Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС[1, 2]

Э. Верхелст, Я. Ваутерс

Верхелст Энн – соискатель степени доктора философских наук в области международного права, Лёвенский центр изучения глобального управления и Института международного права, Лёвенский католический университет, н.с. Исследовательского фонда – Фландрия (FWO); Belgium, Leuven, Oude Markt, 13; E-mail: anne.verhelst@kuleuven.be

Ваутерс Ян – профессор по международному праву и международным организациям, директор Лёвенского центра исследований в области глобального управления и Института международного права при Лёвенском католическом университете; Belgium, Leuven, Oude Markt, 13; E-mail: jan.wouters@ggs.kuleuven.be

Множественные киберинциденты, зафиксированные в последние годы, наглядно показывают, что кибербезопасность стала частью международной повестки. Несколько международных организаций выдвинули инициативы в области управления киберпространством, в частности, Организация Объединенных Наций и Европейский союз. ООН и ЕС стремятся играть ведущую роль в сфере политики по обеспечению устойчивости перед киберугрозами. Тем не менее указанные инициативы до сих пор не обеспечили создание надлежащих регулирующих норм. В представленной статье рассматриваются факторы, осложняющие развитие нормотворчества в киберпространстве и управление киберпространством в международном измерении, а также схожие проблемы, характерные для права Европейского союза. Авторы отвечают на вопрос, являются ли данные препятствия неотъемлемой характеристикой нормотворческого процесса в рамках ООН или ЕС или же их возникновение обусловлено природой киберпространства, в частности, его опорой на передовые технологии. В рамках статьи инициативы ООН рассматриваются в контексте деятельности Группы правительственных экспертов ООН. Более ранние отчеты Группы можно рассматривать в качестве предтечи некоего opinio juris в сфере международного права по вопросам регулирования киберпространства, а дискуссия на площадке Генеральной Ассамблеи ООН демонстрирует отсутствие консенсуса в международном сообществе по рассматриваемому вопросу. В статье также рассматриваются две законодательные инициативы ЕС: Директива ЕС по сетевой и информационной безопасности 2016 г. и Закон о кибербезопасности ЕС 2019 г.

Ключевые слова: кибербезопасность; глобальное управление; международное право; Европейский союз; законотворчество; нормативно-правовое регулирование; Группа правительственных экспертов ООН; Рабочая группа открытого состава; Директива ЕС по кибербезопасности; закон о кибербезопасности ЕС

Для цитирования: Верхелст Э., Ваутерс Я. (2020) Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций. Т. 15. № 2. С. 141–172 (на русском и английском языках). DOI: 10.17323/1996-7845-2020-02-07

---

[1] Статья поступила в редакцию в феврале 2020 г.

[2] Перевод статьи A. Verhelst, J. Wouters "Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives" выполнен с согласия авторов А.А. Игнатовым, м.н.с. Центра исследований международных институтов Российской академии народного хозяйства и государственной службы при Президенте РФ (РАНХиГС).

Введение

В последние два десятилетия кибербезопасность стала неотъемлемым компонентом международных отношений. Несмотря на политическую природу проблемы обеспечения кибербезопасности, в данной сфере до сих пор не созданы надлежащие механизмы международного регулирования. К перечню наиболее очевидных причин, объясняющих подобную инертность, относятся неопределенность масштаба, природы, сущности и понятийного аппарата кибербезопасности [Futter, 2018, p. 202, 209; Nye, 2017, p. 68][3]. Не существует универсального подхода к определению кибербезопасности [European Court of Auditors, 2019]. Эксперты используют этот термин по-разному, в зависимости от контекста [Futter, 2018, p. 205; Kosseff, 2018, p. 995; Kshetri, 2016, p. 3; Schartz, Bashroush, Wall, 2017, p. 53–57]. Авторы обращаются к понятию «кибербезопасность» *sensu stricto*, то есть далее не будут рассматриваться такие вызовы безопасности, как киберпреступность[4], кибертерроризм [Dinniss, 2018; Ivanov, 2015; Fidler, 2015, p. 10–11] и использование кибертехнологий в военных целях [Shmitt, 2017][5].

Данная статья не нацелена на изучение институтов, занимающихся разработкой государственной политики или правовых норм, касающихся перечисленных вызовов кибербезопасности [Council of Europe, 2001][6]. Определение кибербезопасности, которое использует Организация Объединенных Наций (ООН), было предложено Международным союзом электросвязи (МСЭ), а позднее доработано Н. Кшетри (N. Kshetri):

> *«Кибербезопасность подразумевает технологии, концепции, меры государственной политики, процедуры и практики, направленные на защиту активов (компьютеров, инфра-*

[3] Терминологическая неопределенность имеет практическое измерение: определение кибербезопасности в рассматриваемом контексте зависит от того, *что, от кого и каким образом* пытаются защитить, а также от того, возможна ли атрибуция возможностей. Расплывчатость определений означает, что не в каждом случае возможно определить, кто должен принимать ответственность за обеспечение кибербезопасности, что наверняка приведет ко всевозможным затруднениям практического и правового характера.

[4] Понятие «киберпреступность» может быть определено как «преступная деятельность, осуществляемая в основном при помощи компьютеров или компьютерных сетей». Примерами могут служить совершаемые таким образом кражи, нарушение тайны частной жизни, распространение нежелательного контента и вымогательство. Согласно некоторым источникам, к киберпреступности могут быть отнесены кибератаки на критическую инфраструктуру [Kshetri, 2016, p. 3; 2009, p. 141–144]. В рамках данной статьи мы рассмотрим Директиву ЕС по сетевой и информационной безопасности, направленную на защиту критической инфраструктуры; Директива не делает различий между тем, подпадают ли подобные атаки под определение «киберпреступность» или нет. Примерами региональных механизмов, предназначенных для борьбы с киберпреступностью, могут служить Будапештская конвенция о киберпреступности от 23 ноября 2001 г. (вступила в силу 1 июля 2004 г.) и Конвенция Африканского союза о кибербезопасности и защиты персональных данных от 27 июня 2014 г. (вступила в силу 3 июня 2019 г.) [Council of Europe, 2001; African Union, 2014; Orji, 2018].

[5] Далее мы убедимся, что многочисленные инициативы в области обеспечения кибербезопасности охватывают лишь небольшую часть обширной правовой системы, например, защиту критической инфраструктуры (Директива ЕС по сетевой и информационной безопасности), защита частных данных в сети (Генеральный регламент ЕС о защите персональных данных), ведение войны с применением кибертехнологий [Shmitt, 2017]. Следовательно, определение или концепция кибербезопасности зачастую определяются конкретной правовой средой [Kosseff, 2018, p. 985].

[6] Спустя 19 лет после официального подписания 64 государства ратифицировали данную конвенцию [Pupillo, 2018, p. 4].

структуры, приложений, услуг, систем связи и информации) и киберпространства от атак, нанесения ущерба и неавторизованного доступа» [ITU, 2008][7].

В тексте Закона о кибербезопасности Европейского союза (ЕС) используется следующее определение:

«Кибербезопасность означает деятельность, необходимую для защиты сетей и информации, пользователей информационных сетей и иных сторон, которые могут быть затронуты киберугрозами» [European Union, 2019, p. 1].

В последнее время с подачи ООН[8] и ЕС[9] было выдвинуто множество инициатив, затрагивающих различные аспекты кибербезопасности. ООН и ЕС стремятся играть ведущую роль в сфере политики по обеспечению устойчивости перед киберугрозами. Оба института демонстрируют исключительно интересные – и во многом несовпадающие – подходы к нормотворчеству, так как первый является уникальной в своем роде международной организацией, а второй – региональной[10] организацией[11] особого типа. В рамках статьи авторы сравнили подходы указанных институтов к обеспечению кибербезопасности *sensu stricto*.

Авторы статьи пытаются найти ответ на вопрос, как и до какой степени могут быть восполнены лакуны в системе глобального управления в сфере кибербезопасности путем изучения современных тенденций в области международного киберправа и инициатив ООН и ЕС. На уровне общих понятий авторы проанализировали способность международного права адекватно решать проблемы кибербезопасности, в частности, какие препятствия возникают на данном направлении. Далее авторы отвечают на вопрос о том, каким образом кибербезопасность может быть вписана в систему международного права. Вслед за этим авторы рассматривают деятельность Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций (далее – ГПЭ ООН) на предмет наличия в них правового консенсуса. Наряду с проблематикой регулирования киберпространства в глобальном масштабе в рамках статьи рассматриваются региональные инициативы в данной области. ЕС представил множество решений, связанных с различными аспектами обеспечения кибербезопасности. Следует отметить две законодательные инициативы: Директиву ЕС о сетевой и информационной безопасности 2016 г. (далее – Директива) [European Union,

[7] Определение было принято в ходе Полномочной конференции МСЭ в Гвадалахаре (Мексика) в 2010 г. [Kshetri, 2016, p. 3].

[8] Например, Глобальная программа УНП ООН по борьбе с киберпреступностью, Глобальный индекс кибербезопасности МСЭ, Программа «Цифровые “голубые каски” ООН», а также доклады ГПЭ ООН Первого комитета Генеральной Ассамблеи ООН.

[9] Примерами могут служить Стратегия кибербезопасности ЕС 2013 г., создание ENISA (Европейское агентство по сетевой и информационной безопасности), Рамочная концепция ЕС о защите от киберугроз 2014 г. с дополнениями 2018 г., проекты в области защиты от киберугроз в рамках Постоянного структурного сотрудничества по вопросам безопасности и обороны (PESCO), Совместные рамки борьбы с гибридными угрозами 2016 г., Сообщение об усилении системы устойчивости ЕС к киберугрозам и развитии конкурентоспособной и инновационной отрасли кибербезопасности (2016) и Рамочная концепция совместного дипломатического противодействия незаконной деятельности в киберпространстве 2017 г. («Набор инструментов кибердипломатии Европейского союза»).

[10] Особую роль здесь играют наднациональные институты ЕС, подробнее об этом см. в разд. V. См. также: [Schemers, Blokker, 2018, para 60–61, 60–62].

[11] Сейчас уже можно обнаружить тенденции к регионализации повестки в области кибербезопасности, см.: [Henriksen, 2019, p. 5–7].

2016, p. 1] и Закон о кибербезопасности ЕС 2019 г. Проведенный анализ позволил сделать вывод о том, какие препятствия существуют на международном уровне и в рамках законодательства ЕС. В заключительном разделе авторы представляют несколько выводов относительно самой необходимости регулирования киберпространства силами ООН и ЕС. Авторы отвечают на вопрос, являются ли выявленные затруднения неотъемлемой характеристикой нормотворческого процесса в рамках ООН и ЕС или же их возникновение обусловлено природой киберпространства, в частности, его опорой на передовые технологии. Кроме того, статья представляет вывод о том, какая форма регулирования отношений в киберпространстве является наиболее эффективной, обоснованной и перспективной.

Кибербезопасность и международное право: заклятые друзья

Факторы, обуславливающие трудности применения норм международного права в сфере кибербезопасности

К настоящему моменту ООН еще не выработала международную конвенцию по кибербезопасности. Несколько факторов объясняют трудности, которые возникают при попытке совместить существующий порядок создания норм международного права и реалии киберпространства [Tranter, 2007, p. 449].

Высокий темп и технологичность киберреволюции

Цифровизация мира идет небывалыми темпами [Niemann, 2018]. Ожидается, что к концу 2020 г. в мире будет более 20 млрд цифровых устройств [Reuters, 2018][12]. В отличие от того, как создатели норм международного права действовали в XX в., создавая, например, концепцию «исключительной экономической зоны» [United Nations, 1982][13] в рамках морского права и обеспечивая защиту морского дна, определяя его статус как «общего наследия человечества» [United Nations, 1970], киберреволюция идет с такой скоростью и настолько непредсказуемо, что законодатели не поспевают за инновациями [Kittichaisaree, 2017, p. 336].

Суверенность, территориальность, фрагментация юрисдикции и юридической атрибуции

Основой международного права является государственный суверенитет, который, однако, с трудом вписывается в реальность киберпространства [Vergne, Duran, 2014, p. 126–139]. Несмотря на достигнутый консенсус относительно реализации государственного суверенитета в киберпространстве [United Nations, 2017, p. 11], за что нужно поблагодарить ГПЭ ООН, ни одно из существующих государств не может претендовать на суверенитет, который бы охватывал все киберпространство [Schmitt, 2017; Sandage et al., 2013, p. 184]. Так происходит потому, что многие элементы инфраструктуры, на базе которых существует киберпространство, находятся в пределах разных суверенных территорий [Schmitt, 2017] и, следовательно, согласно международному праву, относятся к разным юрисдикциям. Тем не менее Дж. Трачтмэн справедливо отмечает, что раз-

[12] Подсчеты исследовательской компании Gartner [Reuters, 2018; Sandage et al., 2013, p. 1].

[13] Конвенция ООН по морскому праву принята в Монтего-Бэй 10 декабря 1982 г. и вступила в силу 16 ноября 1994 г.

