Анализ

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: АРЕНА СОПЕРНИЧЕСТВА ИЛИ ПУТЬ СОТРУДНИЧЕСТВА?

Александр Федоров

В последнее десятилетие резко проявилась и встала в один ряд с проблемой нераспространения ОМУ проблема международной информационной безопасности. Ведутся серьезные разговоры об информационном противостоянии, информационном оружии как оружии XXI века, по потенциальной эффективности оставляющем далеко позади все известные виды оружия массового поражения. На создание средств защиты информации и средств преодоления уже созданных средств защиты тратятся миллиардные суммы. Ведущие страны мира включают в свои военные доктрины, концепции национальной безопасности, законодательные системы и уголовные законодательства статьи, направленные на противодействие информационным угрозам как отдельной личности, так и государству. В связи с тем, что компьютерная преступность приобрела международный характер, Евросоюз разработал Конвенцию по киберпреступности и 23 ноября 2001 г. открыл ее для подписания; странами «большой восьмерки» в повестки дня Римской и Лионской групп внесены вопросы противодействия кибертерроризму и киберпреступности.

Основываясь на материалах последних четырех сессий ГА ООН[1], можно констатировать, что международная информационная безопасность признана как самостоятельная общемировая проблема, а ее обеспечение как одно из необходимых условий существования человеческого сообщества в «информационный век»[2].

Инициатором вынесения этого вопроса на международный уровень стала Российская Федерация[3]. Однако реакция на российские инициативы оказалась неоднозначной и их путь к признанию – непростым.

Два подхода к определению информационной безопасности

Информационные технологии, являясь в основном мирными, коренным образом меняют военную составляющую безопасности: как ее теорию, влияя на военное искусство (размывая считавшиеся устоявшимися понятия, в частности, предвоенного и начального периода войны), так и практику, значительно повышая эффективность применения других видов оружия. Надо прямо признать, что даже паритет ядерных сил в настоящее время во многом зависит от паритета в информационных технологиях: превосходство в последних может привести к созданию средств, позволяющих нарушать командные коды или процедуры и сделать системы управления ненадежными или неработоспособными. Нарушение информационного обмена или информационных потоков в критических областях (транспорт, связь, энергоснабжение, чрезвычайные ситуации и т.д.), а также вмешательство в них с целью дезорганизации могут нарушить экономические или военные отношения между странами и вызвать ответные действия. К серьезным политическим и экономическим последствиям могут привести успешные психологические операции с применением информационных технологий. Вследствие всего этого информационная сфера государства в случае возникновения войны становится наиболее вероятной целью воздействия информационными же средствами. Соответственно возник и развивается новый феномен безопасности – информационная безопасность, чаще всего выступающий как частный вид общей безопасности личности, общества, государства.

Пожалуй, главным фактором в этом формирующемся феномене является то, что изменилось понимание самой безопасности. Прежние, строившиеся на принципе иерархии угроз системы безопасности, вершиной которых была военная область (и с ней же в основном и ассоциировалось понятие «безопасность»), а другие области занимали подчиненное положение, перестают соответствовать реальным системам угроз. Адекватным разрешением этого противоречия является отказ от традиционной, ориентированной на военный аспект иерархии в системе безопасности и признание невоенных сфер деятельности общества в качестве факторов безопасности наряду с военными сферами, т.е. система безопасности представляется не в виде пирамиды, а в виде сети. При этом в центре (а не на вершине!) любой из таких систем будет связывающая все остальные ее элементы информационная безопасность.

Угрозу безопасности личности, обществу или государству (группе стран) можно в широком смысле определить как то, что в конечном счете существенным образом может ограничить или нанести ущерб имеющемуся уровню самостоятельности (т.е. способности на основе независимо принимаемых решений достигать своих целей, исходя из собственных фундаментальных ценностей и функций) данной личности, общества или государства. При таком определении становится очевидным, что сила, и в частности военная сила, традиционно рассматриваемая как основной инструмент политики безопасности, может быть использована лишь в ограниченном и узко определенном множестве случаев. А тогда критерием значимости разных форм деятельности в различных общественных сферах является их способность обеспечить достижение обществом целей, определяемых его собственной системой ценностей.

Приведенные рассуждения справедливы и в отношении частных видов безопасности, в том числе информационной[4].

Таким образом, сформировались два различных взгляда на проблему обеспечения информационной безопасности: более узкий (традиционный), предусматривающий предотвращение только физического ущерба информационному потенциалу (информационным массивам, системам и сетям) вследствие применения любых вооружений, и более широкий, основанный на сформулированном выше понятии угрозы безопасности и не ставящий во главу угла только защиту от военного или другого разрушающего воздействия. В целом именно к этому сводятся в своей основе расхождения двух основных подходов к проблеме международной информационной безопасности, главными выразителями которых, к сожалению пока в противостоянии друг другу (как ниже будет показано, ничем, кроме как политическими интересами, не обоснованном), вновь являются Россия и Соединенные Штаты Америки.

Сравним подходы аналитиков в России и США к понятиям «информация» и «информационная безопасность»[5] (см. таблицу).

