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

Инез Миямото, *Connections QJ* 20, № 2 (2021): 47-56
https://doi.org/10.11610/Connections.20.2.05

Рецензированная статья

Дезинформация: Политическая реакция для повышения устойчивости граждан

Инез Миямото

Азиатско-Тихоокеанский центр исследований в области безопасности имени Даниэля Иноуйе

Аннотация: Злоумышленники используют фейковые аккаунты в соцсетях и автоматизированные инструменты так называемой компьютерной пропаганды для проведения операций по дезинформации. Хотя технологические компании и исследователи совершенствуют выявление компьютерной пропаганды, они знают, что искоренить социальных ботов и дезинформацию невозможно. Поскольку компьютерная пропаганда продолжает нарастать, правительства должны обратить внимание на разработку политики, снижающей спрос граждан на дезинформацию. Цель этой статьи – исследовать дезинформацию на стыке технологий и устойчивости граждан. Во-первых, будет рассмотрена текущая картина, чтобы понять воздействие дезинформации на общество и его граждан. Во-вторых, будет проанализировано влияние технологий на появление дезинформации. В-третьих, будут рассмотрены методы снижения потребления дезинформации для повышения устойчивости граждан.

Ключевые слова: дезинформация, цифровая грамотность, устойчивость граждан.

Вступление

С развитием соцсетей в Интернете растёт поток нерегулируемого контента. Ушли социально ответственные издатели, редактора и профильные эксперты, которые оценивали информацию в традиционных СМИ.[1] Теперь

[1] Institute for the Study of Diplomacy, *The New Weapon of Choice: Technology and Information Operations Today* (Washington: Institute for the Study of Diplomacy, October 2020), https://georgetown.app.box.com/s/ivwz4irk3un8blngm3wo0t3uwfc6hpz8.

Creative Commons BY-NC-SA 4.0

граждане сами решают, где правда, а где ложь, и злоумышленники пользуются моментом и открытостью демократий, чтобы влиять на общество посредством дезинформации. Дезинформация определяется как целенаправленное использование ложной информации, создаваемой и распространяемой намеренно, для замешательства или введения в заблуждение, что может содержать смесь правды и лжи или намеренное игнорирование контекста.[2] Правительства должны обратить внимание на разработку политики, снижающей потребление дезинформации гражданами, потому что контроль потока дезинформации – сложная задача в условиях, когда контент всё больше генерируют машины.

Правительства, общественные организации и технологические компании признают дезинформацию мировой проблемой, но не могут дать ответ на неё. Злоумышленники сеют раздор и недоверие, применяя новые, лучшие инструменты, заставляя граждан, ставших объектом дезинформации, беспокоиться о последствиях дезинформации в Интернете. Кнуутила с коллегами выяснили, что 53% обычных Интернет-пользователей (154 195 респондентов в 142 странах) озабочены дезинформацией в Интернете, больше всего (65%) – в Северной Америке.[3] Дезинформация волнует их больше, чем Интернет-мошенничество или запугивание.

В этой статье дезинформация рассматривается на стыке технологий и устойчивости граждан. Во-первых, будет рассмотрена текущая картина, чтобы понять воздействие дезинформации на общество и его граждан. Во-вторых, после рассмотрения воздействия технологий на поступление дезинформации, анализируется потребление дезинформации на предмет устойчивости граждан. Заканчивается статья политическими рекомендациями начать реализацию программы устойчивости граждан.

Компьютерная пропаганда

Злоумышленники используют фейковые аккаунты в соцсетях и автоматизированные инструменты так называемой компьютерной пропаганды для проведения операций по дезинформации. Вули и Ховард (2016) определяют компьютерную пропаганду как «алгоритмы, автоматизацию и надзор человека для намеренного распространения вводящей в заблуждение ин-

[2] Samantha Bradshaw and Lisa-Maria Neudert, “The Road Ahead: Mapping Civil Society Responses to Disinformation,” Working Paper (Washington: National Endowment for Democracy, January 2021), https://www.ned.org/mapping-civil-society-responses-to-disinformation-international-forum.

