Матяшова Дарья

Пусть соперничают сто школ: будущее международных режимов «широкой» кибербезопасности

Тренды современного мира повышают требования к глобальной кибербезопасности, борьбе с киберпреступностью и глобальному управлению в этих сферах. С одной стороны, возрастает роль систем ИИ в экономике, что требует формирования единых непротиворечивых стандартов безопасной и надёжной работы таких систем. Другая определяющая тенденция относится к политической сфере – речь идёт о конфронтации между государствами-лидерами в развитии и внедрении цифровых технологий, а также разработке норм поведения в киберсреде. Кибератаки и бреши в национальных сетях становятся основой для политических столкновений, как в случае с Solarwinds, когда из-за уязвимости ПО компании пострадали несколько американских министерств и ведомств. Не последнюю роль в актуализации проблемы глобальной кибербезопасности сыграла и пандемия Covid-19, переселившая множество предприятий в цифровую среду и поставившая ребром вопрос о защите данных о здоровье миллионов людей.

Потребность в более надёжных сетях и более оперативной борьбе с преступностью в них носит глобальный характер. Это означает, что и новые принципы должны быть применимыми и эффективно действующими во всём мире. Однако особенности современных процессов в этой сфере – параллельное существование на базе ООН двух переговорных площадок по кибербезопасности [1], расхождение позиций государств по вопросам киберпреступности из-за различного подхода к определению понятий, отсутствие единого органа по координации борьбы с киберпреступностью и различная правоприменительная практика в этой сфере ставят под вопрос возможность выработки таких правил в целом. Возможно ли вообще создать глобальные всеобъемлющие правила, если за последние 20 лет на общемировом уровне удалось выработать лишь нормы рекомендательного характера?

На самом деле, сформулировать принципы кибербезопасности, которые были бы всеобъемлющими и имеющими глобальный характер, возможно, как показывает кейс доклада Рабочей группы открытого состава (РГОС) ООН 2021 года. Данный доклад был поддержан консенсусом – кроме того, даже страны-члены, не поддержавшие создание РГОС, не стали создавать препятствий для его формулирования и принятия, что говорит в пользу отражения в докладе взглядов большей части международного сообщества [2]. Подобные ширококонсенсусные документы обычно осторожны с выдвижением норм – однако в докладе РГОС целый раздел посвящён «правилам, принципам и нормам ответственного поведения государств». Он подводит черту, суммируя принципы, принятые в резолюциях 70/237 и 73/27 Генассамблеи ООН, и обещая совершенствовать и дополнять их [3].

Что же это за принципы? «Принимать разумные меры для обеспечения целостности цепочек поставок, в том числе путем разработки объективных совместных мер, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ; стремиться предотвратить распространение вредоносных инструментов и методов ИКТ и использование вредоносных скрытых функций; поощрять ответственное сообщение об уязвимостях» [3]. Иными словами, это принципы кибербезопасности в широком смысле

слова – кибербезопасности, не сводящейся к борьбе с последствиями, а обеспечивающей их предупреждение и даже берущей на себя ответственность за смежные отрасли (цепочки поставок), которые она «приручила». В чём-то такая трактовка похожа на концепцию позитивного мира Й. Галтунга [4], в которой мир – это не только отсутствие войны, но и наличие ресурсов и институтов для стабильности и развития.

Что позволило РГОС и принимавшей резолюции Генассамблее выйти на такой уровень? Во-первых, подробная разработанность «негативномировых» принципов, относящихся к борьбе с последствиями киберугроз и защите базовой инфраструктуры, атака на которую знаменовала бы собой конец «отсутствия войны». Такие принципы относились к атрибуции киберинцидентов и классификации критической инфраструктуры и были выработаны в рамках ГПЭ ООН [5], что дало РГОС возможность заниматься более широкой трактовкой с новой повесткой. Во-вторых, признание кибербезопасности сферой, подчиняющейся логике и правилам международного публичного права (в частности, Уставу ООН) [6], которое применимо и в физическом и в цифровом пространстве. Данный доктринальный концепт был закреплён ГПЭ ООН и также поддержан международным консенсусом [7]. Международное право – регулятор широкого спектра взаимоотношений, что соответствует и широкой трактовке кибербезопасности в РГОС.

Однако в данном контексте это не единственный значимый вывод. Более значима обнаруженная связь между «широкой» кибербезопасностью и правом. Кибербезопасность, вписываясь в архитектуру международно-правовых норм, по определению становится объектом глобальных, признаваемых международным сообществом и соблюдаемых даже при отсутствии верховного надсуверенного «контролёра и законодателя». Фактическое единство таких правил достигается за счёт ответственного соблюдения в рамках правовых обычаев, а юридическое – за счёт кодификации и opinion juris. Другой важный вывод связан с тем, что именно opinion juris ГПЭ ООН, столкнувшейся с «конкурентом» в виде РГОС, позволило последней дальше разрабатывать и формулировать нормы по кибербезопасности, подчиняющейся международному праву. Таким образом, нахождение в юрисдикции международного права кибербезопасности – залог постепенного формирования единых глобальных норм последней, чему не сможет противодействовать «расщепление» переговорных и нормотворческих площадок (напротив, их идеи и разработки могут дополнять друг друга).

