Technological Change and Innovation as Security Threats

Jan Martin Rolenc[1,*]

[1]Jan Masaryk Centre for International Studies, Faculty of International Relations, University of Economics, Prague, nám. W. Churchilla 4, Praha 3, 130 67, Czech Republic

Abstract. Technological change and innovation, together with the related development of science, have been perceived as drivers of social and economic progress and public optimism in the globalizing world. Indeed, in the past centuries and especially decades, there has been a huge advancement of humankind that can be both felt and measured. However, people have also learned that science and technology can be misused or abused, or they can have unintended consequences (cf. nuclear fission). Especially in times when the public feels that the change is fast and unprecedented, they also provoke fear and resentment. Science, technological change, and innovation can be presented and perceived as security threats, i.e. securitized. It seems that, now, we are living in one of such historical periods. The goal of the paper is to analyse if and how technological change and innovation are presented or perceived as security threats, especially in the Czech political and public discourse. To reach the goal, we can ask the following research questions: Are science, technological change, and innovation securitized? What are the concrete examples of emerging technologies and innovations that are securitized? (e.g. artificial intelligence and robotics, biotechnologies) Is the narrative present in the Czech political and public discourse? Is the securitization process successful? What are the lessons learned and recommendations for policy?

1 Introduction

Technological change and innovation, together with the related development of science, have been perceived as drivers of social and economic progress and public optimism in the globalizing world. Indeed, in the past centuries and especially decades, there has been a huge advancement of humankind that can be both felt and measured. However, people have also learned that science and technology can be misused or abused, or they can have unintended consequences (cf. nuclear fission). Especially in times when the public feels that the change is fast and unprecedented, they also provoke fear and resentment. Science, technological change, and innovation can be presented and perceived as security threats, i.e. securitized. It seems that, now, we are living in one of such historical periods.

* Corresponding author: rolencj@vse.cz

The goal of the paper is to analyse if and how technological change and innovation are presented or perceived as security threats, especially in the Czech political and public discourse. To reach the goal, we can ask the following research questions: Are science, technological change, and innovation securitized? What are the concrete examples of emerging technologies and innovations that are securitized? (e.g. artificial intelligence and robotics, biotechnologies) Is the narrative present in the Czech political and public discourse? Is the securitization process successful? What are the lessons learned and recommendations for policy?

The paper first identifies the methods that are used in secondary literature and specifies qualitative content analysis and securitization as the method and theoretical concept used in this research. Then, it presents the results of the literature review and of the analysis of the Czech political and public discourse. Finally, the paper discusses the results and some policy implications of the research.

2 Methods and theory: Foresight, content analysis, and securitization

The review of recent academic literature on technological change and innovation as security threats revealed that the methods mostly used are foresight and expert surveys [e.g. 1-5]. The current state of development of science and technology, as well as the complexity and uncertainty surrounding the development require interdisciplinarity and imagination of the highest possible number of experts. This could not have been done by the author of this paper himself; therefore, the first part of the following section 3 presents the key relevant secondary sources.

The second part of the section 3 is based on a qualitative content analysis [6] of the Czech media landscape and governmental or other official documents, as well as on recent public opinion polls. The Czech media are represented by the public television news channel ČT24. The analysed official documents are Policy Statement of the Government of the Czech Republic 2018, Concept of the Czech Republic's Foreign Policy 2015, Security Strategy of the Czech Republic 2015, and Defence Strategy of the Czech Republic 2017. The purpose is to illustrate, which issues are presented and discussed in the Czech political discourse, i.e. which new or emerging technologies and innovations are securitized, how, and if the securitization is successful among the public.

Securitization is (a concept of) a political process developed by the Copenhagen school of security studies [7, 8]. In the process, securitization actors asses certain events, situations, or issues as existential threats to referent objects and, thus, if their effort is socially accepted, they justify exceptional measures (outside the boundaries of normal politics), which it is necessary to accept face to face to the treats. Therefore, any issue may move from outside of politics (depoliticized) to the realm of politics (politicized) and further to the security dimension as a certain type of special politics or the realm "above politics" (securitized issue).