[3] Aleksi Knuutila, Lisa-Maria Neudert, and Philip N. Howard, “Global Fears of Disinformation: Perceived Internet and Social Media Harms in 142 Countries,” COMPROP Data Memo 2020.8, December 15, 2020, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2020/12/Global-Fears-of-Disinformation-v.13.pdf.

формации в соцсетях».[4] К инструментам компьютерной пропаганды относятся, в частности, боты, клоны, робо-тролли и дипфейковые видео.

Первые, боты — сокращение от роботов — это незапрещённые компьютерные программы, например, для автоматизации задач на веб-сайтах. При операциях дезинформации сетевые боты имитируют людей в соцсети, связываясь и взаимодействуя с людьми и системами. Например, это могут быть сетевые боты – фейковые автоматизированные аккаунты, или киборги – аккаунты, используемые человеком при помощи бота. Злоумышленники также массово используют ботов в соцсетях для создания иллюзии единства при онлайн-пропаганде.[5]

Вторые, «левые» аккаунты или клоны – это фиктивные аккаунты, созданные человеком или группой людей для обмана. Например, человек или группа создаёт множество аккаунтов в соцсети для влияния на подписчиков «лайками» или голосованием в постах. Они также могут исказить или увести в сторону онлайн-дискуссию или поддержать конкретный Интернет-аккаунт. Так, русская разведка использовала левый аккаунт в Твиттере под именем Jenna Abrams с 70 000 подписчиков, чтобы влиять на консервативных избирателей на выборах в США в 2016 г.[6]

Третьи, тролли – реальные люди, которые намеренно провоцируют других в Интернете, размещая подстрекательские или оскорбительные посты. Если их аккаунты автоматизированы при помощи программ, они называются робо-тролли и могут генерировать контент.[7] Исследователей тревожит использование робо-троллей экстремистами и террористами. Те испытывают программы искусственного интеллекта (ИИ), генерирующие тексты, которые могут использовать робо-тролли.[8] Генерирующие текст программы (ИИ) могут быть мощным инструментом в руках экстремистов и террористов, потому что они могут быстро плодить пропаганду, которую сейчас люди создают вручную, что занимает много времени.

---

4 Samuel C. Woolley and Philip N. Howard, "Automation, Algorithms, and Politics: Political Communication, Computational Propaganda, and Autonomous Agents – Introduction," *International Journal of Communication* 10 (2016), https://ijoc.org/index.php/ijoc/article/view/6298.

5 Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," Working Paper No. 2017.11 (Oxford: University of Oxford, 2017), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

6 Ben Collins and Joseph Cox, "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World," *The Daily Beast*, November 3, 2017, https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world.

7 Tom Simonite, "To See the Future of Disinformation, You Build Robo-Trolls: AI-Powered Software Is Getting Better and Could Soon Be Weaponized for Online Disinformation," *Wired*, November 19, 2019, https://www.wired.com/story/to-see-the-future-of-disinformation-you-build-robo-trolls.

8 Simonite, "To See the Future of Disinformation, You Build Robo-Trolls."

Четвёртые – инструменты на основе ИИ, позволяющие создавать дипфейковые видео: изменённые цифровыми методами видео для введения в заблуждение. По данным Sensity AI (ранее – DeepTrace), количество дипфейковых видео растёт. 96% дипфейковых видео в интернете – это порнография со знаменитостями без их согласия.[9] Эксперты считают, что число и сложность этих видео будет и дальше расти с появлением новых доступных дипфейковых сервисов и инструментов.[10] Уже сейчас высококачественные дипфейковые видео трудно распознать.[11]

В ответ на рост компьютерной пропаганды технологические компании начали применять контрмеры при помощи ИИ. В то время как компании научились лучше выявлять и блокировать ботов, разработчики ботов начали использовать более продвинутые технологии, например, созданные ИИ изображения, тексты и видео.[12] Поскольку искусственно генерируемый контент имитирует стиль человека, контент ИИ сложно отличить от сгенерированного человеком.[13] Новые сетевые боты больше похожи на аккаунты людей, потому что ИИ используют для создания «гибрида действий автомата и человека».[14] Проблему усложняет то, что злоумышленники могут окутать правдивую информацию ложью, из-за чего технологическим компаниям сложно помечать информацию как достоверную или недостоверную.[15] Как следствие, в будущем граждане не смогут определить достоверность информации или подлинность аккаунта.

