Смирнов Анатолий Иванович, Президент АНО «Национальный институт исследований глобальной безопасности», д-р исторических наук, профессор, Чрезвычайный и Полномочный Посланник РФ в отставке
www.niiglob.ru т. +7 985 77 65 999

Геополитические вызовы информационной безопасности

Планета охвачена беспрецедентной информационной революцией. По оценке многих экспертов она стала не только локомотивом глобализации, но и её нервом, поскольку, наряду с несомненным позитивом, породила ряд принципиально новых геополитических вызовов и угроз.

Planet covered by an unprecedented information revolution. According to many experts, it was not the only driving force of globalization, but also its nerve, because, together with undoubted positive, has generated a number of fundamentally new geopolitical challenges and threats.

Феномен информационной революции выдвинул в иерархии внешнеполитических приоритетов мирового сообщества на одно из ведущих направлений пресечение использования информационно-коммуникационных технологий (ИКТ) в военно-политических, террористических и криминальных целях, а также для вмешательства во внутренние дела суверенных государств.

Обуздать информационное оружие

Именно по этой причине в сентябре 1998 г. в адрес Генерального секретаря ООН было направлено специальное послание[1] Министра иностранных дел России И.С.Иванова. Особый акцент в нем был сделан на необходимости предотвращения появления принципиально новой сферы конфронтации и развязывания военных конфликтов. Практическим развитием этой российской инициативы стало внесение в ходе 53-й сессии Генассамблеи ООН разработанного МИД проекта резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», консенсусом принятый 4 декабря 1998 (A/RES/53/70)[2].

---

[1] А.И.Смирнов. Информационная глобализация и Россия: вызовы и возможности. М.: Парад. 2005. С. 267
[2] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement

С тех пор проблематика международной информационной безопасности (МИБ) в разных её аспектах ежегодно обсуждалась в ООН. В последний раз аналогичная резолюция была принята 13 декабря 2011 года (A/RES/66/24).

Озабоченность России и мирового сообщества данной проблемой отнюдь не случайна. Наряду с сотнями тысяч разновидностей вирусов, шпионских программ, негативным контентом[3] и, казалось бы, безобидным спамом по данным ЦРУ более 120 стран мира разрабатывают принципиально новый вид оружия массового поражения – информационное.[4]

Заметными вехами в решении столь важной для судеб мира проблемы стали итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), состоявшейся 10-12 декабря 2003 года в Женеве и 16-18 ноября 2005 года в Тунисе под эгидой ООН.

Императив: глобальная культура кибербезопасности

С учетом бурного развития ИКТ, веб-сервисов, в том числе глобальных социальных сетей, Генассамблея ООН 17 марта 2010 г. приняла резолюцию «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур».

Признавая растущий вклад ИКТ во все сферы социума (даже появилась наука – инетология) ООН призвала правительства, деловые круги, организации и индивидуальных владельцев и пользователей ИКТ к ответственности за обеспечение безопасности и принятие надлежащих мер для ее укрепления.

Особое место в резолюции уделено важности мандата Форума по вопросам управления Интернетом.

В резолюции также отмечено, что угрозы надежному функционированию важнейших инфраструктур ИКТ и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер,

---

[3] За 2011 г. закрыто 10 тыс. ресурсов, содержащих противонравственный по отношению к детям контент, 150 сайтов с элементами наркопропаганды - http://www.gazeta.ru/business/2012/02/09/3994965.shtml?incut2

[4] Глобальная безопасность: инновационные методы анализа конфликтов. Под общей редакцией А.И.Смирнова. М. Знание. 2011.С.183

отрицательно сказываясь на уровне семейного, национального и международного благополучия.

В этом контексте подготовленный Международным союзом электросвязи в 2009 г. доклад об обеспечении защищенности ИКТ и передовой практике в области формирования культуры кибербезопасности основное внимание уделяет всеобъемлющему национальному подходу к кибербезопасности, не нарушающему свободы слова, свободы передачи информации и надлежащих правовых процедур.

