ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 3 (March)
http://doi.org/10.9770/jesi.2019.6.3(33)

Publisher
http://jssidoi.org/esc/home

INDUSTRY 4.0 AND NATIONAL SECURITY: THE PHENOMENON OF DISRUPTIVE TECHNOLOGY

[1]Tadas Limba, [2]Andrius Stankevičius, [3]Antanas Andrulevičius

[1,2,3] Mykolas Romeris University, Ateities str. 20, Vilnius, Lithuania

E-mails:[1] tlimba@mruni.eu ; [2]stankevicius@mruni.eu , [3]antanas@fin.lt

Received 18 October 2018; accepted 20 January 2019; published 30 March 2019

Abstract. Fourth Industrial Revolution, based on digital platforms is characterized by a convergence of technologies that is blurring the lines between the physical, digital, and biological spheres. These phenomeon disrupts patterns of development and opens new paths to development. (WEFORUM. 2018) Digital technology development presuppose methodological challenges not only to business or individual interest, but holistic approach to national security issues. Hybrid threats, economic crises, social inequalities, and labor migration are among the main challenges of global security. What are possible manifestations of disruptive technology in national security interest in the broader sense? Is it possible timely to identify and react to threats to competitivness, "job killer" or law system? Critical infrastructure are parameter, which identifies assets or system as element of security. Topic reveal interaction between disruptive technology and critical infrastructure in the context of national security. Authors argued, that the theoretical insights, obtained by document analysis, classification, critical analysis, abstraction methods will be useful in practical use, to provide expert knowledge and a deeper understanding manifestations of disruptive technology in security issues at all levels.

Keywords: critical infrastructure; disruptive technology; fourth industrial revolution; national security

Reference to this paper should be made as follows: Limba T., Stankevičius A., Andrulevičius A. 2019. Industry 4.0 and national security: the phenomenon of disruptive technology, *Entrepreneurship and Sustainability Issues* 6(3): 1528-1535. . https://doi.org/10.9770/jssi.2019.6.3(33)

JEL Classifications: O33

Additional disciplines law; sociology

1. Introduction

With the changing global security situation, increase in external threats or emergence of new ones (cyberattacks, on-conventional warfare models, etc.), countries must feel concern regarding consolidation of their security (Novikovas et al., 2017). The fourth industrial revolution (4.0) will have a profound impact on the nature of state relationships and international security, changing the character of security threats while also influencing shifts of

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 3 (March)
http://doi.org/10.9770/jesi.2019.6.3(33)

power, which are occurring both geographically, and from state to non-state actors (Schwab, 2016). It's no doubt, that 4.0 is disrupting economies and sociaties, redifining the busines landscape, often in unexpected ways. Governments and organizations of the world understand that the main efforts should be taken to provide security for their critical infrastructure because only this can ensure the wellbeing of the country and its people, especially when critical infrastructure and energy security has become an argument for political decisions making (Tvaronavičienė, 2018).

Mentioned, that 4.0 are based on digital technology, which determine interconnects and interdependencies between various sector of social life. Government institutions, banking sectors, public and private services, nuclear power plants, power grid operators, water suppliers or waste water treatment companies use information technologies in their day-to-day operations. Everything that uses technologies are based on communication and information systems and that means that it depends on cyber security (Limba et al., 2017).

Emerging technologies presuppose new methodical-theoretical approach of security issues. For example, the manifestation of interest groups in legislative process, using combination of various digital lobbying activities (e-lobbying), or electing system as law institute can be identified as element of critical infrastructure, that's means-element of national security. The vulnerability of the electoral system or the implementation of transparent lobbying activity can result corruption and/or the underground (shadow) economy, what can be an obstacle for sustainable development, which requires respective favorable multi-faceted environment (Stankevičius, Lukšaitė, 2016; Tvaronavičienė, 2016).

To disclosure a precise definition of security is not simple. In one case, it can be too narrow, others- too wide. European Union Internal Security Strategy 2015-2020 as the priorities identified „fight against terrorism, serious and organised crime and cybercrime", and highlighting that „keeping our citizens safe is the main duty of our Governments". Treaty on the Functioning of the European Union- (TFEU) establishes "an internal market, which shall work for the sustainable development of Europe based on balanced economic growth and price stability, a highly competitive social market economy, aiming at full employment and social progress". Above mentioned, presuppose to identify public, economic, social, ecological-environmental, cyber securities. Security, as a evolutionary phenomenon disclosed according to critical infratructure (CI) definition. "Critical infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. (Council Directive 2008/114/EC Article 2). Authors suggest, that CI may be used to explore the impact of disruptive technology on security issues, while treats are difficult to undestand and have resultant nature.

