Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Шон Костиган, *Connections QJ* 20, № 2 (2021): 9-14
https://doi.org/10.11610/Connections.rus.20.2.01

Рецензированная статья

Интернет: суверенный, или глобальный? Россия и Китай настаивают на заключении договора о киберпреступности

Шон Костиган

Европейский центр исследований в области безопасности им. Джорджа Маршалла, https://www.marshallcenter.org/

Аннотация: Под предлогом борьбы с киберпреступностью на международной арене борются два совершенно разных взгляда на киберпространство: модели киберпространства со свободным обменом, которую защищают демократические страны, противостоит так называемая суверенная модель. Продолжаются антидемократические инициативы по переформатированию киберпространства на сугубо национальных условиях, что может ослабить сотрудничество и повысить риски конфликтов и киберпреступности.

Ключевые слова: киберпреступность, киберпространство, суверенитет, сотрудничество, конфликт.

Хаос быстро становится нормой в киберпространстве, где киберпреступники действуют относительно безнаказанно, а новые технологии позволяют национальным государствам оттачивать практику мер воздействия. Компьютеры взламывают почти постоянно — согласно недавнему подсчету, в среднем каждые 39 секунд для устройств, подключенных к Интернету.[1] Если не бороться с киберпреступностью, под угрозой окажется вся вера в способность власти выполнить свои обещания в области безопасности. 61% европейцев обеспокоены возможностью манипуляций на выборах из-за кибератак. Каждый третий американец станет жертвой какого-то киберпреступ-

[1] "Hackers Attack Every 39 Seconds," *Security Magazine*, February 10, 2017, https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.

ления только в этом году, не говоря уже о риске государственного вмешательства.

Дезинформация занимает огромное место в новостях и политике, не меньше, чем во времена COVID-19. Российские кампании дезинформации регулярно распространяли пропаганду о вирусе через аналитические центры и сомнительные службы новостей.[2] Киберпространство стало средой национальной безопасности, влияющей на правительства, корпорации и отдельных граждан. Учитывая такое положение, от универсального договора о киберпреступности, кажется, выиграли бы все.

Под предлогом борьбы с киберпреступностью на международной арене борются два совершенно разных взгляда на киберпространство. Первый в целом можно описать как модель киберпространства со свободным обменом, которую защищают демократические страны. Ему противостоит вторая, так называемая «суверенная модель», где главное внимание уделяется контролю государства над информацией и в конечном счёте над людьми.

18 ноября 2019 г. Комитет ООН 88 голосами против 58 одобрил поддержанную Россией резолюцию о киберпреступности, 34 страны воздержались. Этим успешным для России голосованием была создана Рабочая группа открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер. Хотя это событие может показаться потенциально выгодным, оно несёт прямые последствия для Будапештской конвенции о киберпреступности[3] и существующих механизмов совершенствования борьбы с киберпреступностью, международных и национальных правовых мер, а также долгосрочные внешнеполитические последствия во многих сферах, помимо киберпространства.

Будапештская конвенция – единственная конвенция о киберпреступности, но на неё постоянно оказывает давление Россия и её внешнеполитические партнёры, утверждающие, что само её существование нарушает суверенитет. (Заметим, что Будапештская конвенция открыта для присоединения стран, не входящих в Совет Европы, и является инструментом международного сотрудничество по борьбе с киберпреступностью.)

Россия также активно пытается физически перенести некоторые дискуссии о киберпреступности из Вены, Австрия (где решения принимаются консенсусом) в Нью-Йорк, где голосование большинством голосов может дать России и Китаю существенное преимущество при дальнейших обсуждениях.[4]

---

[2] Julian E. Barnes and David E. Sanger, “Russian Intelligence Agencies Push Disinformation on Pandemic,” *The New York Times*, July 28, 2020, https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html.

[3] Council of Europe, “Convention on Cybercrime,” Treaty No. 185, Budapest, November 23, 2001, www.coe.int/en/web/conventions/full-list/-/conventions/ treaty/185.

