МИР 27.03.2018 | Джозеф С. Най

У войны должны быть правила!

Как будут создаваться новые правовые нормы кибербезопасности?

В феврале генеральный секретарь ООН Антонио Гутьеррес призвал к глобальным действиям для минимизации угроз кибервойн для гражданского населения. Гутьеррес посетовал, что «для этого вида войн нет правовых рамок», и отметил, что пока не ясно, «применима ли к ним Женевская конвенция или международное гуманитарное право».

Десять лет назад кибербезопасность не привлекала большого внимания в качестве международной проблемы. Но после 2013 года ее стали называть одной из главных угроз для США. Хотя о точных цифрах можно спорить, в «Регистре кибероперацій», который ведет Совет по международным отношениям, содержатся данные о почти 200 атаках, организованных 18 государствами с 2005 года (в том числе 20 атак в одном только 2016 году).

Термин кибербезопасность описывает широкий спектр проблем, и они не были главной заботой для небольшого сообщества ученых и программистов, создававших Интернет в 1970-е и 1980-е годы. В 1996 году всего лишь 36 млн человек, или около 1% мирового населения, пользовались Интернетом. К началу 2017 года уже 3,7 млрд человек, или почти половина населения мира, находились в онлайне.

Когда в конце 1990-х годов число пользователей стало быстро расти, Интернет превратился в важнейшую платформу для экономических, социальных и политических контактов. Но вместе с расширением взаимозависимости и экономических перспектив появились угрозы безопасности и уязвимость. Некоторые эксперты ожидают, что число Интернет-подключений может вырасти почти до триллиона к 2035 году, что объясняется развитием новых технологий – большие данные, машинное обучение, Интернет вещей. Число потенциальных целей для атак, которые могут осуществлять как частные, так и государственные игроки, невероятно возрастет, и это будет все что угодно – от систем промышленного контроля до

кардиостимуляторов и беспилотных автомобилей.

Многие эксперты призывают к принятию законов и норм, чтобы обезопасить эту новую среду. Но разработка подобных стандартов в киберпространстве наталкивается на несколько серьезных препятствий. Согласно закону Мура об удваивании мощности компьютеров каждые два года, кибервремя движется очень быстро, а вот человеческие привычки, нормы и государственная практика меняются значительно медленней.

Начать с того, что Интернет является транснациональной сетью сетей, и большинство из этих сетей находятся в частной собственности, поэтому негосударственные структуры играют важнейшую роль. Киберинструменты могут иметь двойное назначение, они быстрые, дешевые, зачастую их легко отрицать, их верификация и атрибуция затруднены, а входные барьеры здесь низки.

Кроме того, хотя Интернет транснационален, инфраструктура (и люди), на которую он опирается, находится внутри различных юрисдикций суверенных государств. При этом крупные государства расходятся в своих целях. Например, Россия и Китай подчеркивают важность суверенного контроля, в то время как многие демократические страны требуют более открытого Интернета.

Однако расшифровка «www» в виде «wild west web» («паутина дикого запада») является карикатурой. В киберпространстве все же существуют некоторые нормы. Государствам потребовалось примерно два десятилетия, чтобы достичь первых соглашений о сотрудничестве для ограничения конфликтов в ядерную эпоху. Если считать датой возникновения международной проблемы кибербезопасности не момент появления Интернета в начале 1970-х, а момент, когда он начал быстро распространяться в конце 1990-х годов, тогда получается, что межправительственному сотрудничеству по вопросам ограничения киберконфликтов сейчас как раз уже почти два десятка лет.

В 1998 году Россия впервые предложила подписать договор на уровне ООН о запрете электронного и информационного оружия (в том числе для пропагандистских целей). Вместе с Китаем и другими членами Шанхайской организации сотрудничества Россия продолжает настаивать на заключении широкого договора в рамках ООН. А США продолжают считать, что соблюдение такого договора невозможно проверить.

Вместо этого генеральный секретарь ООН назначил Группу правительственных экспертов (UNGGE), которые провели первую встречу в 2004 году, а в июле 2015 года предложили комплекс норм, позднее одобренных «Большой двадцаткой». В деятельности ООН группы экспертов не являются чем-то необычным, но крайне редко их работа поднимается из недр этой организации до уровня признания на саммите 20 самых могущественных государств мира. Успех UNGGE был экстраординарным, однако в 2017 году эта группа не смогла согласовать свой следующий доклад.

Куда же мир идет теперь? Нормы могут предлагаться и разрабатываться самыми разными инициаторами политических решений. Например, новая неправительственная Глобальная комиссия по вопросам стабильности в киберпространстве (ее председателем стала Марина Кальюранд, бывший министр иностранных дел Эстонии) выступила с призывом защитить публичное ядро Интернета. Это понятие включает в себя маршрутизацию (routing), систему доменных имен, сертификаты безопасности и критическую инфраструктуру.

Тем временем, правительство Китая, опираясь на регулярные Всемирные Интернет-конференции в Учжэне, опубликовало принципы (уже одобренные Шанхайской организацией сотрудничества), которые призывают признать право суверенных государств контролировать онлайн-контент на своей территории. Но это совсем не обязательно должно противоречить призывам защитить публичное ядро, поскольку здесь речь идет о возможности подключения, а не о контенте.

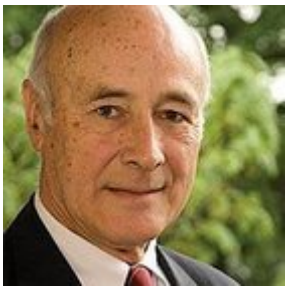
Среди других инициаторов норм – компания Microsoft, которая предлагает заключить новую Женевскую конвенцию об Интернете. Столь же важной является разработка норм, связанных с конфиденциальностью личной жизни и безопасностью; это касается шифрования, программных лазеек, удаления детской порнографии, дезинформации и призывов, разжигающих ненависть, и, наконец, террористических угроз.

Страны-члены ООН обдумывают сейчас следующие шаги в работе над кибернормами, и возможным решением здесь может стать отказ взваливать слишком большое бремя на какой-то один институт, подобный UNGGE. Для достижения прогресса может потребоваться одновременное использование множества площадок. В одних случаях работа над принципами и процедурами, которую будут вести государства со схожим менталитетом, поможет создать нормы, к которым другие страны смогут присоединиться позднее. Например,

Китай и США заключили двустороннее соглашение об ограничении кибершпионажа в коммерческих целях. В других случаях – к ним можно отнести, например, нормы безопасности для Интернета вещей, – возглавить разработку кодексов поведения может частный сектор, страховые компании и некоммерческие организации.

Совершенно определенно, разработка норм кибербезопасности будет длительным процессом. И прогресс на отдельных направлениях не должен тормозиться ожиданием такого же прогресса на других направлениях.

(c) Project Syndicate



Джозеф С. Най
Кембридж

Джозеф С. Най (Joseph S. Nye) - американский политолог и писатель. В администрации Клинтона работал помощником главы Пентагона по вопросам национальной безопасности, возглавлял Национальный совет по разведке США. В настоящее время является профессором в Гарвардском университете, автор книги «Is the American Century Over?»