«Международно-правовые стандарты обеспечения кибербезопасности. Первоочередные задачи»

М. А. Кочубей, руководитель Научно-консультативного совета, Антитеррористический центр СНГ

Тезис первый. Международно-правовую систему обеспечения кибербезопасности (как и безопасности в целом) нельзя рассматривать вне исторического контекста и актуальной структуры мироустройства.

Тезис второй. По состоянию на сегодняшний день международно-правовой системы обеспечения кибербезопасности как таковой не существует.

Тезис третий. Первоочередные задачи правовых стандартов обеспечения кибербезопасности будут решаться вне международного правового поля в привычном его понимании; будут задействованы аттракторы правовых полей национальных государств и их союзов.

Аргументы в пользу первого тезиса.

Обобщенно можно сказать, что в Новой истории система международной безопасности выстраивались по результатам Тридцатилетней европейской войны в 1648г. Именно тогда сложилась Вестфальская система международных отношений. Ее основные положения:

- приоритет национального интереса,

- государственный суверенитет как фундаментальное положение,

- принцип баланса сил,

- принцип действия международного права и регулярной дипломатической практики.

Первая мировая война и ее результаты (речь идет об уничтожении крупнейших европейских монархий) на короткое время сформировали обновленную модель безопасности. Возник даже международно-правовой регулятор – Лига наций.

В Новейшей истории Вестфальский мир был модифицирован по результатам Второй мировой войны. Речь идет о Ялтинско-Потсдамском мировом порядке. Именно по его лекалам формировалась система безопасности, в том числе международно-правовые регуляторы - ООН и ряд других структур. Женевские конвенции образца 1947 г. сформировали матрицу безопасности, в том числе правовые схемы «агрессии», «войны» и т.д.

Эта матрица была уничтожена в результате югославского кризиса, когда авиация НАТО бомбила Белград. В еще большей степени кризис мировой системы правового обеспечения безопасности проявился во время грузино-осетинского военного конфликта, вошедшего в историю как война «08.08.08». Причина находится на поверхности – понятия «войны» и «агрессии», на которые опирается международное право, морально устарели. Достаточно сказать, что в положениях Женевских конвенций само понятие агрессии напрямую связано с понятием «страны-победительницы», это СССР, США, Великобритания. Более того, субъектами агрессии и войны признаются именно государства, тогда как в современном мире источниками угроз, находящимися вне контроля каких-либо международных правовых институтов, стали негосударственные акторы – незаконные вооруженные формирования, международные террористические организации, объединения типа «Анонимус» и т.д.

В сухом остатке – действующие международно-правовые регуляторы (в том числе ООН) вполне эффективны в вопросах мира, но совершенно недееспособны в условиях войн и даже локальных военных конфликтов. Это принципиально важный момент.

Очень многие политологи и юристы в качестве базовой причины этого явления называют глобализацию в сочетании со сложившимся однополярным миром. В одном из своих выступлений председатель Европейского совета Херман ван Ромпей даже заявил, что такие понятия как «Родина», «государство» и «суверенитет» следует выбросить на свалку истории. На мой взгляд, это ложные тезисы. Очевидно, что однополярного мира больше не существует, а государственный суверенитет проявил поразительную выживаемость. Другое дело, что и Вестфальский, и Ялтинско-Потсдамский мир формировались и существовали в условиях принципиально другого технологического уклада, чем современный мир.

Смена технологического уклада – вот ключ к пониманию выстраивания новой системы международно-правовой безопасности, в том числе в киберпространстве.

Соответственно, смена парадигмы правового обеспечения международной безопасности произойдет либо по результатам новой большой войны, либо по результатам урегулирования множества современных военных конфликтов, в том числе реализуемых в киберпространстве, на что уйдет не менее десяти лет.

Аргументы в пользу второго тезиса.

Почему не складывается международно-правовая система обеспечения кибербезопасности? В то время как на национальном и субрегиональном уровне такие нормы уже формируются.