3 Results: Literature review and the Czech political discourse

3.1 Technological change and innovation as security threats in academic literature

Technophobia – the fear, dislike, or avoidance of new technology is as old as the modern science and technology. With the beginning of the industrial revolution, people became afraid of losing their jobs or that their traditional, simple, modest lifestyles would be

destroyed. For example, Luddites, the anti-technology workers in the early modern British textile industry, used to destroy machines or otherwise sabotaged production. But major fears appeared only in the 19th century, as reflected in the literary Romantic movement, and especially in the 20th century and after the WW2. Those fears were driven by nuclear proliferation and the related strategic situation of the so called Mutually Assured Destruction (MAD), the development of other modern military technologies, as well as by the emerging environmental concerns. Paradoxically, the arts, especially literature and the Hollywood film industry, were more prominent in reflecting those developments than academic debates [9].

The recent expert and academic debates discuss security threats related to technological change, often also called risks, challenges, or vulnerabilities, in connection to societal resilience [e.g. 10] and ethical values [e.g. 11-13]. New or emerging technologies, innovation, and the fourth industrial revolution (4IR) will require especially better governance and disruption management [e.g. 10, 14, 15]. Recently, these issues were discussed in the World Economic Forum's (WEF) *Global Risks Reports* [4, 5] and in the publications of the EU-funded project called *Foresight of Evolving Security Threats Posed by Emerging Technologies* (FESTOS) [e.g. 1-3].

The WEF's 2017 report [4] identified 12 key emerging technologies, namely 3D printing, advanced materials and nanomaterials, artificial intelligence (AI) and robotics, biotechnologies, energy capture, storage and transmission, blockchain and distributed ledger, geoengineering, ubiquitous linked sensors, neurotechnologies, new computing technologies, space technologies, and virtual and augmented realities. The WEF's 2019 report [5] suggests that "this is an era of unparalleled resources and technological advancement, but for too many people it is also an era of insecurity." According to the report, the 4IR brings especially "the blurring of the line between the human and the technological."

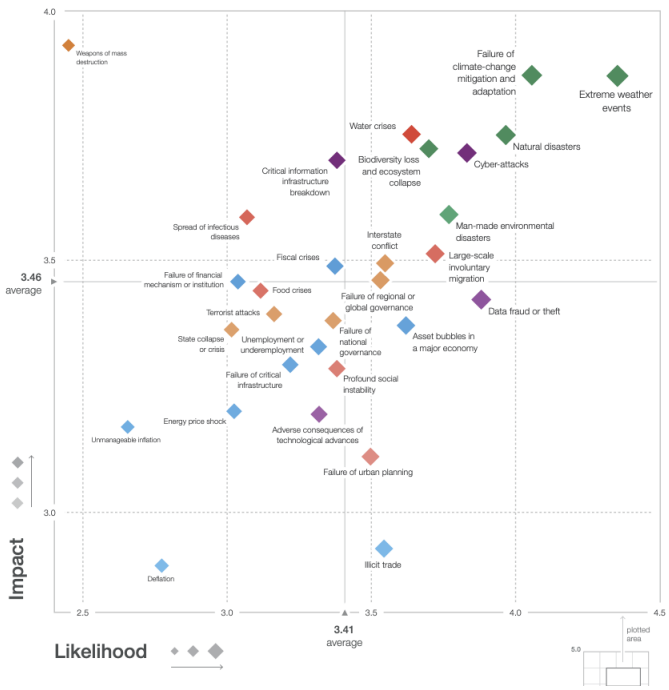

Fig. 1. The global risks landscape [5].