Определения этих двух понятий в любом их изложении до сих пор не являются устоявшимися и общепринятыми. Почему это относится к первому, ясно: к сожалению, до сих пор не удается до конца точно определить это фундаментальное понятие[6]. Столь же ли объективны трудности во втором случае?

Есть у этих понятий и принципиальное отличие. Если первое определяет сам предмет, то второе характеризует его конкретное состояние, причем в определенных внешними

Информация

В России	В США
1. Сообщение, осведомление о положении дел, сведения о чем-либо, передаваемые людьми. 2. Уменьшаемая, снимаемая неопределенность в результате получения сообщений. 3. Сообщение, неразрывно связанное с управлением, сигналы в единстве синтаксических, семантических и прагматических характеристик. 4. Передача, отражение разнообразия в любых объектах и процессах (неживой и живой природы)[7].	1. Факты, данные или сообщения в любых условиях или форме. 2. Значение, которое человек придает данным на основе известных соглашений, используемых при их представлении[8].

Информационная безопасность

В России	В США
Состояние защищенности основных интересов личности, общества и государства в информационном пространстве[9], включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность[10].	Обеспечение защиты информации и информационных систем от неавторизованного доступа или изменения информации при ее хранении, обработке или передаче и противодействие отказу от обслуживания авторизованных пользователей или обеспечению обслуживания неавторизованных пользователей. Информационная безопасность включает необходимые меры определения, документирования и предотвращения таких угроз. Информационная безопасность состоит из компьютерной безопасности и безопасности сетей связи[11].

обстоятельствами условиях потенциального или актуального воздействия на предмет извне. И в этом «основной узел», связывающий абсолютное понятие с вне его находящейся активностью субъекта. Именно эта сторона понятия информационной безопасности дает возможность использовать его в политических целях, в интересах определенных стран и групп.

Анализ рассмотренных фундаментальных понятий способствует адекватному восприятию процесса становления информационной безопасности как самостоятельной проблемы и ее выхода на международный уровень.

В принципе, защита информационного ресурса в ее конкретно-исторических формах – проблема вечная, существующая так же объективно, как и ее контртип – стремление к получению информации, необходимой для оптимизации стратегии деятельности субъекта, общества, государства в соответствующей системе. И в этом смысле заметание лисой своих следов также может рассматриваться как защита информации[12], не говоря уж о мимикрии и защитной окраске у насекомых. То есть защита своей информации (как и стремление к получению чужой) является неотъемлемой функцией субъекта, существующего в динамической, саморазвивающейся системе с разнонаправленными интересами ее участников. Причина в том, что основой коммуникативности субъектов является способность к обмену информацией, которую они используют в своих стратегиях обеспечения жизненных интересов и определения своего положения в этой системе. Следовательно, в общем смысле никоим образом нельзя говорить о проблеме информационной безопасности как о принципиально новой и связывать ее только с развитием информатики и электронных средств передачи и хранения данных[13].

В этом выводе снова проявляется противоречие двух позиций, олицетворяемых российским и американским подходами к проблеме и ее разрешению. В чем разница этих подходов? И столь ли уж они различны?

Подходы к вопросу информационной безопасности нашли отражение в основных концептуальных документах и России, и США. Пересмотрев свои военные приоритеты и национальные интересы в сфере безопасности, обе страны подняли на стратегический уровень задачу защиты информационных ресурсов. Но пути защиты выбраны неодинаковые. Качественно оценить уровень и акцентуацию в подходах стран к этой проблеме можно, в частности, по материалам, представленным ими Генеральному секретарю ООН в соответствии с резолюцией 53/70 Генеральной Ассамблеи ООН.

Позиция России[14] в этих материалах отражается, в частности, в следующих утверждениях: «...Создается реальная угроза использования достижений в информационной сфере в целях, несовместимых с задачами поддержания мировой стабильности и безопасности, соблюдения принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека… В этой связи возникает очевидная потребность в международно-правовом регулировании мировых процессов гражданской и военной информатизации, разработке отвечающей интересам мировой безопасности согласованной международной платформы по проблеме информационной безопасности»[15].

А вот как в тексте доклада Генерального секретаря ООН на 54-й сессии Генеральной Ассамблеи была отражена позиция США[16]: «Соединенные Штаты также полагают, что любое незаконное вмешательство или попытка нарушить или изменить любой аспект их национальных информационных систем представляет собой потенциальную опасность для основных объектов их национальной инфраструктуры, а значит, и угрозу их национальным интересам… Соединенные Штаты полагают, что всем государствам следует принять на национальном уровне меры, необходимые как для охраны их национальных систем, так и для обеспечения того, чтобы преступники или международные террористы, … которые пытаются нарушить функционирование этих систем, карались бы за это по всей строгости закона»[17].

Здесь, как и при сравнении определений понятий «информация» и «информационная безопасность», обращает на себя внимание то, что США рассматривают в качестве объектов информационной угрозы только информационные системы. Если в российском определении информации к данному понятию относится фактически все, что дает представление об объекте, то в американском принимаются во внимание только факты и

семантические значения передаваемых или получаемых (строго говоря – человеком) данных. В соответствии с этим и информационная безопасность в американской трактовке сводится к защите информационных систем, и в первую очередь компьютерных комплексов и сетей связи.