Основная причина связана, главным образом, с жесткой конкуренцией национальных и групповых интересов. В ближайшей перспективе они неразрешимы. Кибератвность военного типа, которая приходит на смену международному терроризму, или, по крайней мере, обеспечивает его апгрейд, - это не самостоятельное явление, а инструмент решения геополитических задач, своего рода форма диалога между наиболее значимыми субъектами современного мира (это и государства, и транснациональные корпорации и другие негосударственные акторы). Кибератвность военного типа – это своего рода аргумент в дискуссии об установлении контроля над ресурсами (самыми разнообразными, в том числе промышленными, энергетическими, человеческими и т.д.).

Приведу пример, образующий прямую аналогию. До настоящего времени мировое сообщество не смогло разработать универсального и принятого всеми государствами-членами ООН понятия терроризма. С точки зрения юридической техники это относительно несложная задача. Но ООН образовывала и расформировывала 34 (!) специальные комиссии для ее решения, пока не признала бесплодность таких попыток. Примерно то же самое сейчас происходит и в связи с попытками формирования глобальных универсальных правовых стандартов в сфере обеспечения кибербезопасности.

Вторя причина связана с неравномерностью ландшафта национального законодательства разных государств. Если в соответствии с ч.4 ст.15

Конституции Российской Федерации нормы международного права доминируют над нормами национального законодательства и подлежат имплементации в случае подписания и ратификации международного правового акта, то в законодательстве США такого приоритета нет. Конституция США не рассматривает нормы международного права как приоритетные/доминирующие по отношению к нормам национального права. Соответственно, нормы международного права будут применяться по принципу целесообразности, подчиняясь национальным интересам. Конституционные механизмы соблюдения норм международного права обеспечивают либо не обеспечивают следование международным стандартам.

Приведу пример. Так, по определению ООН, киберпреступность – это совокупность преступлений, которые совершаются с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. И большинство государств и научных центров ориентируется именно на такое понимание киберпреступности.

Однако, важны детали. А что следует понимать под киберпространством? Здесь начинаются серьезные расхождения.

Согласно определению Объединенного командования США, распространенному в 2006 г., под киберпространством понимается «место, где электронный и электромагнитный спектр используется для хранения, модификации и обмена данными через сетевые системы и соответствующие физические инфраструктуры». Это широкая формулировка, которая, по словам представителей ВВС США, позволит новому командованию работать с такими угрозами, как отслеживание финансовых потоков, использования GPS, радаров, средств глушения и др. В задачи будет входить защита собственных данных и подавление чужих источников информации. В указанном докладе (он был распространен в сенате США) отмечается: «Доминирование в киберпространстве выходит за рамки телекоммуникаций и информационных технологий и требует превосходства по всему электромагнитному спектру - от постоянного тока до дневного света, включая радиоволны, макроволны, инфракрасное излучение, рентгеновские лучи, направленную энергию, а также области, о которых мы еще даже не начали задумываться, для обеспечения глобального командования и управления, глобального доступа и глобальной мощи». Конец цитаты.

Мы не можем вывести позицию военных за рамки нашего внимания, когда предпринимаем попытки сформулировать стратегию борьбы с преступлениями в киберпространстве и защиты инфраструктуры от диверсий. Очевидно, что объекты, функционирование которых зависит от постоянного тока, радиоволн, рентгеновского излучения и ряда других полей, которые военные относят к киберпространству, используются в самой большей степени обычными людьми в обычной мирной жизни.

Допустимо ли причинение вреда некомбатантам, которые используют такие источники энергии, электромагнитные поля для обычной жизни? В какой степени это нарушит их естественные права? Думаю, все понимают, что этот вопрос находится не только в сфере военного права, но и в сфере правового обеспечения кибербезопасности населения. И, к сожалению, этот вопрос не только остается открытым, он практически не обсуждается на юридических площадках.

Есть еще один немаловажный момент, связанный с пониманием самой сущности кибербезопасности. В юридическом пространстве, к сожалению, и до настоящего времени имеет место смешение понятий «информационные войны» и «кибернетические войны», а ведь это понятия хотя и совпадающие, но не идентичные.

