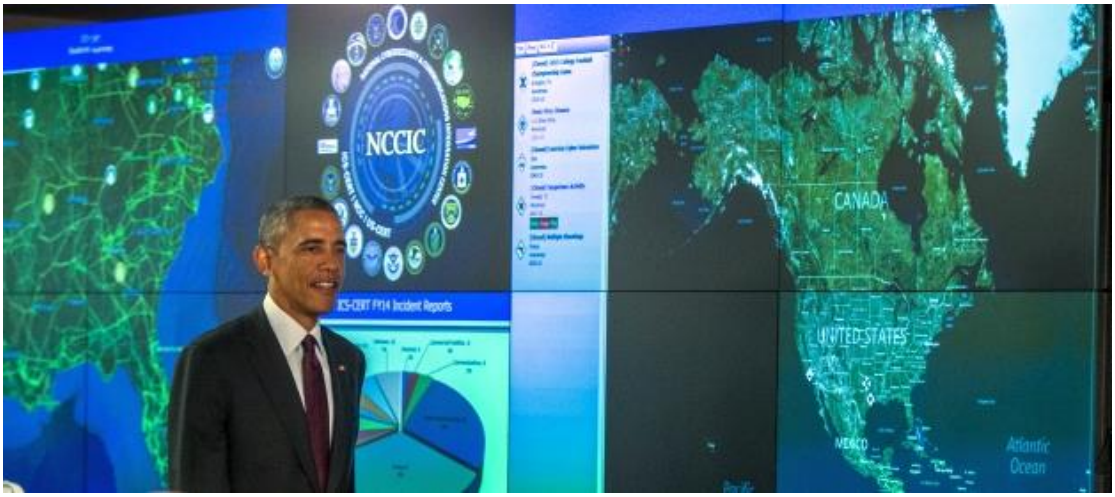
Александра Куликова
Координатор программы «Глобальное управление интернетом и международная информационная безопасность», ПИР-Центр

Возможна ли гонка кибервооружений между Россией и США?

28.01.2015, Александра Куликова

Если США уже планируют вести широкую войну в киберпространстве, как предполагает Эдвард Сноуден, то миру стоит готовиться к опасному вооружению киберпространства и еще большему снижению доверия межу США и Россией в киберпространстве.

На прошлой неделе известный немецкий журнал *Der Spiegel* опубликовал вторую часть разоблачений от бывшего контрактника Агентства Национальной Безопасности (АНБ) Эдварда Сноудена. Согласно опубликованным документам глобальная программа слежения, управляемая США, была лишь только первым этапом более широкой киберстратегии, которая нацелена на подготовку к глобальной кибервойне с другими странами.



Президент США Барак Обама выступает в Центре Национальной Кибербезопасности и Интегрирования Коммуникаций в Арлингтоне, 13 Января. Обама снова призвал Конгресс принять закон о кибербезопасности, который включает положение, поощряющее компании делиться информацией об угрозах с правительством и которое будет их защищать от возможных судебных исков в случае если они будут это делать. Фото: AP

Как свидетельствуют документы, АНБ прямо предполагает, что следующий крупный конфликт произойдет именно в киберпространстве. Кроме того, в материалах содержится план разработки и внедрения вредоносных программ с целью выведения из строя ключевых объектов инфраструктуры противника – банковские системы, электростанции и аэропорты.

После первых разоблачений, сделанных Сноуденом в 2013 году о широкомасштабной электронной слежке, некоторые высказывали надежду, что эти разоблачения приведут к лучшему контролю над деятельностью по обеспечению государственной безопасности и значительному пересмотру принципов работы разведывательных управлений. Теперь все более очевидно, что скорее всего момент для фундаментальных изменений не будет использован в позитивном ключе. То, как страны воспринимают киберугрозы по всему миру, может привести к началу активного и открытого цикла гонки кибервооружений, что будет отражаться на конфиденциальности информации и данных. Кроме того, мы можем уже быть вовлечены в необъявленную «гибридную» войну намного сильнее, чем нам это кажется.

Кибербезопасность после предполагаемой кибератаки со стороны Северной Кореи

С тех пор как в декабре 2014 года была произведена кибератака на Sony Pictures (предположительно спровоцированная выпуском Голливудского фильма «Интервью», который высмеивает северокорейского лидера Ким Чен Ына и изображает покушение на него – прим.ред.) кибервозможности различных государств находятся под еще более пристальным вниманием чем когда-либо. Предполагаемая северокорейская кибератака стала спусковым крючком в кибермобилизации, несмотря на то, что это уже не первая атака такого типа.

