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

М. Капарини & А. Гоголевска
Connections QJ 20, № 1 (2021): 95-104
https://doi.org/10.11610/Connections.rus.20.1.06

Рецензированная статья

Вызовы управления революционными технологиями

Марина Капарини[1] и Агнешка Гоголевска [2]

[1] *Стокгольмский институт исследования мира, http://sipri.org*

[2] *Европейский университет информационных технологий и экономики в Варшаве, http://www.eu.edu.pl/*

Аннотация: Экспонентное развитие цифровой информации и технологий трансформирует механизмы политики (геополитики), общества, экономики и безопасности. Связанные с этим вызовы для управления беспрецедентны, они искажают и позволяют манипулировать публичным дискурсом и политическими последствиями. Одним из самых глубоких изменений, вызванных неограниченным развитием инновационных технологий, является появление новой экономической логики, основанной на повсеместном цифровом слежении за повседневной жизнью людей и перепродаже этой информации для прогнозирования. ЕС реагирует на эти новые условия медленно и неадекватно. Установление действенного контроля над деятелями и процессами, использующими инновационные технологии, потребует не только специальных умений управления данными, но и более глубокого понимания влияния этих технологий, налаживания партнерских отношений между государственным и частным секторами и повышения политической и социальной ответственности корпораций, занимающихся их разработкой и внедрением.

Ключевые слова: управление данными, искусственный интеллект, управление, государственная политика, «капитализм слежки», защита персональных данных.

Вступление

Развитие информационных технологий меняет современное общество. Выделяют два типа технологий. Первый – цифровая информация и телекоммуникации, особенно быстро развивающиеся с 1980-х гг. и дошедшие уже до

сотовой беспроводной связи пятого поколения, или 5G, что обеспечивает лучшую связь и передачу бóльших объемов данных, чем когда-либо.[1] Вторая группа технологий, хоть и имеет разную природу, коллективно именуется «экспонентными технологиями» в связи с беспрецедентными темпами технического прогресса.[2] К ним относятся передовая робототехника и беспилотные летательные аппараты, расширенная и виртуальная реальность, 3D-печать, биотехнологии, блокчейн, «интернет вещей», автономные транспортные средства и, конечно, обучение машин, или же искусственный интеллект (ИИ).[3]

Новые технологии уже нашли множество применений для повышения защиты[4] и безопасности. Они также нарушили традиционные пути передачи информации и, возможно, подорвали демократические принципы и процессы. Они меняют правила игры, разрушая существующие мировые механизмы политики, экономики и безопасности, усиливая отдельных акторов и в то же время подрывая или низвергая устоявшиеся процессы управления и методы контроля. Масштаб задач, возникающих для управления, беспримерен и требует лучшего понимания фундаментального влияния новых технологий на нашу общественную, политическую, экономическую жизнь и геополитику. Политикам и их помощникам также необходимы гораздо более глубокие технические знания и интерес к осуществлению действенного контроля над акторами и процессами, использующими этих технологий.

Информационные технологии и безопасность

Новые технологии «информационно ёмки», они собирают и выдают огромные и все возрастающие объемы данных, что представляет серьезную проблему для эффективного правительственного контроля над инструментами национальной безопасности и даже для способности исполнительной власти контролировать собственные службы безопасности. Данные традиционно разделяли и обрабатывали в базах данных, но ускоренное развитие технологий получения данных в настоящее время требует иной модели управления, основанной на защите данных и межотраслевых комплексных

---

[1] Sascha Segan, “What Is 5G?” *PC Magazine*, February 25, 2021, https://www.pcmag.com/article/345387/what-is-5g; John McCann, Mike Moore, and David Lumb, “5G: Everything You Need to Know,” *techradar*, May 2021, https://www.techradar.com/news/what-is-5g-everything-you-need-to-know.

[2] Creative HQ, “What is Exponential Technology?” https://creativehq.co.nz/what-is-exponential-technology/.

[3] Отличное введение в экспонентные технологии см. в: “Exponential Technology Trends that Will Define 2019,” *SU Blog*, December 10, 2018, https://su.org/blog/exponential-technology-trends-defined-2019/.

[4] Ilya Pozin, “6 Innovative Technologies Designed To Improve Our Safety,” *Forbes*, November 19, 2015, https://www.forbes.com/sites/ilyapozin/2015/11/19/6-innovative-technologies-designed-to-improve-our-safety/.