Этот аспект хорошо прослеживается при анализе документов Международного союза электросвязи, действующего под эгидой ООН. Вот их названия:

- Глобальная программа кибербезопасности
- Руководящие указания для детей по защите ребенка в онлайновой среде
- Руководящие указания для родителей, опекунов и учителей по защите ребенка в онлайновой среде
- Руководящие указания для отрасли по защите ребенка в онлайновой среде
- Руководящие указания для директивных органов по защите ребенка в онлайновой среде
- Элементы для создания глобальной культуры кибербезопасности

Очевидно, что основные усилия Союза были сконцентрированы на контентных киберугрозах и способах их смягчения. Однако, дело совсем разладилось, когда на конференции Международного союза электросвязи в Дубаи фактически произошел раскол организации. Под предлогом нечетких формулировок (например, что считать «нежелательным массовым сообщением») делегации США, Австралия, Канада и ряд стран ЕС покинули конференцию.

Хочу обратить внимание коллег на еще одну проблему, которая в принципе плохо подлежит структурированию, поскольку находится скорее в области философии управления. Технологии управления обществом с определенной долей условности можно разделить на «белые», «серые» и «черные». Им соответствуют различные модели нормативной регламентации и субъектности. Объективно во всем мире «серые» технологии управления стремительно расширяются (в пользу этого тезиса свидетельствует хотя бы и статистика терроризма, масштабов деятельности ЧВК, находящихся практически вне официальной юрисдикции, профашистских организаций и т.д.), заметно потеснив потенциал «белых» технологий, связанных с эффективным применением легальных норм права. Но решать задачу противодействия «серым» технологиям современное общество упорно желает с помощью технологий легальных и юридически оформленных. Это похоже на поиск потерянного ключа исключительно «под фонарем».

В результате «немощь» легальных субъектов, которые должны бы были отвечать за правовое обеспечение кибербезопасности, весьма эффективно компенсируется энтузиазмом и специальными навыками неконвенциональных игроков, которые действуют не в иерархичных, а летучих сетевых структурах.

Иллюстрация новейших событий. В Украине объявилась «Киберсотня», которая ведет пока что контентную войну. Атаке подвергся не только сайт Президента России и официальный сайт Банка России. Пресс-служба сайта крымского референдума (referendum2014.org.ua) сообщила, что ресурс подвергся DDoS-атаке. Установлено, что сканирование серверов перед атакой производилось с территории Иллинойсского университета, расположенного в городах Урбана и Шампейн в США. Напомню, что в городе Урбана с населением 37 тысяч человек присутствует большое количество подсетей, значительно превышающих потребности города, а также 3 (!) аэропорта. За организацией «Киберсотни» стоит Таллинский Объединенный центр передового опыта по кибероборонe НАТО. Артур Сузик и группа специалистов Таллинского центра уже работает в Киеве «для координации электронной войны».

Практически одновременно начала работу группа «КиберБеркут», на их сайте размещена очень интересная информация, в целом соответствующая объявленным намерениям. Именно «КиберБеркут» обнародовал телефонный разговор верховного представителя Евросоюза по иностранным делам и политике безопасности Кэтрин Эштон и главой МИД Эстонии Урмаса Паэта.

Это классический пример реализации «серых» технологий негосударственными акторами, и, разумеется, вне какого бы то ни было правового поля. Это вторжение в киберпространство другого государства «под чужим флагом». Вот это и есть реальное положение вещей.

Аргументы в пользу третьего тезиса.

Шесть стран-участниц ШОС еще в апреле 2011 года издали рекомендательный «Кодекс поведения государств в области международной информационной безопасности». Его цель – определить права и обязанности государств в области информации, чтобы сделать их поведение более конструктивным и ответственным, а также стимулировать сотрудничество на этом направлении, не нарушая прав и фундаментальных свобод человека. Этот документ ШОС предложил вниманию ООН в качестве образца для выработки единого подхода (в августе 2013г. в Нью-Йорке провела заседание Правительственная Экспертная Группа, созданная Генеральной Ассамблеей ООН с целью выработки единого подхода к проблеме Информационной безопасности и киберпреступлений).

Президент России В. Путин выдвинул инициативу преобразовать существующую региональную структуру ШОС по борьбе с терроризмом в универсальный Центр по борьбе с террористическими угрозами на пространстве ШОС. Этот будущий Центр будет механизмом скоординированного и систематизированного сотрудничества стран-участниц ШОС в сфере противодействия любым угрозам безопасности и стабильности. В рамках такого подхода эксперты разработали межправительственное соглашение для стран ШОС о сотрудничестве в сфере международной информационной безопасности. В нем даны определения угрозам информационной безопасности и выделены принципы, области, формы и механизмы сотрудничества, включая и то, как страны-участницы должны координировать свои действия и оказывать взаимную поддержку при противостоянии на этом направлении.