The theory of disruptive innovation was invented by Clayton Christensen. Theory tells us that certain innovations can undermine existing products, firms, or even entire industries. According to C. Christensen, disruptive innovation – an innovation, employing a 'technology' in management, marketing activities and investment policy which transforms information, labour, capital, and materials into products or services of greater value, which becomes the main goal of a company, and, as a consequence, fundamentally changes the established 'rules of the game' in many industries. If a certain technology plays a critical role in a disruptive innovation, it could be defined as "disruptive technology" (DT) (Christensen, Bower, 1996). It determines understanding, that DT is perceived as a process. It is noteworthy, that "Disruptive technology&disruptive innovation" have been of scholarly interest for years, but there is still a need to better understand the nature of disruptions and their relationship to emerging technology processes (Li et al., 2018).

While threats from new technologies are still nascent, difficult to understand or lack legal protections. Therefore, the theory of disruptive innovation can be applied to various industrial contexts: from high-tech to low-tech, and

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 3 (March)
http://doi.org/10.9770/jesi.2019.6.3(33)

from lagging to rapidly changing environments. The big number of articles shows high relevance of DT in future industries (see table No 1).

Table 1: Count of publications in selected emerging or disruptive technologies using either an emerging or disruptive technology framework (Indexes = SCI=EXPANDED, SSCI, A&HCI, ESCI; Timespan = 2006 – 2015)

	Emerging Technology	Disruptive Technology
Nanotechnology	354	15
Big data	10	7
Internet of things	19	1
Electric vehicle	31	1
3D printing	13	6

Source: Li, M., Porter, A.L., Suominen, A.

2. Problem formulation and methodology

The impact of changes, to security, based on DT, can occur in various aspects: for a specific business model, specifically for infrastructure or for a specific investment. The effect may be the creation of a new economic activity, existing modification or destruction. The strategy of security must ensure prevention, detection and response to possible treats in these aspects. The main challenge for governments is timely adoption law norms and principles, solving these problems.

For example cryptocurrency is an innovative payment network and a new kind of money, based on digital technology. The question- how cryptocurrency are influencing EU or its country members economic or financial security? What is response and preparedness from legislative subject, regulating this phenomenon? Is it new form of money, or its element of shadow economy (authors term "shadow economy" use wide meaning, which includes tax evasion, money loundering, corruption, violations of competitiveness and busines activities outside law regulation)?

According to TFEU article 3, “The Union shall establish an economic and monetary union whose currency is the euro“ and does not provide for exceptions or other alternatives to the EU currency. Cryptocurrencies phenomenon have become actual, unregulated problematic issue, presuppose national and regional authorities to solve with law regulation. For example, Polish National Bank and the Financial Supervision Commission jointly issued a warning against investing in virtual currencies, citing price volatility and the risk of fraud, Bank of Lithuania stated, that „financial market participants should not provide services associated with virtual currencies,“ the Finance Minister of Slovakia had noted, „that trade in cryptocurrencies, which is unregulated and anonymous, involves risks of terrorism and organized crime.“

Disruptors such as Coursera, Airbnb, Waze, Uber redefining not only the perception of the business sector (its clear, that education or taxi industry will never be the same), but also systematic aproach to public administrative management. The government protects and regulate the labor market, competitiveness, consumer protection- approve licenses, defining tax policy and establishing a business environment. Question – are these provision properly and timely implemented?

Coursera, Airbnb or Uber represents business sectors (education, accommodation, taxi) which are licensed or include mandatory provisions, for example hygienic, technological or tax accountability. For example, in Uber or Airbnb case its not clear the question of labour law (employee status, social security or social contributions),

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 3 (March)
http://doi.org/10.9770/jesi.2019.6.3(33)

administrative law (licensing, ensuring and enforcing mandatory technical requirements), tax law (appropriate implementation of fiscal policy).

„Yandex. Taxi“ case in Lithuania revealed a systemic problem that concerns legal regulation, technological interdependence, public trust in governance aspects.

