при внесении поправок при присоединении Республики Армения протокол о внесении поправок являлся приложением к договору о присоединении, то в случае присоединения Кыргызской Республики такой протокол подписывался отдельно, но оговаривалось, что он является неотъемлемой частью договора о присоединении.

Обращаем также внимание, что в рамках ЕАЭС получила распространение техника оформления поправок в виде приложений к соответствующим протоколам. Практическая целесообразность использования данной техники заключается в том, что основная часть соглашения «не перегружается» массивом положений о внесении поправок, она удобна для восприятия, что имеет большое значение для правоприменителя, а также при осуществлении внутригосударственных процедур в отношении такого соглашения о поправках.

При наличии большого количества вносимых поправок их изложение в виде приложения к соглашению о поправках следует признать обоснованным и полезным.

Полагаем возможным рекомендовать дальнейшее распространение данной практики, в межгосударственных образованиях, членом которых является Республика Беларусь (СНГ и ОДКБ), а также информирование о ней государственных органов и организаций Республики Беларусь, которые вовлечены в процесс заключения международных договоров.

СУВЕРЕНИТЕТ В КИБЕРПРОСТРАНСТВЕ: AN EST?

А.В. Жалдыбин

Белорусский государственный университет
пр. Независимости, 4, 220030, г. Минск, Беларусь, alexey.zhaldybin@gmail.com

В статье рассматривается актуальная в современное время проблема содержания принципа суверенитета в киберпространстве. Отмечается, что из широкого спектра международно-правовых проблем, присущих кибербезопасности, указанный принцип закономерно пользуется большим вниманием в силу особой чувствительности вопроса — в зависимости от квалификации инцидента в качестве (не) нарушающего суверенитет государство (не) имеет право применять ответные меры. Целью статьи является установление на основе анализа доктринальных источников, международно-правовых документов, а также практики государств основных теорий к применимости принципа суверенитета к киберпространству. Объектом исследования является суверенитет. Предметом исследования является принцип суверенитета в контексте киберпространства. В ходе исследования сделан вывод о существовании государственного суверенитета в киберпространстве, рассмотрены кибератаки, которые могут быть квалифицированы в качестве нарушения суверенитета государства, определено проблемное поле, связанное с дальнейшим развитием регулирования вопроса.

Ключевые слова: суверенитет; государство; кибератака; кибербезопасность; критическая инфраструктура; Таллиннское руководство.

SOVEREIGNTY IN CYBER SPACE: AN EST?

A.V. Zhaldybin

Belarusian State University, Niezaliežnasci Avenue, 4, 220030, Minsk, Belarus

The article assesses a presently topical issue of the contents of sovereignty principle in cyber space with respect to constantly growing number of occurring cyberattacks. It is observed that within

the framework of the whole spectrum of international legal problems related to cyber security, the principle naturally attracts a lot of attention due to its particular sensitivity— depending on qualification of an incident as (non-) violating sovereignty a state may (not) have the right to act in response. The purpose of the article is to determine relevant approaches towards applicability of sovereignty principle basing of a variety of doctrinal sources, international legal documents as well as state practice. The object of the study is sovereignty. The subject of the study is the content of the principle of sovereignty is cyberspace. In the course of the study it was determined that the principle of state sovereignty is applicable to cyber space as well as elaborated on the issues of cyberattacks that may be qualified as violating state's sovereignty and challenges with respect to forthcoming development of the problem.

Key words: sovereignty; state; cyberattack; cyber security; critical infrastructure; Tallinn manual.

Современная картина мира такова, что едва ли каждый месяц в информационную повестку дня попадают громкие новости об очередном инциденте в киберпространстве: их спектр варьируется, начиная с заражений тысяч компьютеров вирусами-вымогателями (Wanna Cry, Petya и др.)[1] и заканчивая атаками на критическую инфраструктуру государства [2]. Если ранее каждый такой случай сопровождался широким общественным резонансом, то в настоящее время все чаще реакция на такие события весьма сдержана и сводится к активизации деятельности компетентных служб по выявлению и борьбе последствиями данных инцидентов. Вследствие учащающейся динамики их совершения в литературе проблемы кибербезопасности относят к разряду наиболее очевидных вызов для человечества в XXI веке и ставят на одну ступень, например, с глобальным потеплением [3].