подходах к управлению данными.[5] Более того, безопасное применение экспонентных технологий в любом элементе сектора безопасности требует предоставления надежных данных ответственным органам. Поэтому правительствам, наряду с традиционной практикой управления, необходимы навыки управления данными. Некоторые правительственные ведомства в последнее время начали переходить от центров обработки данных к облачным вычислениям.[6] Однако в отрасли считают, что государственные органы многих стран противятся переносу правительственных данных в облако, и лишь 10-20 % работы правительств приходится на облачные технологии,[7] что указывает на неготовность многих правительств к этим качественным изменениям.

Информационные технологии сегодняшнего дня имеют иные свойства, чем системы прошлого. К критическим элементам относится малоразмерная техника, например, процессоры, видеокарты и миниатюрные веб-камеры, или нематериальные вещи – специальное программное обеспечение, алгоритмы и техническое ноу-хау, связанное с обучением машин и развитием ИИ. Кроме того, эти информационные технологии часто имеют двойное применение. Например, беспилотник, оснащенный дневной и ночной видеокамерами и РЛС для геосъемки, может быть средством военной разведки или слежки правоохранительными органами, просто меняя конечного пользователя.[8] Аналогичным образом, в то время как шифрование данных связи необходимо для защиты бизнеса или тайных операций от разведки конкурентов, его можно использовать для сокрытия преступной деятельности от правоохранительных органов.[9] А машинный интеллект, используемый для совершенствования Интернет-поисковиков, можно применять и в военных целях, от объединения данных до автономного беспилотного оружия и кибервойн. Эти факторы усложняют контроль передовых технологий традиционными режимами экспортного контроля.[10]

---

5 "Data Governance in the Age of Exponential Technology," *Information Week*, December 28, 2018, https://www.informationweek.com/big-data/data-governance-in-the-age-of-exponential-technology/a/d-id/1333558.

6 Barb Darrow, "Why the U.S. Government Finally Loves Cloud Computing," *Fortune*, September 2, 2016, https://fortune.com/2016/09/02/us-government-embraces-cloud/.

7 IBM, "Transforming Government with Cloud Technologies," https://www.ibm.com/downloads/cas/MEK8LK2B.

8 Pix4D, "4 Reasons Drones Will Revolutionize Accident Scene Response," Medium.com, May 26, 2016, https://medium.com/the-science-of-drone-mapping/4-reasons-drones-will-revolutionize-accident-scene-response-a1db234eeccf.

9 Europol, "Internet Organised Crime Threat Assessment 2018," https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

10 Jade Leung, Sophie-Charlotte Fischer, and Allan Dafoe, "Export Controls in the Age of AI," *War on the Rocks*, August 28, 2019, https://warontherocks.com/2019/08/export-controls-in-the-age-of-ai/.

Чтобы запутать окончательно, искусственный интеллект превращает технологии в «черные ящики», которые, намеренно или нет, могут быть непрозрачными даже для специалистов.[11] Неспециалисты в правительстве и обществе могут быть вообще технически неграмотными в устройствах на основе ИИ, что еще больше усложняет эффективное управление и контроль.[12] За специалистами в ИИ начинается настоящая охота в новой глобальной экономике. Их важность для дальнейших инноваций и их концентрация в горстке крупнейших мировых высокотехнологических компаний становятся вопросом национального благосостояния ближайших десятилетий и элементом геополитической конкуренции, особенно с Китаем.[13] Так, президент США недавно издал *Указ о сохранении американского лидерства в области искусственного интеллекта*. Среди прочего, Указ предусматривает изменение иммиграционной политики, разрешая приглашать и нанимать специалистов в области разработки ИИ [14] – вот вам еще одно свидетельство важности долгосрочного технологического лидерства.

Поскольку над революционными технологиями в государственном и частном секторах будет работать множество различных акторов, необходимы новые инструменты организации безопасности, способные охватить неправительственных и коммерческих деятелей при обеспечении национальной безопасности. Поэтому сегодня правительства должны найти пути эффективного сотрудничества с крупными частными компаниями, небольшими стартапами, НПО, университетами, исследовательскими институтами и даже отдельными лицами. Только так они могут быть в курсе событий и как-то влиять и контролировать деятельность частных компаний, представляющих угрозу национальной безопасности или политической стабильности страны.