В резолюции ООН предложено государствам-членам использовать инструмент добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур, призванный помочь им выявить области, в которых требуется принятие дополнительных мер. Кроме того, рекомендовано государствам-членам и соответствующим региональным и международным организациям, разработавшим стратегии действий в области кибербезопасности и защиты важнейших информационных инфраструктур, поделиться сведениями о передовой практике и мерах, которые могли бы помочь другим странам по обеспечению кибербезопасности.

Позиция России

Как уже отмечалось выше, Россия инициативно и ответственно относится к данной проблематике. Наряду с активным участием в подготовке и подписании Окинавской Хартии «Глобальное информационное общество» (2000 г.), документов ВВУИО (Женева, Тунис), форумов по вопросам управления Интернетом и др., в России действуют Доктрина информационной безопасности (2000 г.), Стратегия развития информационного общества (2008 г.), госпрограмма «Информационное общество (2011-2020 гг.)», а также ряд профильных федеральных законов.

Одним из важных документов последнего времени (май 2009 г.) стала Стратегия национальной безопасности Российской Федерации до 2020 года. Ее пункт 109 гласит, что «угрозы информационной безопасности в ходе

реализации настоящей Стратегии предотвращаются за счет совершенствования безопасности функционирования ИКТ систем критически важных объектов инфраструктуры и объектов повышенной опасности в России, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности».[5]

В этом контексте в России уточнены роль и обязанности заинтересованных сторон, стратегические процессы и участие, сотрудничество между государственным и частным секторами, деятельность в связи с инцидентами и восстановление после сбоев, а также правовые нормы и формирование глобальной культуры кибербезопасности.

Заметный вклад в столь важный процесс вносят, наряду с государственными и иными организациями, институты гражданского общества.

В России разработано необходимое законодательство для расследования киберпреступлений и преследования лиц, виновных в их совершении, с учетом существующих механизмов, в т.ч. резолюций 55/63 и 56/121 Генассамблеи о борьбе с преступным использованием ИКТ.

Что касается Конвенции Совета Европы о киберпреступности (вступила в силу 1 июля 2004 г.), то у российской стороны имеется особое отношение к ней. Данная конвенция устанавливает правовые рамки лишь для борьбы с «традиционными» преступлениями (отмывание денег, мошенничество, вымогательство), совершаемыми с использованием компьютерных систем. К сожалению, в конвенции отсутствует понятие «кибертерроризм».

Россия не присоединилась к конвенции, т.к. имеются серьезные озабоченности и по ее пункту «в» статьи 32, который в нынешней редакции фактически позволяет несанкционированный доступ одного государства к компьютерным данным другого государства. Российский взгляд разделяют

---

[5] http://www.scrf.gov.ru/documents/99.html

многие государства, в т.ч. в формате СНГ, ШОС, ОДКБ и других международных и региональных организаций.

Что предлагает Россия и её партнеры?

В силу вышеизложенного Китай, Россия, Таджикистан и Узбекистан совместно выработали в виде возможной резолюции Генассамблеи «Правила поведения в области обеспечения международной информационной безопасности» (далее - Правила) и направили 12 сентября 2011 г. письмо в адрес Генерального секретаря ООН[6]. Наряду с общепринятыми в международном праве и в вышеуказанных резолюциях положениями (а также с учетом лимита объема для статьи), особого внимания заслуживают следующее:

- не использовать ИКТ, включая сети, для осуществления враждебных действий, актов агрессии, создания угроз международному миру и безопасности или распространения информационного оружия или соответствующих технологий;
- сотрудничать в борьбе с преступной или террористической деятельностью с использованием ИКТ, включая сети, и сдерживать распространение информации террористического, экстремистского и сепаратистского характера, а также подрывающей политическую, экономическую и социальную стабильность государств, их культурный и духовный уклад;
- подтверждать права и обязанности каждого государства, в соответствии с надлежащими нормами и правилами, в отношении законной защиты своего информационного пространства и критической информационной инфраструктуры от ущерба в результате угроз, вмешательства, атак и актов агрессии;

[6] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement

- уважать права и свободы в информационном пространстве, в том числе на поиск, получение, передачу и распространение информации в соответствии с национальным законодательством каждого государства;
- содействовать созданию многосторонних, прозрачных и демократических международных механизмов управления Интернетом, которые позволят обеспечить справедливое распределение ресурсов, способствовать доступу для всех, а также гарантировать стабильное и безопасное функционирование Интернета.