деление юрисдикций не должно быть основанием для отказа от регулирования всего киберпространства: в конце концов, действия в киберпространстве все равно осуществляются на конкретной территории, равно как и их последствия ощущаются в конкретной области [Trachtman, 2013, p. 88]. Тот факт, что отдельные проблемы выходят за рамки конкретных юрисдикций, не является чем-то новым для международного права (вспомним, например, международное морское право, открытый космос, изменение климата). Основные проблемы связаны с юридической атрибуцией: зачастую нелегко определить, кто ответственный, откуда исходит кибератака или кто играет роль посредника [Kshetri, 2016, p. 7; Wheeler, Larsen, 2003, p. 1]. Именно атрибуция представляет наибольшую трудность [Trachtman, 2013, p. 26, 88; Shackelford, Russel, Kuehn, 2016, p. 10; Healey, 2012]. Даже уже существующие нормы киберправа могут утратить свою эффективность, столкнувшись с проблемой атрибутирования [Fidler, 2015, p. 6, 15][14].

Государство vs частный сектор

Третьим фактором, усложняющим взаимоотношения между кибербезопасностью и международным правом, является проблема совместимости ролей государства и частного сектора в киберпространстве [Groupe UMP Assemblée nationale, 2009]. В киберпространстве ведущая роль принадлежит производящим отраслям и частному капиталу. Негосударственные институты осуществляют управление киберпространством в отсутствие каких-либо формальных рамок, что сужает поле деятельности для субъектов нормотворчества (национальных государств) [Hoisington, 2017, p. 95]. М. Хойзингтон (M. Hoisington) утверждает, что неформальное управление представляет собой не что иное, как реликт *lex mercatoria*, частного предпринимательского права времен Средневековья. В этой связи уместен вопрос, должны ли государства контролировать частные компании в киберпространстве, и если да, то до какого предела необходимо расширять рамки правового регулирования деятельности частного сектора в данной области. С другой стороны, нужно определить границы эффективности регулирования кибербезопасности в случае, если в подготовке и имплементации данных правил не участвуют негосударственные акторы.

Роль государства как арбитра киберпространства является предметом ожесточенных дискуссий. С одной стороны, можно утверждать, что национальные государства обязаны устанавливать правовые рамки, ограничивающие или иным способом направляющие деятельность частных компаний в киберпространстве. В данном случае аргументом «за» является перечень обязанностей государств в соответствии с нормами международного права: защита прав человека, поддержание международного мира и безопасности, следование принципу «не навреди» [United Nations, 2006], защита критической инфраструктуры[15] и т.д. Данные обязательства могут быть соблюдены в киберпространстве только при условии, если соответствующие права и обязанности возлагаются и на негосударственных акторов [Kittichaisaree, 2017, p. 22, 335–352].

С другой стороны, существуют доводы против широкого участия государств в регулировании киберпространства: (i) для частного сектора не существует серьезных стимулов для сотрудничества с государственными инстанциями, так как последние могут помешать реализации коммерческих интересов первых [Teplinsky, 2013, p. 310] (репутационный ущерб, прямое воздействие со стороны конкурентов при помощи создавае-

[14] Автор рассуждает об этой проблеме в контексте применения соглашений о киберпреступности для защиты критической инфраструктуры от киберугроз.

[15] См. разд. IV настоящей статьи.

мых технологий); (ii) меры контроля замедляют инновационное развитие [Contreras et al., 2013, p. 1115, 1119]; а также (iii) частный сектор предпочитает иметь дело с нормами частного права как альтернативы уголовному праву [Wall, 2007, p. 25–27]. Альтернативным решением может стать регулирование киберпространства на базе юридически обязательных (или не являющихся таковыми) норм корпоративной этики, которые будут выработаны непосредственно работающими в киберпространстве негосударственными институтами[16].

Описанные подходы не должны восприниматься как взаимоисключающие [Trachtman, 2013, p. 90]: вывод о том, нужно ли в принципе и насколько активно следует участвовать государствам в регулировании киберпространства, зависит от рассматриваемой сферы. «Выбор в пользу того или иного института зависит от предполагаемой эффективности рыночных механизмов, частных компаний, государств или международного права в решении той или иной проблемы» [Ibid.][17]. Немаловажно и то, что Директива налагает обязательства на отдельных представителей частного бизнеса, фактически признавая, что в киберпространстве невозможно обойтись без подобного рода партнерства.

Доводы в пользу применения существующих норм и создания новых

Нужно ли применять существующие нормы международного права в киберпространстве или же должны быть созданы новые, более подходящие для современных вызовов? М. Хойзингтон определил три варианта разрешения обозначенной дилеммы: i) проблемы кибербезопасности должны решаться в соответствии с существующими нормами и в рамках уже созданных структур международного права; ii) киберпространство построено на фундаментально иных законах и, следовательно, требует создания новых правовых норм и структур; iii) существующие нормы могут применяться для обеспечения кибербезопасности, но те из них, которые не соотносятся с уникальной природой отношений в киберпространстве, должны быть отброшены [Hoisington, 2017, p. 87]. Уже представленные международные инициативы больше всего соответствуют первому утверждению: ГПЭ ООН заявила, что международное право, включая Устав ООН, может применяться в киберпространстве (разд. III). *Tallinn Manual* в своей второй редакции переносит основные концепции международного права в киберпространство (следует отметить пункты 1–24), в частности, применяет их в отношении кибервойны.

Кибермания

Кибермания – еще один феномен, осложняющий установление взаимопонимания между международным правом и кибербезопасностью [von Heinegg, 2012, p. 5; Kshetri, 2016, p. 2]. Последние достижения в области киберправа как такового можно охарактеризовать как ограниченные, тогда как со стороны академического сообще-

[16] Над подобным сводом корпоративных норм работает НИСТ (Национальный институт стандартов и технологий). НИСТ сводит воедино согласованные стандарты и наилучшие корпоративные практики в интересах выработки гибкого и экономически эффективного подхода для обеспечения безопасности в киберпространстве для оказания поддержки владельцам и операторам критически важной инфраструктуры в противодействии киберугрозам. Кроме того, НИСТ сотрудничает с правительствами Великобритании, Японии, Южной Кореи, Эстонии, Израиля и Германии. Тем не менее в деятельности НИСТ есть существенный недостаток: его рекомендации недостаточно эффективны для защиты предприятий от целенаправленных и хорошо спланированных кибератак. См.: [Shackelford, Russell, Kuehn, 2016, p. 42].

[17] Выбор в данном случае отражает «истинный смысл понятия “субсидиарность”».

ства и политиков «законам кибервойны» уделяется огромное внимание. М. О'Коннел утверждает, что кибератаки в Эстонии, получившие широкое медийное освещение (2007), киберинциденты во время российско-грузинского конфликта (2008) и ситуация вокруг сетевого червя Stuxnet (2010) создали вокруг мер, принимаемых в интересах кибербезопасности, ореол милитаризованности [O'Connell, 2012, p. 191]. Большинство киберинцидентов на самом деле не пересекают условный рубеж, за которым их можно отнести к «вооруженному нападению» в терминах ст. 51 Устава ООН [ENISA, 2015][18]. Киберугрозы имеют более сложную и многогранную природу и чаще всего угрожают частным компаниям[19].

Промежуточные выводы

Учитывая рассмотренные выше вызовы, становится понятно, почему до сих пор не представлена международная конвенция по вопросам кибербезопасности *sensu stricto*. Ближе всего к категории международной конвенции в рассматриваемой области подходит инициатива ООН, выработанная ГПЭ ООН. Далее мы рассмотрим правовую сущность докладов Группы правительственных экспертов.

Группа правительственных экспертов ООН

Проблематика обеспечения информационной безопасности впервые была включена в повестку ООН в 1998 г., когда Российская Федерация представила Первому комитету ГА ООН проект соответствующей резолюции. Генеральная Ассамблея приняла Резолюцию 53/70 без голосования [United Nations, 1998]. Начиная с 2004 г. ГПЭ ООН анализирует угрозы, возникающие вследствие расширения сферы применения информационно-коммуникационных технологий (ИКТ) в контексте обеспечения международной безопасности, и меры противодействия этим угрозам. Работа ГПЭ сфокусирована на проблемах международного права параллельно с изучением существующих и возникающих вызовов, норм, правил и принципов, мер по укреплению доверия и наращивания потенциала [Ibid., 2020]. Отчеты ГПЭ ООН за 2013 и 2015 гг. в данном контексте наиболее важны. В отчете 2013 г. ГПЭ ООН заявила, что международное право, в частности, Устав ООН, следует применять и в физическом, и в киберпространстве [Ibid., 2013, para 19]. Под этим подразумевается государственный суверенитет и принципы, связанные с понятием «суверенитет». Например, государство обладает юрисдикцией над цифровой инфраструктурой на своей территории, следовательно, государство несет ответственность за международные противоправные действия в киберпространстве, исходящие с его территории [Ibid., para 20; Schmitt, 2017, para 1–13]. В отчете 2015 г. ГПЭ ООН выделила следующие принципы Устава ООН и международного права, применимые в отношении поведения государств в киберпространстве: «государственный суверенитет, суверенное равенство, разрешение споров мирными средствами и невмешательство во внутренние дела других государств» [Ibid., 2015, para 28b]. Перемещение в киберпространство основных принципов международного права, которые в большинстве своем имеют обязательный характер и/или были закреплены решениями Международного суда ООН, должно происходить при соблюдении широкого консенсуса [Henriksen,

[18] Следует также учитывать вышедшие позже доклады.

[19] Преамбула Директивы ЕС, п. 2. См. также: [D'Elia, 2014].

2019, p. 4][20]. Некоторые государства, включая «сверхдержавы», спустя время подтвердили применимость международного права в своих комментариях к докладам ГПЭ ООН и отдельными пунктами стратегий кибербезопасности [République Français, 2018, para 82, 85, 87; Australian Government, 2016, para 7, 28, 40–41; Government of the Russian Federation, 2016, para 34; Gov.UK, 2016, para 63]. «Группа двадцати» одобрила применимость норм международного права в киберпространстве в 2015 г. [G20, 2015, para 26]. Доклады ГПЭ ООН свидетельствуют о формировании консенсуса и определенного *opinio juris* по рассматриваемой проблеме, что важно для создания полноценных международных норм [Wouters, Ryngaert, De Baere, Ruys, 2018, pp. 149–152; Haggenmacher, 1986, p. 5; Bedeman, 2010; Bradley, 2016][21]. Следует отметить, что деятельность государств в киберпространстве, как правило, осуществляется скрытно и имеет противоречивый характер [Väljataga, 2018, p. 4–5].

Тем не менее в июне 2017 г. по итогам 50-й встречи ГПЭ ООН все более или менее значимые зачатки *opinio juris* были окончательно растоптаны. Проявились фундаментальные противоречия между 25 членами ГПЭ, в частности, по вопросам о праве на самооборону и о применении международного гуманитарного права в ходе столкновений в киберпространстве. Делегация Кубы не поддержала прямую отсылку к праву государства на самооборону применительно к киберпространству, заявив, что это приведет к «легитимизации войн с применением ИКТ» [Soesanto, D'Incau, 2017]. Кубинская, российская и китайская делегации выступили с инициативой о создании принципиально нового свода международных правил и о созыве специальной Рабочей группы Генеральной Ассамблеи, открытой для участия всех государств и руководствующейся в принятии решений принципами «прозрачности, инклюзивности и полноценного участия». Делегация США интерпретировала это как попытку обнулить достигнутый ГПЭ ООН прогресс [Bowcott, 2017]. Как отмечалось ранее, в 2013 г. ГПЭ ООН заявила о применимости Устава ООН в киберпространстве, в частности ст. 51, которая утверждает право государств на индивидуальную и коллективную самооборону. Схожее утверждение содержится и в докладе 2015 г.[22] Аргументация кубинской делегации имела не юридический, а скорее политический характер. В 2017 г. итоговый доклад так и не был опубликован. К концу 2018 г. стало очевидно, что ГПЭ ООН зашла в тупик [Soesanto, D'Incau, 2017; Bowcott, 2017; Henriksen, 2019, p. 6–13].

В декабре 2018 г. ГА ООН нашла выход из ситуации, инициировав два независимых процесса для обсуждения проблем безопасности при использовании ИКТ на период с 2019 по 2021 г. Резолюцией 73/27, активно поддержанной Россией [Ruhl et al., 2020], ГА ООН учредила Рабочую группу открытого состава (РГОС), что приветствовали представители Кубы и Китая [United Nations, 2018a]. Одиннадцать дней спустя Генеральная Ассамблея приняла резолюцию по результатам работы шестой Группы правительственных экспертов ООН, которая теперь известна как «Группа правительственных экспертов ООН на 2019–2021 гг. по поощрению ответственного поведения государств

[20] Эти фундаментальные принципы раз за разом воспроизводятся в Tallinn Manual 2.0 как своего рода базовая правовая доктрина киберпространства.

