Securing regional development

Mohammad Chehabeddine, Manuela Tvaronavičienė

INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

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

SECURING REGIONAL DEVELOPMENT*

Mohammad Chehabeddine [1], Manuela Tvaronavičienė [2]

[1]Vilnius Gediminas Technical University, Saulėtekio al. 11, Vilnius, Lithuania
[1]King Khaled International Airport in Riyadh, Saudi Arabia
[2]Daugavpils University, Vienibas Str. 13, Daugavpils LV-5401, Latvia

E-mails: Mohamad.chehab-eddine@vgtu.lt; manuela.tvaronaviciene@vgtu.lt

Received 13 June 2019; accepted 10 December 2019; published 15 March 2020

Abstract. Regional Development is linked to Sustainability, and also, Development is linked to Security, both nationally and globally. The expanded view of Security has opened the discussion of new technologies introduced non-traditional threats that become vulnerable to regional security and thereby to regional development. Five broad types of situations or premises that constitute a security in which threats overlap and interact, those new threats warrant new security paradigms that traditional international relations ignored so far. The purpose of this research is to analyze and study the impact of these new threats to security and how they affect regional development. Protection to the digital ecosystem and critical infrastructure from threats could be by implementing the security program of Governance, Risk, and Compliance (GRC), however, awareness, preparedness, and resilience of societies with the international community are as key preconditions of further secure and sustainable economic development and general well-being. Case studies of new technologies that threaten global societies economically and socially.

Keywords: Regional development; Critical Infrastructure; Cyber Security; Digital Ecosystem; Regional Development; SDGs (Sustainable Development Goals); New Technologies; STEM (Science, Technology, and Engineering, and Mathematics); Sustainable Development, Trans-state threats

Reference to this article should be made as follows: Chehabeddine, M., Tvaronavičienė, M. 2020. Securing regional development. *Insights into Regional Development*, 1(4), 430-442. http://doi.org/10.9770/IRD.2020.2.1(2)

JEL Classification: D83, O18, Q56

* *This research was partly supported by the project, which has received funding from the European Union's Horizon 2020 research and innovation programme European Research Council (ERC) (Grant Agreement Number 830892)*

European Research Council
Established by the European Commission

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

1. Introduction

In the context of new technologies and fast-changing environments due to globalization, trans-state threats become urgent issues to regional security and regional development. This research paper aims to overview major contemporary threats that affect regional development in one or another way. Authors seek to trigger discussion, which ultimately would allow finding efficient ways to prevent those threats or to mitigate their impact, al least.

The research is organized in the following way: at first, authors look at regional development and security concepts. Later interrelations between then are discussed. A separate part of the paper is devoted to threat caused by digitalization processes. The paper finishes with an analysis of concrete selected case studies, which help to blend theory and practice. Specifically, the following case studies are tackled: Stuxnet program against Iran's nuclear program development, WannaCry, and the trade war between China and the USA. The paper finishes with concluding insights.

2. Searching for regional development and security links

Regional development research is conducted having the aim to identify in-depth causes hindering development in particular regions, and finding ways to neutralize them in order the process of economic development was accelerated, and, as a consequence, the general level of living started to increase gradually.

The first connotation of regional development is economical. Differences in economic development can be measured using a wide range of indicators, e.g., by GDP per capita, patterns of income distribution across society, structure of economic sectors, availability of resources, unemployment, gender equality etc. There is a lot of attention to those questions in the scientific literature (e.g., Tvaronavičienė, Gatautis, 2017; Njaramba et al., 2018; Iorio et al., 2018; Tung, 2019 etc.) To conclude, here is almost unanimous agreement about the width of the regional development scope.
The security phenomenon as well as a widay array of contexts. We will try to systemize at least some distinguished aspects below.

At first, let us tackle environmental and ecological security, which is related to the depletion of scarce resources leading to climate change. There is a lot of attention to this broad aspect of security, which emerges as food security (e.g., Faridi, Sulphey, 2019; Tireuov et al., 2018), water security (Moumen et al., 2019; Muniz et al., 2019); deforestation (Cherchyk et al., 2019), energy security (e.g., Rogalev et al.)

