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

Шон Костиган, *Connections QJ* 22, no. 1 (2023): 96-104
https://doi.org/10.11610/Connections.rus.22.1.07

Рецензированная статья

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

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.

Цифровая граница, в которой многие после её появления видели бастион свободы слова и всемирных обменов, оказалась на распутье двух весьма разных мнений, влияющих на будущее киберпространства и прогресса. Первая модель, которую можно назвать моделью открытого киберпространства идеалистов и демократических государств, все чаще сталкивается с ограничительной «суверенной» интернет-парадигмой, которой отдают предпочтение авторитарные правительства. Пока разворачиваются дебаты о будущем киберпространства, разрыв между этими взглядами используют киберпреступники, чьи успехи – и причиняемый ими ущерб – теперь широко признаются в стратегиях национальной безопасности во всём мире.

Поток информации – кровоток современных глобальных систем – находится под угрозой. Правительства и критическая инфраструктура стран мира подвергаются все более активным кибератакам в геометрической прогрессии, и конца этому не видно.[1] В киберпространстве всё чаще видят источник глобальной болезни, поскольку киберпреступники используют уязвимые места, практически не опасаясь последствий, а государства умывают руки, прикрываясь проблемами идентификации, несмотря на то, что технически идентификация становится всё доступнее.[2] Учитывая, что взлом подключённых к Интернету устройств происходит каждые 39 секунд, масштаб угрозы отрицать невозможно. Ставки высоки; если не бороться с киберпреступностью, под угрозой окажется вся вера в способность властей выполнить свои обещания в области безопасности. Обеспокоенность очевидна; большинство европейцев волнуют атаки на правительства их стран.[3] В этом году каждый третий американец станет жертвой какого-то киберпреступления, что указывает на острую необходимость противодействия цифровым угрозам, исходящим как от преступников, так и от государств.

Доверие общества к национальным правительствам и международным структурам подвергается испытаниям с нескольких направлений. По данным ОЭСР, в 2022 году одинаковое число людей доверяли и не доверяли правительству, причём среди молодёжи уровень доверия ещё ниже.[4] На общедоступном веб-сайте Международного валютного фонда удачно описано недоверие к мировому порядку, при особом внимании к четырём факторам: реакция на глобализацию, финансовые кризисы, технологии и искусственный интеллект, и рост популизма.[5] В этой связи стоит отметить, что во время пандемии Covid-19 усилились российские меры дезинформации, ещё больше подрывая доверие,[6] а Китай обвиняют в дальнейшем усилении

---

1 Jonathan Reed, “High-impact Attacks on Critical Infrastructure Climb 140 %,” *Security Intelligence*, June 26, 2023, https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/.

2 Jake Sepich, “The Evolution of Cyber Attribution,” *American University*, April 19, 2023, https://www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm.

3 Thomas Macaulay, “Spate of Cyber Attacks in Europe Increases Concerns about Government Defenses: The Public Sector Is a Growing Target for Cybercrime,” *TNW*, November 9, 2022, https://thenextweb.com/news/cyber-attacks-european-governments-increase-concerns-public-sector-defenses.

4 OECD, “Trust in Government,” www.oecd.org/governance/trust-in-government/.

5 David Lipton, “Trust and the Future of Multilateralism,” *IMF*, May 10, 2018, https://www.imf.org/en/Blogs/Articles/2018/05/10/blog-trust-and-the-future-of-multilateralism.

6 “Disinformation and Russia’s War of Aggression against Ukraine: Threats and Governance Responses,” *OECD*, November 3, 2022, https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/.

хаоса, поскольку он продолжает массовую кражу государственных секретов и интеллектуальной собственности, а также кампании дезинформации.

Москва и Пекин, похоже, мало обеспокоены вопросами своего «доброго имени» или обвинениям в кибератаках и шпионаже – например, во взломе SolarWinds, в котором США официально обвинили Россию.[7] Между тем авторитет западных стран, занимающих схожую позицию, подрывают утечки информации об иностранном шпионаже,[8] новости о массовой слежке,[9] слабое шифрование [10] и общее непонимание широкого спектра новых технических и политических проблем, от распознавания лиц до искусственного интеллекта.