Тем временем компьютерная пропаганда растёт во всём мире. Брэдшоу и др. отмечают, что государственные и политические деятели в 81 стране используют соцсети для распространения компьютерной пропаганды.[16] Такой рост представляет проблему, поскольку компьютерная

---

9 Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, *The State of Deepfakes: Landscape, Threats and Impact* (Amsterdam: Deeptrace, 2019), https://sensity.ai/reports/.

10 Ajder, Patrini, Cavalli, and Cullen, *The State of Deepfakes.*

11 Matt Groh, "DetectDeepFakes: How to Counteract Misinformation Created by AI," по состоянию на 28 января 2021, www.media.mit.edu/projects/detect-fakes/overview.

12 Stefano Cresci, "A Decade of Social Bot Detection," *Communications of the ACM* 63, no. 10 (October 2020): 72-83, https://doi.org/10.1145/3409116.

13 Renée DiResta, "The Supply of Disinformation Will Soon Be Infinite: Disinformation Campaigns Used to Require a Lot of Human Effort, but Artificial Intelligence Will Take Them to a Whole New Level," *The Atlantic*, September 20, 2020, https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400.

14 Cresci, "A Decade of Social Bot Detection."

15 Kate Starbird, "Disinformation's Spread: Bots, Trolls, and All of Us," *Nature* 571, no. 449 (2019), https://doi.org/10.1038/d41586-019-02235-x.

16 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Oxford: University of Oxford, 2021), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report20-FINALv.3.pdf.

пропаганда – «мощный инструмент, способный разрушить демократию».[17,18] Хотя технологические компании и исследователи продолжают совершенствовать распознавание компьютерной пропаганды, они знают, что искоренить сетевых ботов и дезинформацию невозможно. Нужны усилия всего общества для повышения устойчивости граждан к растущей угрозе, которая разрушает доверие в обществе.

Правительства реагируют на дезинформацию с обеих сторон уравнения поступления и потребления. С точки зрения поступления дезинформации важно ограничить поток дезинформации в информационную экосистему. С точки зрения потребления нужно решить проблему потребления гражданами дезинформации.[19] Далее в статье рассмотрены обе части уравнения поступления и потребления дезинформации.

Поступление дезинформации

Очевидно, что решение проблемы поступления дезинформации побуждает правительства, технологические компании и гражданское общество к сотрудничеству для выработки ответа всего общества. Политикам сложно противодействовать поступлению дезинформация из-за отсутствия главного органа, ответственного за противодействие операциям дезинформации. Поэтому в стране может не быть скоординированной политики реагирования. Как следствие, при дезинформационной атаке на внутреннюю политику (например, безопасность на выборах, катастрофы, реагирование на пандемию и вакцинация) профильное ведомство может не иметь средств, чтобы отреагировать на атаку. А когда права и обязанности пересекаются, бывает сложно определить, какое ведомство в государстве должно организовать реагирование (внутренняя безопасность, министерство обороны, министерство юстиции, избирательная комиссия и т.д.). Злоумышленники видят зазоры между правительственными ведомствами и используют их для атак.

Подходы к ограничению дезинформации с точки зрения поступления включают законодательство, правительственных контролёров по проверке фактов и информационные войска, но оценивать их эффективность пока ещё слишком рано.[20] Например, в Германии в 2017 г. приняли Закон о

---

[17] Woolley and Howard, “Computational Propaganda Worldwide.”

[18] Stanford History Education Group (SHEG), “Evaluating Information: The Cornerstone of Civic Online Reasoning,” Working Paper (Stanford: SHEG, 2016), https://stacks.stanford.edu/file/druid:fv751yt5934/SHEG%20Evaluating%20Information%20Online.pdf.

