Киберзащита — многосторонний политический вызов

Аннегрет Бенди, Катрин Алмер

сотрудники Немецкого института международной политики и безопасности.

Недавнее откровение бывшего сотрудника NSA Эдварда Сноудена привело к тому, что проблема кибербезопасности оказалась в центре общественного внимания. Как затрагивается эта тема в политике? Одного взгляда на последние сообщения международных журналов достаточно для того, чтобы понять, что под заголовками о кибербезопасности обсуждаются самые разные аспекты, такие как киберсдерживание в качестве средства борьбы с кибератаками, управление Интернетом или преимущества цифровой дипломатии в качестве профилактического инструмента для большей кибербезопасности. Технические статьи отражают различные аспекты новой политики в области внешней политики и политики безопасности. Дополнительную ценность этой молодой научной дискуссии придаёт то, что она вызывает множество вопросов, на которые должны ответить лица, принимающие решения в политике и экономике в связи с борьбой с киберрисками.

По крайней мере, откровение бывшего сотрудника NSA США, Эдварда Сноудена сделало модной тему кибербезопасности. Чтобы осветить эту тему с разных точек зрения, имеет смысл изучить исследования, связанные с этим вопросом. В отличие от средств массовой информации, в научной литературе сам термин «безопасность» является спорным. Когда дело доходит до кибербезопасности, то, по словам Густава Линдстрома, главы программы евроатлантической безопасности Женевского центра политики безопасности (GCSP), не хватает международных признанных определений для многих терминов, которые являются центральными в дебатах о киберпреступности, кибервойнах и кибертерроризме. Вопрос о том, какие условия должны выполняться для того, чтобы расценить кибератаки как вооружённое нападение в глазах международного права, остаётся без ответа так же, как вопрос о том, какими правами обладают жертвы подобного рода нападений. Кроме того, по словам Линдстрома, наблюдается тенденция наступательного использования кибертехнологий, которую тоже надо учитывать. Дискуссии о кибербезопасности должны быть сосредоточены на вопросе о соответствующих политических и правовых мерах, которые помогут ограничить использование кибероружия.

Навыки кибератаки были разработаны, по Линдстрому, и всё чаще становятся стратегическим инструментом межправительственного разрешения конфликтов. Кроме того, политическим деятелям придётся прийти к соглашению о модели управления Интернетом, будь то для поддержания текущего режима или для обеспечения большего регулирования, как в частности хотят Китай и Россия.

Можно так же почитать литературу по классификации кибертехнологий и их новизне в международных делах и политике безопасности, что предлагает Джеймс А. Льюис, старший научный сотрудник и директор по программе государственной политики и технологиям в Центре стратегических и международных исследований (CSIS), которую он написал для журнала по военно-стратегическим вопросам. Киберметоды используются спецслужбами начиная с 80-х гг., но военные кибератаки появляются только в 90-х гг.

Кибератаки используют новые пути и средства для насильственного исполнения интересов (принуждения) и шпионажа, но не относятся к новой категории конфликта. Было бы неправильным изображать вредоносные программы, такие как Stuxnet и Flame в качестве характеристик нового типа войны; эти атаки не настолько разрушительны, как сила ядерного оружия. Отнести Stuxnet к средству ведения войны даже сложнее международных переговоров, в которых предлагается заблокировать киберпространство.

Сложные киберметоды а ля Stuxnet в настоящее время используются только в Соединённых Штатах, Соединённом Королевстве, Израиле, России и Китае. Другие государства намерены использовать аналогичные возможности. До сих пор не удалось нанести урон с большими физическими повреждениями. Однако, есть сомнения, по Льюису, останется ли это так, если такие страны, как Иран и частные субъекты получат достаточно возможностей для совершения кибератаки. Льюис утверждает, что нужно поддерживать большой политический контекст с учётом сохранения возможности кибератак: он заметил, что откровения о шпионской программе Flame могли послужить тщательной переговорной позиции России в вопросах управления Интернетом и киберпространством.

Киберсдерживание на примере США

Мириам Данн Кэйвелти, начальник исследовательской группы Риски&Устойчивость в центре по исследованию проблем безопасности ETH в Цюрихе, в своей статье в международном журнале Studies Review проанализировал данные о том, как военная риторика берёт верх в связи с киберинцедентами, связанными с безопасностью. Кибербезопасность будет в основном рассматриваться как военная проблема, которая может быть решена военными действиями. Данн Кэйвелти ссылается на данный вопрос и призывает такие кажущиеся очевидными взаимосвязи всегда брать под сомнение.

