В поисках кибермира. Хамадун И. Туре (Hamadoun I. Touré), Генеральный секретарь Международного союза электросвязи и Постоянная группа по мониторингу информационной безопасности Всемирной федерации ученых. 2011, январь, http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-R.pdf (последнее посещение — 4 октября 2012 г.).

[65] Там же.

[66] Video: Hillary Clinton's Remarks for the Budapest Cyber Conference. Secretary of State Hillary Rodham Clinton; Budapest, Hungary. U. S. Department of State. 2012, October 4, http://still4 hill.com/2012/10/05/video-hillary-clintons-remarks-for-the-budapest-cyber-conference/

[67] В Германии началась учебная кибервойна. *Lenta.ru,* 2011, 30 ноября, http://lenta.ru/news/2011/11/30/lunex/(последнее посещение — 4 октября 2012 г.).

[68] Там же.

[69] Активное Участие, Современная Оборона. Стратегическая Концепция Обороны и Обеспечения Безопасности Членов Организации Североатлантического Договора. 2010, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-rus.pdf (последнее посещение — 4 октября 2012 г.).

[70] The Pentagon's New Cyber Command. ISN ETH Zurich. 2010, December 20, isn.ethz.ch/isn/Current-Affairs/ISN-Insights/Detail?lng=en&id=125768&contextid734=125768&contextid735=125766&tabid=125766 (последнее посещение — 4 октября 2012 г.).

[71] Pentagon admits suffering major cyber attack in March. *BBC News.* 2011, 14 July, http://www.bbc.co.uk/news/world-us-canada-14157975 (последнее посещение — 4 октября 2012 г.).

[72] Chinese Military Suspected in Hacker Attacks on U.S. Satellites. Bloomberg. By Tony Capaccio and Jeff Bliss. 2011, 27 October, http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html (последнее посещение — 4 октября 2012 г.).

[73] Half of Critical Infrastructure Providers Have Experienced Perceived Politically Motivated Cyber Attacks. Press Release: Symantec. 2010, October 6, http://finance.yahoo.com/news/Half-of-Critical-iw-478930509.html?x=0&.v=1 (последнее посещение — 4 октября 2012 г.).

[74] Подробнее см.: Sanger David E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. New Yorker: Crown Publishers, 2012. Также см. раздел *Книжные новинки* в этом номере журнала *Индекс Безопасности*.

[75] Cyberwar. The Next Threat to National Security and What to Do About It. By Richard A. Clarke and Robert K. Knake. Ecco. C. 12–17.

[76] Schmitt E., Shanker T. U.S. Debated Cyberwarfare in Attack Plan on Libya. *The New York Times*. 2011, October 17, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1 (последнее посещение — 4 октября 2012 г.).

[77] U.S. reserves right to meet cyber attack with force. *Reuters*. 2011, November 15, http://www.reuters.com/article/2011/11/16/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116 (последнее посещение — 4 октября 2012 г.).

[78] Kennedy J. Plan X: DARPA's Cyberwar. Security. PC World. 2012, August 30, http://www.pcworld.com/article/261720/plan_x_darpa_s_cyberwar.html (последнее посещение — 4 октября 2012 г.).

[79] Двойные стандарты США в киберпространстве. *Peacekeeper.ru. Военно-политическое обозрение*. 2012, 13 августа, http://www.peacekeeper.ru/ru/?module=news&action=view&id=15691 (последнее посещение — 4 октября 2012 г.).

[80] Черненко Е. Хакеров зовут на госслужбу. *Коммерсантъ*. 2012, 1 августа, http://www.kommersant.ru/doc/1992500 (последнее посещение — 4 октября 2012 г.).

[81] См. например: Clarke R., Knake R. Cyberwar. The Next Threat to National Security and What to Do About It. New York: Ecco, 2010. C. 134–136. Brenner J. America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. New York: The Penguin Press, 2011. C. 217–219.

[82] The UK Cyber Security Strategy. Cabinet Office. http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy (последнее посещение — 4 октября 2012 г.).