[19] Alina Polyakova and Daniel Fried, “Democratic Defense Against Disinformation 2.0,” *Atlantic Council*, June 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf.

[20] Olga Robinson, Alistair Coleman, and Shayan Sardarizadeh, “A Report of Anti-Disinformation Initiatives” (Oxford: University of Oxford, August 2019),

правопорядке в сети, обязывающий компании, которые ведут соцсети, удалять проявления ненависти и другие нарушения в контенте. Недостатком этого закона является то, что он может привести к цензуре и ограничить свободу слова.[21]

Ещё одним подходом с точки зрения поступления является внедрение в Евросоюзе добровольного, самостоятельно применяемого стандарта для технологических компаний, таких как Google, Facebook, Mozilla и Twitter. В 2018 г. они подписали Кодекс ЕС по борьбе с дезинформацией и обязались повысить прозрачность политической рекламы, удалив фейковые аккаунты, и решить проблему злонамеренного использования ботов. Первые выводы о Кодексе неоднозначны. Сохраняется нехватка доверия между компаниями, ведущими соцсети, правительствами и гражданским обществом, в основном из-за того, что технологические компании ограничивают доступ к своим данным.[22] В 2020 г. Еврокомиссия дала комплексный ответ на дезинформацию – План действий европейской демократии (European Democracy Action Plan).[23] Одна из его инициатив – сделать Кодекс дополнительным нормативным актом.

Со своей стороны, Эстония, бывшая объектом русской дезинформации с 2007 г., привлекает для этого гражданское общество. Правительство создало добровольные силы безопасности – Лигу защиты Эстонии – под эгидой Министерства обороны. Лига защиты Эстонии помогает кибероборонe, а также мониторит Интернет на предмет дезинформации и ведёт контрпропагандистский блог, чтобы бороться с ложными нарративами. Эстония также привлекает группу интернет-активистов «Балтийские эльфы» для реагирования на русских троллей, сообщения о ботах, распространения контрнарративов.[24] Кроме того, поскольку в Эстонии проживает немалая русская община, там работает русскоязычный телеканал для противодействия дезинформации.

Тайвань – ещё одна страна, чей подход предусматривает участие всего общества в обуздании потока дезинформации. С 2018 г., когда на Тайване впервые назначили Министра информатизации, страна инициировала не-

---

https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/08/A-Report-of-Anti-Disinformation-Initiatives.

[21] "Germany: Flawed Social Media Law," *Human Rights Watch*, February 14, 2018, https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

[22] James Pammet, "EU Code of Practice on Disinformation: Briefing Note for the New European Commission" (Carnegie Endownment for International Peace, March 3, 2020), https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187.

[23] European Commission, "European Democracy Action Plan," accessed February 2, 2021, https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en.

[24] Joseph Robbins, "Countering Russian Disinformation" (Center for Strategic & International Studies, September 23, 2020), https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation.

сколько гражданских технических инициатив для укрепления доверия граждан и гражданского общества. Министр информатизации не только придумал прозрачное правительство, но и объединил усилия правительственных групп, технологических компаний и граждан по противодействию дезинформации. Тайвань реализует ряд успешных инициатив, включая Сеть проверки фактов в Интернете, чат-боты для проверки фактов в соцсетях и мемы против нарративов дезинформации.[25]

Главное преимущество подхода Эстонии и Тайваня – участие граждан в борьбе с дезинформацией. Войну с дезинформацией можно выиграть, только ведя её вместе с гражданами, которые потребляют и распространяют дезинформацию. Если граждане игнорируют дезинформацию, её распространение затухает. В следующем разделе этой статьи мы рассмотрим методы борьбы с потреблением дезинформации.