[21] Следует отметить, что состав членов ГПЭ ООН ограничен, однако в 2013 и 2015 гг. в работе Группы принимали участие представители наиболее влиятельных держав: США, Великобритании, Китая и России.

[22] В 2015 г. ГПЭ ООН в следующих выражениях подтвердила применимость международного гуманитарного права: «(d) Группа отмечает существующие принципы международного права, в том числе, в соответствующих случаях, принципы гуманности, необходимости, пропорциональности и индивидуализации» [ООН, 2015, para 28.d].

в киберпространстве в контексте международной безопасности» [United Nations, 2018b]. Эту резолюцию поддержали США. Необходимо отметить, что хотя РГОС открыта для участия представителей всех заинтересованных сторон[23], в 2019–2021 гг. в ее работе принимают участие представители 25 государств: Австралии, Бразилии, Китая, Эстонии, Франции, Германии, Индии, Индонезии, Японии, Иордании, Казахстана, Кении, Маврикия, Мексики, Марокко, Нидерландов, Норвегии, Румынии, Российской Федерации, Сингапура, ЮАР, Швейцарии, Великобритании, США и Уругвая [Ibid., para 3; Ruhl et al., 2020]. В то время как ГПЭ ООН занимается нормами, правилами, принципами, мерами укрепления доверия и наращивания потенциала, а также тем, как международное право может применяться в киберпространстве[24], РГОС может продолжить разработку или менять существующие нормы, правила и принципы, упомянутые в Резолюции 73/27, меры укрепления доверия и наращивания потенциала, изучать применимость международного права в киберпространстве, существующие и потенциальные угрозы, создать постоянную диалоговую площадку на базе ООН и соответствующие международные механизмы для защиты глобальных информационных систем [United Nations, 2018a, para 5]. Следует подчеркнуть, что «пересекающиеся сферы полномочий ГПЭ ООН и РГОС потенциально могут повысить их эффективность, однако нужно помнить, что РГОС была создана в соответствии с предложением России, замещая, таким образом, предложение США о создании еще одной ГПЭ» [Ruhl et al., 2020][25].

На рис. 1 представлен график работы Группы правительственных экспертов ООН (ГПЭ) и Рабочей группы открытого состава (РГОС) на 2019–2021 гг.

[23] Некоторые эксперты считают, что это свидетельствует о стремлении России привлечь к участию как можно больше государств, разделяющих ее цели в киберпространстве, см.: [Grisby, 2018; Iasiello, 2019].

[24] См.: Geneva Internet Platform, Digital Watch Observatory (https://dig.watch/processes/un-gge#view-7541-3).

[25] Авторы считают, что указанные форматы работы не только конкурируют между собой, но рискуют перейти к открытому конфликту. Они утверждают, что «США и их союзники рассматривают РГОС как площадку для взаимодействия с новыми стейкхолдерами, которые будут поддерживать существующие нормы, разработанные Группой правительственных экспертов. Россия, напротив, скорее склоняется к ревизии устоявшихся норм через механизмы РГОС в соответствии со своими интересами. В то время как в 2015 г. ГПЭ заявила о применимости норм международного гуманитарного права в киберпространстве, РГОС создавалась без учета данного положения». См.: [Iasiello, 2019]: «РГОС провела общую встречу в середине сентября 2019 г. Многие разногласия, связанные, например, с международным гуманитарным правом, которые ранее препятствовали достижению консенсуса, проявились вновь. Представители Китая и России в Группе правительственных экспертов не поддерживали развитие данного направления, однако другие государства-члены, например, Египет, выступили в ее поддержку, в меньшей степени педалируя важность данной проблематики в сравнении с остальными. Гораздо важнее то, что государства, лишенные возможности выразить свою позицию в рамках ГПЭ, обрели голос. Такие государства, как Иран, получили возможность заявить о своей позиции по обсуждаемым вопросам. Расширение состава членов РГОС отвечает интересам Китая, Ирана и России, которые демонстрируют схожесть позиций в вопросах регулирования киберпространства. Кроме того, формат дискуссии, открытый для каждого государства – члена ООН, дает им возможность выдвигать на передний план приоритетные вопросы, например, цифровой суверенитет (и все связанные с данной концепцией явления, например, контроль над нежелательной информацией), заручаясь поддержкой малых государств, которые не имели бы права голоса в рамках ГПЭ. Именно поэтому авторитарные или закрытые государства поддерживают предложения Китая и России. Неудивительно, что страны Запада, такие как Австралия, Великобритания и США, выступили против создания РГОС».

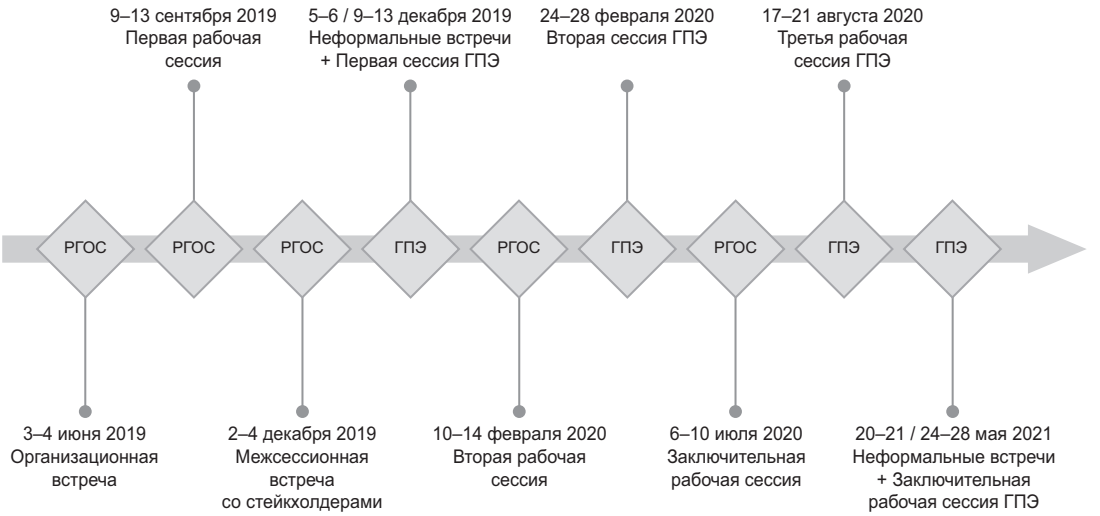

Рис. 1. График работы ГПЭ и РГОС на 2019–2021 гг.

Источник: Управление ООН по вопросам разоружения (https://www.un.org/disarmament/ict-security/).

В контексте деятельности РГОС мы анализируем документы, принятые по итогам рабочих встреч и находящиеся в свободном доступе: i) организационная встреча 3–4 июня 2019 г. [United Nations, 2019a; 2019b]; ii) первая рабочая встреча 9–13 сентября 2019 г. [Ibid., 2019c; 2019d][26]; iii) неформальная встреча со стейкхолдерами 2–4 декабря 2019 г.[27] и iv) вторая рабочая встреча 10–14 февраля 2020 г.[28] Анализ документов показал, что РГОС в настоящее время находится на этапе обмена мнениями по вопросу о приоритетах деятельности Рабочей группы. В частности, представители стран-членов высказали мнение, что «новые (существующие) ГПЭ и РГОС должны оказывать взаим-

[26] См. также: OEWG Chair's letter to Member States on the First Substantive Session; Updated list of experts for the presentations on the six areas outlined in paragraph 5 (a) – (f) of the provisional agenda of the OEWG (A/AC.290/2019.1) as of 28 August 2019 (https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/280819-Updated-list-of-experts-first-substantive-session-OEWG-on-developments-in-the-field-of-information-and-telecommunications.pdf).

[27] OEWG Chair's letter to the Member States for the intersessional meeting (1 November 2019); Chair's letter to the Participants of the OEWG informal intersessional consultative meeting (26 November 2019); Calendar of Side Events; OEWG Chair's letter on the summary report of the informal intersessional consultative meeting from 2–4 December 2019 (28 January 2020). См.: Open-ended Working Group. United Nations Office for Disarmament Affairs (https://www.un.org/disarmament/open-ended-working-group/).

[28] Неполный список документов включает: The OEWG Chair's letter to Member States on the second substantive session; Chair's working paper for the second substantive session; Draft Programme of Work for the second substantive session; Tentative draft structure of the report (substantive component); Background paper on existing UN bodies and processes related to the mandate; Background paper on International Law in the GGEs; Background paper on Regular institutional dialogue; OEWG Chair's letter to Member States for the second substantive session (4 February 2020); Draft Organization of Work of the second substantive session. См.: Open-ended Working Group. United Nations Office for Disarmament Affairs (https://www.un.org/disarmament/open-ended-working-group/). Следует также обратить внимание на опубликованные материалы, представленные отдельными странами, а также неформальные предложения со стороны международных организаций. См. также: [Kaspar, Kumar, 2019].

ную поддержку и сглаживать противоречия»[29]. Анализ документов, опубликованных по итогам неформальной встречи и первой рабочей сессии ГПЭ в декабре 2019 г., приводит к схожим результатам[30]. Подобный исход ожидаем, поскольку РГОС обязана предоставить отчет о своей деятельности к 75-й сессии Генеральной Ассамблеи, которая состоится во второй половине 2020 г.[31] Группа правительственных экспертов ООН предоставит свой отчет в ходе 76-й сессии ГА ООН в 2021 г. [United Nations, 2018b, para 3].

Сегодня никто не возьмется утверждать, особенно в свете последних событий, что в 2013 и 2015 гг. ГПЭ ООН своими отчетами представила некий *opinio juris* от лица всего международного сообщества, однако эти отчеты доказывают применимость международного права в киберпространстве. Пока трудно сказать, к каким результатам придут РГОС и ГПЭ, в частности, будут ли пересмотрены принципы международного права, что в конечном счете приведет к выработке международного консенсуса, или, напротив, изначально существующие политические противоречия сведут на нет любые попытки выработать взаимоприемлемое решение. А. Хенриксен утверждает, что стагнация процесса по линии ГПЭ ООН в 2017 г. приведет к появлению региональных инициатив, например, на уровне ЕС[32]. Насколько это утверждение может соответствовать действительности, мы рассмотрим в следующем разделе.

Директива ЕС 2016 г. и Закон о кибербезопасности 2019 г.

Анализ документов ЕС по проблемам кибербезопасности доказывает стремление Евросоюза занять в данной сфере лидирующую позицию[33].

Директива ЕС стала первым в своем роде юридически обязательным документом горизонтального прямого действия в сфере кибербезопасности *sensu stricto.* Целью Директивы является защита критической инфраструктуры (поставщиков жизненно важных и цифровых услуг) от кибератак, которые могут оказать «существенный разрушительный эффект» [European Union, 2016, article 6]. Европейский Парламент и Совет ЕС приняли Директиву 6 июля 2016 г. со сроком имплементации странами-членами до

[29] OEWG, Chair's working paper in view of the Second substantive session (10–14 February 2020) (https://www.un.org/disarmament/wp-content/uploads/2020/01/191231-oeeg-chair-working-paper-second-substantive-session.pdf).

[30] На момент написания данной статьи документы второй сессии ГПЭ ООН (24–28 февраля 2020 г.) еще не были опубликованы.

[31] United Nations Office for Disarmament Affairs, Fact Sheet Intergovernmental Processes On The Use Of Information And Telecommunications In The Context Of International Security 2019–2021 (https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+and+GGE+processes+-+2.pdf).

[32] Хенриксен утверждает, что регионализация систем обеспечения кибербезопасности в виде правовых подсистем различной глубины является нежелательной с учетом глобального распространения сети Интернет. Тем не менее он признает, что регионализация повестки кибербезопасности дает определенные преимущества, позволяя, например, избежать продолжительного периода обсуждения, способствуя достижению консенсуса по более сложным вопросам и т.п. [Henriksen, 2019, p. 6]. Незадолго до провала ГПЭ в 2017 г., советник президента США по внутренней безопасности Том Боссерт заявил, что «настало время рассмотреть иные подходы <...> США продолжат работать с небольшой группой партнеров-единомышленников» [Bossert, 2017].

[33] См., например: [European Union, 2019, recital 15; European Commission, 2013a, p. 7, 11; 2013b, p. 5; 2018, p. 1; Westby, 2019; Fantin, 2019; Niebler, 2019]. См. также примечание 7 (номера сносок в английском оригинале и в данной статье расходятся, в исходной версии ссылка была под номером 13. – *Примеч. пер.*).

9 мая 2018 г. Цель Директивы была сформулирована следующим образом: «...обеспечить высокий средний уровень сетевой и информационной безопасности» [European Union, 2016][34]. Принятие Директивы было обусловлено отсутствием правовых норм в области кибербезопасности в законодательстве стран ЕС. Даже после принятия соответствующих норм между странами – членами Евросоюза сохранялись значительные расхождения. Европейские законодатели были обеспокоены тем, что «масштаб, частотность и организованность кибератак возрастают; они могут привести к неспособности частного бизнеса выполнять свои функции, существенным финансовым потерям в масштабах всей экономики ЕС и создать угрозы в социальной сфере» [Ibid.][35].