Тем не менее, такой подход не снимает вопросов о специфических для кибербезопасности проблемах – речь, в частности, идёт о киберпреступности, относящейся главным образом к национальному уголовному праву, несмотря на свой трансграничный потенциал, и праве войны и мира для киберпространства. Последнее стало камнем преткновения, застопорившем работу ГПЭ ООН в 2017-2018 гг. и едва не обратило вспять дискуссию о применимости международного права к киберпространству - в конце концов, ст. 51 Устава ООН утверждает право на самооборону. В обоих случаях значимое место в дискуссии занимают национальные разногласия в трактовках информационного суверенитета и приоритезации его защиты, затруднения в отделении государственных акций от действий третьих лиц, а в случае с правом войны и мира – ещё и принципом пропорциональности и одновременно – исключительно военной направленности ответного удара в условиях, когда кибератака способна повредить гражданскую инфраструктуру и нанести вред мирным жителям [6]. В этих аспектах добиться создания единых правил

посредством имеющихся механизмов экспертных групп, мультистейкхолдерных форумов и даже резолюций действительно сложно, но, поскольку речь идёт о международных процессах со своими законами, возможно.

В контексте права войны и мира кибератаки – это не только злонамеренные действия, но и применение определённого вида инструментов поражения (иначе говоря, оружия). Исторически международные отношения умели сдерживать применение оружия не только за счёт гонки вооружений, достижения баланса сил и пр., но и за счёт добровольно взятых на себя обязательств и паттернов ответственного поведения – чаще всего закреплённых в международных соглашениях – которые рано или поздно становились общим правилом – как из-за того, что обязательства сначала скреплялись подписями лидеров ведущих держав, примерам которых хотелось и приходилось следовать, так и из-за того, что оружие оказывалось слишком грозным, чтобы не связывать себя никакими правилами. Совокупность таких правил называется международным режимом, а ярчайшим его примером является режим нераспространения ядерного оружия, сформировавшийся на пике холодной войны. Учитывая опасности кибероружия в современном мире и всепроникающий характер ИКТ-систем, позволяющий им интегрироваться в другие вооружения, вероятность формирования «режима цифрового нераспространения», способного закрыть лакуны права войны и мира для киберпространства, весьма велика.

Подтверждение этому – обязательства, взятые на себя сначала лидерами США и КНР в 2015 г., а уже в 2021 г. – лидерами США и России. В первом случае две кибердержавы взяли на себя обязанность воздерживаться от кибершпионажа и противодействовать ему [8] – впрочем, для режима такая цель оказалась слишком амбициозной и требовала более широкого, кооперативного, а не конфронтационного подхода к безопасности. Поэтому даже экономические интересы, заложенные в сделку, её не спасли. Иными словами, она оказалась «пробой пера», лакмусовой бумажкой для оценки того, что нужно сдерживать и что сдерживать возможно. Более реалистичным и осторожным, но за счёт этого и более реализуемым – а значит, более подходящим на роль «модельного договора», который смогут взять за основу для взаимных соглашений другие страны - оказалась женевская договорённость между В. Путиным и Дж. Байденом о создании механизма двухсторонних консультаций по кибербезопасности – своего рода, экспертного «красного телефона» - и абсолютной защите от атак 16 отраслей критической инфраструктуры США [9].

Что касается борьбы с киберпреступностью, то здесь на руку всему миру может сыграть сосуществование на политической арене двух весомых «нормативных сил» - российской и европейской, и, соответственно, сосуществование в политико-правовом поле двух проектов - их проекций. Европейская Будапештская конвенция к декабрю 2020 г. добилась ратификации в 65 государствах на пяти континентах, несмотря на право доступа к компьютерным данным из открытых источников без согласия страны-хранительницы данных для участников и отсутствия в тексте 2001 года многих актуальных угроз, таких как сетевое мошенничество и ботнеты [10]. Последние берёт в расчёт российский проект конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности», за который проголосовали 88 государств, но который столкнулся с оппозицией 55 других членов ООН – стран НАТО и ЕС [11]. Между тем фундаментальных противоречий с Будапештской конвенцией проект конвенции ООН не содержит. Их статьи 20-22 и 21-27 созвучны (с учётом того, что российский проект более детализирован в

техническом плане), а предложение создать «межправительственный комитет экспертов … для разработки международной конвенции о противодействии использованию ИКТ в преступных целях» [12] не мешает членам Совета Европы и дальше добиваться глобального признания Будапештской конвенции. Или, что более продуктивно, работать в международном экспертном комитете и продвигать свои нормы по борьбе с киберпреступностью, ставшие с 2001 г. более созвучными с вниманием к государственным функциям и превентивным мерам по обеспечению безопасности – а значит, более универсальными в глобальном масштабе. О последнем свидетельствуют Директива ЕС 2016 г. и Закон ЕС о кибербезопасности – если в первой на государства возлагаются обязанности по созданию групп быстрого реагирования, разработке стратегий и планов взаимодействия, а к обеспечению безопасности подключаются частные компании, то во втором Агентство ЕС по кибербезопасности – ENISA - обязуется содействовать развитию потенциала защиты государств-членов [8]. При этом ЕС остаётся на международной арене авторитетным нормотворцем, а его инициативы позитивно воспринимаются на международной арене. Такая кооперация нормативных сил, комбинирующая европейский нормотворческий авторитет, российскую инициативу, основанную на наблюдении за техническими трендами, и следование тенденциям в обеспечении кибербезопасности может дать миру единые правила по защите от киберпреступности.