Франк Киллуфо, директор Института политики внутренней безопасности (HSPI) и содиректор Кибер Центра Национальной и Экономической Безопасности (CCNES) университета им.Джорджа Вашингтона, Шэрон Кардаш, заместитель директора HSPI и Джордж Сэлмирэги, адвокат и консультант HSPI, напротив, уверены в этом. В газете Military and Strategic Affairs они представляют несколько ключевых моментов стратегии киберсдерживания США. Для защиты важных инфраструктур как, например, водоснабжения и электропитания, авторы рекомендуют Штатам разработать стратегию киберзащиты. Соединенные Штаты должны продемонстрировать руководство киберполитикой и следовать конкретному плану. Ключевые моменты американской гегемонии заключаются не только в том, что ее военные силы все больше расширяются и грозят нанести удар первыми, но и в том, чтобы фактически быть в состоянии отразить кибератаки военным способом. Для этого необходимо сохранять передовые позиции США в области науки и технологий. Цели и мотивы потенциальных противников должны оперативно идентифицироваться, чтобы суметь предпринять адекватные контрмеры. Несмотря на огромный технический прогресс и одновременно дефицит информации по отношению к преступникам, правительство США должно уметь противостоять их навыкам в использовании технологий. По мнению авторов, должны быть установлены жесткие стимулы для частного сектора, чтобы защитить важные стратегические инфраструктуры. Также, если это необходимо, возможна кооперация с международными союзами в области кибертехнологий.

Еще до заявления Эдварда Сноудена для программы мониторинга Prism американский журналист Джеймс Бэмфорд в журнале Wired Magazine критиковал нынешнюю киберполитику США. Бамфорд пишет о NSA уже многие десятилетия. Он определяет, как под руководством генерала Кейт Александра был расширен мониторинг интернет-программ, и как при этом, в зависимости от тех или иных последствий для общества, состоялась политическая дискуссия. Исходя из официальной позиции США, под кибербезопасностью, по мнению Бамфорда, подразумевается то, что Пентагон, несмотря на сокращения бюджетных расходов на 4,7 млрд. долларов для «операций в киберпространстве» к 2014 г., фактически подал заявку на 1 млрд. долларов больше, чем в прошлом году. Значительная доля киберорганизации под руководством генерала Александра будет запущена в работу. Должно финансироваться создание порядка 13 групп по кибератакам. Для правительства США созданы так называемые Zero-Day-Exploits, которые, попадая в «плохие руки», являются огромным пробелом в безопасности. Zero-Day-Exploit является, по мнению компании «Лаборатория Касперского», «вредоносным программным обеспечением, который одновременно обнаруживает ошибки, уязвимость приложения или системы, и с помощью которого данные действия можно использовать в других целях. У производителя не остается времени для предоставления Patch (исправления программного обеспечения) и IT-

администраторы не приходят к тому, чтобы своевременно задействовать другие защитные механизмы». Атаки, использующие уязвимость системы, будут как бы «ахиллесовым бизнесом безопасности», — как процитировал бывший разведчик Бамфорд. Соответственно, отсюда и вытекают высокие суммы, которые выплачивают заинтересованные стороны Zero-Day-Exploits и благодаря которым, по словам Бамфорда, выходит опасная и неконтролируемая гонка кибер-вооружений с собственным черным рынком.

Нормы регрессии и роль БРИКС.

Хотя некоторые эксперты по безопасности выступают за расширение государственных возможностей кибератаки, необходимо услышать и других ученых в области интернет-управления, которые заявляют о тенденциях к секьюритизации за счет гражданских свобод.

Данный факт констатировал Рональд Дж.Дайберт, директор Канадского центра по глобальным исследованиям в области безопасности и Citizen Lab в школе по политике безопасности Университета Торонто, и Масаши Крете-Нишибата, менеджер по исследованиям в Citizen Lab в своих статьях для газеты Global Governance, где представляют «нормы регрессии» глобального управления. Они являются тем, что большинство правил размещены таким образом, что ограничивают киберпространство как «открытое достояние свободной информации и коммуникации». Речь идет о том, что происходит развитие, направленное в сторону традиционных форм государственного контроля. К государственному традиционному контролю причисляются цензура, а также ограничения или прерывания интернет-доступа для того, чтобы предотвратить массовые беспорядки и протесты. Форумы, которые поощряли нормы контроля, определяют авторов из Международного Союза Электросвязи (ITU) или региональных организаций, таких как Шанхайская Организация Сотрудничества (ШОС). Упрощает государственную цензуру импорт и экспорт соответствующих технологий как для кибер-защиты, фильтрации коммерческой деятельности в интернете, так и для мониторинга или использования в определенных наступательных операциях.