Директива накладывает множество обязательств на страны-члены, включая обеспечение минимального уровня национальной готовности путем назначения компетентных органов, ответственных за выполнение положений Директивы, создания групп быстрого реагирования, разработки национальных стратегий и планов взаимодействия[36]. Немаловажно, что Директива накладывает обязательства на две категории частных компаний: поставщиков жизненно важных и цифровых услуг[37]. Для них список обязательств включает: i) принятие соответствующих технических и организационных мер для противодействия угрозам информационной безопасности; ii) подготовку и внедрение планов обеспечения непрерывности деловой деятельности; iii) информи-

[34] Преамбула Директивы, разд. 4.

[35] Преамбула Директивы, разд. 2.

[36] Каждое государство-член обязуется поддерживать минимальный уровень готовности, для этого они обязаны назначить ответственные за реализацию Директивы органы [European Union, 2016, article 8], создать группы реагирования на компьютерные кризисы (“Computer Emergency Response Teams” – CERTs или “Computer Security Incident Response Teams” – CSIRTs) [Ibid., 2016, article 9], а также разработать и принять соответствующие национальные стратегии сетевой и информационной безопасности и планы взаимодействия [Ibid., article 7]. Национальные органы должны сотрудничать друг с другом в сетевом формате, обеспечивающем безопасность и эффективность взаимодействия, включая обмен информацией, обнаружение и реагирование на сетевые и информационные угрозы на всем пространстве ЕС. Государства-члены должны обмениваться информацией и сотрудничать в интересах предотвращения сетевых и информационных угроз согласно Плану взаимодействия Европейского союза для обеспечения сетевой и информационной безопасности [Ibid., article 11]. Важнейшей обязанностью государств-членов является составление списка поставщиков жизненно важных услуг [Ibid., article 5]. Кроме того, требуется развитие культуры риск-менеджмента [Ibid., part 4, 44]; частный сектор и государственные институты должны взаимодействовать и обмениваться информацией [Ibid., part 35]. См. также: [Roex, 2016].

[37] Директива фокусируется на двух типах частных компаний (ст. 1, 4, 5, 14, 16): (i) поставщики жизненно важных услуг и (ii) поставщики цифровых услуг. Согласно п. 2 ст. 15 Директивы, поставщики жизненно важных услуг определены как «компании, обеспечивающие предоставление услуг, критически важных для поддержания социальной и/или экономической активности, при этом предоставление данных видов услуг опирается на сетевые и информационные системы, а инциденты, связанные с нарушением безопасности данных систем, могут препятствовать предоставлению данных услуг». Приложение II Директивы содержит приблизительный список секторов, в которых государства-члены должны определить ключевых поставщиков жизненно важных услуг. Список включает: банковский сектор, фондовый рынок, транспортировку и распределение энергии, воздушный, железнодорожный и морской транспорт, здравоохранение, интернет-услуги и государственные услуги. Вне правовых рамок Директивы остаются объекты применения ядерной энергии [Lemmens, 2018]. К поставщикам цифровых услуг, на которых также распространяются обязательства в рамках Директивы, отнесены онлайновые торговые площадки, поисковые системы и «облачные» сервисы. Все они указаны в Приложении III Директивы. При подготовке документа остальные виды цифровых услуг были оценены как не столь важные [Roex, 2019]. Директива не обязывает государства-члены составлять список ключевых поставщиков цифровых услуг, оставляя им свободу действий [Markopoulou et al., 2019, p. 4].

рование групп реагирования о всех значимых инцидентах, связанных с информационной безопасностью. До сих пор не ясно, что в рамках Директивы включается в понятие «существенный разрушительный эффект»[38]. Остается открытым вопрос о том, как это понятие будет применяться на практике.

Далее мы переходим к Закону о кибербезопасности ЕС, принятому Постановлением 2019/881 Европейского парламента и Совета ЕС от 17 апреля 2019 г. о Европейском агентстве по кибербезопасности (ENISA) и о сертифицировании технологий в области информационной и коммуникационной безопасности [European Union, 2019]. Постановление вступило в силу 27 июня 2019 г. Правовым базисом Постановления выступает ст. 114 Договора о функционировании Европейского союза (TFEU). Постановление тем самым направлено на реализацию задачи построения функционирующего внутреннего рынка согласно ст. 26 Договора [Ibid., 2012; Mitrakas, 2018, p. 411]. Принятие закона о кибербезопасности было обусловлено рядом факторов, в частности, стремлением ЕС занять лидирующую позицию на международном рынке технологий безопасности наряду с осознанием того, что существующая система не может обеспечить своевременное противодействие определенным угрозам, о чем свидетельствуют недавние кибератаки [Fantim, 2019]. По сути, данный закон впервые представил систему сертифицирования технологий цифровой безопасности на всем пространстве ЕС[39]. Подобная система призвана снизить риск фрагментации единого рынка[40] и повысить конкурентоспособность ЕС на глобальном уровне [Mitrakas, 2018, p. 411]. Наличие сертификата будет свидетельствовать о том, что продукт или услуга соответствуют заданным критериям и обеспечивают определенный уровень защищенности от киберугроз [Ibid., p. 413][41]. Одним из важных положений Закона является требование к государствам-членам о назначении одного или более компетентных органов для выполнения задач по сертифицированию, либо о наделении соответствующими функциями органов другого государства при наличии соответствующей договоренности[42]. Кроме того, Закон наделяет ENISA постоянным мандатом и более широким набором функций[43]. Статья 6 Закона о кибербезопасности указывает, что ENISA будет содействовать государствам-членам в развитии их потенциала (например, в разработке и внедрении принципов распространения информации об уязвимостях[44] и создании национальных групп экстренного реагирования, что напрямую связывает Закон о кибербезопасности с Директивой[45], однако указанные меры не являются юридически обязательными.

[38] Отдельные указания относительно того, что следует понимать под «существенным разрушительным эффектом», содержатся в ст. 6, 14 и 16 Директивы, а также в разд. 27, 28 и 38 Преамбулы.

[39] Это было сделано в интересах создания единого рынка ИКТ-продукции и услуг, на что указано в ст. 51 Закона о кибербезопасности. Следует также обратить внимание на цели системы сертификации, перечисленные в той же статье.

[40] Например, во Франции уже существует собственная система сертификации “Certification Sécuritaire de Premier Niveau”. См.: [Mitrakas, 2018, p. 412].

[41] Отметим, что указанные меры в настоящее время имеют статус добровольных. По истечении четырехлетнего периода Европейская комиссия будет вправе наделить их обязательным статусом. См. [Fantin, 2019].

[42] Пункт 1 ст. 58 Закона о кибербезопасности.

[43] Таким образом, ЕС рассматривает ENISA как надежную инстанцию при решении вопросов, связанных с внедрением стандарта связи 5G. См.: [Fantin, 2019].

[44] Пункт 1.b ст. 6 Закона о кибербезопасности.

[45] Пункт 1.d ст. 6 Закона о кибербезопасности.

Кибербезопасность и право ЕС: непреодолимый антагонизм?

Ранее мы выделили пять факторов, обосновывающих трудности, связанные с созданием норм международного права в сфере кибербезопасности. Далее мы рассмотрим, какие из этих факторов имеют место в правовой системе ЕС.

Высокий темп и технологичность киберреволюции

Высокий темп и технологичность являются неотъемлемыми элементами киберреволюции, и этот факт находит отражение как в инициативах ООН, так и в решениях Европейского союза. Очевидно, что географическая ограниченность, эксклюзивность состава членов, а также принципиальность соблюдения определенных стандартов при вступлении в состав объединения, отсутствие за столом переговоров крупных кибердержав наряду с уже существующими правовыми инструментами, компетенциями и наднациональными структурами Евросоюза помогают объединению идти в ногу с киберреволюцией.

Суверенность, территориальность, фрагментация юрисдикции и юридической атрибуции

Отсутствие в киберпространстве каких-либо территориальных ограничений является его базовой характеристикой; предложения ООН и ЕС учитывают это обстоятельство. В контексте рассмотренной ранее Директивы следует отметить следующее: поскольку критическая инфраструктура стран Евросоюза в основном располагается внутри его границ (например, системы очистки воды, больницы, ж/д пути)[46] и, следовательно, внутри его собственной юрисдикции, страны ЕС могут обеспечивать ее защиту без опоры на международное право [Fidler, 2015, p. 9–10], тем самым не испытывая затруднений, связанных с фрагментацией юрисдикции. Схожий принцип заложен и в Законе о кибербезопасности, ст. 58 которого гласит:

> *«Каждое государство-член назначает один или несколько национальных органов по сертификации кибербезопасности на своей территории или, с согласия другого государства-члена, назначает один или несколько национальных органов по сертификации кибербезопасности, созданных в этом другом государстве-члене, для выполнения указанных задач. Национальные органы по сертификации кибербезопасности обязуются: (a) контролировать и применять правила... для мониторинга соответствия продуктов ИКТ, услуг ИКТ и процессов ИКТ требованиям европейских сертификатов кибербезопасности, которые были выданы на их соответствующих территориях...; контролировать и обеспечивать соблюдение производителями и поставщиками продуктов ИКТ, услуг ИКТ или процессов ИКТ правил, установленных на соответствующих территориях...»*[47].

Юридическая атрибуция и в данном контексте представляет наиболее проблемную область. Эта проблема характерна и для ЕС; в перспективе она может ослабить эффективность европейских инициатив в области кибербезопасности.

[46] Приложение II Директивы ЕС.

[47] Статья 58.1, ст. 58.7(a) и ст. 58.7(b) Закона о кибербезопасности.

Государство vs частный сектор

Киберпространство управляется частными институтами согласно неформальным правилам и нормам, что создает трудности как для ЕС, так и для ООН. Авторы Директивы указали на важность введения обязательств как для государственных органов, так и для представителей частного сектора, в частности, на поставщиков жизненно важных и цифровых услуг, перечисленных в Приложении II и Приложении III Директивы соответственно. ЕС обладает соответствующим опытом, правовыми инструментами и достаточно развитым внутренним рынком для внедрения подобных требований. Директива и Закон о кибербезопасности позволяют государствам – членам ЕС вводить меры наказания в случае несоблюдения положений упомянутых документов[48], но при этом нет никаких гарантий, что частный бизнес будет заинтересован сотрудничать с государством в ущерб своим коммерческим интересам, а новые правила не станут препятствием инновационному развитию. Все еще не ясно, как страны ЕС будут интерпретировать понятие «киберинцидент со значительным разрушительным воздействием» и смогут ли они добиться от поставщиков жизненно важных и цифровых услуг соблюдения обязательства об информировании соответствующих инстанций о подобных инцидентах[49], без чего Директива будет лишена смысла.

Доводы в пользу применения существующих норм и создания новых

Директива и Закон о кибербезопасности являются примерами норм, созданных после того, как проблема кибербезопасности приобрела политический оттенок. Евросоюз с его широкими возможностями в сфере нормотворчества может задавать геополитические параметры рассматриваемого вопроса, что в данной ситуации имеет определяющее значение.

Кибермания

Для Европейского союза всепроникающая сущность кибертехнологий представляет меньшую проблему, нежели для ООН, и, следовательно, данный фактор не нуждается в подробном разборе. ЕС не наделен подобным ООН мандатом в отношении поддержания международного мира и безопасности; различаются они и количеством государств-членов. ООН, в свою очередь, не имеет схожих с ЕС полномочий в области экономической политики и конкуренции, а также внутреннего рынка.

Юридическая обязательность

Как и любой закон ЕС, Закон о кибербезопасности носит юридически обязательный характер на всем пространстве Евросоюза с момента вступления в силу 27 июня 2019 г.[50] Директива ЕС также является юридически обязательным документом[51]. Тем не менее юридическая сила Закона и Директивы никак не превозносит их над не самы-

[48] Статья 21 Директивы ЕС и ст. 65 Закона о кибербезопасности.

[49] Статья 14.3 и ст. 16.3 Директивы ЕС.

[50] Статья 288, §2 Договора о функционировании Европейского союза: Art 288, para 2 TFEU: «Регламент имеет общее действие. Он является обязательным в полном объеме и подлежит прямому применению во всех государствах-членах».

[51] Статья 288, §3 Договора о функционировании Европейского союза: «Директива имеет обязательную силу для каждого государства-члена, кому она адресована, в отношении результата, которого требуется достичь, но оставляет в компетенции национальных инстанций выбор формы и способов достижения».

ми удачными инициативами ООН в сфере кибербезопасности. Нет ничего сложного в том, чтобы объяснить, каким образом в ЕС достигается консенсус относительно юридически обязательных мер. Помимо вполне очевидных причин (правовые инструменты в распоряжении ЕС, компетенции, наднациональные институты, клубный характер объединения), тот факт, что Директива вводит юридически обязательные меры для защиты критической инфраструктуры, не является чем-то чуждым для европейского права[52]; кроме того, подобные меры обеспечения кибербезопасности широко обсуждаются на международном уровне [European Commission, 2005; 2009; 2013c; United Nations, 2004; Melzer, 2011]. Директива и Закон о кибербезопасности стали продуктами отлаженного за долгие годы и прекрасно функционирующего внутреннего нормотворческого механизма ЕС.