The National Cyber Security Centre under the Ministry of National Defence of Lithuania carried out initial analysis of “Yandex. Taxi” application for smartphones, which was actively offered for Lithuanian users since 26 July 2018. The analysis of the application revealed that it requires access to a large amount of sensitive data and permissions to device functions, which might be excessive. The app has the ability to turn on the device camera and microphone (take pictures and videos, record sound), access contact list (phone book, social media accounts’ information), control the phone call services, identify phone status and identity, control the text message service (intercept messages), modification or deletion of the contents on the smartphone’s storage, determine precise GPS location of the device, manage network access (receive data, monitor and control network connections, manage Wi-Fi access). Analysis showed that the app regularly connected and exchanged data with 11 unique IP addresses (10 of which are of the Russian Federation) via encrypted channels. It should be noted that, this analysis has recommendatory nature, but in public discourse determined contradictory opinions. Its not clear, is a threat to national security interests or not?

Attention is, however, to be focused on the fact, that DT manifest to security issues *straightforward* nature - through the main economic activity and *indirectly* through technological interdependence (for example, uber, airdnb, coursera are based on digital platforms (mobile app)).

Authors reveals classification of DT and CI, and provides a comparative analysis of these phenomena, according law and scientific documents, literature.

First classification of DT is based in terms of timing (early/late) and reaction to changes, (external/internal). It leads to understand awareness of technology’s potential and better understanding the strategy of response to DT, which involves a three-step process: building awareness (sensing), building capability (responding), and building commitment (scaling) (Birkinshaw et al., 2018).

Content of these classification presuppose to compare DT as CI, according to following analysis.

CI are distiguished in external (outside EU) and internal (inside EU). Internal are possible to divide to European CI (which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State) and National CI (These criteria would be developed by each Member State taking into account as a minimum the following qualitative and quantitative effects of the disruption or destruction of a particular infrastructure) (COM (2006) 786).

Second: analysing DT that are potentially disruptive to business, to government, and to society by two levels of disruptive technologies. Its possible to identify two levels of of disruptive technologies: a) disruption is a localized change, within a market or industry, b) disruption has much larger influences, affecting many industries and substantially changing societal norms and institutions (Schuelke, 2018).

Criteria referred to identify critical infrastructure comprise the following: *economic* effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects); *public* effects criterion (assessed in terms of the impact on public confidence, physical

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 3 (March)
http://doi.org/10.9770/jesi.2019.6.3(33)

suffering and disruption of daily life; including the loss of essential services); *political* criterion. (Council Directive 2008/114/EC).

Third. Technological interdependece of DT. Inter-dependence is a major challenge for risk management in critical infrastructure. This is because economies and societies rely on interdependent and inter-connected infrastructure systems. This gives rise inter alia to a phenomenon known as "cascading events" – that is, once one disruption occurs, others are likely to follow within systems and processes that are connected to the infrastructure affected by the initial disruption (OECD 2008). The same indication are inherent to CI: "The identification and analysis of interdependencies, both geographic and sectoral in nature, will be an important element of improving critical infrastructure protection in the EU". (COM(2006) 786).

3. Discussion

The disruptive changes brought by the fourth industrial revolution are redefining how public institutions and organizations operate, mentioned external and internal nature. Its presuppose countries and governments relate to each other: the interconnected and interdependent nature of today's economy and society means that even a disruption outside of the EU's borders may have a serious impact on the Community and its Member States. (COM(2006) 786). The main problem of the increasing vulnerability can be associated with the complexity of the system and integration process: the small elements of the systems or small systems are integrated into larger systems which increases the system complexity and creates conditions for vulnerabilities to arise not only in domestic but also in countries interconnected systems; new modern technology usage is usually motivated by the increasing need for efficiency, but it is not considered from the security and especially cyber security position due to a lack of proper understanding of the vulnerable areas and limitations as well as a lack of possibilities to enforce the responsibility of private sector players to reduce the effect of their negligence on society or some part of society (Kroger, 2008).

Examples Cryptocurrency or Yandex Taxi cases reveals disccusion about "Broken Windows" theory and regulating these examples. Wilson and Kelling, who advocated for stopping smaller crimes by maintaining The Environment In Order To Prevent Bigger Ones, brought the theory. While is not clear status of cryptocurrency, social-legal relations in this area reminiscent of "fight without rules": not clear tax regulation, protection of law values etc. Case of Yandex Taxi disclose another discussion: Lithuanian Institution issued recommendations for applications safe usage, but others neighbour countries – dont. In one hand, we can identify these situation as a law loophole – we have unregulated, existing situation, which generating monetary circulation. According to "Broken windows" theory, - bad habits and behaviours tend to be contagious allow some ideas or behaviours to "spread like viruses" (Wilson, Kelling, 1982). Other hand - social, legal, financial instability between government, business and society. For example Yandex Taxi case – it Is possible to determine the legal discussion on the protection of competition, presumption of innocence, reputation or freedom of economic activity.