Почему многостороннее сотрудничество достаточно трудно организовать и какую роль играют страны БРИКС (Бразилия, Россия, Индия, Китай и Южная Африка) в сфере Интернет-управления и кибербезопасности, — об этом рассказывают Ганс Эберт и Тим Мауэр в издании Third World Quarterly. Страны БРИКС совместно противостоят политике США. Но, вместе с тем, у данных стран различные стратегии во внешней политике. Россия и Китай, в частности, склонны применять государственный контроль в Интернет-сообществе, и они были нацелены на создание правил международной координации через ITU. Обе страны стремились организовать международный Кодекс поведения в области

информационной безопасности. Индия, Бразилия и Южная Африка (IBSA), напротив, применяют «межправительственную» модель с целью нормотворчества Интернет-сообщества, для чего специально создаются международные организации, которые также включают в себя негосударственные заинтересованные стороны. IBSA-страны находятся на позиции, отрицающую интернет-цензуру и закрытые сети, позиционируя при этом себя в качестве «Swing States» по вопросам глобальной дискуссии. В данном контексте такое непоследовательное поведение стран БРИКС связано с тем, что в одних странах господствует демократия, в других — нет. По словам авторов, значительную роль здесь играют и другие факторы: во-первых, различный исторический опыт, во-вторых, мобилизация общества под воздействием СМИ, в-третьих, сопряжение между информационной безопасностью и дискуссией по правам человека и, в-четвертых, экономический подъем Китая, который предлагает возможность для развивающихся стран освободиться от зависимости США и разграничить свои интересы от интересов передовых держав. В качестве примера для четвертого пункта можно привести также совместное сотрудничество Индии с США или Бразилии с США под эгидой Интернет-управления и кибербезопасности.

Цифровая дипломатия.

Роль общественной дипломатии обсуждается Николасом Калл, профессором общественной дипломатии Университета Южной Калифорнии в Лос Анджелесе в своей статье для газеты International Studies Review. Он изображает то, как современные информационные и коммуникативные технологии были использованы в американской общественной дипломатии, описывает диалог с представителями третьих стран. Ответственный за это был с 1953 года до 1999 года Государственный департамент как высоко инновационное Информационное агентство США. Автор сетует о том, что информационно-технические средства используются не достаточно часто. Первые откровения Викиликс и переломы в арабском мире с декабря 2010 г. вызваны тем, что были усиленны информационно-технические возможности для ведения диалога по сравнению с тем, как они были использованы ранее. Дипломатия может быть активирована на цифровых форумах и далее с помощью индивидуально используемых каналов. «Общественная дипломатия 2.0» — это следствие идеи о горизонтальной Сети, что подразумевает под собой использование социальных Сетей и онлайн-сообществ.

Мариэте Шааке, нидерландский член-депутат европейской либерально-демократической партии в собственной статье для газеты Security and Human Rights идет еще дальше. Она поднимает значимость цифровой свободы так же основательно, как и значимость ответственности, которая «вырастает» из дипломатии Евросоюза. Арабская весна показала эффективность

современных информационно-коммуникативных технологий. Здесь находится Евросоюз — рычаг, открывающий доступ к демократизации.

По мнению автора, в эпоху информационных технологий европейская политика должна возобновляться с целью укрепления прав по защите человека. Дипломатия Евросоюза должна изменить свою политику, воспринимать собственную свободу и обходить стороной цензуру или предотвратить это путем экспорта технологий. Цифровая свобода подразумевает также традиционные права человека такие, как право на свободу слова и собраний. Шааке в своей статье пропагандирует ориентацию информационной внешней политики на права человека, которая имеет большое значение в сфере экономики частного сектора. Кроме того, информационная свобода ЕС должна вставать на защиту самой себя с тем, чтобы Союз заслуживал доверие и полностью отвечал собственным принципам. В отношении чего, как раз таки, Европа будет глубоко следить извне. Несмотря на это, Шааке видит в «оцифровке» риски, грозящие области политики безопасности и внешней политике. Тем не менее, информационно-коммуникативные технологии должны служить в условиях демократии соблюдению свободы прав человека.