В процесс выработки оптимальных решений для предотвращений киберинцидентов, а также определения механизма их противодействию широко вовлечено академическое сообщество. Наиболее выдающимся академическим трудом международного коллектива авторов принято считать Таллиннское руководство по международному праву, применимому к кибервойне 2017 г. [4] (актуальная версия 2.0.) (далее – Таллиннское руководство), которое помимо регулирования широкого круга международно-правовых вопросов, связанных с применением кибератак в межгосударственных отношениях, также определяет наиболее важные концепты применительно к киберпространству. Оба данных направления находятся в тесной взаимосвязи, в связи с чем, прежде чем ответить на один из наиболее существенных вопросов права кибербезопасности: «Нарушается ли суверенитет государства в случае совершения в отношении него кибератаки?», – необходимо определить, можно ли вообще говорить о распространении государственного суверенитета на киберпространство. Данный вопрос сложно назвать новым [5, с. 678], однако по сегодняшний день он не потерял своей актуальности.

В настоящее время в литературе встречается концепция, в соответствии с которой суверенитета в киберпространстве не существует. Исследователями отмечается противоречие между принципом суверенитета и самим «духом» интернета, который основывается на идее неограниченного доступа, в то время как государственная машинерия слишком громоздка, географически и технологически ограниченна для регулирования киберпространства [6, с. 179; 7, с. 830]. Вторая линия аргументации данной позиции основывается на утверждении, что киберпространство является общим достоянием человечества (*res communis omnium*) по аналогии с открытым морем, международным воздушным простран-

ством, открытым космосом, а потому не подлежит присвоению каким-либо государством [8, с. 1645].

Вместе с тем более обоснованным, чем вышеуказанный, представляется другой подход, согласно которому государственный суверенитет все же распространяется на киберпространство. Логично утверждение что оно *per se* подразумевает существование соответствующей физической киберинфраструктуры, которая располагается на государственной территории, в отношении которой, бесспорно, распространяется государственная юрисдикция. Кроме того, государства обладают юрисдикцией в отношении осуществляемых на его территории мероприятий в киберпространстве, а также ведут борьбу с киберпреступлениями и др. [9].

В связи с этим рациональным видится подход, воспринятый в Таллиннском руководстве, в соответствии с которым при определении суверенитета учитываются три компонента киберпространства: физический (компьютеры, кабели, роутеры, серверы и т.д.), логический (приложения, данные, протоколы, которые непосредственно обеспечивают обмен информацией) и социальный (физические лица и организации, вовлеченные в процессы), в отношении каждого из которых государства реализуют суверенные полномочия [4, с. 20].

Допуская применимость принципа суверенитета к киберпространству в литературе обращается внимание на неидентичность подходов к пониманию содержания суверенитета в разных средах (сухопутное, морское, воздушное, космическое и киберпространство) [11].

Так, например, в случае с космическим пространством согласно статье 2 Договора о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела 1967 г. «космическое пространство, включая Луну и другие небесные тела, не подлежат национальному присвоению ни путем провозглашения на них суверенитета, ни путем использования или оккупации, ни любыми другими средствами» [12].

Согласно статье 1 Чикагской конвенции о Международной гражданской авиации 1944 г. «Договаривающиеся государства признают, что каждое государство обладает полным и исключительным суверенитетом над воздушным пространством над своей территорией» [13], а несогласованный пролет через воздушное пространство государства является серьезным нарушением международного права [14, с. 54].

В свою очередь в соответствии со статьей 2 Конвенции ООН по морскому праву 1982 г. «суверенитет прибрежного государства распространяется за пределы его сухопутной территории и внутренних вод […] на примыкающий морской пояс, называемый территориальным морем. […] Суверенитет над территориальным морем осуществляется *с соблюдением* настоящей Конвенции и других норм международного права» [15]. При этом исходя из принципа свободы навигации Конвенцией прямо предусмотрено право мирного прохода, предполагающее возможность морских судов иностранных государств пересекать территориальное море государства (при соблюдении определенных требований) (статья 17) [15].

Из вышеприведенных примеров видно, что объем суверенитета варьируется в зависимости от особенностей конкретного пространства. Американские исследователи проблематики суверенитета Г. Корн и Р. Тэйлор также отмечают, что принцип суверенитета, бесспорно, является универсальным по своему характеру, однако его содержание зависит от особенностей правового режима кон-

кретной среды [16]. Видится, что данный подход является рациональным, при этом, по нашему мнению, если особенности киберпространства с технической точки зрения международному сообществу уже известны (оно является творением человечества), то отсутствие универсального подхода к пониманию правового режима киберпространства оставляет вопрос содержания принципа суверенитета в киберпространстве без осязаемых перспектив разрешения. В том числе наиболее значимая правовая проблема в данном контексте – квалификация нарушения суверенитета в киберпространстве.