Таким образом, американская трактовка есть, по сути, лишь сужение российской. И в этом смысле американская и российская позиции непротиворечивы; можно сказать, что российская исчерпывающим образом дополняет американскую, та же, в свою очередь, благодаря своей более узко очерченной проблематике обеспечивает глубину проработки вопроса.

На самом деле такой подход американцев имеет под собой сугубо национальную основу – как ментальную (чисто американский прагматизм), так и фактическую (актуальность для США решения задачи защиты «электронной информации»). Соединенные Штаты на сегодняшний день являются общепризнанным лидером в области компьютерной обработки данных. На их долю приходится до 46% мирового парка персональных компьютеров. США являются и наиболее активным пользователем сети Интернет: за 1999 г. с территории США было зафиксировано 100 млн обращений (с территории России только 2 млн)[18]. Передача основной массы информационных сообщений и проведение практически всех финансовых расчетов, включая заметную часть розничных, производятся с использованием компьютерных сетей и сетей связи. Поэтому более чем оправданны беспокойства официальных лиц и аналитиков США именно за эту область своей инфосферы.

Почему актуальна проблема информационной безопасности?

В настоящее время количество существующих средств обработки информации и средств информационного воздействия стало так велико, что явно проявилась необходимость в защите первых от применения вторых. Во многих развитых странах сформировалась фундаментальная зависимость основных сфер жизнедеятельности личности, общества и государства (коммуникации и связи, экономика, политика, наука, культура, обеспечение национальной и международной безопасности и др.) от нормального обмена информацией, надежного функционирования информационных и телекоммуникационных систем, технологий и средств. Во многих странах информация стала в значительной степени определять жизнедеятельность как общества в целом, так и отдельного человека. Отсюда и настораживающая многих перспектива: увеличение военного потенциала, прежде всего высокоразвитых стран, за счет использования в военных целях новейших информационных технологий и средств воздействия на индивидуальное и общественное сознание, т.е. того, что в последнее время принято называть информационным оружием. Это чревато изменением глобального и региональных балансов сил, дополнительной напряженностью между традиционными и нарождающимися центрами силы, появлением новых сфер конфронтации. Признано, что потенциальное разрушительное воздействие уже известных видов информационного оружия на экономику и социум в целом многократно превышает результаты применения традиционных видов оружия массового поражения. А в связи с относительной дешевизной, скрытостью производства и размещения, эффективностью применения как в военное, так и в мирное время, возможностью в большом числе случаев использовать мирные технологии в качестве информационного оружия такой способ увеличения своего военного потенциала для многих стран становится крайне заманчивым[19]. Имеется достаточно сведений о развертывании рядом стран целенаправленных исследований и разработок соответствующих технических средств, технологий и методик их практического применения, которые в совокупности позволили бы осуществлять непосредственный контроль над информационным ресурсом потенциального противника, а в необходимых случаях и прямо вмешиваться в него. Ведется, а в некоторых странах уже завершена разработка комплексных средств информационного противоборства с вероятными противниками и проведения информационных операций как в условиях военных конфликтов различной степени интенсивности, так и в мирное время, причем не только на стратегическом, но и на оперативном и даже тактическом, вплоть до поля боя, уровнях. Большое внимание уделяется вопросам защиты собственного информационного пространства от действия информационного оружия со стороны враждебных государств, несанкционированного воздействия на инфосферу.

Масштабы и объемы финансирования ведущихся в этих направлениях НИОКР (только на программы защиты киберпространства от криминальных и

террористических угроз в 2002 г. предусматривается выделить почти 200 млн долл., на 2003 г. запланировано в полтора раза больше[20]) позволяют утверждать, что разработка средств ведения информационного противоборства становится неотъемлемым элементом государственной военно-технической политики. Способность отдельной страны вести войну в информационном пространстве многими «стратегами» уже рассматривается как дополнительный фактор сдерживания и обеспечения военно-политического паритета, весомость которого сравнима со сдерживающим эффектом ядерного оружия.

Так что же все-таки сулит человечеству информатизация – путь к всеобщему благосостоянию или очередной виток гонки вооружений на новом качественном уровне и новую основу для противостояния? Как и в случаях с другими видами прорывных (в смысле выхода на создание принципиально новых видов оружия) направлений науки и техники, в отношении информационных технологий такое противопоставление некорректно и бессмысленно. В определенной мере будет и то и другое. И надеяться только на возобладание разума над политическим и экономическим интересом здесь так же малоперспективно, как и в области других видов вооружений. Никто не сумел найти внешние рычаги воздействия на Израиль, Индию и Пакистан и заставить их отказаться от стремления к обладанию ядерным оружием. Мировое сообщество имеет лишь один пример добровольного ухода с дороги ядерного вооружения – ЮАР, но и в этом случае были причины внутреннего характера[21], совершенно фиктивные в отношении оружия информационного: его применение во внутриполитических целях может быть и уже является ничуть не менее эффективным, чем в целях воздействия на противника за границами своего государства.

Благодаря своему лидерству в информационной сфере США всегда были озабочены главным образом не столько воздействием, которое оказывают информационные технологии, сколько способом их применения для оказания заданного воздействия. Лишь позднее возник вопрос о влиянии информационных технологий на общество и национальную инфраструктуру применительно к своей стране. И немедленно выяснилось, что и гражданские, и военная сферы становятся предметом террористических и криминальных поползновений.