Наряду с Правилами - «мягким» вариантом - Россия совместно со своими партнерами подготовила концепцию «юридически обязывающей» Конвенции обеспечения международной информационной безопасности для обсуждения в ООН. Концепция была представлена на закрытой встрече 21-22 сентября 2011 г. в Екатеринбурге руководителей спецслужб и силовых ведомств 52 стран, организованной Совбезом России[7].

В развитие данной встречи были продолжены консультации с экспертами из Китая и Индии, состоялись переговоры в Брюсселе, Лондоне, Берлине. Выяснилось, что Великобритания и США выступают с критикой документа, якобы распространяющего цензуру и закрепляющего безусловное право стран регулировать национальные сегменты интернета по своему усмотрению. Кроме того, основные пункты концепции противоречат политике США, в частности, кибердоктрине Белого дома, которая позволяет Пентагону активно реагировать на кибератаки из-за рубежа.[8]

Объективности ради следует отметить, что существующие в концепции формулировки могут предполагать достаточно широкую трактовку. Так, среди угроз перечислены «эрозия культурных ценностей», экспансия другого государства и распространение информации, «разжигающей межнациональную, межрасовую и межконфессиональную вражду» и т.д.[9]

---

[7] http://www.scrf.gov.ru/news/19/674.html
[8] См. http://www.gazeta.ru/business/2012/02/09/3994965.shtml
[9] http://m.gazeta.ru/business/2012/02/09/3994965.shtml

Многие из данных проблем стали темой дискуссий на Шестом международном форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму» (23–26 апреля 2012 г., Гармиш-Партенкирхен (Германия), в работе которого приняли участие ведущие эксперты из 17 стран.

Они впервые публично оценили предложенный РФ проект конвенции ООН «Об обеспечении информационной безопасности». Спецкоординатор МИД РФ по вопросам политического использования ИКТ (в ранге посла по особым поручениям) А.В.Крутских сообщил, что уже около 120 стран «активно экспериментируют в области ведения информационных или кибервойн». Обсуждение этого документа будет продолжено на следующей подобной встрече в июне в Санкт-Петербурге. В августе же его обсудят в Нью-Йорке - на сессии группы правительственных экспертов ООН по информационной безопасности.

Посол также посетовал, что, «по некоторым данным, ряд стран намерен заболтать российское предложение». Сравнив угрозу кибервойны с гигантским астероидом, мчащимся к Земле, он предупредил: «У человечества нет времени на болтовню». Впрочем, от дипломатов, силовиков и экспертов из 17 стран, прибывших в Баварию, конкретных действий не ждали - организаторы рассматривали форум как репетицию перед Санкт-Петербургом и Нью-Йорком. Участников попросили лишь оценить российский проект конвенции и представить свои идеи. Официальных лиц из США на форуме не было, а ряд участников из стран-союзников Вашингтона признавались «Ъ»[10], что американцы и им советовали не ехать в Баварию, дабы не «легитимировать» российскую инициативу. Эксперты считают, что, до тех пор, пока России нечего противопоставить в этой области, США не согласятся ни на какие ограничительные меры. Вице-премьер Дмитрий Рогозин в марте объявил, что

[10] http://www.kommersant.ru/pda/kommersant.html?id=1924818

скоро у РФ появится свое киберкомандование. Однако, по данным «Ъ», конкретных шагов в этом направлении пока не предпринято».

Резюмируя, следует отметить, что «твиттер-революции» в арабском мире (и не только!), т.е. мягкая сила 2.0, возросшая угроза использования информационного оружия, «цифрового джихада», активизация киберпреступности, реальное применение вируса Stuxnet не только для кибершпионажа, но и диверсий в Иране[11], - всё это императивно диктует необходимость обеспечения международной информационной безопасности.

[11] http://housea.ru/index.php/pulse/16012 Официальное письмо SIEMENS о вирусе STUXNET с комментариями