[4] U.S. Department of State, “State Department Official on Multilateral Cyber Efforts,” Special Briefing, Office of the Spokesperson, Press Correspondents Room, December

Более того, Россия и Китай могут использовать такие победы в ООН не только для достижения своих далеко идущих целей, бросающих вызов всеобщим правам человека и идеалам открытого, свободного и неделимого Интернета, а также установленному после Второй мировой войны мировому порядку, который Россия и, главное, Китай считают в основном западной конструкцией, по их мнению, несправедливо выгодной западным государствам.

Учитывая эти шаги, в статье утверждается, что Западу нужно готовиться к будущим международным переговорам, которые могут пойти не по плану, включая дальнейшие успехи Китая и России в получении контроля над информацией и изменении киберпространства, каким мы его знаем.

Российское предложение глобальной конвенции о киберпреступности и стремление России продвигать «Рабочую группу открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности»[5] – это прежде всего политические шаги к достижению цели России: создать «систему международной информационной безопасности».[6] Система, которую Кремль стремится создать, будет основана на «Конвенции о международной информационной безопасности», где важные роли отводятся ООН и Международному союзу электросвязи. Кроме того, российская концепция опирается на сильный, даже абсолютный государственный суверенитет, что перечёркивает реальные или предполагаемые международные обязательства государства.[7]

Аргументы России в пользу так называемого суверенного Интернета («Рунета») выделяют несколько аспектов автономной безопасности. Задача создания отдельного российского Интернета была поставлена в Доктрине информационной безопасности 2017 г.[8] – «развитие национальной системы управления российским сегментом сети ‘Интернет’». Контекст этой задачи

19, 2019, https://web.archive.org/web/20191220024014/https://www.state.gov/state-department-official-on-multilateral-cyber-efforts/.

5 United Nations Office for Disarmaments Affairs, “Developments in the Field of Information and Telecommunications in the Context of International Security,” https://www.un.org/disarmament/ict-security/.

6 “Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020,” approved by the President of the Russian Federation on 24 July, 2013, доступ на 29 сентября 2020, http://en.ambruslu.com/highlights-in-russia/basic-principles-for-state-policy-of-the-russianfederation-in-the-field-of-international-information-security-to-2020.html.

7 Alena Epifanova, “Deciphering Russia’s ‘Sovereign Internet Law’: Tightening Control and Accelerating the Splinternet,” *German Council on Foreign Relations*, January 16, 2020, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

8 *Доктрина информационной безопасности Российской Федерации*, утверждена Указом Президента Российской Федерации № 646 5 декабря 2016 г.

– «формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства, что не прямо, но фактически намекает на угрозу информационной безопасности, ощущаемую со стороны США. Цель «национального сегмента Интернета», как его ещё называют – защита собственно информации и критической информационной инфраструктуры России в случае угрозы стабильности, безопасности и функциональности.

Иногда русские оправдывают кажущуюся необходимость удержать внутрироссийский трафик в пределах территориальных границ финансовыми аргументами: с учетом этого стоимость международной маршрутизации в будущем может сильно вырасти.[9] Требование предварительной установки российского программного обеспечения для «отслеживания, фильтрации и перенаправления интернет-трафика»[10] можно рассматривать в контексте информационной безопасности, защиты критической инфраструктуры и поощрения отечественных исследований и разработок.[11] Очевидно, что расширение сферы действия федеральных (Роскомнадзора) правоприменительных механизмов с маршрутизации трафика на все устройства ИКТ тоже усиливает политический и информационный контроль над людьми.

Похоже, что цель этих шагов – создать неопределенность, чтобы разрушить проделанную работу и консенсус в отношении международных норм в киберпространстве, подрывая при этом базовые ценности открытого, бесплатного и доступного Интернета. По мнению многих экспертов, Россия и Китай рука об руку стараются навязать жёсткий подход к киберпространству под контролем государства. Это реализация их авторитарной политики, резко противоречащей демократическому порядку и подрывающей основы глобального экономического порядка и деловых интересов в долгосрочной перспективе.