Authors argued, that methodological classification of DT, disclosure possible interaction between DT and CI in the context of security.

Technological interdependence between CI elements presupposes to reveal discussion about interaction between DT and cyber security. Its possible to identify mutual problematic aspects to security issues. As mentioned above, DT can directly affect national security in different vectors, for example economic or competetivenes fields. More deeper problem exist vulnerability of DT in case of cyber security. These problem define not only private interest, but also public. For example, if we define cryptocurrency define as a currency (money), its pressupose reliable, secure billing instrument meaning, which must be resistant to fraud, illegal cyber trick or digital counterfeiting.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 3 (March)
http://doi.org/10.9770/jesi.2019.6.3(33)

Hence, its necessary to ensure not only security of network and information systems but also juridical, economic and tax aspects. According to Directive (EU) 2016/1148- 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

Lithuanian Cybersecurity law defines cyber security as a set of legal, information dissemination, organizational and technical measures which are needed to be taken to prevent, detect, analyze and respond to cyber incidents, which are described as the event or activity that causes or may cause or allow: unauthorized access to communication and information systems (CIS), electronic communications networks or industrial process control systems; can disrupt or change information systems, including the management takeover; electronic communications networks or industrial process control operations to destroy, damage, delete or modify electronic information, withdraw or restrict access to electronic nformation, as well as enable to absorb or otherwise use non-public information in electronic format by unauthorized persons (Law on Cyber Security of the Republic of Lithuania, 2014). Nowadays when the threats are increasing rapidly, you need to think about the solutions that have more complex measures. It is time to think about a cyber security management model which has considered all strategic aspects, without limitation only a technical issue (Limba et al., 2017).

The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role to play in spurring research, development and innovation in those areas. (Directive (EU) 2016/1148).

Consequently, the disruption that the fourth industrial revolution will have on existing political, economic and social models will therefore require that empowered actors recognize that they are part of a distributed power system that requires more collaborative forms of interaction to succeed. (WEFORUM, 2018).

4. Conclusion

It should be emphasized, that DT is identified as CI by three criteria, established by the EU law regulation.

Understanding and modelling potential technological disruptions as critical infrastructure in the context of security issues, will require taking a holistic perspective. It will help to improve security culture: better understand the boundary between disruptive technology as a sustainable phenomenon and security aspects.

Exploratory analysis of DT examples pressupose provision, that legal regulation appears to be routine (delayed) in response to the consequences, but not to prevention or regulate current situation. This leads to a collision of double standards - in one case, the negative impact of technology on security issues (Yandex Taxi LT, Cryptocurrency) is emphasized, otherwise the guarantee of freedom of initiative of the economic activity guarantees the providers of technology with legitimate expectations. An appropriate, timely adapt law system to changes, primary feature of successful suistanable development and economy. The timely identification of DT as CI is likely to help identify the potential threats to security principles properly and clearly.

Study revealed, that there is a need systematically to develop research interaction between DT and cyber security, responding effectively to the challenges of security of network and information systems, law regulation aspects.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 3 (March)
http://doi.org/10.9770/jesi.2019.6.3(33)

References

Bank of Lithuania (2018), Lithuania's Central Bank to Issue the World's First Digital Collector Coin, [online]. [cit.2018-09-22]. Available at: https://www.lb.lt/en/news/lithuania-s-central-bank-to-issue-the-world-s-first-digital-collector-coin

Birkinshaw, J., Visnjic, I., Best, S. (2018). Responding to a potentially disruptive technology: How big pharma embraced biotechnology. *California Management Review*, 60(4), 74-100. https://doi.org/10.1177/0008125618778852

Christensen, C. M., Bower, J. L. (1996). Customer power, strategic investment, and the failure of leading firms. Strategic management journal, 17(3), 197-218. https://doi.org/10.1002/(SICI)1097-0266(199603)17:3<197::AID-SMJ804>3.0.CO;2-U

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75. Communication from the Commission on a European Programme for Critical Infrastructure Protection COM/2006/0786 final.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Avaible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

Kroger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, 93(12), 1781–1787. http://dx.doi.org/10.1016/j.ress.2008.03.005

Law on Cyber Security of the Republic of Lithuania. Available at: https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4

Li, M., Porter, A.L., Suominen A. (2018). Insights into relationships between disruptive technology/innovation and emerging technology: A bibliometric perspective. *Technological Forecasting and Social Change*, pp. 285-296, https://doi.org/10.1016/j.techfore.2017.09.032