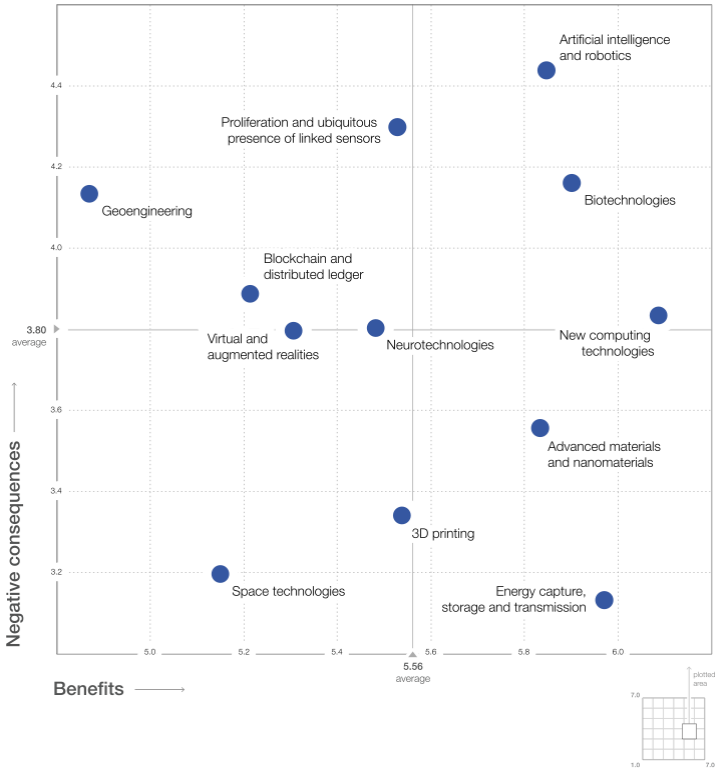

Fig. 2. Perceived benefits and negative consequences of 12 emerging technologies [4].

Among all global risks, the surveyed experts identified four threats related to technology (see Fig. 1). According to them, cyber-attacks are the most likely risk with highest impact. The other three threats are data fraught or theft, critical information infrastructure breakdown, and adverse consequences of technological advances in general. In more detail, if we compare the perceived benefits and negative consequences of the 12 key emerging technologies, the two outstanding are AI and robotics and biotechnologies (see Fig. 2). Therefore, they are the most pressing in need of better governance and management. Some technologies are not much beneficial but threaten with relatively high negative consequences, such as geoengineering. On the other hand, space technologies will supposedly bring least benefits but also will have least negative consequences.

The FESTOS project run between 2009 and 2011 by various researchers [e.g. 1-3] identified 80 emerging technologies, out of which 33 were assessed by experts in terms of their potential abuse by terrorists or organized crime. Their findings are summarized in two rankings of ten technologies – by "abuse potential" and "threat intensity" (see Fig. 3). Both criteria combined, on the top of the list there are advanced AI, internet of things, cyborg insects, and cloud computing. The potential threats are suggested for example in [1].

Priority	*By potential of abuse*	*By threat intensity*
1	Smartphone mash-ups	Advanced AI
2	Internet of things	Human enhancement
3	Cloud computing	Swarm robotics
4	New gene transfer technologies	Cyborg insects
5	Advanced AI	Internet of things
6	Synthetic biology	Water catalyzing explosive reactions
7	Cyborg insects	Fuels and processes for nuclear technologies
8	Energetic nanomaterials	AI-based robot-human interaction
9	RFID	Cloud computing
10	Autonomous mini robots	Programmable matter

Fig. 3. Prioritisation of top ten signals of change represented by emerging technologies [3].

3.2 Technological change and innovation as security threats in the Czech political and public discourse

The analysis of the Czech political discourse as reflected in the public news television channel ČT24 reveals two recent themes in the narrative. One is robotization and automatization of the industry as a threat to employment and economic and social stability. For example, on June 19, 2017, Ms Michaela Marksová, at that time the minister for labour and social affairs, said that "there are concerns that many jobs will be lost due to digitization and robotization. There will be changes, but new professions will arise, more people will be needed in services" [16]. Similarly, on May 9, 2019, the Czech prime minister Mr Andrej Babiš suggested that "electric cars are clearly a step towards the beginning of the end of the automotive industry in Europe" [17], though the source of the threat was innovation in the automotive industry due to environmental concerns.

Another theme in the Czech discourse is cyber-security. On December 17, 2018, the Czech National Cyber and Information Security Agency warned against the use of software and hardware by Chinese companies Huawei Technologies and ZTE Corp. that supposedly pose a cyber threat. There were concerns over business and military espionage by the Chinese government [18]. On September 25, 2019, the Agency repeated that foreign states such as Russia or China remain the biggest cyber-threat for the country. Concretely, "they have the human, financial and time resources to make their cyberspace operations technically sophisticated and persistent. Their main motivation is strategically and politically important information and gaining military benefits for possible future conflicts." In connection with this, the Czech Foreign Ministry has repeatedly faced a major cyber-attack. The Agency also warned against the attacks against critical infrastructures such as energy, transport, or communication [19].