The second broad security aspect is related to human, community, and societal security focuses on widespread issues such as structural and cultural violence, notably gender violence, sexual and public health botheration, forced migrations, and economic and resource injustice.

The third security aspect is state-centered national defense, which focuses on traditional state rivalry, military war, the geostrategic Great Game, and new areas such as natural resources (water and oil) and dark operations in cyberspace.

We would distinguish the fourth, hybrid, mixed forms of insecurity, which combine state military dimensions with forms of dislocation (food and water crises, trafficking, radical ideologies), disruptive groups (organized crime, gangs, terrorists, drug cartels, pirates, anti-democratic forces) and technologies affecting civil societies.

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

Let us recall sustainable development facets now.

Elements or pillars of Sustainable Development (Environment, Society, and Economy) interact with each other to develop the required sustainable development. Attending one of these at the expense of the others is bound to lead to unsustainable dynamics and outcomes (Khagram et al. 2003).

In 2015, the United Nations promoted the seventeen Sustainable Development Goals (SDGs). Intersectional linkages among these objectives are especially revelatory of the forces structuring non-military security. Each goal has its own set of measurable indicators. The goals apply to all nations, with no distinctions between developed and developing countries. Though extremely lofty goals, UN agencies, and other organizations continue to promote these universal goals globally. The SDGs replaced the eight Millennium Development Goals that unfolded from 2000 to 2015. ("Case Studies | 2015 UN-Water Annual International Zaragoza Conference. Water and Sustainable Development: From Vision to Action. 15-17 January 2015," n.d.)

As Khagram et al. "the brilliance of 'sustainability' lies in its ability to provide 'space' for serious attempts to deal with the real, dynamic, and complex relationships among societies, economies and natural environments, as well as between past, present and future. Within this broad space, a range of perspectives that differ on what is to be sustained, what is to be developed, the linkage between such differing views, and the extent of the future envisioned have emerged. What is to be sustained? The most common answer to this question is 'life support systems,' where the life to be supported is first and foremost human life. What is to be developed? As a rule, when development is discussed in the context of sustainability, The Economy is prioritized. Growth in production is seen as providing opportunities for employment and consumption.
What are the links between? Fundamentally all visions of sustainable development are characterized by the joint consideration of what is to be sustained and what is to be developed. These goals were seen as equal in importance and linked together" (Khagram et al. 2003).

In order to make the policies of regional development successful, we have to be able to identify the reasons for regional disparities and social problems which could be from economic, social-economic, social-cultural, environmental along with the concerned people in each project, because the indicators of regional performance that are based on GDP alone, consequently fail to account for broader questions about the distribution of resources in terms of social well-being, for example considering the question of 'what kind of regional development and for whom' (Pike et al., n.d.) or, alternatively, what kind of development model is inclusive and economically and socially sustainable.

It is obvious that there is nexus between Security and Sustainable Development facets, both nationally and globally. According to Stewart, three types of connection could be distinguished:

1. The immediate impact of security/insecurity on well-being and, consequently, development achievements, i.e., security's role as part of our objectives(Stewart, n.d.-a).
2. The way that insecurity affects (non-security) elements of development and economic growth, or the security instrumental role (Stewart, n.d.-a).
3. The way development affects security or the development instrumental role (Stewart, n.d.-a).

The security policies contribute to development policies to enhance security; also, the development policies contribute to security policies to enhance development. There are connections between security and development through policies. However, in an increasingly interconnected and complex world, security and development are indistinguishably linked, especially in the least-developed countries (Stewart, n.d.-b).

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

For over 20 years, development has been connected to security through the concept of human security. The relationship can be complex, lagging development can lead to grievance, and then conflict that can threaten development (Security and development | SIPRI," n.d.).

For example, the movement of manpower may reduce the production of exports, thereby reducing foreign exchange earnings, import potential, and consequently further constraining output, leading to a decline in employment and earnings (Stewart, n.d.-b). Conversely, with high levels of security, leading to development and development, further promoting security (Stewart, n.d.-b). But unfortunately, this cycle can be broken because it is easy to have relatively high levels of security without necessarily experiencing economic growth, or to have high levels of security and economic growth, but not inclusive growth so the potential for conflict remains (Chandler, 2007).