США оказались едва ли не в первую очередь (если считать абсолютные цифры) подверженными атакам на их локальные компьютерные сети, рабочие станции и серверы, имеющие выход в глобальные сети. Так, Computer Emergency Response Team Coordination Center (CERT/CC), например, сообщает о том, что в 1997 г. было 2 134 инцидентов, в 2000 г. – 21 756 и в первые три квартала 2001 г. – почти 35 000 инцидентов.

Не всегда это были просто хакеры, но последние нанесли существенный урон как отдельным пользователям, так и всему государству. До последних лет, по разным оценкам, до 94% подобных преступлений исходило от внутренних пользователей[22]. По мере развития Интернета и принятия информационных технологий на вооружение политическими и преступными группировками ситуация, естественно, меняется и становится трудно анализируемой, однако, согласно одному из исследований Совета национальной безопасности США, по меньшей мере 13 стран имеют программы ведения информационной войны против США. Кроме того, американцы отмечали кибератаки со стороны китайских, французских, израильских, российских и других хакеров. По заявлению спецслужб США, им удается выявить не более 10% тех, кто предпринимает попытки незаконно проникнуть в правительственные компьютерные системы[23].

Фиксировались нападения на компьютерные сети практических всех государственных учреждений. Только по подсчетам Пентагона, его компьютерные сети «взламываются» примерно 250 тыс. раз в год, при этом не менее 500 раз это серьезные попытки проникновения в секретные системы. По оценке руководителя подразделения информационных операций военно-морских сил США Дж. Ньюмана[24] компьютерные сети ВМС США подвергаются атакам 12 000 раз в год, правда, лишь 0,5% из них достигают успеха. В частном секторе наиболее впечатляющим было известное хищение санкт-петербургским хакером В. Левиным из нью-йоркского «CityBank» 10 млн долл. Только в 1998 г. в США зарегистрировано (т.е. принято к уголовному рассмотрению) свыше 300 преступлений такого рода, но более мелких[25]. В начале февраля 2000 г. в течение трех дней (с 8-го по 10-е) была проведена массированная атака на самые популярные веб-сайты в Интернете (Yahoo!, Amazon.com, CNN и др.). Кроме неудобств, созданных частным пользователям[26], эта акция нанесла

заметный ущерб финансовым рынкам США и способствовала резкому падению котировок акций. В результате индекс Доу Джонса рухнул почти на 260 пунктов (около 2,4%), композитный индекс электронной биржи НАСДАК не только перестал расти, но и упал более чем на 64 пункта (около 1,5%). Нападающие предприняли самый простой ход, «завалив» серверы ложными запросами. Но даже в этих условиях ФБР, перед которым президент США (!) поставил задачу разобраться, вынуждено было признаться в своей беспомощности, заявив лишь о том, что атаки проводились в разное время из разных мест, в том числе из-за рубежа[27].

Близкой по форме к военной была атака на целый ряд серверов государственных учреждений США, осуществленная китайскими хакерами в период разрешения конфликта в связи с захватом американского самолета в КНР и гибелью китайского летчика. Начатая как по команде и так же организованно оконченная хакерская атака привела к блокировке большого числа систем; это показало, что в информационной войне, в том числе в противоборстве с США, КНР уже представляет существенную силу.

Конечно, информационным нападениям подвергаются не только американские информационные системы. На территории Западной Европы ежегодно фиксируется до 300 проникновений хакеров в военные, государственные и коммерческие сети. Известны нападения на информационные сети Китая, Тайваня, Индии, Индонезии. Идет прямое информационное противоборство Пекина и Тайбэя[28], противостояние хакерских групп Армении и Азербайджана[29]. Весной 2002 г. антиглобалистами были сдублированы сайты Всемирной торговой организации[30].

Не обошла чаша сия и Россию. Один из наиболее известных примеров: 12 февраля 2000 г. произошло, пусть не столь масштабное, но качественно весьма значительное проникновение в один из самых крупных российских серверов «Росбизнесконсалтинг». Взломав защиту, хакер от имени чеченских националистов поместил доступное всем клиентам обращение, содержащее призывы к физическому устранению Владимира Путина как основного виновника произошедших на Северном Кавказе событий. Еще долго головной болью российских спецслужб будет сайт «Кавказ», руководимый и наполняемый с территории США, что исключает применение каких либо мер воздействия к его организаторам, действия которых иначе как террористические и подрывные квалифицировать трудно.

Такая ситуация вызывает беспокойство. И все страны предпринимают определенные шаги как в правовой, так и в технической сфере. В национальные уголовные законодательства внесены статьи, предусматривающие значительную ответственность за компьютерные преступления; в ряде международных организаций начаты исследования, направленные на борьбу с компьютерной преступностью. К работе по противодействию актам информационной агрессии привлечены десятки государственных ведомств. Директор ЦРУ Джордж Тенет прямо заявил, что борьба с компьютерными взломщиками является первостепенной задачей правоохранительных органов США[31].

