Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

M. Caparini & A. Gogolewska
Connections QJ 20, no. 1 (2021): 91-100
https://doi.org/10.11610/Connections.20.1.06

Research Article

Governance Challenges of Transformative Technologies

Marina Caparini [1] *and Agnieszka Gogolewska* [2]

[1] *Stockholm International Peace Research Institute, http://sipri.org*

[2] *European University of Information Technology and Economics In Warsaw, http://www.eu.edu.pl/*

Abstract: The rise of digital information and exponential technologies are transforming political/geopolitical, social, economic, and security arrangements. The challenges they pose to governance is unprecedented, distorting and used to manipulate public discourse and political outcomes. One of the most profound changes triggered by the unconstrained development of innovative technologies is the emergence of a new economic logic based on pervasive digital surveillance of people's daily lives and the reselling of that information as predictive information. EU responses to this new environment have been slow and inadequate. Establishing effective controls over the actors and processes harnessing innovative technologies will require not only specialized data governance skills but a deeper understanding of the impact of these technologies, the forging of partnerships across the public-private divide, and the establishment of greater political and social accountability of corporate actors involved in their development and application.

Keywords: Data governance, artificial intelligence, governance, public policy, surveillance capitalism, data privacy.

Introduction

The rise of innovative technologies is having a transformative impact on contemporary society. Two types of technologies stand out. The first is digital information and telecommunications, which has been developing ever more rapidly since the 1980s and is now entering the fifth-generation cellular wireless, or 5G,

enabling better connectivity and transfer of larger amounts of data than ever.[1] The second cluster of technologies, although differently engineered, are collectively defined as "exponential technologies" due to their unprecedented rate of technical progress.[2] They include advanced robotics and drones, augmented and virtual reality, 3D printing, biotech, blockchain, the Internet of Things (IoT), autonomous vehicles and, of course, machine learning, which is also known as Artificial Intelligence (AI).[3]

The new technologies have already found many applications for enhancing safety[4] and security. They also have disrupted traditional ways of sharing information and have possibly undermined democratic principles and processes. They are the ultimate game-changer, globally disrupting existing political, economic, and security arrangements, empowering certain actors while subverting or overturning long-established governance processes and control regimes. The scale of challenges posed to governance is unprecedented and requires a heightened understanding of the fundamental impact new technologies have on our social, political, economic, and geopolitical spheres. It is also imperative that policy-makers and those who assist them develop a much deeper technological awareness and interest in exerting effective controls over the actors and processes by which these technologies are harnessed.

Innovative Technologies and Security

The new technologies are 'data-hungry,' gathering and producing enormous and ever-increasing amounts of data and posing significant challenges to effective government control over the instruments of national security and even the executive's ability to control their own agents in the security sector. Traditionally, data was fragmented and managed in data silos. But the accelerated data-generating technologies of today demand a different management model founded on data security and cross-sectoral, holistic approaches to data governance.[5] Moreover, the safe use of exponential technologies in any security domain re-

[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] For an excellent guide to exponential technologies, see: "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/.

[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.

quires supplying reliable data to responsible agencies. Therefore, governments need to acquire skills in data governance alongside traditional governance practices. Some government agencies have recently begun moving from data centers to cloud computing.[6] However, industry sources suggest that public authorities in many countries have resisted moving government data to the cloud and only 10-20 percent of government work uses the cloud,[7] a sign that many governments are poorly prepared for this qualitative change.