По мнению экспертной группы по подготовке Таллиннского руководства совершенная кибератака будет являться нарушением суверенитета государства в случае, если будет причинен осязаемый физический ущерб (имуществу, гражданам, инфраструктуре и т. д.); выведены из строя элементы киберинфраструктуры; направлена на нарушение (захват) государственных функций [4, с. 20–21]. По нашему мнению, квалификация таких ситуаций не вызывают сомнения в силу очевидности серьезности последствий.

Однако более значимым вызовом на современном этапе является ситуация, в которой субъекты международного права предпринимают попытки использования неопределенностей в правовом регулировании киберпространства. Так, американский юрист Э. Дженсен отмечает,что государства начинают толковать принцип суверенитета в киберпространстве в таком ключе, чтобыпри осуществлении кибератак воздействовать на киберинфраструктуру другого государства в объеме, *не оказывающем* негативного воздействия на осуществление последним функций государственного управления [17, с. 741], т.е. в пограничной ситуации, когда есть сложности с квалификацией. Аналогичным образом эксперты, готовившие Таллиннское руководство, оказались не в состоянии ответить на вопрос, будет ли являться нарушением суверенитета ситуация, в которой в результате кибератаки не наносится ни один из вышеуказанных видов ущерба [4, с. 21].

Существенной проблемой в данном отношении является отсутствие достаточного объема международной практики. По мнению главного редактора Таллиннского руководства М. Шмитта наиболее вероятно, что в течение следующих пяти лет изменится понимание содержания именно принципа суверенитета в киберпространстве [18]. Аналогичным образом, советник по правовым вопросам Государственного секретариата США Б. Эган отмечает, что государства сталкиваются с ситуацией правового вакуума в отсутствие конкретной практики. Для изменения сложившейся ситуации государствам необходимо явно и публично высказаться по вопросу применения норм международного права к киберпространству[19, с. 180].

Кроме того, полагается, что данный вопрос следует рассматривать в контексте общей проблемы применения норм международного права к киберпространству, поскольку с принципом суверенитета взаимосвязаны принципы невмешательства, неприменения силы и др. Каждый из них содержит ряд конкретных вопросов, до настоящего момента обсуждаемых лишь в теоретической плоскости. Совершенная в 2007 году кибератака в отношении Эстонии вызвала первую волну обсуждения указанной проблематики, вмешательство в президентские выборы в США в 2016 году — вторую.

Таким образом, можно говорить о дихотомичном характере рассматриваемой проблематики: с одной стороны, совершение кибератак оказывают негатив-

ное влияние на систему международной безопасности, вследствие чего закономерной является работа по их предотвращению, в том числе посредством установления правил поведения в киберпространстве. Однако, с другой стороны, само правовое регулирование может развиться только базируясь на субстантивной государственной практике, а в рассматриваемом случае — практике совершения кибератак одним государством в отношении другого, повлекших серьезные последствия. Например, если в ответ на кибератаку на объект критической инфраструктуры (атомную электростанцию и др.) государство ответит кинетической атакой в порядке реализации права на самооборону. Данная ситуация станет тем необходимым мощным импульсом к развитию правового регулирования кибербезопасности, которое поспособствует поиску ответов на имеющиеся вопросы. Вместе с тем полагаем, что одного инцидента будет недостаточно для развития регулирования, как, например, в случае с запуском первого искусственного спутника Земли 4 октября 1957 года в контексте космического права. Доступ к космическому пространству в силу технологических, финансовых и других аспектов фактически имеет лишь небольшое количество государств, а формирование практики в этой отрасли сопряжено с большим расходованием ресурсов. В свою очередь киберпространство покрывает абсолютно все без исключения страны в независимости от уровня их развития. Очевидно, что осуществление разрушительных кибератак *ipso facto* предполагает наличие развитой технологической базы, однако доступ к данной среде не предполагает значительных ограничений. Это дает основание полагать, что достаточно большой круг субъектов теоретически сможет внести вклад в развитие необходимой практики: больший, чем круг государств, форсирующих формирование практики в других сферах международного права, связанных с научно-техническим прогрессом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Cyber-attack: Europol says it was unprecedented in scale [Electronic resource]: BBC. – Mode of access: https://www.bbc.com/news/world-europe-39907965. – Date of access: 15.01.2019.

2. Smith, R. Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say [Electronic resource] / R.Smith // Wall Street Journal. – Mode of access: https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110?redirect=amp. – Date of access: 15.01.2019.

3. Feledy, B. Cyber security and Sovereignty Two levels of digital autonomy [Electronic resource] / BotondFeledy // Think Vishegrad. – Mode of access: http://europeum.org/data/ articles/8-feledy. – Date of access: 15.01.2019.