Вопросы кибербезопасности были выдвинуты на первый план в ежегодном послании Президента США Конгрессу 20 января, тем самым обозначая их наивысший приоритет – особенно на фоне атаки на Sony. Эта кибератака помогла начать переход от «обеспокоенности» к политическим инструментам.

«Мы хотим убедиться, что наше правительство интегрирует разведку для борьбы с киберугрозами, точно также, как это было сделано для борьбы с терроризмом» - сказал Обама, призывая Конгресс принять новый закон.

Предложенное законодательство поможет в достижении поставленных целей путем нового регулирования защиты информации и совершенствования кибербезопасности критических инфраструктурных объектов, правительственных компьютеров и сетей. В то же время, защита гражданских свобод и личной неприкосновенности будет формироваться соответственно этим целям. По иронии судьбы, заранее заявленная законодательная повестка по киберсфере в речи Обамы совпала с публикацией новых материалов от Сноудена в Der Spiegel от 16 января этого года. Документы отобразили подводную часть айсберга, где массовая слежка были лишь верхушкой.

Как сообщается, США разрабатывали вредоносные программы, «способные парализовать компьютерные сети, а вместе с ними и потенциально всю инфраструктуру, которую они контролируют, включая энерго- и водоснобжение, фабрики, аэропорты и денежные потоки».

Сообщения, предполагающие, что АНБ взломало северокорейские сети еще до атаки на Sony, четко вписываются в общую картину. Взламывая сети заранее, Америка могла начать применять быстрые ответные меры, удерживая «Интранет» Северной Кореи нерабочим в течение нескольких часов. Хотя эксперты говорят, практически невозможно полностью идентифицировать инициатора кибератаки, то, что увидел мир, выглядит как модель обмена атаками в кибервойне, за которой последовали публичные призывы защищать граждан и усилить национальную кибербезопасность.

Учитывая последние документы Сноудена, мы имеем три главных вывода:

1. Идея, что Интернет может быть платформой для ведения войны, больше не выдумка и не теория
2. В отсутствие широко признанной международно-правовой системы определения кибервойны и точных инструментов идентификации происхождения кибератак, трудно локализовать их во времени и пространстве и даже назвать это «войной» даже притом, что очевидно, она уже продолжается некоторое время. (таким образом, выбор термина был - «гибридная война», где киберэлементы используются все чаще, в отличие от обычных вооружений).
3. Гонка кибервооружений на национальном уровне или союзном уровне скорее всего будет отражать текущую геополитическую расстановку сил.

Новые региональные киберсоюзы для борьбы с невидимыми кибератаками

Пока мир «переваривает» потенциальные масштабы инициативы АНБ по созданию вредоносных программ, США и Великобритания уже объявили о своем намерении провести объединенные киберучения. Британские органы безопасности и разведки, такие как Управление правительственной связи Великобритании (УПСВ) и МИ-6 наряду с их американскими аналогами – АНБ и ФБР, инсценируют кибератаки на ключевые финансовые инфраструктуры Лондон Сити и Уолл Стрит, чтобы протестировать их надежность.

Если такие тренировки станут обыкновенной практикой, то следующими целями потенциальных атак могут стать элементы критической инфраструктуры стран, чья защита необходима для системной целостности составляющих национальной безопасности – энергосистемы, ядерные реакторы, телекоммуникационные и транспортные объекты.

То, что назвали «борьбой с тенями» на специальной сессии Мирового Экономического Форума в Давосе, уже значит больше, чем просто метафора, учитывая сложности с определением источника киберагрессии, согласно Лаборатории Касперского.

Такая деятельность до сих пор остается безнаказанным де юре, но не де факто, так как решение по поводу того, производить контратаку или нет, в основном происходит по собственному усмотрению стран ввиду отсутствия значимых и общепринятых международных норм регулирования.

В то время, когда и Обама и британский премьер-министр Дэвид Кэмерон испытывают сейчас сложности в своей политической карьере, они оба нашли удобный популистский инструмент для продвижения киберповестки, обращаясь к переживаниям электората по поводу вопросов безопасности, особенно после атаки на Шарли Эбдо.

Для Кэмерона задача удержания баланса «безопасность – конфиденциальность» на родине является особенно сложной, учитывая последние утечки информации от Сноудена о том, что GCHQ перехватывала электронную переписку журналистов, а также вызвавшие широкий резонанс предложения относительно ужесточения политики в области криптографии, чтобы вынудить США надавить на свои Интернет-компании.