Опираясь на свои интересы и уже инициированную работу, Соединенные Штаты, вероятно, имели даже некоторое моральное право не поддерживать российские международные инициативы 1998–1999 гг. Не претерпела изменения их позиция и в 2000 г. Вынеся на 55-ю сессию ГА ООН собственный проект резолюции по борьбе с кибертерроризмом, США подтвердили, что они придают превалирующее значение борьбе с информационной преступностью[32].

Однако можно с той же уверенностью констатировать, что, несмотря на достаточно жесткую официальную позицию Вашингтона, фактические подходы США и России к проблеме все более сближаются, и именно на основе российской позиции. И объясняется это в первую очередь ситуацией в самих Соединенных Штатах.

Так, например, в период завершения 54-й сессии ГА ООН (декабрь 1999 г.[33]) в течение всего 10 дней в США проходили три представительные научные встречи, которые заслуживают самого пристального внимания. Это конференция «Международное сотрудничество в борьбе с компьютерной преступностью и терроризмом», научный семинар «Интернет и международные системы: информационная технология и американская политика принятия решений в международной сфере» и круглый стол «Информационная война и кибертерроризм: заслон кибернетическим угрозам в новом тысячелетии»[34]. Если конференция

задумывалась как международная (что, правда, не совсем получилось – участвовало всего два неамериканца из Израиля и Норвегии), то остальные встречи были чисто национальными. Они показали, что американские ученые далеко не солидарны с дипломатами и военными. В частности, на примере косовского конфликта на семинаре с очевидностью было продемонстрировано, что существует не теоретическая возможность, а самое практическое наличие и эффективность информационного оружия. На заседании круглого стола прозвучала еще более близкая российскому пониманию проблемы сентенция: в отношении кибертерроризма было прямо указано на политическую мотивацию как обязательную характеристику этого вида преступления. Осталось лишь признать, что такие действия могут производиться в интересах не только отдельных личностей или политических групп, как это было, например, в ходе индонезийского кризиса в октябре 1999 г.[35], но и в интересах государств или групп государств, – и это было бы изложением российской позиции. Но пока этого не прозвучало. Впрочем, термин «информационное оружие» здесь уже воспринимался как определяющий все виды и способы воздействия на инфосферу, т.е. практически так же, как и в российской трактовке.

Тщательного изучения требуют материалы упомянутой конференции. Итоговый документ представительнейшего национального форума (конференция проводилась в рамках ежегодного Национального форума безопасности), в работе которого участвовал, в частности, Уильям Перри, в случае, если бы он стал государственным, полностью изменил бы взгляд на позицию Соединенных Штатов по вопросу международной информационной безопасности.

Уже в первых строках этого документа записано: «Транснациональный характер мировых информационных систем и их использования влечет за собой повышение значимости международных соглашений, направленных на защиту от известных методов воздействия». Далее следуют предложения, касающиеся действий, которые могли бы быть предприняты на международной арене. Предлагается целый ряд достойных поддержки мероприятий: от «выработки единой системы определений действий, подлежащих запрету» до «сотрудничества по выработке технических мер с целью минимизации вмешательства в частную сферу»[36]. Если под «действиями, подлежащими запрету» понимать и неспровоцированную агрессию против государства (а именно так это отметила в 1985 г. Генеральная Ассамблея ООН, осудив своей специальной резолюцией агрессию против Никарагуа) и допустить, что преступные действия могут исходить не только от частных лиц, но и от государства или группы стран (заметим, что государственный терроризм, т.е. преступление, совершаемое государством, вполне допускается американской политической теорией и практикой), то под такими предложениями мог бы подписаться любой оппонент американской позиции. Интересно и, хочется верить, символично то, что такой документ принят на конференции в Стэнфордском университете, когда ректором и куратором этой проблематики там была Кондолиза Райс, нынешний помощник президента США по национальной безопасности.

Всего за три месяца до этого, в августе 1999 г. в Монтерее (США, штат Калифорния) в Центре по исследованию терроризма и нетрадиционных войн (Center for the Study of Terrorism and Irregular Warfare) Морской высшей школы (Naval Postgraduate School – NPS) опубликован отчет, названный «Cyberterror: Prospects and Implications». Позже, анализируя этот документ, известный американский профессор, специалист по информационной безопасности Дороти Деннинг пишет: «Информационное пространство стало больше, чем пространство для электронной коммерции и связи. Оно стало цифровым полем боя»[37].

Интересно, что проходившие в 2000 и 2001 гг. в США научные дискуссии, хотя и во многом откликнулись на официальный «призыв» и в существенно большей степени уделили внимание преступности в информационной сфере, не ушли от сформулированных оценок общей угрозы информационных войн и констатировали все новые ее проявления. В октябре 2000 г. та же NPS публикует по материалам проведенной конференции второй доклад с подробным исследованием вопросов международного противодействия организованному кибертерроризму различных национальных и международных организаций. Четкие оценки необходимости международных соглашений и примерные их схемы прозвучали на проходившей в июне 2001 г. в Берлине конференции «Ограничение вооружений в информационном пространстве» (Arms Control in Cyberspace)[38].