Видение будущего, основанное на настоящем

Как минимум с 2016 года дезинформация со стороны России вызывает глубокую обеспокоенность многих правительств и исследователей во всём мире. Эти кампании политической войны, которые в сфере безопасности иногда называют «активными мерами», используются Россией десятки лет,[11] но с появлением соцсетей и Интернета их стоимость снизилась, а охват и потенциальное воздействие существенно возросли. В период Covid-19 дезинформация заняла центральное место в многочисленных новостях и политических дискуссиях. Примечательно, что усилия России по дезинформации последовательно продвигают лживые версии о вирусе через сомнительные новостные платформы и аналитические центры.[12]

Одним из элементов этой гремучей смеси является деятельность кибердиверсантов разных мастей, от хакеров до сотрудников спецслужб. В

---

7 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.

8 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.

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

10 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.

11 Jolanta Darczewska and Piotr Żochowski, *Active Measures. Russia’s Key Export*, Point of View 64 (Warsaw, Poland: OSW Centre for Eastern Studies, June 2017), https://www.osw.waw.pl/en/publikacje/point-view/2017-05-30/active-measures-russias-key-export.

12 Ben Dubow, Edward Lucas, and Jake Morris, *Jabbed in the Back: Mapping Russian and Chinese Information Operations During the COVID-19 Pandemic* (Washington D.C.: Center for European Policy Analysis (CEPA), December 2, 2021), https://cepa.org/comprehensive-reports/jabbed-in-the-back-mapping-russian-and-chinese-information-operations-during-the-covid-19-pandemic/.

последнее время сама НАТО стала объектом политических хакерских атак, приведших к катастрофическим утечкам внутренних документов.[13] Манипулирование информацией посредством краж и утечки избранных данных, а также использование активных меньшинств стало новой нормой. Демократические правительства подразделяют различные информационные кампании по принципу MDM: на искажённую информацию, дезинформацию, и злонамеренную информацию (*misinformation*, *disinformation*, *malinformation*).[14]

В ежегодной оценке угроз аппарата Директора национальной разведки за 2023 год чётко описана киберугроза, исходящая от Китайской Народной Республики (КНР): «Китай, вероятно, в настоящее время представляет самую широкую, самую активную и постоянную угрозу кибершпионажа для правительственных и частных сетей США. Киберизыскания и экспорт соответствующих технологий Китая увеличивают угрозу агрессивных кибероперацийпротив США ... Китай почти наверняка способен осуществлять кибератаки, способные нарушить работу служб критической инфраструктуры в Соединенных Штатах, включая нефте- и газопроводы и железные дороги».[15]

На сегодняшний день неспровоцированная агрессивная война России против Украины пошла не так, как планировала Россия, что снизило активность её кибератак в других местах. Как отмечается в Ежегодной оценке угроз, «война в Украине была ключевым фактором в определении приоритетов кибероперацийРоссии в 2022 году. Хотя её киберактивность, связанная с войной, оказалась ниже, чем мы ожидали, Россия остаётся важной киберугрозой, совершенствует и использует свои возможности шпионажа, влияния и нападения. Россия рассматривает кибервмешательство как внешнеполитический рычаг, позволяющий влиять на решения других стран».

Поскольку киберпространство оказалось в центре национальной безопасности, влияя на правительства, предприятия и отдельных лиц во всём мире, очевидно, что всеобъемлющий договор о киберпреступности может стать шагом к защите всех людей. 7 марта 2023 года Россия представила Открытой рабочей группе ООН по безопасности и использованию информационных и коммуникационных технологий обновленное предложение по Конвенции ООН об обеспечении международной информационной

---

[13] A.J. Vicens, “NATO Investigating Breach, Leak of Internal Documents,” *CyberScoop*, October 3, 2023, accessed October 5, 2023, https://cyberscoop.com/nato-siegedsecbreac/.

[14] Canadian Centre for Cyber Security, “How to Identify Misinformation, Disinformation, and Malinformation,” ITSAP.00.300, February 2022, https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300.