В то время как новая волна вопросов безопасности обеспечивает хорошее оправдание для ограничения гражданских свобод, включая возможное возрождение печально известного UK Communications Data Bill (также известного как «Snoopers' Charter», отложенная в сторону после первых разоблачений Сноудена) и попытки провести необходимые положения в предложенный в прошлом году антитеррористический законопроект[1] сделают

[1] Вторая попытка группы членов Палаты Лордов включить положения Snoopers' Charter в антитеррористический законопроект была снята с голосования 2 февраля http://www.bbc.com/news/uk-politics-31096177

криптографию полем для перетягивания каната между государством и частным сектором.

Россия надеется улучшить свои возможности в киберпространстве и найти новых киберсоюзников

Хотя нет ничего удивительного в таком совместном предприятии США и Великобритании - они сотрудничают по целому ряду проблем в обороне и безопасности в формате «5-ти глаз» - Россия получила довольно четкий сигнал в контексте современных геополитической напряженности.

Первые российские учения в киберпространстве летом 2014 года выявили систематические уязвимости, что привело к призывам создать резервную дублирующую систему DNS и активизации мер для обеспечения кибербезопасности на национальном уровне. Новая Военная доктрина России, подписанная в конце декабря 2014 года, квалифицирует киберопасность как «военную опасность», которая при определенных условиях может стать «военной угрозой», характеризующейся прямой возможностью военного конфликта.

Киберопасность также может быть незамедлительно квалифицирована как военная угроза, если она нацелена на объекты критической инфраструктуры в ядерных, космических, химических и фармацевтических объектах. Тогда как, по мнению экспертов, кибер-элементы Военной доктрины России не всегда гладко вписываются в общую конву и существующей терминологии не хватает четкости, очевидно, что ряд доктринальных документов будут пересмотрены для включения в них киберизмерения. Другие страны в это время заняты обновлением своих кибер-стратегий[2].

Еще осенью 2014 года Россия и Китай объявили о своей решимости подписать соглашение о сотрудничестве в киберпространстве в 2015 году. В то время как любое соглашение не будет легким для России, учитывая, что в последнее время пространство для маневров заметно уменьшилось, ожидается, что эта договоренность будет более значительной, чем аналогичная, подписанная с США еще в 2013 году.

Это не удивительно, так как российские и китайские позиции гораздо ближе по целому ряду вопросов управления в киберпространстве. Совместные киберучения могли бы стать частью этого двустороннего соглашения в будущем. Россия также могла бы продвинуть сво. киберповестку в рамках таких союзов, как БРИКС (Бразилия, Россия, Индия, Китай и Южная Африка), Шанхайская организация сотрудничества (ШОС), Организации Договора о коллективной безопасности (ОДКБ), или в недавно созданном Евразийском Экономическом союзе, чтобы соответствовать заявке НАТО на коллективную кибероборону.

[2] 10 февраля СМИ опубликовали информацию о запуске в США нового агентства по борьбе с киберугрозами. Как прокомментировал новость бывший сотрудник ФБР по киберпреступности Скотт Ларсон, «мы находимся в гонке разведывательных вооружений и мы не можем бездействовать».

Новая политика кибербезопасности НАТО призывает всех членов обмениваться своим опытом в кибербезопасности. Она была одобрена на саммите в сентябре 2014 года, после чего последовали широкомасштабные ноябрьские киберучения для проверки системных уязвимостей инфраструктуры. Вероятно, что подобные мероприятия будут отражены в небольших коллективных усилиях, инициированных Россией с возможной поддержкой ее союзниками.

Будущая угроза усиливающейся гонки кибервооружений

Поскольку стороны сейчас пересматривают свои стратегические партнерские отношения, а также обороноспособность в связи с кризисом на Украине, дальнейшее развитие гонки кибервооружения вызывает много тревог в связи с ее непредсказуемостью и отсутствием правовой совместимости. 9 января, члены ШОС представили обновленный проект Международного кодекса поведения в области информационной безопасности в Организацию Объединенных Наций, в надежде установить общие правила под эгидой ООН.

Тем не менее, национальные и недавно запущенные региональные инициативы скорее направлены на использование сложившейся ситуации для достижения краткосрочных политических целей, чем на реализацию всеобъемлющего проекта в рамках ООН, который, скорее всего, будет провален. Возможно, это слишком оптимистично пытаться разрабатывать общие правила для честной игры, когда стороны уже начали развертывать кибероружие.

Ссылка на оригинал:

Is a cyber-arms race between the US and Russia possible?

28 January 2015