На данный момент многое указывает на то, что практически все описанные факторы, которые затрудняют разработку мер в области кибербезопасности, являются неотъемлемыми свойствами кибербезопасности как таковой. Следовательно, они присутствуют как на международном, так и на региональном уровне, и воздействуют на нормотворческий процесс как на уровне ООН, так и в ЕС, несмотря на различия между институтами. Это не означает, что только ООН или только ЕС должен заниматься созданием норм в области кибербезопасности *sensu stricto.* Совсем недавно в ходе второй рабочей встречи РГОС представитель ЕС заявил:

> *«Европейский союз и страны – члены ЕС поддерживают дальнейшее взаимодействие в данной сфере с ключевыми международными и региональными партнерами и организациями, представителями гражданского, научного и делового сообществ в интересах избежания дублирования усилий и поиска возможностей для синергии и распределения ответственности для поддержания скоординированности и согласованности наших коллективных действий»*[53].

Заключение

В данной статье мы определили пять факторов, обуславливающих длительность процесса создания международной системы регулирования киберпространства и трудности применения международного права для обеспечения кибербезопасности. К этим факторам относятся высокая скорость осуществления деятельности в киберпространстве и цифровизации в международном масштабе; фрагментированная юрисдикция и сложность юридической атрибуции; проблематика соотношения роли государства и частного сектора в управлении киберпространством; целесообразность адаптирования существующих норм международного права к реалиям киберпространства; а также феномен «кибермании».

Европейский союз представил два юридически обязательных документа по вопросам кибербезопасности *sensu stricto.* До сих пор нет ясности, насколько эффективно будет осуществляться внедрение и исполнение обязательств, накладываемых данны-

[52] См. ст. 2 п. (a) в [Совет Европейского союза, 2008, p. 78], а также Приложение II в [European Commission, 2005, p. 20].

[53] EU Non-Paper on Capacity Building to Advance Peace and Stability in Cyberspace, for the Work of the Open-Ended Working Group on 'Developments in the Field of Information and Telecommunications in the Context of International Security', submitted to the second substantive session of the OEWG (10–14 February 2020) (https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/eu-non-paper-submission-oewg-2019.pdf).

ми документами[54]. Юридически обязательный характер Директивы ЕС и Закона о кибербезопасности ЕС не означает, что инициативы ООН в данной сфере обернулись провалом. Напротив, «мягкое право» может быть эффективнее любых формальных обязательств, что очень характерно для международного права [Wouters et al., 2018, p. 165–167; Pauwelyn et al., 2012, p. 159–160; Boyle, 1999, p. 901–912; Virally, 1983; Reisman, 1988]. Результаты работы ГПЭ ООН в 2004–2017 гг. доказывают, что международное право может применяться как для регулирования деятельности государств в киберпространстве, так и для достижения консенсуса между ведущими государствами (Китай, Россия, США). Тем не менее, ответив на вопрос «возможно ли», ГПЭ ООН зашла в тупик при ответе на вопрос «каким образом» [Henriksen, 2019, p. 2]. В настоящее время существует реальная опасность дробления процесса на платформе ООН на два направления – ГПЭ и РГОС, что снизит вероятность достижения консенсуса. Развитие системы обеспечения кибербезопасности на уровне ООН стагнирует скорее из-за политических, нежели правовых причин. В то же время для Европейского союза открывается «окно возможностей». В любом случае, неверно рассматривать вопрос о предпочтительной площадке для выработки норм в области кибербезопасности в рамках дихотомии ООН – ЕС. Вместо этого следует искать возможности для объединения усилий и синергии. Крайне неблагоприятным представляется исход, при котором политическая борьба и прочие разногласия поставят точку в данном процессе.

Источники

African Union (2014). Convention on Cyber Security and Personal Data Protection of 27 June 2014, entry into force on 3 June 2019. Режим доступа: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (дата обращения: 09.03.2020).

Albrecht D. (2018) Chinese Cybersecurity Law Compared to EU-NIS-Directive and German IT-Security Act // Computer Law Review International. Vol. 19. No. 1. P. 1–6. Режим доступа: https://doi.org/10.9785/cri-2018-190102.

Australian Government (2016). Australia's Cyber Security Strategy: Enabling Innovation, Growth and Prosperity. Department of Home Affairs. Режим доступа: https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf (дата обращения: 09.03.2020).

Bederman D. (2010) Custom as a Source of Law. Cambridge: Cambridge University Press.

Bowcott O. (2017) Dispute Along Cold War Lines Led to Collapse of UN Cyberwarfare Talks // The Guardian. 23 August. Режим доступа: https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges (дата обращения: 09.03.2020).

Boyle E. (1999) Some Reflections on the Relationship of Treaties and Soft Law // International and Comparative Law Quarterly. Vol. 48. No. 4. P. 901–913. Режим доступа: https://doi.org/10.1017/S0020589300063739.

Bradley C. (ed.) (2016) Custom's Future: International Law in a Changing World. Cambridge: Cambridge University Press.

Contreras J., de Nardis L., Teplinsky M. (2013) Mapping Today's Cybersecurity Landscape. American University Law Review. Vol. 62. No. 5. P. 1113–1130. Режим доступа: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1883&context=aulr (дата обращения: 09.03.2020).

[54] Причиной этому служат не только правовые особенности, которые мы рассмотрели в настоящей статье, но и политические мотивы. См., например: [Ducuing, 2019, p. 23–24; Albrecht, 2018, p. 1–6; Markapoulou et al., 2019, p. 1–11; Mitrakas, 2018, p. 411–441 : 4; Pupillo, 2018, p. 1–6; Fantin, 2019].

Council of Europe (2001). Budapest Convention on Cybercrime, ETS No 185, open for signature 23 November 2001, entry into force 1 July 2004. Режим доступа: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (дата обращения: 09.03.2020).

D'Elia D. (2014) La guerre économique à l'ère du cyberspace [Economic Warfare in the Cyberspace Era] // Hérodote. Vol. 152/153. No. 1. P. 240–260. Режим доступа: https://www.cairn.info/revue-herodote-2014-1-page-240.htm (дата обращения: 09.03.2020).

Ducuing C. (2019) On the Edge of the NIS Directive: The Proposed CITS Delegated Regulation, Friend or Foe? CiTiP Working Paper, KU Leuven Centre for IT & IP Law. Режим доступа: https://dx.doi.org/10.2139/ssrn.3486978.

European Commission (EC) (2005). Green Paper on a European Programme for Critical Infrastructure Protection. COM/2005/0576 final/. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52005DC0576 (дата обращения: 09.03.2020).

European Commission (EC) (2009). Protecting Europe From Large-Scale Cyber Attacks and Disruptions: Improving Preparedness, Security and Resilience. Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. COM (2009) 149 final. Режим доступа: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF (дата обращения: 21.04.2020).

European Commission (EC) (2013a). Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union. COM (2013) 48 final 2013/0027 (COD). Режим доступа: https://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-48-EN-F1-1.Pdf (дата обращения: 21.04.2020).

European Commission (EC) (2013b). Making European Critical Infrastructures More Secure. Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection. SWD (2013) 318 final. Режим доступа: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf (дата обращения: 21.04.2020).

European Commission (EC), High Representative of the European Union for Foreign Affairs and Security Policy (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, JOIN (2013) 1 final. Режим доступа: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (дата обращения: 21.04.2020).

European Commission (EC) (2018). Building Strong Cybersecurity in Europe. State of the Union, 12 September. Режим доступа: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_en.pdf (дата обращения: 21.04.2020).

European Court of Auditors (2019). Challenges to Effective EU Cybersecurity Policy. Briefing Paper, March. Режим доступа: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (дата обращения: 21.04.2020).

European Union (EU) (2008). Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection // Official Journal of the European Union, L 345/75. Vol. 51. P. 75–82. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.345.01.0075.01.ENG&toc=OJ:L:2008:345:TOC (дата обращения: 21.04.2020).

European Union (EU) (2012). Consolidated Version of the Treaty on the Functioning of the European Union // Official Journal of the European Union C 326. Vol. 55. P. 47–200. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.326.01.0001.01.ENG&toc=OJ:C:2012:326:TOC#C_2012326EN.01004701 (дата обращения: 21.04.2020).

European Union (EU) (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS Directive) // Official Journal of the European Union, L 194/1. Режим доступа: http://data.europa.eu/eli/dir/2016/1148/oj (дата обращения: 21.04.2020).

European Union (EU) (2018). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Com-

munications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // Official Journal of the European Union, L 151/1. Режим доступа: http://data.europa.eu/eli/reg/2019/881/oj (дата обращения: 21.04.2020).

European Union (EU) (2019). EU Non-Paper on Capacity Building to Advance Peace and Stability in Cyberspace, for the Work of the Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security," Submitted to the Second Substantive Session of the OEWG (10–14 February 2020). Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/eu-non-paper-submission-oewg-2019.pdf (дата обращения: 21.04.2020).

European Union Agency for Cybersecurity (ENISA) (2015). Annual Incident Reports 2015. Режим доступа: www.enisa.europa.eu/publications/annual-incident-reports-2015 (дата обращения: 21.04.2020).

Fantin S. (2019) Weighting the EU Cybersecurity Act: Progress or Missed Opportunity? CiTiP Blog, KU Leuven Centre for IT & IP Law. 19 March. Режим доступа: https://www.law.kuleuven.be/citip/blog/weighting-the-eu-cybersecurity-act-progress-or-missed-opportunity/ (дата обращения: 21.04.2020).

Fidler D. (2015) Wither the Web? International Law, Cybersecurity and Critical Infrastructure Protection // Georgetown Journal of International Affairs. Vol. 8. P. 8–20. Режим доступа: https://www.repository.law.indiana.edu/facpub/2452 (дата обращения: 21.04.2020).

Futter A. (2018) Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies // Journal of Cyber Policy. Vol. 3. No. 2. P. 201–216. Режим доступа: https://doi.org/10.1080/23738871.2018.1514417.

Geneva Internet Platform, Digital Watch Observatory (n. d.). UN GGE and OEWG. Режим доступа: https://dig.watch/processes/un-gge#view-7541-3 (дата обращения: 21.04.2020).

Gov.UK (2016). National Cyber Security Strategy 2016–2021. Режим доступа: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (дата обращения: 21.04.2020).

Government of the Russian Federation (2016). Doctrine of Information Security of the Russian Federation. Ministry of Foreign Affairs of the Russian Federation, 5 December. Режим доступа: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 (дата обращения: 21.04.2020).

Grigsby A. (2018) The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. Net Politics Blog. 15 November. Council on Foreign Relations. Режим доступа: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased (дата обращения: 21.04.2020).

Group of 20 (G20) (2015). G20 Leaders' Communiqué. Antalya, 15–16 November. Режим доступа: http://www.g20.utoronto.ca/2015/151116-draft-communique.pdf (дата обращения: 21.04.2020).

Groupe UMP Assemblée nationale (2009). Le législateur et les questions de société: quelle méthode pour quels choix? Rapport d'étape du groupe de travail animé par Hervé Mariton, député de la Drôme à la demande de Jean-François Copé [The Legislator and Questions for Society: Which Method for Which Choices? Progress Report for the Working Group Led by Hervé Mariton, Member of the Drôme at the Request of Jean-François Copé]. 12 May. Режим доступа: https://www.unaf.fr/IMG/pdf/rapport_d_etape_mai_2009.pdf (дата обращения: 21.04.2020).

Haggenmacher P. (1986) La doctrine des deux éléments du droit coutumier dans la pratique de la Cour Internationale [The Doctrine of the Two Elements of Cusstomary Law in the Practice of the International Court] // Révue générale de droit international public. Vol. 90.

Harrison Dinniss A. (2018) The Threat of Cyber Terrorism and What International Law Should (Try To) Do About It // Georgetown Journal of International Affairs. Vol. 19. P. 43–50. Режим доступа: https://doi.org/10.1353/gia.2018.0006.

Healey J. (2012) Beyond Attribution: Seeking National Responsibility for Cyberattacks. Issue Brief, Atlantic Council. Режим доступа: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/ (дата обращения: 21.04.2020).

Henriksen A. (2019) The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace // Journal of Cybersecurity. Vol. 5. No. 1. Режим доступа: https://doi.org/10.1093/cybsec/tyy009.

Hoisington M. (2017) Regulating Cyber Operations Through International Law: In, Out or Against the Box? Ethics and Policies for Cyber Operations / M. Taddeo, L. Glorioso (eds). Oxford: Springer International.

Iasiello E. (2019) OEWG or GGE: Which Has the Best Shot of Succeeding? // Technative. 5 December. Режим доступа: https://www.technative.io/oewg-or-gge-which-has-the-best-shot-of-succeeding/ (дата обращения: 21.04.2020).