В условиях де-факто разворачивающейся гонки «информационных вооружений» позиция Российской Федерации в области международной информационной безопасности заключается в недопущении использования информационно-коммуникационных технологий для силового разрешения межгосударственных противоречий. Российская сторона выступает за выработку универсального международно-правового документа, констатирующего наличие угроз международной информационной безопасности военно-политического, преступного, в том числе террористического, характера, и предусматривающего возможность

осуществления совместных мер по минимизации ущерба национальным интересам отдельных государств и интересам международного сообщества в целом. Россия и ряд других стран выступили с инициативой принятия Генеральной ассамблеей ООН кодекса поведения, который способствовал бы достижению мира и безопасности в киберпространстве. Постоянные представители Китая, России, Таджикистана и Узбекистана направили генеральному секретарю ООН Пан Ги Муну обращение с призывом утвердить Кодекс поведения, регламентирующий использование странами информационных технологий. Кодекс призван обеспечить международную стабильность, способствовать борьбе с киберпреступностью и предотвращению использования киберпространства в террористических целях.

Особые моменты – электронные расследования, судебное преследование в условиях экстерриториальности актов или смешанной юрисдикции. Терминологический консенсус, необходимый для запуска Проекта международных расследований, достигнут, скорее всего, не будет. Особое значение, кроме того, в этом контексте приобретает вопрос о соотношении традиционного суверенитета и кибернетического суверенитета. Очевидно, что они пересекаются, но не совпадают. Киберрасследования в любом случае должны быть формализованы через уголовно-процессуальное законодательство, в том числе в случае создание межгосударственных следственно-оперативных групп. По УПК какого государства будут действовать такие группы? Этот вопрос напрямую связан с правовым (политическим) и кибернетическим суверенитетом, и он остается открытым.

Государства-участники ОБСЕ приняли в ноябре 2007 года Решение Совета министров о защите важнейших объектов энергетической инфраструктуры от террористических актов [MC.DEC/6/07], согласно которому они обязуются сотрудничать и рассматривать все необходимые меры на государственном уровне для обеспечения соответствующей защиты ВОЭИ от террористических атак. В соответствии с решением, Антитеррористическое подразделение ОБСЕ (АТП) организовало 11-12 февраля 2010 года в Вене, по инициативе Соединенных Штатов Америки, Экспертный семинар по вопросам государственно-частного партнерства в области защиты неядерной энергетической инфраструктуры от террористических актов. Анализ работы этой площадки показал, что европейцы в сфере обеспечения кибербезопасности критически важных объектов энергетической инфраструктуры пошли точно по такому же пути, что и Россия, т.е. сформировали и реализуют приемы и схемы защиты на основе национального опыта и национального законодательства с последующим переводом наиболее эффективных правовых и технологических решений на субрегиональный уровень в европейских масштабах.

В России обеспечение безопасности КВО ТЭК от кибератак развивается достаточно нетрадиционным, но вполне эффективным способом.

Собственно говоря, именно КВО ТЭК стали полигоном для разработки, отточки и апробирования соответствующих правовых, управленческих, инженерных технологий и решений. Несомненно, что сама матрица формирующейся системы киберзащиты будет спроецирована и на другие системные объекты, не связанные с ТЭК. В этом смысле очевидно, что Минэнерго и Минтранс России проводят гигантскую работу, поскольку фактически «прокладывают лыжню» для других секторов экономики и социального управления. Заслуживает уважения та последовательная и высокопрофессиональная позиция, которую предъявляют оба эти ведомства при решении задач обеспечения безопасности КВО ТЭК.

С правовой точки зрения здесь важен и еще один момент. Матрица обеспечения кибербезопасности КВО ТЭК в России, как и в Европе, выращивается «снизу». Никаких «руководящих разъяснений» от глобальных международных структур уровня ООН в виде глобальных конвенций ждать не следует, в ближайшие годы их не будет. А проблема защиты КВО ТЭК актуализируется на глазах. Полагаю, что решение о «строительстве дома с очень приблизительным архитектурным проектом» в сложившейся геополитической и геоправовой ситуации является единственно правильным, что, разумеется, не снимает необходимости проработки вопроса и на уровне глобальных международных структур.