Информационные технологии и общественно-политическая сфера

Информационные технологии все больше влияют на качество и характер политики в результате нескольких взаимосвязанных процессов. СМИ и информационное пространство существенно изменились, и многие политики

---

[11] Will Knight, “The Dark Secret at the Heart of AI,” *MIT Technology Review*, April 11, 2017, https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/.

[12] См. Amitai Etzioni and Oren Etzioni, “Should Artificial Intelligence Be Regulated?” *Issues in Science and Technology* 33, no. 4 (Summer 2017), https://issues.org/perspective-should-artificial-intelligence-be-regulated/.

[13] Ann Scott Tyson, “In Race to Dominate AI, US Researchers Debate Collaboration with China,” *The Christian Science Monitor*, May 3, 2019, https://www.csmonitor.com/World/Asia-Pacific/2019/0503/In-race-to-dominate-AI-US-researchers-debate-collaboration-with-China.

[14] “Maintaining American Leadership in Artificial Intelligence,” Executive Order 13859 of February 11, 2019, https://www.federalregister.gov/documents/2019/02/14/ 2019-02544/maintaining-american-leadership-in-artificial-intelligence.

сейчас получают новости через социальные сети.[15] Социальные сети влияют на восприятие информации и формирование позиции.[16] Пользователи соцсетей подвергаются эффекту «герметичной среды» из-за персонализованных алгоритмов поисковиков, подталкивающих нас к тем, кто думает, как мы, фильтруя статьи и веб-сайты при онлайн-поиске и сужая количество новостных источников, которые мы выбираем.[17] Полученный в результате фильтр предлагает статьи, отражающие, укрепляющие и усиливающие наши убеждения.[18] Кроме того, чем активнее сообщество (единомышленников) в соцсети, тем больше оно изолировано от иных взглядов и тем больше поляризуются его взгляды.[19]

Разумные приложения развились настолько, что могут манипулировать и поляризовать политический дискурс.[20] Цифровые технологии позволяют менять лица в реальном масштабе времени; *Adobe* создает «фотошоп для аудио», способный редактировать диалог так же легко, как фотографию; канадский *Lyrebird* предлагает сервис, способный подделать голос на основе всего нескольких минут звучания. Когда *Google* открыл код своего *TensorFlow*, это быстро привело к появлению *FakeApp*, позволяющего убедительно заменить лицо на кадрах с чьим-то телом.[21] Компания *OpenAI* недавно создала фейковый текстовый редактор, который, как говорят, настолько хорош в имитации стиля и темы письма, что его не выпустили в оборот из-за боязни злоупотреблений.[22] В будущем подделка данных и намеренная дез-

---

[15] В 2018 г. примерно две трети, или 68% американцев получали новости из соцсетей. Elisa Shearer and Katerina Eva Matsa, “News Use Across Social Media Platforms 2018,” *Pew Research Center*, September 10, 2018, www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/.

[16] Ana Lucía Schmidt, *et al.*, “Anatomy of News Consumption on Facebook,” *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 12 (March 2017): 3035-3039, https://doi.org/10.1073/pnas.1617052114, https://www.pnas.org/content/114/12/3035

[17] Schmidt, *et al.*, “Anatomy of News Consumption on Facebook.”

[18] Eli Pariser, “Beware Online ‘Filter Bubbles,’” *TED2011*, March 2011, https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles.

[19] Roheeni Saxena, “The Social Media ‘Echo Chamber’ is Real,” *Ars Technica*, March 13, 2017, https://arstechnica.com/science/2017/03/the-social-media-echo-chamber-is-real/.

[20] Это 100% поддельное видео Барака Обамы наглядно показывает ненадежность того, что когда-то считалось достоверными данными. См. James Vincent, “Watch Jordan Peele Use AI to Make Barack Obama Deliver a PSA about Fake News,” *The Verge*, April 17, 2018, https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed.

[21] Tad Friend, “How Frightened Should We Be of A.I.?” *The New Yorker*, May 7, 2018, https://www.newyorker.com/magazine/2018/05/14/how-frightened-should-we-be-of-ai.

[22] Alex Hern, “New AI Fake Text Generator May be too Dangerous to Release, Say Creators,” *The Guardian*, February 14, 2019, https://www.theguardian.com/technology/2019/feb/14/elon-musk-backed-ai-writes-convincing-news-fiction.