К этому времени уже многие американские исследователи признают, что информационное пространство надо рассматривать как возможное поле боя, на деятельность в нем надо распространить положения международного права, а также что законность в действиях в киберпространстве является основой международного мира и безопасности[39].

Компромисс вполне возможен

Таким образом, справедливо предположить, что позиции аналитиков сходятся и в пределе своем близки к российской. И причина, видимо, не в прозорливости российских аналитиков, как научных, так и государственных. Некоторое отставание России в сфере информатизации от западных стран, и в первую очередь США, позволили использовать накопленный там опыт и увидеть тенденции, признание которых американцами на официальном уровне требовало отказа от некоторых уже прозвучавших и юридически оформленных установок.

Тем самым не лишены основания следующие выводы.

1. В российских и американских подходах к проблеме нет принципиального отличия, исключающего возможность найти общие точки и устранить имеющиеся расхождения.
2. Позиции сторон сводятся к признанию актуальности создания международного механизма предотвращения информационных войн и борьбы с информационной преступностью, включая терроризм.

Несмотря на то что количество нерешенных вопросов велико, лишь часть из них требует дальнейшего обсуждения, в том числе в конференционном формате. С другой стороны, без диалога наших стран говорить об укреплении безопасности в мире не приходится. Опыт обсуждения проблем оружия массового уничтожения и других неконвенциальных видов вооружений только подчеркивает необходимость побороть «робость» в этом вопросе. Если в будущем одна из жизненно важных систем страны будет подвергнута «удачной» кибератаке и будет подозрение (хотя в действительности и ложное), что это сделало государство-оппонент, то запустят ли США или Россия свои ядерные ракеты, по сути, лишь потому, что они не общались или недостаточно общались друг с другом по этой проблеме? Отказ от совместной работы по контролю за немирным использованием информационных средств и технологий будет только поощрять непонимание и страх.

Естественным развитием двусторонних контактов были бы международно-правовое оформление общих пунктов позиций всех заинтересованных стран, выработка международных документов и гармонизация национальных правовых систем. И здесь опыт работы США в области национального законодательства был бы не только важен, но и крайне ценен. Однако пока никаких подвижек в этом направлении нет[40]. Определенным исключением можно считать работу по противодействию кибертерроризму и киберпреступности, активизированную особенно в рамках «G-8» после 11 сентября 2001 г.

В ряде разделов международного права существуют нормы, которые можно было бы отнести к отдельным элементам или обстоятельствам конкретных «информационных операций», однако до настоящего времени не существует единого четкого понимания, *что* есть «военные действия» в инфосфере.

Создание системы международного регулирования деятельности в инфосфере представляется достаточно сложной задачей, так как существует множество систем и структур, которые потенциально могут стать объектами атак, разнообразны способы нападения, огромно количество потенциальных агрессоров и, кроме того, происходит быстрое совершенствование как потенциальных объектов агрессии, так и информационного оружия и технологий его применения. До сих пор не найден даже общий подход к определениям и понятийному аппарату. Еще не выработаны фундаментальные внешнеполитические решения, определяющие долговременные интересы стран в связи с возможным принятием на вооружение или, напротив, отказом от применения средств информационной войны. С одной стороны, имеется очевидная заинтересованность военных в получении возможностей проникновения в информационные системы противника и воздействия на них при наличии надежной защиты собственных сетей. Информационное оружие привлекает их целым рядом уникальных преимуществ перед другими вооружениями: оно минимизирует потери в живой силе, не наносит ущерба технике, зданиям и сооружениям, не требует

передислокации воинских контингентов и т.д. С другой стороны, государство, располагающее разветвленной информационной инфраструктурой (а любое государство в будущем видит себя именно таким), уязвимо по отношению к компьютерным атакам, демократическое – к психологическому воздействию на население, авторитарное – к воздействию на представителей правящей элиты, и все это также окажет влияние на позицию политического руководства при разработке норм международного права в этой области.

Появление отдельного международного правового акта, направленного на существенное ограничение или запрещение информационного оружия, в ближайшем будущем маловероятно. Однако никто и не отклоняет идею начала работы по подготовке такого документа. Напротив, 56-я сессия ГА ООН по инициативе России приняла решение о создании специальной группы правительственных экспертов для анализа проблемы и выработки рекомендаций с целью формирования практических шагов в обеспечении системы международной информационной безопасности. Уже не в качестве отдельных специалистов, а в качестве облеченных полномочиями представителей направивших их стран они смогли бы подготовить квалифицированные предложения и предложить их Генеральному секретарю и Генеральной Ассамблее ООН.

В связи с недостаточной изученностью и динамичностью проблемы ее рассмотрение должно вестись как в научном, так и в дипломатическом формате. В свете высказанных выше тенденций к сходимости процессов выработки национальных позиций уже в ближайшие годы могут быть определены общие подходы к ее решению. На их основе, но только под эгидой ООН возможно вслед за тем выработать международные документы (первоначально, вероятно, в форме декларации или концепции), официально от имени мирового сообщества формулирующие и международноправовым образом закрепляющие принципы международной информационной безопасности. При этом, естественно, следует исходить из необходимости рассмотрения и принятия международным сообществом таких принципов в комплексе, т.е. с учетом угроз как военного, так и криминального (в том числе и террористического) характера применительно и к военным, и к гражданским сферам.