Потребление дезинформации

Один из путей сократить потребление дезинформации – цифровая грамотность и знания о дезинформации.[26] Доказано, что цифровая грамотность может быть эффективной стратегией борьбы с дезинформацией.[27] Поскольку общепринятого определения цифровой грамотности нет, в этой статье цифровая грамотность включает медийную, новостную и информационную грамотность и определяется как «способность использовать информационно-коммуникационные технологии для поиска, оценки, создания и передачи информации, требующая когнитивных и технических навыков».[28]

Часто считают, будто пожилые люди более восприимчивы к дезинформации, чем молодые, из-за того, что им сложно пользоваться цифровыми технологиями. Есть данные, что пожилые люди чаще делятся дезинформацией в соцсетях.[29] Но молодые люди, более привычные к технологиям, тоже подвержены дезинформации из-за низкой цифровой грамотности. Группа изучения истории Стэнфордского университета (Stanford History Ed-

---

[25] Rorry Daniels, “Taiwan’s Unlikely Path to Public Trust Provides Lessons for the US,” *Brookings*, September 15, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/09/15/taiwans-unlikely-path-to-public-trust-provides-lessons-for-the-us.

[26] Polyakova and Fried, “Democratic Defense Against Disinformation 2.0.”

[27] Andrew M. Guess et al., “A Digital Media Literacy Intervention Increases Discernment Between Mainstream and False News in the United States and India,” *Proceedings of the National Academy of Sciences* 117, no. 27 (2020): 15536-15545, htpps://www.pnas.org/content/pnas/117/27/15536.full.pdf.

[28] American Library Association (ALA), “Literacy for All: Adult Literacy through Libraries,” (Chicago: ALA, 2019), http://www.ala.org/aboutala/sites/ala.org.aboutala/files/content/Literacy%20for%20All_Toolkit_Online.pdf.

[29] Andrew Guess, Jonathan Nagler, and Joshua Tucker, “Less Than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook,” *Science Advances* 5, no. 1 (January 2019), https://doi.org/10.1126/sciadv.aau4586.

ucation Group) выяснила, что студентам школ, ВУЗов и колледжей трудно оценить достоверность информации в соцсетях. Они ошибочно считают информацию достоверной, исходя из неверных фактов: верхние результаты поиска в поисковике, принадлежность сайта к домену .org или аккаунт в Твиттере с большим числом подписчиков.[30] Эти недостатки указывают на необходимость цифровой грамотности общества.

Политики и педагоги переосмысливают основы цифровой грамотности, включая критическое мышление и гражданскую активность в программы обучения. Ранее правительства больше занимались развитием цифровых навыков, необходимых для инициатив «цифровой трансформации», что не всегда включало критическое мышление и гражданскую активность. Однако более новые программы включают устойчивость граждан. Так, в Канаде в 2019 г. предложили совместную инициативу «Цифровой гражданин» (Digital Citizen). Эта инициатива поддерживает гражданскую активность, в частности, разработку учебных материалов, инвестиции в программы исследований и медийную грамотность (гражданскую, новостную и цифровую).[31] Есть и неправительственные программы. Например, два института Университета Южной Флориды (Флоридский центр кибербезопасности (Florida Center for Cybersecurity) и Флоридский центр методик обучения (Florida Center for Instructional Technology)) объединились с неприбыльным беспартийным аналитическим центром «New America» для развития навыков киберграждан у школьников. Они планируют создать Рабочую группу по кибергражданству (Cyber Citizenship Working Group) для взаимодействия с деятелями гражданского общества и Портал кибергражданства (Cyber Citizenship Portal), где будут представлены образовательные материалы для общественности.[32]

Пока ещё рано оценивать эффективность программ обучения цифровой грамотности и информированности. Более того, цифровая грамотность граждан – лишь первый шаг к новым знаниям и навыкам, таким, как алгоритмическая грамотность и информационная грамотность (об ИИ).[33] Чтобы подготовиться к новым вызовам, политикам нужно стратегическое предвидение, дабы лучше подготовить граждан к дезинформационным атакам

---

[30] Stanford History Education Group, “Evaluating Information: The Cornerstone of Civic Online Reasoning.”

[31] UNESCO, “Digital Citizen Initiative,” *UNESCO Diversity of Cultural Expressions*, по состоянию на 1 февраля 2021, https://en.unesco.org/creativity/policy-monitoring-platform/digital-citizen-initiative.