International Telecommunications Union (ITU) (2008). Overview of Cybersecurity, Recommendation ITU–T X.1205. Режим доступа: https://www.itu.int/rec/T-REC-X.1205-200804-I (дата обращения: 21.04.2020).

Ivanov E. (2015) Combating Cyberterrorism Under International Law // Baltic Yearbook of International Law Online. Vol. 14. No. 1. P. 55–69. Режим доступа: https://doi.org/10.1163/22115897-90000120.

Kaspar L., Kumar S. (2019) Cyber Norms in NYC: Take-Aways From the OEWG Meeting and UNIDIR Cyber Stability Conference. Global Partners Digital. 12 June. Режим доступа: https://www.gp-digital.org/cyber-norms-in-nyc-takeaways-from-the-oewg-meeting-and-unidir-cyber-stability-conference/ (дата обращения: 21.04.2020).

Kittichaisaree K. (2017) Future Prospects of Public International Law of Cyberspace. Public International Law of Cyberspace / K. Kittichaisaree (ed.). Switzerland: Springer International.

Kosseff J. (2018) Defining Cybersecurity Law // Iowa Law Review. Vol. 103. No. 3. Режим доступа: https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/ (дата обращения: 21.04.2020).

Kshetri N. (2009) Positive Externality, Increasing Returns and the Rise in Cybercrimes // Communications of the ACM. Vol. 52. No. 12. Режим доступа: https://doi.org/10.1145/1610252.1610288.

Kshetri N. (2016) Global Cybersecurity: Key Issues and Concepts. The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies / N. Kshetri (ed.). Springer International Publishing.

Lemmens L. (2018) België werkt aan omzetting NIS-richtlijn voor uniforme beveiliging netwerk- en informatiesystemen [Belgium is Working on the Transposition of the NIS Directive for Uniform Security of Network and Information Systems] // Wolters Kluwer Online. 22 November. Режим доступа: https://polinfo.kluwer.be/newsview.aspx?contentdomains=POLINFO&id=VS300653460&lang=nl (дата обращения: 21.04.2020) (in Dutch).

Markopoulou D., Papakonstantinou V., de Hert P. (2019) The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation // Computer Law & Security Review. Vol. 35. No. 6. P. 1–11. Режим доступа: https://doi.org/10.1016/j.clsr.2019.06.007.

Melzer N. (2011) Cyberwarfare and International Law. UNIDIR Resources, UN Institute for Disarmament Research. Режим доступа: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (дата обращения: 21.04.2020).

Mitrakas A. (2018) The Emerging EU Framework on Cybersecurity Certification // Datenschutz und Datensicherheit. Vol. 42. P. 411–444. Режим доступа: https://doi.org/10.1007/s11623-018-0969-2.

Niebler A. (2019) Cybersecurity Act: New Momentum for Europe // The European Files. 25 March. Режим доступа: https://www.europeanfiles.eu/industry/cybersecurity-act-new-momentum-for-europe (дата обращения: 21.04.2020).

Niemann K. (2018) Unternehmensarchitektur und Digitalisierung: Eine Disziplin im Wandel [Enterprise Architecture and Digitalization: A Discipline in Change] // HMD Praxis der Wirtschaftsinformatik. Vol. 55. No. 5. P. 907–927. Режим доступа: https://link.springer.com/article/10.1365/s40702-018-00441-1 (дата обращения: 21.04.2020).

Nye J. (2016/17) Deterrence and Dissuasion in Cyberspace // International Security. Vol. 41. No. 3. P. 44–71. Режим доступа: https://doi.org/10.1162/ISEC_a_00266.

O'Connell M. (2012) Cyber Security Without Cyber War // Journal of Conflict & Security Law. Vol. 17. No. 2. P. 187–209. Режим доступа: https://www.jstor.org/stable/26296226.

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019a). Updated List of Experts for the Presentations on the Six areas Outlined in Paragraph 5 (a) – (f) of the Provisional Agenda of the OEWG (A/AC.290/2019.1) as of 28 August 2019. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/280819-Updated-list-of-experts-first-substantive-session-OEWG-on-developments-in-the-field-of-information-and-telecommunications.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019b). Chair's Letter to the Member States for the Intersessional Meeting. 1 November. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/oewg-chair-letter-to-member-states-for-intersessiona-meeting.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019c). Chair's Letter to the Participants of the OEWG Informal Intersessional Consultative Meeting. 26 November. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/chairs-letter-to-participants-of-oewg-meeting-26-11-19.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019d). Calendar of Side Events. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/oewg-side-events-calendar.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019e). Chair's Letter to Member States on the Second Substantive Session. 31 December. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-letter.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019f). Chair's Letter to Member States on the First Substantive Session. 21 August. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/08/210819-OEWG-Chairs-letter-to-the-member-states-for-the-first-substantial-session.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020a). Chair's Letter on the Summary Report of the Informal Intersessional Consultative Meeting from 2–4 December 2019. 28 January. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020b). Chair's Working Paper for the Second Substantive Session in View of the Second Substantive Session (10–14 February 2020). Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-working-paper-second-substantive-session.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020c). Draft Programme of Work. Second Substantive Session – New York, 10–14 February 2020. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-draft-pow-second-substantive-session.pdf (дата обращения: 21.04. 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020d). Tentative Structure of the Substantive Component of the Report. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-tentative-draft-structure-of-report-substantive-component.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020e). An Initial Overview of the UN System Actors, Processes and Activities on ICT-Related Issues of Interest to the OEWG, by Theme. Background Paper. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020f). International Law in the Consensus Reports of the United Nations Groups of Governmental Experts. Background Paper. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-international-law-in-the-gges.pdf (дата обращения: 21.04.2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020g). "Regular Institutional Dialogue" in the Consensus Reports of the United Nations Groups of Governmental Experts and the Mandate of the OEWG. Background Paper. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-regular-institutional-dialogue.pdf (дата обращения: 21.04.2020).

Orji U.J. (2018) The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability // Masaryk University Journal of Law and Technology. Vol. 12. No. 2. P. 91–129. Режим доступа: https://doi.org/10.5817/MUJLT2018-2-1.

Pauwelyn J., Wessel R., Wouters J. (eds) (2012) Informal International Lawmaking. Oxford: Oxford University Press.

Pupillo L. (2018) EU Cybersecurity and the Paradox of Progress. CEPS Policy Insights No. 2018/06, Centre for European Policy Studies. Режим доступа: https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/ (дата обращения: 21.04.2020).

Reisman M. (1988) Remarks in Panel: A Hard Look at Soft Law // Proceedings of the American Society of International Law. Vol. 82. P. 373–377. Режим доступа: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1747&context=fss_papers (дата обращения: 21.04.2020).

République Français (2018). Revue stratégique de cyberdéfense [Cyber Defence Strategic Review]. Secrétariat Général de la Défense et de la Sécurité Nationale. 12 February. Режим доступа: http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/ (дата обращения: 21.04.2020).

Reuters Plus (2018). The Internet of Things Era: 6 Ways to Stay Safe. 7 June. Режим доступа: https://www.reuters.com/article/idUSWAOA6XIH2J6Z1858 (accessed 10 March 2020).

Roex R. (2016) EU keurt eerste algemene cybersecurity-wet goed [EU Adopts First General Cybersecurity Law] // Wolters Kluwer Online. 16 August 2016. Режим доступа: https://legalworld.wolterskluwer.be/nl/nieuws/domein/strafrecht/eu-keurt-eerste-algemene-cybersecurity-wet-goed/ (дата обращения: 21.04.2020) (in Dutch).

Ruhl C., Hollis D., Hoffman W., Maurer T. (2020) Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. Paper No. 26, Carnegie Endowment for International Peace. Режим доступа: https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110 (дата обращения: 21.04.2020).

Sandage J. et al. (2013) Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime. Режим доступа: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (дата обращения: 21.04.2020).

Schatz D., Bashroush R., Wall J. (2017) Towards a More Representative Definition of Cyber Security // The Journal of Digital Forensics, Security and Law. Vol. 12. No. 2. P. 53–74. Режим доступа: https://doi.org/10.15394/jdfsl.2017.1476.

Schermers H., Blokker N. (2018) International Institutional Law. Amsterdam: Brill Nijhoff.

Schmitt M. et al. (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

Shackelford S., Russell J., Kuehn A. (2016) Unpacking the International Law on Cybersecurity Due Diligence: Lessons From the Public and Private Sectors // Chicago Journal of International Law. Vol. 17. No. 1. Режим доступа: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil (дата обращения: 21.04.2020).

Soesanto S., D'Incau F. (2017) The UN GGE is Dead: Time to Fall Forward. Commentary. 15 August. European Council on Foreign Relations. Режим доступа: https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance (дата обращения: 21.04.2020).

Teplinsky M. (2013) Fiddling on the Roof: Recent Developments in Cybersecurity // American University Business Law Review. Vol. 2. No. 2. P. 225–322. Режим доступа: https://pdfs.semanticscholar.org/bf5d/e28421900aa225e054fd92e5f0a5bf9e03a0.pdf (дата обращения: 21.04.2020).

The White House (2017). Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017. Tel Aviv. 26 June. Режим доступа: https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/ (дата обращения: 21.04.2020).

Trachtman J. (2013) Cyberspace and Cybersecurity. The Future of International Law: Global Government / J. Trachtman (ed.). Cambridge: Cambridge University Press.

Tranter K. (2007) Nomology, Ontology, and Phenomenology of Law and Technology // Minnesota Journal of Law Science & Technology. Vol. 8. No. 2. P. 449–474. Режим доступа: https://scholarship.law.umn.edu/mjlst/vol8/iss2/7 (дата обращения: 21.04.2020).

United Nations (UN) (1970). Declaration of Principles That Control the Sea-Bed and Ocean Floor, and the Subsoil Thereof, Beyond the Limits of National Jurisdiction. General Assembly Resolution A/RES/2749 (XXV). Режим доступа: https://digitallibrary.un.org/record/201718?ln=en (дата обращения: 21.04.2020).

United Nations (UN) (1982). Convention on the Law of the Sea. Concluded at Montego Bay on 10 December 1982, entry into force on 16 November 1994. United Nations Treaty Series. Vol. 1833. I-31363. Режим доступа: https://treaties.un.org/doc/Publication/UNTS/Volume%201833/volume-1833-A-31363-English.pdf (дата обращения: 21.04.2020).

United Nations (UN) (1998). Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Resolution A/RES/53/70. Режим доступа: https://undocs.org/A/RES/53/70 (дата обращения: 21.04.2020).

United Nations (UN) (2004). Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures. General Assembly Resolution A/RES/58/199. Режим доступа: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (дата обращения: 21.04.2020).

United Nations (UN) (2013). Report of Group of Governmental Experts on Information and Telecommunications Developments in the Context of International Security. General Assembly Document A/68/98. Режим доступа: https://undocs.org/A/68/98 (дата обращения: 21.04.2020).

United Nations (UN) (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/70/174. Режим доступа: https://undocs.org/A/70/174 (дата обращения: 21.04.2020).

United Nations (UN) (2018a). Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Resolution A/RES/73/27. Режим доступа: https://undocs.org/A/RES/73/27 (дата обращения: 21.04.2020).

United Nations (UN) (2018b). Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. General Assembly Resolution A/RES/73/266. Режим доступа: https://undocs.org/A/RES/73/266 (дата обращения: 21.04.2020).

United Nations (UN) (2018c). Draft Conclusions on Identification of Customary International Law, With Commentaries. Режим доступа: https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf (дата обращения: 21.04.2020).

United Nations (UN) (2019a). Provisional Agenda. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/AC.290/2019/1. Режим доступа: https://undocs.org/A/AC.290/2019/1 (дата обращения: 21.04.2020).

United Nations (UN) (2019b). Note by the Secretariat: Organization of the Work of the Open-Ended Working Group. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/AC.290/2019/ORG/CRP.1. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/sec-note-oewg-crp.pdf (дата обращения: 21.04.2020).

United Nations (UN) (2019c). Note by the Secretariat: Organization of Work of the First Substantive Session. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/AC.290/2019/2. Режим доступа: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/08/A-AC.290-2019-2.pdf (дата обращения: 21.04.2020).

United Nations (UN) (2020h). Draft Organization of Work of the Second Substantive Session. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). General Assembly Document A/AC.290/2020/1. Режим доступа: https://undocs.org/en/A/AC.290/2020/1 (дата обращения: 21.04.2020).

United Nations (UN) Office for Disarmament Affairs (n. d.). Open-Ended Working Group. Режим доступа: https://www.un.org/disarmament/open-ended-working-group/ (дата обращения: 21.04.2020).

United Nations (UN) Office for Disarmament Affairs (2019). Intergovernmental Processes on the Use of Information and Telecommunications in the Context of International Security 2019–2021. Fact Sheet. Режим доступа: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+and+GGE+processes+-+2.pdf (дата обращения: 21.04.2020).