Governmental and other official documents also touch upon some of the issues identified by academia. The Policy Statement of the Government of the Czech Republic 2018 discusses energy security and self-sufficiency, hybrid- and cyber-security, hackers, infrastructure and data abuse, secure data sharing in healthcare, and food security (agriculture 4.0, smart farming). The Concept of the Czech Republic's Foreign Policy 2015 claims that due to technological progress in military affairs, the country will face growing military capabilities of other powers. The Security Strategy of the Czech Republic 2015 warns against malicious use or disruption of infrastructure (ICT, energy), growing role of non-state actors in this area, and also cyber-attacks (time-space compression, asymmetry, infrastructure, political and economic espionage). Finally, the Defence Strategy of the Czech Republic 2017 discusses hybrid campaigns, disinformation (information war), and again, cyber-attacks.

In order to decide whether the Czech political securitization moves are successful, it is necessary to look into the recent public opinion polls. The poll by a Czech research agency MEDIAN from December 2018 concerning people's expectations and perceived threats in 2019 [20] identified mostly nowadays mainstream threats such as terrorism, climate change, or migration. It also lists two threats related to technological change and innovation, namely disinformation from Russia or China and decline of labour in traditional sectors (industry, agriculture). Earlier polls conducted by the Public Opinion Research Center of the Czech Academy of Sciences, such as that concerning the security situation in Europe from November 2018 [21] or another regarding concerns and security risks for the Czech Republic from December 2017 [22], do not discuss any technology-related threats at all.

4 Discussion and conclusion

There are dozens of emerging and new technologies and innovations that are to come in the foreseeable future. However, it is hard to imagine them now, especially the all possibilities of their convergence. Due to the uncertainty and because "all technologies are inherently prone to potential misuse and […] the necessary regulations usually lag behind the technologies" [1], fears among the public can arise. This is nothing new, but the recent research is relatively scarce and sometimes art (literature, film) is better in portraying the fears or the security threats generated by technological change, that are perceived.

The reviewed academic literature identifies some technological threats that are relatively likely and (will be) intensive such as cyber-attacks, artificial intelligence and robotics, and biotechnologies. In the Czech political discourse, we identified especially the securitization of robotics and automation, particularly in relation to the automotive industry that produces a substantial part of the country's GDP. There are fears that they will lead to loss of employment and ensuing social and economic instability. Specialized national agencies and official documents also often mention cyber-threats. But the rest of all the possible concerns and threats is entirely absent from the Czech narrative.

Unsurprisingly, the Czech public only repeats the fears verbalized in politics and policies, but even those securitization moves are not very successful. The biggest threat perceived at the beginning of 2019 was water scarcity and then other mainstream fears such as terrorism or migration. Therefore, we can confirm Hauptman's observation that "the public is rather badly informed about dangers of new technologies and that governments tend to underestimate the potential threats" [1].

Czech politicians and experts should accept the fact that, apart from the hope of solutions of the problems we face, new technologies can become security threats through having unintended consequences or being misused. They should also expect that the public fears do not necessarily have to reflect the "objective" existence, intensity, or nature of threats, but they can be "only" perceived or imagined and, thus, still have unsettling social and economic effects. Politicians and experts should intensify the public discussion in order to become better at managing technological change and to avoid the previously mentioned issues. There is also potential for further research in the Czech context, concretely to learn if and how Czech scientists, researchers, and experts see technological change and innovation as technology threats and which solutions they suggest.

This paper is an output of the science project IG VŠE F2/58/2018 "Kritická analýza současného bezpečnostního diskursu a praxe v České republice" (Critical analysis of the current security discourse and practice in the Czech Republic).