Представим некоторый обзор развития национальных практик по данному вопросу.

Отчасти по результатам деятельности ОБСЕ в **Евросоюзе** 19 июня 2013 года вступила в силу Стратегия кибербезопасности**.** Согласно документу, полномочия Европейского агентства сетей и информационной безопасности продлены на следующие семь лет. Правительствам стран ЕС предписано создать органы, отвечающие за кибербезопасность, а финансовым, транспортным и энергетическим компаниям — разработать меры по противодействию киберугрозам. Еще одной мерой должно стать создание единого рынка продуктов киберзащиты. Создатели программы рассчитывают на сотрудничество между частным и государственным секторами.

В феврале 2011 года в **Германии** была принята «Стратегия безопасности в киберпространстве» и основано Национальное агентство киберзащиты. Последнее взаимодействует с полицией, разведкой и Федеральным управлением по информационной безопасности. В стратегии есть секретная часть, предполагается, что она посвящена системе контрмер против информационных атак.

В мае 2011 года **США** обнародовали «Международную стратегию по действиям в киберпространстве», в которой объявили о готовности использовать любые средства для нейтрализации угроз — дипломатические, информационные, военные и экономические. В июле стало известно о

собственной стратегии действий в киберпространстве Пентагона, основанной на «**тактике активной обороны**». В ней кибератаки приравниваются к военным действиям с возможностью реагировать на них как на акт агрессии.

В мае 2013г. стратегия в области кибербезопасности принята в **Индии.** На основе документа будет создана сеть правительственных агентств, дополнительные средства пойдут на исследовательские программы в области кибербезопасности. В рамках стратегии 150 инженеров Организации оборонных исследований и разработок Индии (DRDO) уже ведут разработку собственной независимой операционной системы.

10 июня 2013 года аналогичный документ принят в **Японии.** Он, в частности, предполагает создание базы данных зараженных сайтов, проведение ежегодных учений (имитаций) атак, создание к 2016 году центра кибербезопасности с широкими полномочиями.

Специальные структуры по борьбе с кибертерроризмом и кибердиверсиями созданы, как вы знаете, в США, Германии, Китае, Иране, Израиле, Франции, ряде других государств. Соответствующее решение прорабатывается в российском военном ведомстве.

В ноябре 2013г. Совет Федерации провел парламентские слушания, посвященные «**Концепции стратегии кибербезопасности РФ**». Основные положения: создать национальную систему защиты от кибератак, усилить ответственность за киберпреступления и создать преимущества для отечественных IT-компаний. Концепция предусматривает разделение ответственности за защиту в этой сфере: государство должно заниматься правовым регулированием, а также координацией усилий участников процесса; бизнес — обеспечивать безопасность критической инфраструктуры, находящейся в частной собственности, внедрять и соблюдать стандарты; общество — повышать уровень цифровой грамотности и участвовать в оценке усилий государства и бизнеса. В экспертную группу сенатора Гаттарова входили в основном представители бизнеса и НКО — "Лаборатории Касперского", InfoWatch, CISCO, а также Ru-Center, РАЭК, РАРИО и других структур. Ранее этой темой занимались Совбез, Минкомсвязь, ФСБ, МВД и МИД.

Основная проблема (помимо конкуренции ведомств) – разночтения ключевых терминов. Термин «кибербезопасность» используется в западных странах, а Россия активно продвигает понятие «информационная безопасность». В ООН Россия внесла для рассмотрения **концепцию Конвенции международной информационной безопасности.**

Примечательно, что к угрозам информационной безопасности отнесены действия, совершаемые с целью подрыва политической, экономической и социальной систем другого государства, психологическую обработку населения.

И в заключение. Кибервойна уже идет. Однако, нормы международного права не могут дать ответы на следующие вопросы: Когда кибервойна считается начавшейся? Кто является ее субъектами? Каков статус комбатантов и некомбатантов? Каковы допустимые действия в ходе кибервойны? И если гиперболизировать ситуацию – какого цвета знамя и над каким городом должно быть поднято, чтобы кибервойна считалась завершенной?