Хотя голосование в 3-м Комитете ООН показало отсутствие консенсуса о начале переговоров или создании нового правового инструмента по киберпреступности, нужно понимать, что эти попытки не одиноки. Более того, нет консенсуса в отношении сферы регулирования такого нового договора по этому вопросу. Кроме того, страны Западной Европы, похоже, признают, что этот процесс отвлечёт внимание от реформ национального законодательства и развития потенциала, по сути срывая эти усилия.

---

[9] По словам экспертов Касперского, сейчас всего 2% внутрироссийского трафика пересекает границы страны.

[10] "Russia Internet: Law Introducing New Controls Comes into Force," *BBC*, November 1, 2019, https://www.bbc.com/news/world-europe-50259597.

[11] For an opposite view see Alexandra Prokopenko, "Russia's Sovereign Internet Law Will Destroy Innovation," *The Moscow Times*, April 21, 2019, www.themoscowtimes.com/2019/04/21/russias-sovereign-internet-law-will-destroy-innovation-a65317.

Новый международный правовой инструмент по киберпреступности будет дублировать нынешнюю работу и сорвёт решение открытой межправительственной экспертной группы ООН (intergovernmental expert group, IEG)[12] о проведении всестороннего исследования проблемы киберпреступности и реакции на неё стран-участниц.

Россия не только продолжает, но и усиливает призывы к «системе международной информационной безопасности». Тем временем ряд экспертов утверждает, что Западу не удаётся убедить и привлечь на свою сторону другие страны.[13] Москва и Пекин, по-видимому, равнодушны к попыткам «пристыдить» их, обвинениям в кибератаках и шпионаже, например, взломе при помощи SolarWinds.[14] Тем временем на власти западных стран-единомышленников обрушиваются утечки в результате иностранного шпионажа,[15] сообщения о массовой слежке,[16] ухудшение шифрования,[17] и особенно правительственные ожидания помощи корпораций. Чтобы эффективно парировать антидемократические инициативы, Западу нужно устранить одну из трех основ стратегии Кремля: общее недоверие к ИКТ, пробелы в существующем международном праве, или нарратив об экзистенциальной угрозе. Другой путь повышения киберустойчивости – определить общие национальные интересы и задачи разных лагерей и континентов, например, в рамках Основ ответственных действий государств в киберпространстве[18] и Парижского призыва к доверию и безопасности в киберпространстве.[19] Чтобы идти вперёд, Запад должен готовиться к

---

[12] IEG – главный процесс в области киберпреступности на уровне ООН.

[13] Sally Adee, "The Global Internet Is Disintegrating: What Comes Next?" *BBC*, May 15, 2019, www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

[14] Sean S. Costigan, "Charting a New Path for Cybersecurity after SolarWinds." *Diplomatic Courier*, January 4, 2021, www.diplomaticourier.com/posts/charting-a-new-path-for-cybersecurity-after-solarwinds.

[15] Patricia L. Bellia, "WikiLeaks and the Institutional Framework for National Security Disclosures," *Yale Law Journal* 121, no. 1448 (2012), April 2, 2012, Notre Dame Legal Studies Paper No. 12-59, https://ssrn.com/abstract=2033207.

[16] Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (June 2014): 121-144.

[17] Aaron Brantly, "Banning Encryption to Stop Terrorists: A Worse than Futile Exercise," *CTC Sentinel* 10, no. 7 (August 2017): 29-33, https://ctc.usma.edu/wp-content/uploads/2017/08/CTC-Sentinel_Vol10Iss7-10.pdf.

[18] "Joint Statement on Advancing Responsible State Behavior in Cyberspace," United States Department of State, September 23, 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/ and "Eleven Norms of Responsible State Behaviour in Cyberspace," Federal Department of Foreign Affairs FDFA, April 7, 2021, https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html.

[19] "Paris Call for Trust and Security in Cyberspace – Paris Call," https://pariscall.international/en/.

возможному обсуждению договора. Если подготовиться к такому худшему сценарию, можно найти возможность избежать его.

Примечание

Представленные здесь взгляды принадлежат исключительно автору и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

Благодарность

Connections: The Quarterly Journal, Vol. 20, 2021, вышел при поддержке правительства США.

Об авторе

Шон Костиган – см. резюме на стр. 8 этого издания, https://doi.org/10.11610/Connections.rus.20.2.00.