На подготовительных этапах[41] на этом пути могли бы быть разработаны системы понятий, используемых при анализе и обсуждении проблемы; основы построения глобальной системы обеспечения международной информационной безопасности; соглашения по частным вопросам, включая противодействие международному информационному терроризму и преступности; основные принципы, подлежащие учету в национальных законодательствах с целью гармонизации последних. Тогда же могут быть согласованы основы организации механизма обеспечения безопасности международного информационного пространства и его взаимодействия с международными системами, функционирующими в сфере информатизации, телекоммуникации, средств массовой информации и прав человека, а также экспортного контроля[42].

Завершающим этапом должно стать подписание всеми членами международного сообщества многостороннего договора (или конвенции), окончательно закрепляющего принципы обеспечения международной информационной безопасности и вводящего в действие механизм контроля безопасности международного информационного пространства.

Абсолютно очевидно, что полезные и реализуемые результаты на этом пути могут быть получены только на основе самого широкого международного сотрудничества. И трудно переоценить роль, которую в этом процессе могут сыграть США и Россия. Их единство на пути предотвращения гонки информационных вооружений и развязывания информационных войн может решить новые сложные проблемы, порожденные вхождением человечества в информационную эру, и обеспечить реальную международную информационную безопасность. Только такая однополюсность может дать позитивные гарантии миру.

---

[1] 53, 54, 55 и 56-я сессии Генеральной Ассамблеи ООН (1998–2001 гг.) на основании консенсуса приняли резолюции 53/70, 54/49, 55/28 и 56/19 под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», которые посвящены вопросу создания в перспективе международного механизма предотвращения гонки информационного оружия и информационных войн.

[2] В англоязычной литературе на эту тему широкое распространение получил термин «information age». Этот эпитет не представляется излишне патетическим и может быть использован и в русском переводе.

[3] Впервые вопрос был поднят в выступлении российской делегации в мае 1996 г. на Международной конференции по глобальному информационному сообществу в Мидранде (ЮАР). Спонтанно поднятый вопрос о назревающем «новом вызове» повлек неожиданно бурную реакцию. Проблема оказалась не только интересной для большинства участников, но, как выяснилось, практически созревшей для обсуждения. Для российских экспертов, занимавшихся в то время этой проблемой, стало ясно – ее надо выносить на переговорный уровень. (Подробнее см. Крутских А.В. Информационный вызов накануне 21 века. *Международная жизнь*. 1999. № 2.)

[4] Отсюда же с очевидностью следует и определение понятия «информационное оружие» как средства реализации угрозы (т.е. нарушения) информационной безопасности. Ниже мы еще обратимся к этому моменту. Следует заметить, что разница в определении информационной безопасности обязательно влечет разницу в средствах ее нарушения. То есть, что важно, более фундаментальным становится не понятие информационного оружия – как средства воздействия на информацию, а понятие информационной безопасности – как стационарного состояния информации, ее ненарушенности.

[5] Поскольку США, в отличие от России, не выносили официально на международный уровень свои системы определений в данной области, то здесь и далее их определения даются по доступным автору открытым внутренним национальным источникам.

[6] Выше дано определение по словарю 1983 г. В более поздних советских и российских изданиях, в том числе и в самой свежей четырехтомной «Новой философской энциклопедии» (М.: Мысль, 2001), это понятие как самостоятельное либо вообще отсутствует, либо никак не определяется.

[7] Философский энциклопедический словарь. М., 1983.

[8] U.S. DOD. Dictionary of Military Terms.

[9] Информационное пространство (инфосфера) – сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, информационно-телекоммуникационную инфраструктуру и собственно информацию.

[10] Пятьдесят четвертая сессия Генеральной Ассамблеи Организации Объединенных Наций. Доклад Генерального секретаря «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Нью-Йорк, 1999. A/54/213. (Текст на русском языке.) С. 17.

[11] U.S. DOD. Dictionary of Military Terms.

[12] Если Н. Винер считал оправданным моделирование нейрона водопроводным краном, то и наше сравнение имеет право на существование.

[13] См. Расторгуев С.П. Философия информационной войны. М.: «Вузовская книга», 2001.

[14] Эта позиция нашла свое подтверждение в новой редакции Концепции национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 10 января 2000 г. № 24), отмечающей, что «серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, … разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним». В соответствии с этим в ряду важнейших задач обеспечения информационной безопасности Российской Федерации стоит «противодействие угрозе развязывания противоборства в информационной сфере».

[15] Пятьдесят четвертая сессия Генеральной Ассамблеи Организации Объединенных Наций. Доклад Генерального секретаря «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Нью-Йорк, 1999. A/54/213. (Текст на русском языке.) С. 15.

[16] Там же. С. 23.

[17] Примечательно, что это было написано менее чем через год после утверждения председателем Комитета начальников штабов США и придания гласности документа, носящего название «Объединенная доктрина информационных операций» (Joint Doctrine for Information Operations. Joint Pub 3-13, Joint Chiefs of Staff, 1998), в котором в практическом плане «рассматриваются вопросы интеграции и синхронизации наступательных и оборонительных информационных операций … в поддержку военных действий на стратегическом, оперативном и тактическом уровнях». Документ сам по себе очень интересен, но для получения представления об уровне проработки вопросов ведения информационной войны и проведения информационных операций в вооруженных силах США рекомендуем сразу обратиться к приложению D (Appendix D), содержащему ссылки на ранее выпущенные документы.