Конечно, ничего из описанного выше не возникнет само собой – и дальнейшее формулирование правил в рамках ГПЭ и РГОС, и нормотворчество по профилю киберпреступности, и глобальный режим по кибербезопасности требуют дополнительных усилий от всех участников мирового сообщества. В рамках формирования международного режима современные «киберсилы» - прежде всего, США, КНР, Россия, в некоторой степени ЕС – должны конкретнее прописывать в своих соглашениях «запретные» для кибератак сферы, последствия за нарушения запретов и механизмы разрешения конфликтов. Когда это будет прописано, соглашения можно будет брать за основу кодексов, конвенций и резолюций. В сфере унификации норм по борьбе с киберпреступностью от участников – сейчас это главным образом Совет Европы и ЕС, Россия и её союзники по ШОС и БРИКС – требуется не отвергать инициативы друг друга, а сверять их, дополнять имеющиеся документы тем, что соответствует актуальным трендам, вести постоянный диалог по гармонизации, желательно на базе ООН, формулируя единый и универсальный подход к балансу между достижением безопасности и защитой суверенитета. Наконец, нормотворческая работа ГПЭ и РГОС должна продолжаться, а результаты её – дополнять друг друга. Дабы избежать дублирования диалога, но совершенствовать взаимодополнение, можно создать единую группу, в которой ГПЭ и РГОС были бы подкомитетами с чётко разделёнными полномочиями. В этом может помочь формат Программы действий по ответственному поведению в киберсреде, который оставляет место для рабочих групп по конкретным вопросам, чтобы не утяжелять повестку, не требуя при этом от своих участников обязательного достижения консенсуса и протекая как экспертный диалог [13]. Наконец, всему этому требуются механизмы имплементации на национальном уровне, которые ещё предстоит разработать.

Единые нормы, принципы и правила по кибербезопасности и борьбе с киберпреступностью возможны – для их выработки и принятия создано достаточно механизмов, постепенно отлаживающих свою работу и уже признавших кибербезопасность подчинённой единым международным нормам. Для более спорных сфер механизмы

находят сами международные отношения – соглашения об «неприкосновенных инфраструктурах» и последствиях за их атаки имеют перспективы стать режимом и сгладить острые углы в гуманитарном праве кибербезопасности, а у механизма межправительственного комитета экспертов, особенно если к нему присоединятся СЕ и ЕС, есть потенциал для дальнейшей унификации права по борьбе с киберпреступностью. Главное – приложить международные усилия и сосредоточиться на глобальных вызовах, а не локальных противоречиях.

Источники:

1. А. Толстухина - Лучше две киберрезолюции, чем ни одной // РСМД URL: https://russiancouncil.ru/analytics-and-comments/analytics/luchshe-dve-kiberrezolyutsii-chem-ni-odnoy/
2. О. Шакиров - Широкий киберконсенсус // РСМД URL: https://russiancouncil.ru/analytics-and-comments/analytics/shirokiy-kiberkonsensus/
3. Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report // UN General Assembly URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
4. Томильцева Д. А. Примирение как воспроизводство мира: теоретические возможности переосмысления // Полития. 2013. №4 (71).
5. Киберкодекс чести. Эксперт ЦПУР Олег Шакиров — о новых международных договоренностях по кибербезопасности // Коммерсантъ URL: https://www.kommersant.ru/doc/4856188
6. Koch H. H. International Law in Cyberspace // HARVARD INTERNATIONAL LAW JOURNAL. 2012. №54.
7. Э. Верхелст, Я. Ваутерс Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций: образование, наука, новая экономика. 2020. №2.
8. The U.S.-China Cyber Agreement: A Good First Step // Rand Corp. URL: https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html
9. Е. Черненко - Кибер любит тишину // Коммерсантъ URL: https://www.kommersant.ru/doc/4866452
10. Конвенция о компьютерных преступлениях // Совет Европы URL: https://rm.coe.int/1680081580
11. Россия открыла в ООН сезон охоты на киберпреступников // Совет Европы URL: https://www.kommersant.ru/doc/3803933?from=doc_vrez
12. Проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности // МИД РФ URL: https://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3025418
13. A. Gery, F. Delerue – A new UN path to cyber stability // Cyber Digital Europe URL: https://directionsblog.eu/a-new-un-path-to-cyber-stability/