Väljataga A. (2018) Tracing Opinio Juris in National Cyber Security Strategy Documents. NATO Cooperative Cyber Defence Centre of Excellence Paper. Режим доступа: https://ccdcoe.org/library/publications/tracing-opinio-juris-in-national-cyber-security-strategy-documents/ (дата обращения: 21.04.2020).

Vergne J., Duran R. (2014) Cyberespace et Organisations "Virtuelles": L' état Souverain a-t-Il Encore un Avenir? [Cyberspace and "Virtual" Organizations: Does the Sovereign State Still Have a Future?] // Regards Croisés sur L'Économie. Vol. 1. No. 14. P. 126–139. Режим доступа: https://www.cairn.info/revue-regards-croises-sur-l-economie-2014-1-page-126.htm (дата обращения: 21.04.2020).

Virally M. (1983) La distinction entre textes internationaux de portée juridique et textes internationaux dépourvus de portée juridique (à l'exception des textes émanant des organisations internationales). Annuaire de l'Institut de Droit International Session de Cambridge. Vol. 60. P. 166–327.

von Heinegg W. (2012) The Tallinn Manual and International Cyber Security Law. Yearbook of International Humanitarian Law. The Hague: TMC Asser Press.

Wall D. (2007) Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity.

Westby J. (2019) Why the EU Is About to Seize the Global Lead on Cybersecurity // Forbes. 31 October. Режим доступа: https://www.forbes.com/sites/jodywestby/2019/10/31/why-the-eu-is-about-to-seize-the-global-lead-on-cybersecurity/#6dd3771b2938 (дата обращения: 21.04.2020).

Wheeler D., Larsen G. (2013) Techniques for Cyberattack Attribution. IDA Paper P-3792, Institute for Defense Analysis. Режим доступа: https://www.researchgate.net/publication/235170094_Techniques_for_Cyber_Attack_Attribution (дата обращения: 21.04.2020).

Wouters J., Ryngaert C., De Baere G., Ruys T. (2018) International Law: A European Perspective. Oxford. Hart Publishing.

Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives

A. Verhelst, J. Wouters

Anne Verhelst – PhD Researcher in International Law, Leuven Centre for Global Governance Studies and Institute for International Law, KU Leuven and Fellow of Research Foundation – Flanders (FWO); 13 Oude Markt, Leuven, Belgium; E-mail: anne.verhelst@kuleuven.be

Jan Wouters – Full Professor of International Law and International Organizations, Director of the Leuven Centre for Global Governance Studies and Institute for International Law, KU Leuven; 13 Oude Markt, Leuven, Belgium; E-mail: jan.wouters@ggs.kuleuven.be

Abstract

The many recent cyber incidents have shown how cybersecurity has entered the realm of international relations. Several international organizations have taken cybersecurity policy initiatives, notably the United Nations (UN) and the European Union (EU). Both organizations aspire to a leading role in enhancing cybersecurity resilience. To date, however, these initiatives have not resulted in much regulation. This article examines which factors make lawmaking and the regulation of cybersecurity difficult at the international level, and whether some of these impediments are shared at the EU legislative level. Are difficulties in regulating cybersecurity embedded in the normative processes at the UN or the EU, or are they inherent to the high-tech phenomenon of cyber? As for the UN, the article looks at the work of the UN Group of Governmental Experts (GGE). While previous reports of the UN GGE seemed to point to an emerging international opinio juris, recent developments in the UN General Assembly (UNGA) show a strongly divided international community. At the EU level, the article discusses the two main legislative initiatives on cybersecurity that have seen the light of day: the 2016 Directive on Network and Information Security and the 2019 Regulation on the EU Cybersecurity Act.

Key words: cybersecurity; global governance; international law; European Union; lawmaking; regulation; policy; UN GGE; Open-ended Working Group; NIS Directive; EU Cybersecurity Act

For citation: Verhelst A., Wouters J. (2020) Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. *International Organisations Research Journal*, vol. 15, no 2, pp. 141–172 (in English). DOI: 10.17323/1996-7845-2020-02-07

References

African Union (2014). Convention on Cyber Security and Personal Data Protection of 27 June 2014, entry into force on 3 June 2019. Available at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 9 March 2020).

Albrecht D. (2018) Chinese Cybersecurity Law Compared to EU-NIS-Directive and German IT-Security Act. *Computer Law Review International*, vol. 19, no 1, pp. 1–6. Available at: https://doi.org/10.9785/cri-2018-190102.

Australian Government (2016). Australia's Cyber Security Strategy: Enabling Innovation, Growth and Prosperity. Department of Home Affairs. Available at: https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf (accessed 9 March 2020).

Bederman D. (2010) *Custom as a Source of Law*. Cambridge: Cambridge University Press.

Bowcott O. (2017) Dispute Along Cold War Lines Led to Collapse of UN Cyberwarfare Talks. *The Guardian*, 23 August. Available at: https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges (accessed 7 March 2020).

Boyle E. (1999) Some Reflections on the Relationship of Treaties and Soft Law. *International and Comparative Law Quarterly*, vol. 48, no 4, pp. 901–13. Available at: https://doi.org/10.1017/S0020589300063739.

Bradley C. (ed.) (2016) Custom's Future: International Law in a Changing World. Cambridge: Cambridge University Press.

Contreras J., de Nardis L., Teplinsky M. (2013) Mapping Today's Cybersecurity Landscape. *American University Law Review*, vol. 62, no 5, pp. 1113–30. Available at: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1883&context=aulr (accessed 21 April 2020).

Council of Europe (2001). Budapest Convention on Cybercrime, ETS No 185, open for signature 23 November, entry into force 1 July 2004. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed 20 April 2020).

D'Elia D. (2014) La guerre économique à l'ère du cyberspace [Economic Warfare in the Cyberspace Era]. *Hérodote*, vol. 152/153, no 1, pp. 240–60. Available at: https://www.cairn.info/revue-herodote-2014-1-page-240.htm (accessed 21 April 2020).

Ducuing C. (2019) On the Edge of the NIS Directive: The Proposed CITS Delegated Regulation, Friend or Foe? CiTiP Working Paper, KU Leuven Centre for IT & IP Law. Available at: https://dx.doi.org/10.2139/ssrn.3486978.

European Commission (EC) (2005). Green Paper on a European Programme for Critical Infrastructure Protection. COM/2005/0576 final/. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52005DC0576 (accessed 21 April 2020).

European Commission (EC) (2009). Protecting Europe From Large-Scale Cyber Attacks and Disruptions: Improving Preparedness, Security and Resilience. Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. COM (2009) 149 final. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF (accessed 21 April 2020).

European Commission (EC) (2013a). Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union. COM (2013) 48 final 2013/0027 (COD). Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-48-EN-F1-1.Pdf (accessed 21 April 2020).

European Commission (EC) (2013b). Making European Critical Infrastructures More Secure. Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection. SWD (2013) 318 final. Available at: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf (accessed 21 April 2020).

European Commission (EC) (2018). Building Strong Cybersecurity in Europe. State of the Union, 12 September. Available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_en.pdf (accessed 21 April 2020).

European Commission (EC), High Representative of the European Union for Foreign Affairs and Security Policy (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, JOIN (2013) 1 final. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed 21 April 2020).

European Court of Auditors (2019). Challenges to Effective EU Cybersecurity Policy. Briefing Paper, March. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (accessed 20 April 2020).

European Union (EU) (2008). Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. *Official Journal of the European Union*, L 345/75, vol. 51, pp. 75–82. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.345.01.0075.01.ENG&toc=OJ:L:2008:345:TOC (accessed 21 April 2020).

European Union (EU) (2012). Consolidated Version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union C 326*, vol. 55, pp. 47–200. Available at: https://eur-lex.europa.eu/

legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.326.01.0001.01.ENG&toc=OJ:C:2012:326:TOC#C_20123 26EN.01004701 (accessed 21 April 2020).

European Union (EU) (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS Directive). *Official Journal of the European Union, L 194/1*. Available at: http://data.europa.eu/eli/dir/2016/1148/oj (accessed 20 April 2020).

European Union (EU) (2018). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union, L 151/1*. Available at: http://data.europa.eu/eli/reg/2019/881/oj (accessed 22 April 2020).

European Union (EU) (2019). EU Non-Paper on Capacity Building to Advance Peace and Stability in Cyberspace, for the Work of the Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security," Submitted to the Second Substantive Session of the OEWG (10–14 February 2020). Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/eu-non-paper-submission-oewg-2019.pdf (accessed 8 March 2020).

European Union Agency for Cybersecurity (ENISA) (2015). Annual Incident Reports 2015. Available at: www.enisa.europa.eu/publications/annual-incident-reports-2015 (accessed 7 March 2020).

Fantin S. (2019) Weighting the EU Cybersecurity Act: Progress or Missed Opportunity? CiTiP Blog, KU Leuven Centre for IT & IP Law, 19 March. Available at https://www.law.kuleuven.be/citip/blog/weighting-the-eu-cybersecurity-act-progress-or-missed-opportunity/ (accessed 6 March 2020).

Fidler D. (2015) Wither the Web? International Law, Cybersecurity and Critical Infrastructure Protection. *Georgetown Journal of International Affairs*, vol. 8, pp. 8–20. Available at: https://www.repository.law.indiana.edu/facpub/2452 (accessed 23 April 2020).

Futter A. (2018) Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies. *Journal of Cyber Policy*, vol. 3, no 2, pp. 201–16. Available at: https://doi.org/10.1080/23738871.2018.1514417.

Geneva Internet Platform, Digital Watch Observatory (n. d.). UN GGE and OEWG. Available at: https://dig.watch/processes/un-gge#view-7541-3 (accessed 7 March 2020).

Gov.UK (2016). National Cyber Security Strategy 2016–2021. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (accessed 9 March 2020).

Government of the Russian Federation (2016). Doctrine of Information Security of the Russian Federation. Ministry of Foreign Affairs of the Russian Federation, 5 December. Available at: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 (accessed 9 March 2020).

Grigsby A. (2018) The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. Net Politics Blog, 15 November. Council on Foreign Relations. Available at: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased (accessed 11 March 2020).

Group of 20 (G20) (2015). G20 Leaders' Communiqué. Antalya, 15–16 November. Available at: http://www.g20.utoronto.ca/2015/151116-draft-communique.pdf (accessed 21 April 2020).

Groupe UMP Assemblée nationale (2009). Le législateur et les questions de société: quelle méthode pour quels choix? Rapport d'étape du groupe de travail animé par Hervé Mariton, député de la Drôme à la demande de Jean-François Copé [The Legislator and Questions for Society: Which Method for Which Choices? Progress Report for the Working Group Led by Hervé Mariton, Member of the Drôme at the Request of Jean-François Copé]. 12 May. Available at: https://www.unaf.fr/IMG/pdf/rapport_d_etape_mai_2009.pdf (accessed 6 March 2020).

Haggenmacher P. (1986) La doctrine des deux éléments du droit coutumier dans la pratique de la Cour Internationale [The Doctrine of the Two Elements of Cusstomary Law in the Practice of the International Court]. Révue générale de droit international public, vol. 90.

Harrison Dinniss A. (2018) The Threat of Cyber Terrorism and What International Law Should (Try To) Do About It. *Georgetown Journal of International Affairs*, vol. 19, pp. 43–50. Available at: https://doi.org/10.1353/gia.2018.0006.

Healey J. (2012) Beyond Attribution: Seeking National Responsibility for Cyberattacks. Issue Brief, Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/ (accessed 9 March 2020).

Henriksen A. (2019) The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, vol. 5, no 1. Available at: https://doi.org/10.1093/cybsec/tyy009.

Hoisington M. (2017) Regulating Cyber Operations Through International Law: In, Out or Against the Box? Ethics and Policies for Cyber Operations (M. Taddeo, L. Glorioso (eds)). Oxford: Springer International.

Iasiello E. (2019) OEWG or GGE: Which Has the Best Shot of Succeeding? *Technative*, 5 December. Available at: https://www.technative.io/oewg-or-gge-which-has-the-best-shot-of-succeeding/ (accessed 22 April 2020).

International Telecommunications Union (ITU) (2008). Overview of Cybersecurity, Recommendation ITU–T X.1205. Available at: https://www.itu.int/rec/T-REC-X.1205-200804-I (accessed 22 April 2020).

Ivanov E. (2015) Combating Cyberterrorism Under International Law. *Baltic Yearbook of International Law Online*, vol. 14, no 1, pp. 55–69. Available at: https://doi.org/10.1163/22115897-90000120.

Kaspar L., Kumar S. (2019) Cyber Norms in NYC: Take-Aways From the OEWG Meeting and UNIDIR Cyber Stability Conference. Global Partners Digital, 12 June. Available at: https://www.gp-digital.org/cyber-norms-in-nyc-takeaways-from-the-oewg-meeting-and-unidir-cyber-stability-conference/ (accessed 21 April 2020).

Kittichaisaree K. (2017) Future Prospects of Public International Law of Cyberspace. Public International Law of Cyberspace (K. Kittichaisaree (ed.)). Switzerland: Springer International.

Kosseff J. (2018) Defining Cybersecurity Law. Iowa Law Review, vol. 103, no 3. Available at: https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/ (accessed 20 April 2020).