Innovative technologies of today do not have the same properties as the systems of the past. Among the critical elements are small pieces of hardware such as processors, graphics cards, and miniature webcams, or intangibles such as dedicated software, algorithms, or technical know-how associated with machine learning and AI development. Moreover, these innovative technologies tend to be dual-use. For example, a drone equipped with day and night vision cameras and a radar for use in geological mapping surveys can become an instrument for military or law enforcement surveillance by simply changing the end-user.[8] Similarly, while encryption of telecommunications data is necessary to protect business or security operations from competitive intelligence, it may also be used to conceal organized criminal activity from an investigation by law enforcement agents.[9] And machine intelligence that has been employed to refine internet browser search platforms can also be applied to the means of warfare, from data fusion to autonomous unmanned weapons systems and cyberwar. Such factors make the most advanced technologies difficult to control by traditional export control regimes.[10]

To make matters more complicated, artificial Intelligence turns technologies into "black boxes" that, intentionally or not, maybe opaque even to experts.[11] Non-specialists in governments and society may, for all intents and purposes, be technically illiterate vis-à-vis AI-based devices, raising further challenges to their

---

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/.

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/.

effective governance and control.[12] AI specialists are quickly becoming one of the most sought-after resources in the new global economy. Their importance in driving further innovation and their concentration in a handful of the largest global tech firms are becoming an issue of national well-being in the coming decades and a component of geopolitical competition, particularly with China.[13] In a recent example, the President of the United States issued the *Executive Order on Maintaining American Leadership in Artificial Intelligence*. Among other things, the Order provides for changes in immigration policy, allowing to recruit and retain specialists in the field of AI development[14] – yet another sign of the importance of long-term technological leadership.

As there will be many different actors working on transformative technologies across the public and private sectors, new tools of security governance are needed that can encompass non-governmental actors and commercial actors in the shaping of national security. Thus, the governments of today need to find ways to cooperate effectively with large private enterprises, small startups, NGOs, universities, research institutes, and even individuals. Only in such a way can they keep abreast of developments and yield a degree of influence and control over the activities of the private entities if they constitute a threat to the country's national security or political stability.

Innovative Technologies and the Civic and Political Sphere

Innovative technologies are increasingly affecting the quality and nature of the political sphere through several interrelated processes. The media and information landscape has undergone important changes, and a large proportion of individuals within the body politic now receive much of their news through social media.[15] Social media affects the way that information is consumed and opinions are formed.[16] Consumers of social media have become subject to an "echo

[12] See 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.

[15] In 2018 some two-thirds or 68% of Americans accessed news on social media. Elisa Shearer and Katerina Eva Matsa, "News Use Across Social Media Platforms 2018," *Pew Research Center*, September 10, 2018, https://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

chamber" effect due to personalized search engine algorithms that tend to steer us towards those who think like us, filtering the articles and websites that are returned in online searches and narrowing the number of news sources we select.[17] The resulting "filter bubble" delivers articles that tend to reflect, reinforce and amplify our existing beliefs.[18] Further, the more active a community (of like-minded individuals) is on social media, the more segregated it is from differing views, and the more polarized its views become.[19]

As intelligent applications have progressed, so has the potential to manipulate and polarize political discourse.[20] Digital technologies can perform face swaps in real time; Adobe is creating a "Photoshop for audio" that can edit dialogue as easily as a photo; Canadian Lyrebird offers a service that can fake an individual voice based on only a few minutes of audio. When Google made its TensorFlow code open-source, it swiftly led to FakeApp, enabling a convincing swap of someone's face onto footage of somebody else's body.[21] Recently, the company OpenAI has created a fake text editor that reportedly is so good at imitating a given writing style and subject that they have not released it for fear of its malicious use.[22] In the future, the corruption of data and deliberate misinformation using these technologies may undermine national justice systems and initiate or aggravate existing conflicts. The pervasive penetration of the Internet and the ease with which anonymous actors can spread mis- and dis-information has opened democratic systems to political manipulation. As demonstrated by the now-defunct Cambridge Analytica—the data firm which improperly accessed the user data of up to 87 million Facebook users to build voter profiles in attempts to sway the 2016 US presidential election in favor of Donald Trump and was implicated in misinformation that swayed the UK Brexit referendum—the misuse of such technologies has a significant potential to confuse public discourse and sow discord.