[18] Данные приводятся по: Модестов С.А. Незримая война обостряется. *Независимое военное обозрение*. 2000. № 3 (176).

[19] По некоторым данным, в той или иной степени разработки таких средств ведутся в 120 странах. Для сравнения: разработки в области ядерного оружия ведутся не более чем в 20 государствах.

[20] Приводится по: Homeland Security Handbook, 2001.

[21] Перспектива попадания ядерного оружия в руки правительства черного большинства была малоприятной как для правительства Де Клерка, так и для его союзников. Однако далеко не все верят, что заверения ЮАР в уничтожении всей документации и переориентации всех специалистов полностью соответствуют действительности. Не до конца ясны и реальные возможности и результаты, достигнутые ЮАР к моменту падения режима апартеида, не до конца ясен даже вопрос, проводили ли они ядерные испытания.

[22] Черешкин Д.С. и др. Защита информационных ресурсов в условиях развития мировых открытых сетей. М.: ИСА РАН. 1997. С. 33.

[23] *Newsweek*. 2000. February 14.

[24] Интервью радиостанции *Немецкая волна*, 19 июля 1999.

[25] *Computer Weekly*. 1999. April 15. P. 30.

[26] О том, сколько таковых, можно судить по тому, что, по данным *ИТАР-ТАСС* (10 февраля 2000 г.), только за декабрь 1999 г. к системе «Yahoo» обратились 36 миллионов пользователей.

[27] Данные приведены по материалам *ИТАР-ТАСС* за 10-14 февраля 2000 г.

[28] Модестов С.А. Незримая война обостряется. *Независимое военное обозрение*. 2000. № 3 (176).

[29] *ИТАР-ТАСС*. 2000. 14 февраля.

[30] *Euronews*. 2002. March 12.

[31] *Newsweek*. 2000. February 14.

[32] Однако факт того, что для проведения второй волны супертеррористических атак осенью 2001 г. (распространение вируса сибирской язвы) террористы избрали почтовые отправления, т.е. неэлектронный информационный канал связи, вероятно, должен внести изменения в позицию США по данному вопросу.

[33] Умышленно берем интервал, далекий от 11 сентября 2001 г., т.е. период «спокойной», « стационарной» жизни.

[34] Отметим, что в отличие от рассмотрения этой проблемы на дипломатическом уровне, которое началось с 1996 г., примерно с начала 1990-х гг. вопрос «информационного

оружия» и «информационных войн» довольно широко обсуждался специалистами; появилось большое число публикаций; на многих конференциях, семинарах, симпозиумах в том или ином виде поднимались вопросы «немирного» использования программно-технических разработок и путей защиты информационного ресурса от их воздействия.

[35] Сразу после референдума о независимости этой провинции Индонезии общественная организация «East Tymor Campaning» провела с территорий Испании, Португалии и Франции атаку на государственные интернетовские сайты Индонезии. Поражены веб-страницы, принадлежащие правительственным организациям Индонезии, созданы и внедрены новые компьютерные вирусы, специально предназначенные для поражения индонезийских информационных объектов. Эти информационные операции, проведенные, отметим, с территории Европы (вот пример «трансграничности» информационного оружия), явились примером прямого применения информационного оружия для решения конкретных внутриполитических задач.

[36] International Cooperation to Combat Cyber Crime and Terrorism. Conference Overview. Stenford University, 1999. P. 1-2.

[37] Denning Dorothy E. Cyberwarriors Activists and Terrorists Turn to Cyberspace. Harvard International Review. 2001. Vol. XXIII, No. 2, Summer. P. 70-75.

[38] Проведена фондом Heinrich Böll Foundation. Berlin, Germany, June 29-30, 2001.

[39] См., в частности, Walter Gary Sharp, Sr. Cyberspace and the Use of Force. Aegis Research Corporation, 2000. P. 135-140.

[40] В мае 1999 г. юристами Пентагона подготовлен и после этого дважды после доработок переиздан обзор «An Assessment of International Legal Issues in Information Operations», содержащий комплексную оценку применимости и достаточности имеющейся в распоряжении мирового сообщества законодательной базы в отношении информационной войны. Эксперты не видят необходимости для США в организации работы по внесению новых договорных обязательств применительно к условиям информационной войны в различные разделы уже действующего на мировой арене законодательства. Исключением, по их мнению, является область международного уголовного права, в которой усилия американцев по улучшению взаимной юридической помощи и заключению соглашений о выдаче преступников должны получить дальнейшее развитие.

[41] Подробнее см. Крутских А.В., Федоров А.В. О международной информационной безопасности. *Международная жизнь*. 2000. № 2.

[42] Имеется в виду взаимодействие в части контроля за экспортом товаров и услуг в сфере информатизации и телекоммуникаций, которые могут иметь военное или двойное применение, а также средств и продуктов для производства психотронного оружия.

См. также с. 7, 48