информация с использованием этих технологий может разрушить национальные системы правосудия и спровоцировать или обострить имеющийся конфликт. Повсеместное проникновение Интернета и легкость, с которой анонимные пользователи могут распространять дезинформацию, открыли демократические системы для политических манипуляций. Как продемонстрировала не существующая ныне информационная компания *Cambridge Analytica*, которая неправомерно получила доступ к данным почти 87 млн. пользователей Facebook, чтобы создать профили избирателей в попытках повлиять на президентские выборы в США в 2016 году в пользу Дональда Трампа, и была замешана в дезинформации, повлиявшей на референдум в Великобритании о выходе из ЕС, неправомерное использование таких технологий может серьезно запутать общественное мнение и посеять раздор.

Проблема признана публично. Согласно недавнему исследованию, большинство европейцев (85%) назвали фейковые новости проблемой своих стран. Восемь из десяти (83%) назвали фейковые новости проблемой демократии в целом, а больше трети (39%) сказали, что власти страны должны бороться с распространением фейковых новостей.[23]

Кроме того, новые технологии наблюдения дают службам безопасности возможности, делающие традиционные методы правительственного надзора неэффективными. Ярким примером является коммерческое шпионское ПО под названием *Pegasus*. После установки оно дает операторам неограниченный доступ к личным данным в мобильных телефонах, включая пароли, контакты, события, текстовые сообщении и голосовые звонки из популярных приложений. *The Citizen Lab* выявил 45 стран, где могли шпионить операторы *Pegasus*. По крайней мере десть операторов оказались вовлеченными в слежку за границей.[24] Даже если закон разрешает лишь дистанционное электронное наблюдение, без записи или хранения данных, учитывая технические возможности шпионского ПО, будет очень трудно доказать нарушение закона разведывательными службами, если они сами не сознаются в злоупотреблениях. Это делает надзор исполнительных органов за службами такой же иллюзией, как и защиту личной жизни граждан.

Новая экономическая логика «капитализма слежки»

Влияние информационных технологий ныне выходит далеко за рамки правоохранительной деятельности, внутренней и национальной безопасности и ведения войн, а также манипуляций в политической и гражданской сфе-

[23] "New Report Highlights Inconsistent Approach to Combating Disinformation," Oxford Internet Institute, University of Oxford, August 22, 2019, https://www.oii.ox.ac.uk/news/releases/new-report-highlights-inconsistent-approach-to-combatting-disinformation/.

[24] Bill Marczak, *et al.*, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab*, University of Toronto, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

рах. Мы наблюдаем появление сложных, управляемых данными, взаимосвязанных технологических систем, проникающих во все сферы человеческой деятельности. Цифровые технологии пронизывают нашу деятельность, слова, образы и действия дома и в магазине, в средствах массовой информации, образовании, на отдыхе и в обществе, а также наши социальные отношения. Далее информация, получаемая с помощью этих технологий, беспрецедентно обобщается, пакуется в профили с высокой степенью прогнозирования и открыто продается любому заинтересованному субъекту при почти полном отсутствии юридических ограничений или государственного надзора.

По мнению Шушаны Зубофф, глубокие изменения, вызванные почти не ограниченным и не регулируемым развитием информационных технологий за последние 20 лет, породили новую экономическую логику, ставшую преемником промышленного капитализма. Отслеживание и поиск данных поисковиков и приложений социальных сетей, смартфонов и датчиков позволяет коммерсантам составлять подробные профили людей, их повседневных привычек и действий, симпатий и антипатий. Окружающие нас устройства и технологии собирают объемы данных о каждом действии, сказанном или написанном слове и даже проявленных эмоциях и перепродают коммерсантам в рамках новой социально-экономической логики накопления, получившей название «капитализм слежки».[25] При «капитализме слежки» прибыль получают от слежки и изменения поведения людей. Данные наблюдений в реальном масштабе времени за повседневной деятельностью, разговорами, эмоциями людей монетизируются, продаются и перепродаются компаниям, стремящимся влиять на людей и массово менять их поведение.[26] По мнению Зубофф, все эти изменения привели к возникновению поведенческого фьючерсного рынка, где торгуют прогнозами человеческой деятельности.[27] Этот рынок прогнозов действий людей чрезвычайно прибылен: прибыль *Google* за четыре года выросла на 3500 % на фоне быстрого развития в этой области. «Капитализм слежки» в настоящее время вездесущ и стремятся собирать поведенческие данные не только для компаний и технологий Кремниевой долины, но и других отраслей и компаний.[28]

Но в то время как сбор и объединение больших объемов данных происходят повсеместно, серьезная асимметрия информации затрудняет понимание обществом и правительствами. Коммерсанты заявляют о собствен-

---

[25] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

[26] Shoshana Zuboff, “The Secrets of Surveillance Capitalism,” *Frankfurter Allgemeine Zeitung*, March 5, 2016, https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html.