---

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 This 100% fake video of Barak Obama vividly demonstrates the corruption of what was once considered hard data. See 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.

The problem has been publicly recognized. According to the recent survey, a majority of Europeans (85%) described fake news as a problem in their countries. A further eight out of ten (83%) said "fake news" was a problem for democracy in general, while over a third (39%) said national authorities should be responsible for combating the rise of "fake news."[23]

Furthermore, the new surveillance technologies empower security institutions to a degree that renders traditional methods of government oversight ineffective. A case in point is the commercial spyware called Pegasus. Once installed, it allows operators unlimited access to private data in mobile phones, including passwords, contact lists, calendar events, text messages, and live voice calls from popular apps. The Citizen Lab has identified 45 countries where Pegasus operators may have been conducting surveillance operations. At least ten operators appeared engaged in cross-border surveillance.[24] Even if laws allow only for remote electronic invigilation without recording or storing the data, given the technical abilities of the spyware, it would be very difficult to prove the intelligence services to be on the wrong side of the law unless they admitted to wrongdoing. Thus, executive oversight of the services is becoming illusory, as is the protection of privacy for citizens.

The New Economic Logic of "Surveillance Capitalism"

The impact of innovative technologies now extends well beyond the realms of law enforcement, internal and national security and warfare, and beyond the manipulation of the political and civic spheres. We witness the emergence of complex, data-driven, interconnected technological systems that penetrate all spheres of human activity. Digital technologies permeate our activities, words, images, and interactions in our homes and places of commerce, media, education, leisure, and communities, and our social interactions. Moreover, the information from these technologies is harvested to an unprecedented degree, packed into highly predictive profiles, and openly sold to any interested actor, with an almost complete lack of legal constraint or government oversight.

According to Shoshana Zuboff, the profound changes wrought by the relatively unconstrained and unregulated development of innovative technologies over the past 20 years have given rise to a new economic logic that is the successor of industrial capitalism. Data tracking and mining of web engines and social media applications, smart devices, and sensors enable commercial actors to compile detailed profiles of individuals, their daily habits and activities, their likes

[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/.

and dislikes. Volumes of data on every activity, spoken or written word, and even the emotions we display are collected by the devices and technologies that surround us and resold as predictive information by and to commercial actors in a new economic and social logic of accumulation that has been termed "surveillance capitalism."[25] In surveillance capitalism, profits derive from the surveillance and modification of human behavior. Data based on real-time surveillance of people's daily activities, conversations, emotions are monetized and sold and resold to companies that want to influence people and modify their behavior at scale.[26] According to Zuboff, all those developments have led to the creation of a behavioral futures market that trades in predictions of human activity.[27] This market in predictive human futures is extremely lucrative: Google's profits increased 3,500 percent over four years on the back of its rapid development in this area. Surveillance capitalism is now ubiquitous, with the impetus to hoover behavioral data encompassing not only Silicon Valley firms and technologies but other industries and firms.[28]

But while the big data collection and packaging is pervasive, serious information asymmetries hamper understanding by societies and governments. Commercial actors assert proprietary control over such data, which is combined and resold manifold times, with an underlying logic of using it to influence future behavior. Google Nest, a smart home temperature system, provides a telling example. Its data scraping and collection through the related suite of apps and features is so extensive that it would require a diligent client who installs a single thermostat to review almost 1000 related privacy agreements.[29] This indicates the additional problem of lack of informed consent to the collection and reselling of data about consumers. Such systems pose huge challenges to the ability of people and their governors to understand and govern them. Developments in scope and scale have overwhelmed and bypassed traditional approaches to governing these spheres through law and policy, to the extent that a growing number of observers maintain they pose unprecedented implications for human agency and autonomy.[30]

---

[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.

[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).