4. Tallinn Manual on the International Law Applicable to Cyber Warfare / M.N. Schmitt [and others] M.N. Schmitt ed. – 2nd ed. – Cambridge University Press, 2017. – 598 p.

5. Wu, T.S. Cyberspace Sovereignty? – the Internet and the International System / T.S.Wu // Harvard Journal of Law&Technology. – 1997. – Vol.10 (3). – P. 647–666.

6. Boyle, J. Foucault in cyberspace: surveillance, sovereignty and hardwired censors/ J. Boyle // University of Cincinnati law review. – 1997. – Vol.66. – P.177–206.

7. Lotrionte, C. State sovereignty and self-defense in cyberspace: a normative framework for balancing legal rights / C.Lotrionte // Emory international law review. – 2012. – Vol. 26. – P. 825–919.

8. Shmitt, N., Vihul, L. Respect for Sovereignty in Cyberspace / N.Schmitt, L.Vihul // Texas law review. – 2017. –Vol. 95. – P. 1640–1671.

9. Cyberspace Policy Report to Congress Pursuant to the National Authorization Act for fiscal year 2011 [Electronic resource]: U.S. Department of Defense. – Mode of access: https://ns archive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059. – Date of access: 15.01.2019.

10. Island of Palmas case (Netherlands vs. USA), Arbitral Award / Permanent Court of Arbitration, 4 April 1928 [Electronic resource]. – Mode of access: http://legal.un.org/ riaa/cases/vol_II/829-871.pdf. – Date of access: 15.01.2019.

11. Assessment of international legal issues in information operations [Electronic resource]: U.S. Department of Defense. – Mode of access: http://www.au.af.mil/au/awc/awcgate/ dod-io-legal/dod-io-legal. – Date of access: 15.01.2019.

12. Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела [Электронный ресурс]: прин. резолюцией 2222 (XXI) Генер. Ассамблеи, 19 декабря 1966 г. // Организаций Объединенных Наций. – Режим доступа: http://www.un.org/ru/documents/ decl_conv/ conventions/outer_space_governing.shtml. – Дата доступа: 15.01.2019.

13. Конвенция о международной гражданской авиации [Электронный ресурс]: [заключена в г. Чикаго 07.12.1944 г.] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018.

14. Engvers, A. The Principle of Sovereignty in the Air. To what extent can it be upheld against aerial intruders? / A.Engvers. – Lund: Lund University Press, 2001. – 59 p.

15. Конвенция ООН по морскому праву [Электронный ресурс]: [заключена в г. Монтего Бей 10.12.1982 г.] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018.

16. Corn, G. Tallinn Manual 2.0 – Advancing the Conversation [Electronic resource] / G. Corn // Just security. – Mode of access: https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation. – Date of access: 15.01.2019.

17. Jensen, E.T. The Tallinn Manual 2.0: Highlights and Insights / E.T.Jensen // Georgetown Journal of International law. – 2017. – Vol. 48. – P. 735–778.

18. Schmitt, M. N. Remarks at the Atlantic Council Meeting: “Tallinn Manual 2.0 on the International law Applicable to cyber operations” [Electronic resource] / M.N.Schmitt // Atlantic Council. – Mode of access: https://www.atlanticcouncil.org/events/webcasts/ international-law-and-cyber-operations-launch-of-the-tallinn-manual-2-0. – Date of access: 15.01.2018.

19. Egan, B. J. International law and stability in cyberspace / B.J. Egan // Berkeley Journal of International Law. — 2017. — Vol. 35. — P. 169—180.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ СВОБОДЫ ПРЕДОСТАВЛЕНИЯ УСЛУГ В РАМКАХ ЕС И ЕАЭС

М.В. Полудеткина[1)], И.С. Кузнецова[2)]

[1)]*Белорусский государственный университет,*
пр. Независимости, 4, 220030, г. Минск, Беларусь, poludetkinamv@gmail.com
[2)]*Белорусский государственный университет*
пр. Независимости, 4, 220030, г. Минск, Беларусь, kuznetsova.i.s@mail.ru

В Европейском Союзе (ЕС) на данный момент, как и в Евразийском экономическом союзе (ЕАЭС) действует свобода предоставления услуг. Актуальность данной статьи обоснована высокой значимостью рынка услуг в интеграционных объединениях, а также тем, что процесс либерализации предоставления услуг является одним из самых неравномерных. В статье представлен сравнительный анализ правового регулирования свободы предоставления услуг в ЕС и ЕАЭС, на основании которого выявлены сходства и различия в подходах к правовому регулированию данной свободы.

Ключевые слова: услуга; свобода предоставления услуг; ЕС; ЕАЭС.