[27] Zuboff, *The Age of Surveillance Capitalism*.

[28] Shoshana Zuboff, “Facebook, Google, and a Dark Age of Surveillance Capitalism,” *Financial Times Magazine*, January 25, 2019, https://www.ft.com/content/7fafec06-1ea2-11e9-b126-46fc3ad87c65.

ном контроле над такими данными, которые многократно объединяются и перепродаются с целью их использования для влияния на будущее поведение. Наглядный тому пример – температурная система для умного дома *Google Nest*. Снятие и сбор ею данных с помощью связанного набора приложений и функций настолько обширен, что потребовался бы прилежный клиент, который должен просмотреть почти 1000 связанных соглашений о конфиденциальности, чтобы установить один термостат.[29] Это указывает на дополнительную проблему отсутствия информированного согласия на сбор и перепродажу данных о потребителях. Такие системы создают огромные препятствия для способности людей и власти понимать их и управлять ими. Изменения в объеме и масштабах превзошли и обошли традиционные подходы к управлению этими сферами с помощью закона и политики до такой степени, что все больше наблюдателей видят в этом беспрецедентные последствия для человеческой деятельности и независимости.[30]

Регулирование

Пока что реакция ЕС на появление революционных технологий была медленной и разочаровывающей по большинству пунктов и не привела к качественным изменениям в законодательной базе стран-участниц. Так, регуляторная деятельность ЕС в области искусственного интеллекта не соответствует темпам развития этих технологий. ЕС выработал ряд руководящих принципов ЕС для приемлемого ИИ: (1) законность, (2) этичность, и (3) четкость, и сейчас приступает к этапу комитета высокого уровня и добровольных пилотных проектов.[31] Вряд ли это адекватный ответ на техническую революцию, он не требует даже единой скоординированной реакции национальных законодательных органов стран-участниц.

Введение новых регламентов ЕС, поощряющих использование новых технологий в интересах европейской безопасности, идет так же медленно, как и для использования беспилотников. Органы регулирования ЕС с 2015 г. не продвинулись далее создания Агентства по безопасности полётов ЕС и обновления правил авиационной безопасности.[32] Как результат, несмотря

[29] Guido Noto La Diega and Ian Walden, "Contracting for the 'Internet of Things': Looking into the Nest," Queen Mary School of Law Legal Studies Research Paper no. 219/2016, February 1, 2016, https://ssrn.com/abstract=2725913.

[30] James Bridle, *The New Dark Age: Technology and the End of the Future* (London: Verso Books, 2018).

[31] European Commission, "Ethics Guidelines for Trustworthy AI," https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[32] European Commission, "Impact Assessment Accompanying the Document 'Proposal for a Regulation of the European Parliament and of the Council on Common Rules in the Field of Civil Aviation and Establishing a European Union Aviation Safety Agency, and Repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council'," https://eur-lex.europa.eu/resource.html?uri=cellar:ec9e79f3-9ce9-11e5-8781-01aa75ed71a1.0001.02/DOC_2&format=PDF.

на успешные испытания беспилотников для морской разведки,[33] *Frontex*, например, не разрешают использовать беспилотники у Средиземноморского побережья из-за отсутствия правил.

