Секция «Мировая политика»

Кибертерроризм как вызов международной безопасности - перспективы совместного противодействия

Ревский Александр Дмитриевич
Соискатель
Московский государственный университет имени М.В. Ломоносова, Исторический факультет, Москва, Россия
E-mail: revskiy@yandex.ru

Сегодня трудно представить жизнь без компьютера и, соответственно, без всех возможностей, которые предоставляет интернет. Но, получив колоссальные преимущества, человечество подвергло себя и серьезной опасности — поражение одного элемента сети вызывает сбои в работе всех остальных. Такая взаимозависимость дает возможность злоумышленникам угрожать безопасности не только отдельных граждан, но и жизнеобеспечению целых государств, находясь за тысячи километров от них. Сравнить с этим можно только угрозу применения ядерных ракет. Преступники получили возможность угрожать обществу в виртуальном мире — пространстве, которое еще три десятка лет назад даже сложно было себе вообразить.

Кибертеррористы, а именно так стали называть людей, специализирующихся на взломе компьютерных систем, постепенно научились организовывать отдельные кибератаки в глобальные сети, положив тем самым начало истории кибервойн.

Одна из первых подобных кибервойн произошла в апреле 2007 г., когда в связи с решением Эстонского правительства о переносе памятника Воину-Освободителю организованным атакам подверглись сайты государственных структур этой страны. Крайне болезненным этот удар стал вследствие наличия в Эстонии развитой системы так называемого «электронного государства», к которой так активно стремятся перейти не только европейские, но и ведущие азиатские страны. Благодаря ей, большая часть государственного делопроизводства в этой балтийской стране ведется в электронном виде: через интернет транслируются заседания правительства, здесь можно заполнить анкету на получение паспорта, оплатить коммунальные счета и даже проголосовать (Эстония стала первой в мире страной, организовавшей в 2005 г. выборы местных органов власти через интернет[n1]). Суммарный ущерб для такого высокотехнологичного государства в результате этих хакерских атак по приблизительным подсчетам должен был превысить 30 млн. эстонских крон[n2].

Апрельские события 2007 г. выявили необходимость проведения совместных мероприятий и организации специализированных центров по защите своих информационных и коммуникационных систем от кибератак. Первым, кто вывел обсуждение этой темы на международный уровень, был командующий силами обороны Эстонии А.Лаанеотс. Уже в начале мая 2007 г. он посетил Брюссель и поднял этот вопрос на заседании военных комитетов НАТО и ЕС. Министр обороны Эстонии Яак Аавиксоо подошел к теме кибертерроризма несколько с другой стороны: он предложил рассматривать любую кибератаку против государства с точки зрения положений статьи 5 Вашингтонского договора, которая трактует нападение на одного из членов Альянса как нападение на всех его участников[n3].

Россия и Китай — два государства, которые в настоящее время выделяются экспертами стран Запада в качестве основных источников киберугроз. Так, доклад «НАТО и киберзащита» упоминает несколько эпизодов компьютерных атак со стороны России: в апреле 2007 г. состоялась атака на сайты госучреждений Эстонии, в июле 2008 г. - атака литовских сайтов в результате принятия Сеймом закона о запрещении к употреблению на собраниях и митингах на всей территории Литвы символики СССР и приравнивание ее к символике Третьего Рейха, в августе 2008 г. в ходе Южноосетинского конфликта была проведена атака на сайты правительственных структур Грузии[n2], и в ноябре 2008 г. - атака компьютерных сетей Центрального командования США[n4].

Однако эксперты, признают, что реальная картина - намного сложнее, поскольку, во-первых, крайне сложно определить, кто же является истинным «заказчиком» кибератаки, так как зараженные вирусом машины, осуществляющие кибератаку, могут находиться на территории совершенно другого государства, а, во-вторых, главную угрозу в будущем, скорее всего, будут представлять негосударственные структуры.

Сложность определения настоящего заказчика кибератаки не позволила государствам — членам НАТО в ходе Лиссабонского саммита в ноябре 2010 г. признать кибератаку действием, подпадающим под положения статьи 5, хотя еще в середине 2010 г. группа экспертов НАТО во главе с бывшим госсекретарем США М.Олбрайт в своем докладе пришли к заключению, что компьютерная атака против жизненно важных инфраструктур стран Альянса должна приравниваться к вооруженному нападению, и, тем самым, оправдывает ответный удар военными средствами[n5].

Если в концепции 1999 г., не говоря уже о концепции 1991 г. нет ни слова о киберугрозе, то в Новой стратегической концепции НАТО поставила кибертерроризм в число основных угроз, с которыми Альянс может столкнуться уже в ближайшем будущем[n6].

Последствием политики «перезагрузки» явилось то, что международные организации и США стали активно привлекать Россию к подготовке конвенции по ведению кибервойны. Одной из основных ее задач является попытка выведения из-под кибератак «гражданских» объектов в интернете. Кроме того, обсуждается возможность создания международного трибунала для суда над киберпреступниками[n7]. Решение о начале работы над правилами ведения войн в киберпространстве было инициировано в мае 2010 г. на первом саммите по кибербезопасности в Далласе.

Литература

1. http://www.inosmi.ru
2. http://kommersant.ru
3. http://www.rbcdaily.ru
4. http://ras.delfi.ee
5. http://itgator.ru
6. http://www.nato.int
7. http://kramtp.info