Кибербезопасность оказывает огромное влияние на права и свободы, но у этого есть обратная сторона. Данные взаимоотношения довольно критически рассматривает Стивен С. Беннет в статье под заголовком «Право быть забытым» в Berkeley Journal of International Law. Права Интернет-пользователей заключаются в том, что определенная информация может ими контролироваться путем ее сохранения или уничтожения. Беннет обозначил те усилия и меры для защиты информации, которые предпринимала Европа начиная с 2000 года. К этому относятся правила, которыми должны оперировать и которые должны придерживаться все организации в ЕС. В США, напротив, право на свободу слова оценивается выше, чем защита данных. Сегодня экономика базируется на Интернет технологиях, что, по словам Беннет, является ключевой ролью в гармонизации международной политики по защите информации. В связи с последними событиями в США, происходившими с 2010 года, можно установить, что Соединенные Штаты вносят большую открытость по вопросам защиты данных, а также для проведения совместного диалога с ЕС. Этот диалог может быть значительно упрощен благодаря введению ЕС единого стандарта защиты данных, таким образом, оба партнера могли бы работать, по крайней мере, на минимальных стандартах. Несмотря на такого рода прогресс, остается вопрос о том, как обращаться с юридической стороны с существующими проблемами конфиденциальности информации. Особенно возникает неуверенность в том, насколько широко развита компетенция судов ЕС в отношении тех участников, которые действуют за пределами ЕС, но оказывают на нее влияние. Существование таких вопросов в безграничном киберпространстве оказывается традиционной концепцией юрисдикции, которая основана на суверенитете определенной территории. Хотя, по

мнению Беннета, быстрая разработка общих стандартов права является своего рода амбициозным проектом. Но, с другой стороны, это поможет расширить взаимопонимание и уменьшить правовую неопределенность, возникающую вследствие издержек и торговых барьеров.

Следующая тема: большие данные

«Большие данные могут дать представление о возможных событиях будущего», — рассказывает Кеннет Нейл Цукер и Виктор Майет Шонбергер в Foreign Affairs. Использование больших данных соотносится с идеей того, что сегодня они должны обрабатываться относительно недорогими и мощными компьютерами. Основная часть данных есть решающий фактор в определенных процессах.

В настоящее время практически все может быть отображено в данных, например, в данных GPS, которая функционирует на основе определения местоположения. Но то, почему большие данные, тем не менее, уходят на второй план, имеет свои причинно-следственные связи. Только с долей вероятности можно утверждать, что это могло бы способствовать, по мнению авторов, решению многих проблем человечества. Цукер и Майер Шонбергер приводят яркие примеры конструктивного использования больших данных, например, в медицине или предоставлении государственных услуг. Такого рода данные также могут быть полезны в борьбе с изменением климата. Разнообразные датчики, расположенные по всему миру могут обеспечить огромное количество данных, которые помогут разрешить проблему глобального потепления и более точно определить и изучить наиболее эффективные возможности изменить среду «вручную». Но огромные объемы данных, находящиеся, в частности, в руках недемократических государств могли бы, по словам авторов, привести к увеличению разрыва между гражданами и государством.

Кибербезопасность как новый политический вызов

В данной дискуссии необходимо также указать на то, что цифровая революция не только открывает возможности, но и создает значительные риски. Между странами уже фактически началась гонка вооружений в Интернете. Кроме того, Эдвард Сноуден, обладающий инсайдерской информацией британских и американских программ эпиднадзора, пришел к выводу о том, что для внешней политики и безопасности огромное значение имеют большие данные. «Вы должны знать врага, чтобы суметь победить его», — этот принцип, который сформулировал около 2,5 тысяч лет назад китайский военный стратег Сунь Цзы, имеет место быть и сегодня, в эпоху Интернет-технологий. Эффективные меры безопасности ИТ могут быть приняты только тогда, когда известно, какие методы и средства

злоумышленник использует, чтобы взломать компьютер своего противника. В то же время, можно отметить, что цифровая революция происходит по-разному. Таким образом, существует цифровой разрыв (digital divide) между странами ОЭСР и странами, не принадлежащими к ОЭСР. Это, в свою очередь, означает, что возможности распределены неравномерно к мировому доступу сети Интернет и к другим (цифровым) информационно-коммуникационным технологиям, и в значительной степени зависят от социальных факторов. Кибербезопасность подразумевает под собой также и человеческую безопасность. В связи с этим остается открытым вопрос о модернизации, создающей кибербезопасность или же новой дипломатии, которая сейчас входит в сцепление с цифровой революцией. Из положений, обсуждавшихся здесь, можно сделать вывод о том, что данная дискуссия только набирает обороты. Вопросы, рассматриваемые в статьях, наглядно иллюстрируют аспекты того, что кибербезопасность во многих областях политики играет большую роль, и что различные информационные технологии могут сильно изменить реальность. Таким образом, кибербезопасность является для европейской и международной внешней политики безопасностью с новыми вызовами.