[15] *Annual Threat Assessment of the U.S. Intelligence Community* (Office of the Director of National Intelligence, February 6, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

безопасности.[16] Открытая рабочая группа по информации и телекоммуникациям в контексте международной безопасности – это инициатива Организации Объединенных Наций (ООН). На момент написания этой статьи в сентябре 2021 года Открытая рабочая группа служила форумом для обсуждения мирного использования ИКТ и предотвращения конфликтов в результате их использования. Страны-участницы ООН, в том числе Россия, приняли участие в работе Открытой рабочей группы и поделились своими взглядами на нормы, правила и принципы ответственного поведения в киберпространстве.

Россия утверждает, что юридически обязывающий договор необходим из-за очевидных недостатков существующего международного права. Однако некоторые страны, включая Швецию, Южную Корею, Колумбию, Австрию и США, считают, что такого пробела нет. Вместо этого эти страны настаивают, что требуется более точное толкование и разъяснение существующего международного права. Кроме того, эти государства полагают, что если девятистраничное российское предложение получит поддержку в ООН, оно может подорвать ответственность государств за действия в киберпространстве и создать серьёзную угрозу цифровым правам человека.[17]

Туман неопределённости

Исторически сложилось так, что взгляды России на международную кибербезопасность часто расходятся со взглядами многих стран Запада. Москва уже давно выступает за «суверенный Интернет» и поддерживает меры государственного контроля над потоками информации.[18] Предложение России о глобальной конвенции по киберпреступности отражает эту точку зрения и усиливает государственный суверенитет в сфере киберпространства. Однако интервенция и преступления России в Украине резко контрастируют с заявленными ею дипломатическими инициативами.[19]

---

[16] "Updated Concept of the Convention of the United Nations on Ensuring International Information Security" (United Nations, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf.

[17] Isabella Wilkinson, "What Is the UN Cybercrime Treaty and Why Does It Matter?" *Chatham House*, August 2, 2023, https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter.

[18] Timmy Broderick, "Russia Is Trying to Leave the Internet and Build Its Own," *Scientific American*, July 12, 2023, https://www.scientificamerican.com/article/russia-is-trying-to-leave-the-internet-and-build-its-own/.

[19] Mercedes Page, "The Hypocrisy of Russia's Push for a New Global Cybercrime Treaty," *The Interpreter*, March 7, 2022, https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty.

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 Открытая рабочая группа для всестороннего исследования киберпреступности и мер её предотвращения. Хотя это событие может показаться потенциально прогрессивным, оно несёт прямые негативные последствия для Будапештской конвенции о киберпреступности [20] и существующих механизмов совершенствования борьбы с киберпреступностью, международных и национальных правовых мер, а также долгосрочные внешнеполитические последствия во многих сферах, помимо киберпространства.

Будапештская конвенция остаётся единственной конвенцией о киберпреступности, но против неё постоянно выступает Россия и её внешнеполитические партнёры, утверждающие, что само её существование нарушает их суверенитет. (Заметим, что Будапештская конвенция открыта для присоединения стран, не входящих в Совет Европы, и является инструментом международного сотрудничества в борьбе с киберпреступностью.)

Предложение России о глобальной конвенции по борьбе с киберпреступностью, а также стремление России создать Открытую рабочую группу по разработкам в области информации и телекоммуникаций в контексте международной безопасности [21] следует понимать прежде всего как политические шаги по продвижению российской цели создания «системы международной информационной безопасности».[22] Система, которую стремится создать Кремль, будет основана на Конвенции о международной информационной безопасности, в которой Организация Объединенных Наций и Международный союз электросвязи будут играть главную роль. Более того, эта российская концепция опирается на сильный и даже абсолютный государственный суверенитет, что подрывает и перечёркивает международные обязательства государств, реальные или предполагаемые.[23]

В то же время российские аргументы в пользу создания так называемого суверенного Интернета (известного как Рунет) подчёркивают несколько аспектов безопасности, достигаемых путём автономии. Цель создания

---

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

[21] 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/.

[22] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, утверждены Президентом Российской Федерации 24 июля 2013 года, http://www.scrf.gov.ru/security/information/document114/.