В некоторых случаях регуляторные меры даже непреднамеренно чрезмерно подвергли граждан ЕС опасности электронного наблюдения, как в случае с Директивой ЕС о хранении данных связи.[34] Эта Директива была направлена на усиление борьбы с терроризмом, но одновременно открыла двери для усиления слежки спецслужб за гражданами в ряде европейских стран, таких, как Чехия, Кипр, Эстония, Финляндия, Франция, Германия, Ирландия, Польша и Великобритания, включив право служб неограниченно использовать данные связи в национальное законодательство. Службы ожидаемо начали использовать данные непропорционально и без привязки к угрозам национальной безопасности. В Польше, например, разведслужбы в 2014 г. просили раскрыть данные связи рекордные 2,35 миллиона раз.[35]

Защита личной жизни стала еще одной проблемой для регуляторных органов ЕС. Хотя создание Общего регламента защиты данных (*General Data Protection Regulation*, *GDPR*) является шагом в правильном направлении с точки зрения защиты личной жизни, это неадекватный ответ на основные вопросы, поднятые информационными технологиями и рынком поведенческих фьючерсов. Еврокомиссия и национальные правительства были пассивны и неэффективны в привлечении *Cambridge Analytica* и *Facebook* к ответственности за вмешательство в национальные выборы и подрыв демократических систем. На результат голосования по *Brexit* повлияли не слишком законные действия *Facebook* и связанных с ним компаний, нарушавших британские избирательные законы и подрывавших демократические процедуры.[36] Однако попытки привлечь Марка Цукерберга и *Facebook* к ответственности провалились. А после голосования по *Brexit* практика сбора поведенческих данных для прогнозирования и влияния на будущее поведение быстро расширилась.

---

[33] Frontex, “Frontex Begins Testing Unmanned Aircraft for Border Surveillance.” See also Ilkka Tikanmäki, Jari Räsänen, Harri Ruoslahti, and Jyri Rajamäki, “Maritime Surveillance and Information Sharing Systems for Better Situational Awareness on the European Maritime Domain: A Literature Review,” in *Digital Transformation, Cyber Security and Resilience of Modern Societies*, ed. Todor Tagarev, Krassimir T. Atanassov, Vyacheslav Kharchenko, and Janusz Kacprzyk (Cham: Springer, 2021), 117-135, https://doi.org/10.1007/978-3-030-65722-2_8.

[34] Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, abolished 2014.

[35] “Rok z ustawą inwigilacyjną. Co się zmieniło,” *Fundacja PANOPTYKON*, January 18, 2017, https://panoptykon.org/biblio/rok-z-ustawa-inwigilacyjna.

[36] См. Carole Cadwalladr, “Facebook’s Role in Brexit and the Threat to Democracy,” TED2019, April 2019, https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy.

Заключение

В то время, как инновационные технологии меняют экономику, безопасность и, пожалуй, саму политическую логику современной жизни, политикам и законодателям необходимо становиться более технически грамотными. Слушания в Конгрессе в апреле 2018 г., на которых Марк Цукерберг отвечал на вопросы американских сенаторов и членов Палаты представителей, четко показали непонимание многими представителями американского правящего класса элементарных аспектов современных цифровых платформ.[37] Но проблема уходит своими корнями еще глубже, отражая нашу неспособность понять и подумать об экспонентных технологических изменениях и слиянии разных технологий. Лучшее понимание политиками этих процессов необходимо для обеспечения действенности законов об экспонентных технологиях и для минимизации правительствами вреда от их применения для своих граждан и политических систем. Правила должны касаться не только технических или организационных аспектов; законодателям также следует найти пути усиления политической и социальной ответственности корпораций, занимающихся разработкой, продажей и применением информационных технологий.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами авторов и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторах

Д-р Марина Капарини – старший научный сотрудник и директор программы государственного управления и общества СИПРИ. Ее исследования охватывали миротворчество и связь безопасности с развитием. Марина изучала разные аспекты организации безопасности и правосудия в постконфликтных и посттоталитарных условиях, включая развитие полиции, надзор за разведкой, отношения между гражданскими и военными и регулирование деятельности частных военных и охранных компаний. В последнее время занимается миротворческой деятельностью и укреплением полиции, вынужденным переселением и организованной преступностью. До прихода в СИПРИ в декабре 2016 г. работала на руководящих должностях в Норвежском институте международных отношений, Международном центре правосудия переходного периода и Женевском центре демократического контроля над вооруженными силами.
E-mail: marina.caparini@sipri.org

Агнешка Гоголевска – см. краткую справку на стр. 34 этого выпуска.

[37] “Zuckerberg Explains the Internet to Congress,” https://www.youtube.com/watch?v=ncbb5B85sd0.

Благодарность

Журнал *Connections: The Quarterly Journal*, Vol. 20, 2021 издается при поддержке правительства США.