Выступление депутата Государственной Думы Российской Федерации, члена Комитета по безопасности и противодействия коррупции, члена российской делегации в Парламентской ассамблее ОБСЕ Ильи Костунова

30 сентября 2016 г., Скопье

Уважаемые коллеги,

Позвольте обратить ваше внимание на тему мер доверия в области международной информационной безопасности.

Понятие «меры укрепления доверия» введено в политико-дипломатический лексикон Заключительным актом СБСЕ 1975 г., частью которого является Документ по мерам укрепления доверия и некоторым аспектам безопасности и разоружения. Его положения получили развитие в Документе Стокгольмской конференции по мерам укрепления доверия и безопасности и разоружению в Европе (1986 г.) и Венских документах 1990, 1992, 1994, 1999 и 2011 годов.

В большой степени эти меры появились как ответ на неприемлемый уровень угрозы взаимного ядерного уничтожения.

Одной из подобных мер стало создание национальных центров по уменьшению ядерной опасности в 1987 г. в СССР и США. Были внедрены и другие меры доверия, показавшие свою эффективность не только в вопросах ядерной безопасности, но и в контроле за обычными вооружениями. Например, Договор по открытому небу, прямые линии связи между военно-политическим руководством, советы, рабочие группы... межпарламентские конференции, такие как наши, тоже являются эффективными мерами доверия.

Сегодня же резко возросла зависимость от информационно-коммуникационных технологий (ИКТ) традиционных сфер жизнедеятельности государства и общества. Данные технологии стали рассматриваться не только как инструмент развития, но и как средство военно-политического противоборства.

Следует отметить, что ИКТ сами по себе не являются оружием. В ряде международно-правовых документов, в частности докладе Группы правительственных экспертов ООН по МИБ 2013 г., отмечается, что ИКТ являются технологиями двойного назначения, т.е. могут быть потенциально использованы в военных целях.

Во-первых, их низкая стоимость по сравнению с ядерными и обычными вооружениями. Эксперты в области защиты информации сходятся во мнении, что именно сочетание низкой цены и высокой эффективности обуславливает привлекательность применения ИКТ в военных конфликтах в будущем.

Так, по некоторым оценкам, организация компьютерной атаки типа «отказ в обслуживании» (так называемая DDoS-атака, англ. Distributed Denial of Service) стоит в среднем около 4 центов США на один компьютер, что позволяет провести целую кампанию, затраты на организацию которой будут сопоставимы с закупкой одной танковой гусеницы.

Анонимность и возможность использования посредников являются вторым преимуществом ИКТ как потенциального средства противоборств.

Наконец, некоторые виды компьютерных атак, например, упомянутый выше «отказ в обслуживании», имеют масштабируемый в зависимости от намерений заказчика атаки эффект. Наиболее ярко это проявилось в ходе мощных DDoS-атак, которым в 2012 г. подвергся ряд телекоммуникационных компаний по всему миру, включая американский холдинг At&T, крупнейший мировой хостинг-провайдер GoDaddy, поставщика «облачных» услуг Cloudflare, компанию Spamhaus, составляющую «черные списки» поставщиков спама и др.

Так, DDoS-атака на последнюю была организована базирующимся в Нидерландах хост-провайдером Cyberbunker, который таким образом выразил свое несогласие с решением Spamhaus внести его в «черный список» спамеров. В ходе данной атаки была зарегистрирована беспрецедентная мощность потока трафика в 300 Гбит/с.

По мнению экспертов в области информационной безопасности, DDoS-атака на Spamhaus стала самой масштабной из публично известных в истории Интернета. Глава компании «Клаудфлэр», которая сама ранее подверглась схожему нападению, утверждает, что «эти действия… по сути, сопоставимы с ударом ядерной бомбы. Вот так просто нанести ущерб подобного масштаба».

То есть не только государства могут быть субъектами и объектами атак, но и любая группа, обладающая минимальными финансами.

В отличие от организации DDoS-атак, разработка сложного вируса типа Stuxnet, поразившего ядерные объекты Ирана, стоит, предположительно, порядка 3 млн. долл. США. Но все равно это обошлось заказчикам значительно дешевле, чем стоила бы серия авиаударов по укрепленным объектам.

Закладка на ключевом маршрутизаторе в Сирии на три дня оставила всю страну без интернета, подстегнув беспорядки на улицах.

Взлом базы данных ВАДА (всемирного антидопингового агентства) нанес существенный ущерб репутации спортсменов, которые легально получали запрещенные для других спортсменов медицинские препараты.

Очевидно, что опасности в области информационных технологий экспоненциально возрастают. И требуются специальные меры по уменьшению киберопасностей.

Я обращаюсь к коллегам с призывом поддержать на национальном уровне работу по внедрению мер укрепления доверия в области информационных технологий.

И, конечно, меры доверия в области информационной безопасности должны учитывать национальные интересы всех стран и не должны давать односторонних преимуществ какому-либо другому государству. Потому что наша цель - единая и неделимая безопасность.

Спасибо за внимание.