ВНЕШНЯЯ ПОЛИТИКА И БЕЗОПАСНОСТЬ 29.06.2021 | Ричард Н. Хаасс

«Киберэквивалент» контроля над вооружениями

Кибератаки могут стать оружием массового уничтожения. Миру необходимы соглашения об урегулировании поведения в киберпространстве.

Во время холодной войны на встречах на высшем уровне между Соединенными Штатами и Советским Союзом часто доминировали соглашения об установлении ограничений на ядерное оружие и системы для его доставки. США и Россия все еще обсуждают эти темы, но на недавней встрече в Женеве президент США Джо Байден и президент России Владимир Путин гораздо больше внимания уделили тому, как регулировать поведение в другой сфере – киберпространстве. Ставки столь же высоки.

Нетрудно понять почему. Киберпространство и Интернет занимают центральное место в работе современной экономики, общества, политической системы, вооруженных сил и почти всего остального, что делает цифровую инфраструктуру заманчивой мишенью для желающих вызвать катастрофические сбои и нанести максимальный ущерб с минимальными затратами.

Более того, государственные и негосударственные структуры могут проводить кибератаки с высокой вероятностью остаться неузнанными, что еще больше усиливает соблазн развивать и использовать эти возможности. Мы знаем, когда и откуда запущена ракета, но может потребоваться много времени, чтобы обнаружить за этим скрытую кибератаку, а поиск виновных может занять еще больше времени. Такой медленный и неопределенный процесс ослеживания криминальной цепочки делает угрозу возмездия, которая лежит в основе сдерживания, недостижимой.

Возможности совершать кибератаки могут стать оружием массового уничтожения,

Выдвижению этого вопроса на повестку дня встречи Байдена и Путина способствовало то, что Россия увеличила агрессивность действий в киберпространстве, как путем создания фальшивых учетных записей в

когда стратегически важные объекты находятся под угрозой

социальных сетях для влияния на американскую политику, так и получением доступа к критически важной инфраструктуре, такой как электростанции. Актуальность проблемы подчеркивает тот факт, что так поступает не одна РФ: по некоторым данным, КНР в 2015 г. получила доступ к 22 млн досье сотрудников правительства США, по информации из которых можно определить, кто работал или работает на американские разведслужбы.

Точно так же КНДР осуществила кибератаку на компанию «Sony» (и взломала все виды частной переписки), пытаясь заблокировать распространение сатирического фильма, изображающего убийство лидера страны. Все это похоже на своего рода современный Дикий Запад, где почти у всех есть ружья, а закон и шериф практически бездействуют.

Традиционно США предпочитали в значительной степени неструктурированный Интернет – «открытый, интероперабельный, безопасный и надежный», согласно политике, установленной примерно 10 лет назад, – чтобы способствовать свободному распространению идей и информации. Но энтузиазм США по поводу такого Интернета ослабевает, поскольку противники используют эту открытость для подрыва американской демократии и кражи интеллектуальной собственности, важной для функционирования и сравнительных преимуществ экономики Штатов.

Встает вопрос, который легче задать, чем ответить на него: где провести границы и как заставить других принять их? Во-первых, США не лишены своих противоречий, так как они тоже осуществляют шпионаж в киберпространстве (это похоже на вскрытие конвертов для чтения чужой почты) и, как сообщается, вместе с Израилем установили вредоносное ПО для саботажа ядерной программы Ирана. Таким образом, любой запрет на деятельность в киберпространстве предположительно будет частичным.

Одна из перспективных идей – реализация того, что обсуждали Байден и Путин, а именно: запретить атаки на критически важные объекты инфраструктуры, включая, помимо прочего, плотины, объекты добычи нефти и газа, электрические сети, медицинские учреждения, атомные электростанции и системы управления

ядерным оружием, аэропорты и крупные заводы. Возможности совершать кибератаки могут стать оружием массового уничтожения, когда такие важные объекты находятся под угрозой.

Любой запрет на деятельность в киберпространстве предположительно будет частичным

Даже при таком соглашении контроль соблюдения договоренностей может оказаться невозможным, поэтому США также захотят ввести определенную степень сдерживания, чтобы гарантировать, что каждая из сторон соблюдает свои обязательства. Сдерживание может включать заявленную готовность к симметричным ответам: если вы собираетесь атаковать нашу важную инфраструктуру или наносите по ней удар, мы сделаем то же самое с вашей. Сдерживание также может быть асимметричным: если вы угрожаете нашим объектам или атакуете их, мы наложим на вас санкции или предпримем действия против ваших интересов в другом месте.

Любое такое соглашение также должно быть подкреплено односторонними действиями, если учитывать ставки и реальность того, что другие договоренности (вспомним обещание не красть интеллектуальную собственность со стороны Китая в 2015 г.) уже нарушались. К примеру, США хотели бы предпринять шаги для уменьшения уязвимости своих систем, представляющих особую ценность.

Также необходимо будет заявить или обсудить, что утверждения о незнании или отрицании причастности правительства к агрессивной кибератакивности, подобные тому, как В.Путин заявил, что правительство его страны не имело никакого отношения к атакам из России в целях вымогательства выкупа, приниматься не будут. Здесь можно провести аналогию с терроризмом: после терактов 11 сентября 2001 года США ясно дали понять, что не будут разделять террористические группы и правительства, которые предоставили им поддержку или убежище. Таким образом, РФ будет нести ответственность за деяния групп, действующих с ее территории. Настаивание на ответственности должно усилить стимул России обуздать такое поведение.

Возможно, со временем пакт между Соединенными Штатами и Россией станет образцом, к которому могут присоединиться КНР, Европа и другие страны. В случае принятия его Китаем можно было

бы добавить запреты на кражу интеллектуальной собственности (и наказания за нарушение запретов). Ничто из этого не означает разоружения, но это «киберэквивалент» контроля над вооружениями, с которого лучше всего начать.

(c) Project Syndicate 2021



Ричард Н. Хаасс
Нью-Йорк

Ричард Н. Хаасс (Richard N. Haass) - президент Совета по международным отношениям (США), до этого работал директором по планированию политики Госдепартамента США (2001-2003 гг.) и был специальным посланником президента Джорджа Буша в Северной Ирландии и координатором политики будущего Афганистана.