Kshetri N. (2009) Positive Externality, Increasing Returns and the Rise in Cybercrimes. *Communications of the ACM*, vol. 52, no 12. Available at: https://doi.org/10.1145/1610252.1610288.

Kshetri N. (2016) Global Cybersecurity: Key Issues and Concepts. The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies (N. Kshetri (ed.)). Springer International Publishing.

Lemmens L. (2018) België werkt aan omzetting NIS-richtlijn voor uniforme beveiliging netwerk- en informatiesystemen [Belgium is Working on the Transposition of the NIS Directive for Uniform Security of Network and Information Systems]. Wolters Kluwer Online, 22 November. Available at: https://polinfo.kluwer.be/newsview.aspx?contentdomains=POLINFO&id=VS300653460&lang=nl (accessed 21 April 2020) (in Dutch).

Markopoulou D., Papakonstantinou V., de Hert P. (2019) The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation. *Computer Law & Security Review*, vol. 35, no 6, pp. 1–11. Available at: https://doi.org/10.1016/j.clsr.2019.06.007.

Melzer N. (2011) Cyberwarfare and International Law. UNIDIR Resources, UN Institute for Disarmament Research. Available at: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (accessed 9 March 2020).

Mitrakas A. (2018) The Emerging EU Framework on Cybersecurity Certification. *Datenschutz und Datensicherheit*, vol. 42, pp. 411–4. Available at: https://doi.org/10.1007/s11623-018-0969-2.

Niebler A. (2019) Cybersecurity Act: New Momentum for Europe. *The European Files*, 25 March. Available at: https://www.europeanfiles.eu/industry/cybersecurity-act-new-momentum-for-europe (accessed 21 April 2020).

Niemann K. (2018) Unternehmensarchitektur und Digitalisierung: Eine Disziplin im Wandel [Enterprise Architecture and Digitalization: A Discipline in Change]. HMD Praxis der Wirtschaftsinformatik, vol. 55, no 5, pp. 907–27. Available at: https://link.springer.com/article/10.1365/s40702-018-00441-1 (accessed 21 April 2020).

Nye J. (2016/17) Deterrence and Dissuasion in Cyberspace. *International Security*, vol. 41, no 3, pp. 44–71. Available at: https://doi.org/10.1162/ISEC_a_00266.

O'Connell M. (2012) Cyber Security Without Cyber War. *Journal of Conflict & Security Law*, vol. 17, no 2, pp. 187–209. Available at: https://www.jstor.org/stable/26296226.

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019a). Updated List of Experts for the Presentations on the Six areas Outlined in Paragraph 5 (a) – (f) of the Provisional Agenda of the OEWG (A/AC.290/2019.1) as of 28 August 2019. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/280819-Updated-list-of-experts-first-substantive-session-OEWG-on-developments-in-the-field-of-information-and-telecommunications.pdf (accessed 9 March 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019b). Chair's Letter to the Member States for the Intersessional Meeting. 1 November. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/oewg-chair-letter-to-member-states-for-intersessiona-meeting.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019c). Chair's Letter to the Participants of the OEWG Informal Intersessional Consultative Meeting. 26 November. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/chairs-letter-to-participants-of-oewg-meeting-26-11-19.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019d). Calendar of Side Events. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/oewg-side-events-calendar.pdf (access 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019e). Chair's Letter to Member States on the Second Substantive Session. 31 December. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-letter.pdf (access 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2019f). Chair's Letter to Member States on the First Substantive Session. 21 August. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/08/210819-OEWG-Chairs-letter-to-the-member-states-for-the-first-substantial-session.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020a). Chair's Letter on the Summary Report of the Informal Intersessional Consultative Meeting from 2-4 December 2019. 28 January. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf (accessed 10 March 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020b). Chair's Working Paper for the Second Substantive Session in View of the Second Substantive Session (10–14 February 2020). Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-working-paper-second-substantive-session.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020c). Draft Programme of Work. Second Substantive Session – New York, 10–14 February 2020. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-draft-pow-second-substantive-session.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020d). Tentative Structure of the Substantive Component of the Report. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-tentative-draft-structure-of-report-substantive-component.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020e). An Initial Overview of the UN System Actors, Processes and Activities on ICT-Related Issues of Interest to the OEWG, by Theme. Background Paper. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020f). International Law in the Consensus Reports of the United Nations Groups of Governmental Experts. Background Paper. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-international-law-in-the-gges.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) (2020g). "Regular Institutional Dialogue" in the Consensus Reports of the United Nations Groups of Governmental Experts and the Mandate of the OEWG. Background Paper. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-regular-institutional-dialogue.pdf (accessed 22 April 2020).

Orji U.J. (2018) The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability. *Masaryk University Journal of Law and Technology*, vol. 12, no 2, pp. 91–129. Available at: https://doi.org/10.5817/MUJLT2018-2-1.

Pauwelyn J., Wessel R., Wouters J. (eds) (2012) *Informal International Lawmaking*. Oxford: Oxford University Press.

Pupillo L. (2018) EU Cybersecurity and the Paradox of Progress. CEPS Policy Insights No 2018/06, Centre for European Policy Studies. Available at: https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/ (accessed 20 April 2020).

Reisman M. (1988) Remarks in Panel: A Hard Look at Soft Law. *Proceedings of the American Society of International Law*, vol. 82, pp. 373–7. Available at: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1747&context=fss_papers (accessed 21 April 2020).

République Français (2018). Revue stratégique de cyberdéfense [Cyber Defence Strategic Review]. Secrétariat Général de la Défense et de la Sécurité Nationale, 12 February. Available at http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/ (accessed 9 March 2020).

Reuters Plus (2018). The Internet of Things Era: 6 Ways to Stay Safe. 7 June. Available at: https://www.reuters.com/article/idUSWAOA6XIH2J6Z1858 (accessed 10 March 2020).

Roex R. (2016) EU keurt eerste algemene cybersecurity-wet goed [EU Adopts First General Cybersecurity Law]. Wolters Kluwer Online, 16 August 2016. Available at: https://legalworld.wolterskluwer.be/nl/nieuws/domein/strafrecht/eu-keurt-eerste-algemene-cybersecurity-wet-goed/ (accessed 21 April 2020) (in Dutch).

Ruhl C., Hollis D., Hoffman W., Maurer T. (2020) Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. Paper No 26, Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110 (accessed 22 April 2020).

Sandage J. et al. (2013) Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 21 April 2020).

Schatz D., Bashroush R., Wall J. (2017) Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*, vol. 12, no 2, pp. 53–74. Available at: https://doi.org/10.15394/jdfsl.2017.1476.

Schermers H., Blokker N. (2018) *International Institutional Law*. Amsterdam: Brill Nijhoff.

Shackelford S., Russell J., Kuehn A. (2016) Unpacking the International Law on Cybersecurity Due Diligence: Lessons From the Public and Private Sectors. *Chicago Journal of International Law*, vol. 17, no 1. Available at: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil (accessed 21 April 2020).

Schmitt M. et al. (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

Soesanto S., D'Incau F. (2017) The UN GGE is Dead: Time to Fall Forward. Commentary, 15 August. European Council on Foreign Relations. Available at: https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance (accessed 22 April 2020).

Teplinsky M. (2013) Fiddling on the Roof: Recent Developments in Cybersecurity. *American University Business Law Review*, vol. 2, no 2, pp. 225–322. Available at: https://pdfs.semanticscholar.org/bf5d/e28421900aa225e054fd92e5f0a5bf9e03a0.pdf (accessed 21 April 2020).

The White House (2017). Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017. Tel Aviv, 26 June. Available at: https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/ (accessed 10 March 2020).

Trachtman J. (2013) Cyberspace and Cybersecurity. The Future of International Law: Global Government (J. Trachtman (ed.)). Cambridge: Cambridge University Press.

Tranter K. (2007) Nomology, Ontology, and Phenomenology of Law and Technology. *Minnesota Journal of Law Science & Technology*, vol. 8, no 2, pp. 449–74. Available at: https://scholarship.law.umn.edu/mjlst/vol8/iss2/7 (accessed 21 April 2020).

United Nations (UN) (1970). Declaration of Principles That Control the Sea-Bed and Ocean Floor, and the Subsoil Thereof, Beyond the Limits of National Jurisdiction. General Assembly Resolution A/RES/2749 (XXV). Available at: https://digitallibrary.un.org/record/201718?ln=en (accessed 21 April 2020).

United Nations (UN) (1982). Convention on the Law of the Sea. Concluded at Montego Bay on 10 December 1982, entry into force on 16 November 1994. United Nations Treaty Series, vol. 1833, I-31363. Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%201833/volume-1833-A-31363-English.pdf (accessed 22 April 2020).

United Nations (UN) (1998). Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Resolution A/RES/53/70. Available at: https://undocs.org/A/RES/53/70 (accessed 21 April 2020).

United Nations (UN) (2004). Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures. General Assembly Resolution A/RES/58/199. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (accessed 21 April 2020).

United Nations (UN) (2013). Report of Group of Governmental Experts on Information and Telecommunications Developments in the Context of International Security. General Assembly Document A/68/98. Available at: https://undocs.org/A/68/98 (accessed 21 April 2020).

United Nations (UN) (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/70/174. Available at: https://undocs.org/A/70/174 (accessed 21 April 2020).

United Nations (UN) (2018a). Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Resolution A/RES/73/27. Available at: https://undocs.org/A/RES/73/27 (accessed 22 April 2020).

United Nations (UN) (2018b). Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. General Assembly Resolution A/RES/73/266. Available at: https://undocs.org/A/RES/73/266 (accessed 22 April 2020).

United Nations (UN) (2018c). Draft Conclusions on Identification of Customary International Law, With Commentaries. Available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf (accessed 29 May 2020).

United Nations (UN) (2019a). Provisional Agenda. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/AC.290/2019/1. Available at: https://undocs.org/A/AC.290/2019/1 (accessed 22 April 2020).

United Nations (UN) (2019b). Note by the Secretariat: Organization of the Work of the Open-Ended Working Group. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/AC.290/2019/ORG/CRP.1. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/sec-note-oewg-crp.pdf (accessed 22 April 2020).

United Nations (UN) (2019c). Note by the Secretariat: Organization of Work of the First Substantive Session. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the

Context of International Security. General Assembly Document A/AC.290/2019/2. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/08/A-AC.290-2019-2.pdf (accessed 22 April 2020).

United Nations (UN) (2020h). Draft Organization of Work of the Second Substantive Session. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). General Assembly Document A/AC.290/2020/1. Available at: https://undocs.org/en/A/AC.290/2020/1 (accessed 22 April 2020).

United Nations (UN) Office for Disarmament Affairs (n. d.). Open-Ended Working Group. Available at: https://www.un.org/disarmament/open-ended-working-group/ (accessed 10 March 2020).

United Nations (UN) Office for Disarmament Affairs (2019). Intergovernmental Processes on the Use of Information and Telecommunications in the Context of International Security 2019–2021. Fact Sheet. Available at: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+and+GGE+processes+-+2.pdf (accessed 8 March 2020).

Väljataga A. (2018) Tracing Opinio Juris in National Cyber Security Strategy Documents. NATO Cooperative Cyber Defence Centre of Excellence Paper. Available at: https://ccdcoe.org/library/publications/tracing-opinio-juris-in-national-cyber-security-strategy-documents/ (accessed 22 April 2020).

Vergne J., Duran R. (2014) Cyberespace et Organisations "Virtuelles": L' état Souverain a-t-Il Encore un Avenir? [Cyberspace and "Virtual" Organizations: Does the Sovereign State Still Have a Future?] *Regards Croisés sur L'Économie*, vol. 1, no 14, pp. 126–39. Available at: https://www.cairn.info/revue-regards-croises-sur-l-economie-2014-1-page-126.htm (accessed 21 April 2020).

Virally M. (1983) La distinction entre textes internationaux de portée juridique et textes internationaux dépourvus de portée juridique (à l'exception des textes émanant des organisations internationales). Annuaire de l'Institut de Droit International Session de Cambridge, vol. 60, pp. 166–327.

von Heinegg W. (2012) The Tallinn Manual and International Cyber Security Law. Yearbook of International Humanitarian Law. The Hague: TMC Asser Press.

Wall D. (2007) Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity.

Westby J. (2019) Why the EU Is About to Seize the Global Lead on Cybersecurity. *Forbes*, 31 October. Available at: https://www.forbes.com/sites/jodywestby/2019/10/31/why-the-eu-is-about-to-seize-the-global-lead-on-cybersecurity/#6dd3771b2938 (accessed 21 April 2020).

Wheeler D., Larsen G. (2013) Techniques for Cyberattack Attribution. IDA Paper P-3792, Institute for Defense Analysis. Available at: https://www.researchgate.net/publication/235170094_Techniques_for_Cyber_Attack_Attribution (accessed 21 April 2020).

Wouters J., Ryngaert C., De Baere G., Ruys T. (2018) *International Law: A European Perspective*. Oxford. Hart Publishing.