[32] “Cyber Florida, Florida Center for Instructional Technology and New America Launch New Partnership to Improve ‘Cyber Citizenship’ Skills for K-12 Students,” *New America* (International Security), December 16, 2020, www.newamerica.org/international-security/press-releases/cyber-florida-fcit-new-america-partnership-to-improve-cyber-citizenship.

[33] Ramesh Srinivasan, “This Is How Digital Literacy Can Transform Education,” *World Economic Forum*, March 3, 2020, https://www.weforum.org/agenda/2020/03/why-is-digital-literacy-important.

нового поколения. Подводя итоги, начальной точкой повышения устойчивости граждан являются следующие политические рекомендации:

Политическая рекомендация №1: Повышать цифровую грамотность всех граждан

Правительства должны разработать программу цифровой грамотности для обучения цифровой грамотности всех граждан, выработав её стандарт или принципы. Существует много систем, используемых в качестве основы создания программы цифровой грамотности. В их числе – Глобальные основы цифровой грамотности (Digital Literacy Global Framework) Организации Объединённых Наций по вопросам образования, науки и культуры (ЮНЕСКО), Основы цифровой грамотности граждан (Digital Competence Framework for Citizens) Европейского Союза и Основы цифрового интеллекта (DQ) д-ра Ю Хьон Пак.

Заложив основы, правительство должно разработать программу обучения цифровой грамотности, соответствующую потребностям граждан на разных этапах жизни (первичный, вторичный и третичный уровень). Разработав программы обучения для разных уровней, педагоги и учителя смогут быстро адаптировать материал к своей учебной программе. Методы обеспечения доступности контента для взрослых включают организацию массовых открытых онлайн-курсов и создание онлайн-видео для самообучения на протяжении всей жизни. Навыки цифровой грамотности на только повысят устойчивость граждан к дезинформации, но и подготовят их к неминуемой цифровой трансформации, то есть переустройству общества в результате внедрения цифровых технологий.

Политическая рекомендация №2: Включать цифровую безопасность в ежегодные кампании информирования о кибербезопасности

Осведомленность граждан начинается с кампаний информирования общественности. Многие правительства уже используют ежегодный месяц или неделю кибербезопасности для повышения безопасности в Интернете и пропаганды мер безопасности. Поскольку главный элемент кибербезопасности – это понимание онлайн-угроз для безопасности граждан, информирование о дезинформации необходимо. В частности, нужно рассказывать о сетевых ботах и об оценке источников информации в интернете. Кампания информирования даёт ещё одну возможность привлечь внимание граждан к дезинформации.

Политическая рекомендация №3: Усиливать гражданское общество, укрепляя доверие и информируя об использовании компьютерной пропаганды государством и политиками

Укрепление доверия и обмен информацией повышает устойчивость граждан. Граждане не поймут масштаб и силу компьютерной пропаганды против их страны, если они не вооружены информацией. Им нужно знать, кто

совершил дезинформационную атаку, какую, где, когда и как, и как они могут противостоять дезинформации. Поскольку политическая компьютерная пропаганда может быть организована государством, правительства не всегда могут рассказать все детали атаки по соображениям секретности. Для достижения доверия правительству надо найти способ откровенно сообщить об атаке, в то же время придерживаясь требований безопасности. Информацию также следует доносить простым языком, избегая технических терминов и канцляризмов.

Правительства также могут поощрять партнёрство государства с частным сектором для обмена информацией и сотрудничества при решении задач технической компьютерной пропаганды и устойчивости граждан. Поскольку технологические компании владеют данными, необходимыми правительству, общественным организациям и учёным для выработки мер противодействия, партнерство позволяет вырабатывать инновационные решения путём привлечения граждан и укреплять доверие благодаря обмену информацией и открытому диалогу. Сейчас правительства, технологические компании и гражданское общество больше, чем когда-либо, должны сотрудничать для укрепления доверия и устойчивости граждан.

Примечание

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

Благодарность

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

Об авторе

Инез Миямото – профессор кибербезопасности в Азиатско-Тихоокеанском центре исследований в области безопасности имени Даниэля Иноуйе.
Электронная почта: miyamotoi@dkiapcss.net