Regulations

So far, EU responses to the advent of transformative technologies have been slow and disappointing on most counts and failed to deliver qualitative change in legislative frameworks of member states. For example, the regulatory activities of the EU in the realm of Artificial Intelligence do not match the pace of development of those technologies. The EU has so far elaborated the set of EU guidelines for trustworthy AI being: (1) lawful, (2) ethical, and (3) robust, and is now entering the stage of the high-level committee and voluntary pilot projects.[31] It is hardly an adequate response to the technological revolution and does not yet require a standardized and coordinated response from national legislatures in member countries.

Introducing new EU regulations fostering the use of new technology for European security has been slow, too, as is the case for drone flights. EU regulators since 2015 have failed to go beyond establishing the European Union Aviation Safety Agency and updating aviation safety rules.[32] Consequently, despite successful testing of drones for maritime surveillance,[33] Frontex, for example, has been prevented from using unmanned aerial vehicles along the Mediterranean coast due to a lack of regulations.

In some cases, regulatory efforts have even inadvertently over-exposed the EU citizens to electronic surveillance, as in the case of the EU directive on data retention in telecommunication.[34] The directive aimed to enhance efforts against terrorism. However, it also paved the way to intensified surveillance of citizens by intelligence services in several European countries such as the Czech Republic, Cyprus, Estonia, Finland, France, Germany, Ireland, Poland, and the UK by embedding the rights of services to unrestricted use of telecommunication data in national laws. Predictably, the services started using the data out of pro-

---

[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.

[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.

portion and without connection to national security threats. In Poland, for example, the intelligence services asked for disclosure of telecommunication data a record 2.35 million times in 2014.[35]

Privacy protection has been another challenge to EU regulators. While the General Data Protection Regulation (GDPR) establishment is a step in the right direction in terms of privacy, it is an inadequate response to the major issues raised by innovative technologies and the behavioral futures market. The European Commission, alongside the national governments, was passive and ineffective in holding Cambridge Analytica and Facebook responsible for interfering in national electoral processes and undermining democratic systems. The outcome of the Brexit vote was heavily influenced by the largely illicit actions of Facebook and Facebook-related campaigns, breaking British electoral laws and subverting democratic procedures.[36] However, attempts to hold Mark Zuckerberg and Facebook accountable have failed. And since the Brexit vote, the practices of collecting behavioral data to predict and influence future behavior have grown apace.

Conclusions

As innovative technologies transform the economic, security, and arguably political logic of contemporary life, policy-makers and legislators need to become far more technologically literate. The Congressional hearings of April 2018 in which Mark Zuckerberg responded to questions posed by US senators and members of the house of representatives clearly demonstrated the failure of many in the American governing class to understand some of the most basic aspects of modern digital platforms.[37] However, the problem goes even deeper, reflecting our inability to find ways to understand and think about exponential innovative technological change and the convergence of multiple technologies. Better understanding by policy makers of these processes is necessary if laws on exponential technologies are to be effectively regulated and controlled, and if governments aim to effectively minimize the harm to their citizens and political system from their effects. Regulations should not only concentrate on the technological or organizational side of affairs; legislators should also find ways to provide for greater political and social accountability of corporate organizations involved in developing, selling, or applying innovative technologies.

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

[36] See 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.

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

Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 20, 2021, is supported by the United States government.

About the Authors

Dr. **Marina Caparini** is a Senior Researcher and Director of the Governance and Society Programme at SIPRI. Her research focuses on peacebuilding and the nexus between security and development. Marina has conducted research on diverse aspects of security and justice governance in post-conflict and post-authoritarian contexts, including police development, intelligence oversight, civil-military relations, and the regulation of private military and security companies. She has recently focused on police peacekeeping and capacity-building, forced displacement, and organized crime. Prior to joining SIPRI in December 2016, she held senior positions at the Norwegian Institute for International Affairs, the International Center for Transitional Justice, and the Geneva Centre for the Democratic Control of Armed Forces.
E-mail: marina.caparini@sipri.org

Agnieszka Gogolewska - see the short CV on p. 32 of this issue.