Limba, T., Plėta, T., Agafonov K., Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, 4(4), 559-573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

Narodowy Bank Polski (NBP) and the Polish Financial Supervision Authority (KNF) (2017). "Virtual Currencies". https://www.knf.gov.pl/knf/en/komponenty/img/Statement_by_NBP_and_KNF_on_virtual_currencies_7_07_2017_57364.pdf

Novikovas, A., Novikovienė, L., Shapoval, R., Solntseva, K. (2017). The peculiarities of motivation and organization of civil defence service in Lithuania and Ukraine. *Journal of Security and Sustainability Issues*, 7(2), 369-380. http://dx.doi.org/10.9770/jssi.2017.7.2(16)

Schuelke, L. (2018). A model for understanding the orders of magnitude of disruptive technologies. *Technological Forecasting and Social Change*, pp: 261-274. https://doi.org/10.1016/j.techfore.2017.09.033

Stankevičius, A., Lukšaitė, A. (2016). Transparent lobbying for sustainability: case of Lithuania. *Entrepreneurship and Sustainability Issues*, 4(2), 220-227. http://dx.doi.org/10.9770/jesi.2016.4.2(9)

The Global Competitiveness Report (2016–2017) Avaible at: http://www3.weforum.org/docs/GCR20

OECD. 2008. *Protection of 'critical infrastructure' and the role of investment policies relating to national security*. Available at: https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

Schwab, K. (2016). The Fourth Industrial Revolution. Geneva: World Economic Forum. ISBN 1944835008 77p.

The National Cyber Security Centre under the Ministry of National Defence of Lithuania. Information bulletin on investigation of the „yandex. Taxi"application and recommendations for applications safe usage (2018), Available at: https://www.nksc.lt/doc/en/analysis/2018-08-09%20Yandex%20Taxi%20application%20analysis.pdf

The Slovak Spectator (2018), Finance Minister Plans to Start Taxing Bitcoin, Avaible at: https://spectator.sme.sk/c/20733083/financial-minister-plans-to-start-taxing-bitcoin.html , archived at https://perma.cc/NN5W-JEJY

Treaty on the Functioning of the European Union, Article 3. Official Journal of the European Union C 202. Available at: https://www.ecb.europa.eu/

Tvaronavičienė, M. (2018). Towards internationally tuned approach towards critical infrastructure protection. *Journal of Security and Sustainability Issues*, 8(2), 143-150. https://doi.org/10.9770/jssi.2018.8.2(2)

Tvaronavičienė, M. (2016). Start-ups across the EU: if particular tendencies could be traced. *Entrepreneurship and Sustainability Issues*, 3(3), 290-298. http://dx.doi.org/10.9770/jesi.2016.3.3(6)

Wilson, J. Q., Kelling, G. L. (1982). Broken Windows: The Police and Neighborhood Safety, *The Atlantic*, 29(31), 29–38. Available at: https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/

Tadas LIMBA is associate professor at the Mykolas Romeris University (e-mail: tlimba@mruni.eu). He obtained PhD degree in management from Mykolas Romeris University in 2009. He is the head of Joint Study Programs "Informatics and Digital Contents" with Dongseo University in South Korea taught en English at Mykolas Romeris University. His research interests include over than 15 Years of experience in a field of E-Government, E-Business, IT application for the organizational change and Digital Contents. He is actively developing and expanding the relations for the future prospectives of the common activities with Dongseo University. Tadas Limba has over 30 scientific publications on different topics related with New Public Management, E-Government, E-Signature, E-Time Stamping, E-Business, E-Marketing, IT and Patent Law, Biotechnology Strategies. He is also the international expert in a field of E-Government and has trained the Faculty Members of Public Administration Academy of Republic of Armenia and Eurasian International University in Armenia in 2014. Tadas Limba visited Communication University of China in 2014 and had the research internships at Arizona State University, USA and at Dongseo University, South Korea in 2015.
ORCID ID: orcid.org/0000-0003-2330-8684

Andrius STANKEVIČIUS, Mykolas Romeris University, Faculty of Public security, Department of Law, lector. Research interests: public security, interest groups, lobbying.
ORCID ID: orcid.org/0000-0002-2528-0497

Antanas ANDRULEVIČIUS, JSC "Financial Figures", consultant. Research interests: disruptive technologies, crypto currency, national security, Industry 4.0.
ORCID ID: orcid.org/0000-0002-5531-5267