[23] 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.

отдельного российского интернета была обозначена в доктрине информационной безопасности 2017 года [24] как «развитие национальной системы управления российским сегментом сети 'Интернет'». Контекст этих амбиций «обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнёрства» неявно, но по существу касается предполагаемой угрозы информационной безопасности со стороны США. Целью «национального сегмента сети 'Интернет'», как его ещё называют, была защита информации как таковой и обеспечение безопасности критической инфраструктуры России в случае возникновения угроз стабильности, безопасности и функциональной целостности.

Кроме того, некоторые эксперты по внешней политике в России оправдывают цель организации внутрироссийского трафика в пределах территориальных границ финансовыми аргументами: по их расчётам, стоимость международных маршрутов в будущем может стать слишком высокой.[25] Аналогичным образом, требование предварительно установить российское программное обеспечение для «отслеживания, фильтрации и перенаправления интернет-трафика» [26] можно рассматривать в контексте информационной безопасности, защиты критической инфраструктуры и развития национальных рынков исследований и разработок.[27] Очевидно, что расширение охвата федеральных (Роскомнадзора) механизмов правоприменения от маршрутизации трафика на все устройства ИКТ также усиливает политический и информационный контроль над гражданами.

Используя дипломатию как оружие, Россия продолжает угрожать духу неограниченного Интернета, предвещая мрачное будущее разделённого киберпространства, в котором доминируют несколько влиятельных стран.[28] При различии технических подходов, Россия и Китай параллельно навязывают, по мнению многих экспертов, контролируемый государством апокалиптический подход к киберпространству в мире. Эта политика резко противоречит демократическому порядку и подрывает основы глобальной экономики и коммерческий интерес в долгосрочной перспективе.

---

[24] Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646.

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

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

[27] Противоположный взгляд см. 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.

[28] Rishi Iyengar, Robbie Gramer, and Anusha Rathi, "Russia Is Commandeering the U.N. Cybercrime Treaty," *Foreign Policy*, August 31, 2023, https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty/.

Новый международно-правовой документ по киберпреступности также будет дублировать существующие наработки и предвосхищать выводы открытой межправительственной экспертной группы (International expert group, IEG) ООН [29] по всестороннему исследованию проблемы киберпреступности и мер реагирования на неё со стороны стран-участниц. Более того, нет единого мнения относительно масштабов такого нового договора по кибербезопасности. Кроме того, западные страны, похоже, осознают, что этот процесс может отвлечь усилия от национальных законодательных реформ и текущего наращивания возможностей, по сути подрывая внутренние меры борьбы с киберпреступностью.

В поиске прогрессивного видения киберпространства

Чтобы эффективно дать отпор антидемократическим инициативам, Западу необходимо разрушить один из трёх столпов стратегии Кремля: общее недоверие к ИКТ, недостаточность существующего международного права или идеологию экзистенциальной угрозы. Ещё одним способом повышения устойчивости в кибердискурсе является определение общих национальных интересов и целей для всех лагерей и континентов, например, с помощью Принципов ответственного поведения государств в киберпространстве [30] и Парижского призыва к доверию и безопасности в киберпространстве.[31] Стоит отметить, что, по мнению ряда экспертов, Запад не добился особых успехов в попытках убеждения и взаимодействия с государствами за пределами своего периметра.[32]

Чтобы двигаться вперед, Запад должен подготовиться к обсуждению договора как к одному из возможных вариантов будущего. Готовясь к этому худшему сценарию, необходимо найти новые возможности, позволяющие его избежать. В этот критический период демократическим странам крайне важно объединиться, восстановить стандарты киберпространства и выступить за целостное видение цифрового мира, прежде чем он расколется без надежд на восстановление.

---

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

[30] “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/ и “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.

[31] “Paris Call for Trust and Security in Cyberspace – Paris Call,” https://pariscall.international/en/.

[32] 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.

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. 22, 2023, вышел при поддержке правительства США.

Об авторе

Шон Костиган – см. резюме на стр. 7 этого издания, https://doi.org/10.11610/Connections.rus.20.2.00