References

1. A. Hauptman, Illuminating the "dark side" of emerging technologies. In D. Meissner, L. Gokhberg, O. Saritas (eds.). *Emerging technologies for economic development*, 263-285 (2019)
2. A. Hauptman, Y. Raban, Foresight of cyber security threat drivers and affecting technologies. *Foresight* **20,** 353-363 (2018)
3. A. Hauptman, Y. Sharan, Foresight of evolving security threats posed by emerging technologies. *Foresight* **15,** 375-391 (2013)
4. World Economic Forum, *The global risks report 2017, 12th edition.* (World Economic Forum, Geneva, 2017)
5. World Economic Forum, *The global risks report 2019, 14th edition.* (World Economic Forum, Geneva, 2019)
6. J. Gerring, Discourse and content analysis. *Qualitative Methods: Newsletter of the American Political Science Association Organized Section on Qualitative Methods* **2,** 15-39 (2004)
7. M. Albert, B. Buzan, Securitization, sectors and functional differentiation. *Security Dialogue* **42,** 413-425 (2011)
8. T. Balzacq, S. Leonard, J. Ruzicka, "Securitization" revisited: theory and cases. *International Relations* **30,** 494-531 (2016)
9. D. Dinello, *Technophobia!: Science Fiction Visions of Posthuman Technology*. (University of Texas Press, Austin, 2006)
10. K. Tsukahara, Strengthening disaster risk governance to manage disaster risk: Output of the global forum on science and technology for disaster resilience 2017. *Journal of Disaster Research* **13,** 1177-1180 (2018)
11. D. Rychnovska, R. Braun, Socially responsible innovation in security: Critical reflections. *Critical Policy Studies* **13,** 366-368 (2019)
12. M. Finnemore, Ethical dilemmas in cyberspace. *Ethics & International Affairs* **32,** 457-462 (2018)
13. D. Rychnovska, Governing dual-use knowledge: From the politics of responsible science to the ethicalization of security. *Security Dialogue* **47,** 310-328 (2016)
14. M. Mayer, M. Acuto, The global governance of large technical systems. *Millennium – Journal of International Studies* **43,** 660-683 (2015)
15. P. Adey, B. Anderson, Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue* **43,** 99-117 (2012)
16. ČT24, *Kvůli digitalizaci zanikne až 53 procent pracovních míst, domnívá se Špidla. Jiní jsou střídmější* (June 19, 2017), Avaliable at: https://ct24.ceskatelevize.cz/ekonomika/2156298-kvuli-digitalizaci-zanikne-az-53-procent-pracovnich-mist-domniva-se-spidla-jini (accessed October 14, 2019)
17. ČT24, *Summit EU zdůraznil jednotu. Elektroauta jsou krok k začátku konce automobilového průmyslu, řekl Babiš* (May 9, 2019), Avaliable at: https://ct24.ceskatelevize.cz/svet/2809376-summit-eu-zduraznil-jednotu-elektroauta-jsou-krok-k-zacatku-konce-automobiloveho (accessed October 14, 2019)
18. ČT24, *Český úřad pro kybernetickou bezpečnost varuje před produkty čínských firem Huawei a ZTE* (December 17, 2018), Avaliable at: https://ct24.ceskatelevize.cz/ekonomika/2682797-cesky-urad-pro-kybernetickou-bezpecnost-varuje-pred-produkty-cinskych-firem-huawei (accessed October 14, 2019)

19. ČT24, *Největší kyberhrozbou pro Česko zůstávají cizí státy. Zpráva NÚKIB ukazuje hlavně na Rusko a Čínu* (September 25, 2019), Avaliable at: https://ct24.ceskatelevize.cz/domaci/2934071-nejvetsi-kyberhrozbou-pro-cesko-zustavaji-cizi-staty-zprava-nukib-ukazuje-hlavne-na (accessed October 14, 2019)
20. MEDIAN, *Rok 2019 – očekávání a hrozby* (2019), Avaliable at: http://www.median.eu/cs/wp-content/uploads/2019/01/OCEKAVANI_OD_ROKU_2019.pdf (accessed October 14, 2019)
21. CVVM, *Hodnocení bezpečnostní situace v Evropě – listopad 2018* (2019), Avaliable at: https://cvvm.soc.cas.cz/cz/tiskove-zpravy/ostatni/negativni-jevy-bezpecnost/4805-hodnoceni-bezpecnostni-situace-v-evrope-listopad-2018 (accessed October 14, 2019)
22. CVVM, *Veřejnost o svých obavách a bezpečnostních rizicích pro Českou republiku - prosinec 2017* (2018), Avaliable at: https://cvvm.soc.cas.cz/cz/tiskove-zpravy/ostatni/negativni-jevy-bezpecnost/4506-verejnost-o-svych-obavach-a-bezpecnostnich-rizicich-pro-ceskou-republiku-prosinec-2017 (accessed October 14, 2019)