3. Expanded views of security

The classical view of security was described by Barry Buzan, who claimed that the concept of security is, in itself, a more versatile, penetrating and useful way to approach the study of international relations than either power or peace (Buzan, Hansen, 2009).

However, threats to security can have socio-economic roots, including races over natural resources, spillover effects of environmental degradation, economic and social disparities, economic and political migration, and natural disasters, among others (Paleri, 2008).

Beyond traditionally recognized issues of threats to state and national territory, beyond sovereignty, territorial disputes, geopolitics, and military-diplomatic affairs, there are many security threats that have trans-national nature since their violence affecting many parts of the world (Korab-Karpowicz, 2017).

These trans-state threats are recent, and blurred by all sorts of flows and forces, from environmental dynamics to technological development, from human and animal migrations to microorganism infection, from terrorist groups to financial flows, and from climate change to the global mass culture due to globalization that has both an integrative and fragmenting process, complex and asymmetrical interdependence, which increase the borderless of international relations, thereby shaping and transforming security issues in new and unexpected ways. (Korab-Karpowicz, 2017).

Security theorists interpret security in different ways as follows. Traditionalists purport security to inter-state military-political dangers for the sake of intellectual and pragmatic clarity. Wideners extend security concepts to inter-state threats from social, economic, and environmental issues. Deepeners integrate all sources since insecurity comes from and affects all: states, individuals, private entities, communities and the environment (Martinovsky, 2011; Prause et al., 2019).

Forms of threats that don't have the state are trans-state (migrations, technological challenges, global crime, and terrorism), sub-state (gender issues, urban misgovernance), and nonhuman (ecosystem dynamics, micro-pathogens).

The following typology clarifies the five broad types of situations or premises that constitute a security in which threats overlap and interact.

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

First, traditional state-centered threats: examples include nuclear proliferation in India, Iran, and North Korea; espionage among leading nations; territorial challenges in Crimea, the Middle East, and the East China Sea; and regional tensions (Koreas, India–Pakistan, and Iran–Saudi Arabia).

Second, New threats interact and combined with old threats creating interlocking problems. For instance, climate change (desertification of large swaths of the Syrian territory), misgovernance, economic hardship, overpopulation, factionalism, and the terrorist contagion from neighboring Iraq (all "unconventional" threats) contributed to the Syrian civil war and foreign military intervention, which in turn heightened the (traditional) tension between Russia and the United States, between Iran and Saudi Arabia, and between Iran and Israel.

Third, New developments of unconventional insecurity, such as climate change and gender discrimination, interact in ways that frustrate traditional conceptual definitions, conceptual maps, and national policies. States and other security actors have to innovate and combine forces in often unexpected ways.

As "non-physical security, diversification of threats, and the salience of identity are key effects of globalization in the security realm" (Cha, 2000), the new security environment in the twenty-first century is essentially intermestic (international and domestic) and combines more variables, dimensions, and instruments, including military or military-grade resources mobilized by non-state actors such as criminal gangs, irredentist movements, and terrorists.

Fourth, unconventional security challenges will likely shape our future. "Low politics" or "soft" issues, failed to register them as "systemic threats," and often deprioritized them in comparison to traditional, state-centered threats, they are now morphing into an increasingly recognized as "hard security" and "high politics" challenges in the twenty-first century. For instance, the massive migrations affecting Europe over the past few decades feed nationalistic, anti-Islamic forces; the rise of the authoritarian, anti-democratic right; electoral volatility; Brexit; and the possible unraveling of the European Union and the Western alliance.

Another example, the AIDS epidemic is seriously straining the family structure, social fabric, and economic development of many sub-Saharan countries. In these countries, the virus incapacitates and kills millions of workers, parents, and citizens; it creates generations of orphans, undermines community life, jeopardizes agriculture production and governance structures, causes immense suffering, and is a national, regional, and global security risk.

Fifth, the Future already arrived in several ways. Some new threats appeared as traditional threats such as diseases, gender violence, under-development, and crime; these threats are deeply modified today by globalization, which warrants fresh examination. Recent trends give clues as to what tomorrow holds: for instance, climate change is not some future threat; it has been affecting many regions for some time, and will only worsen.

Dominant countries, regions, social groups, gender, and race live in different geographical and social places and different time frames from the dominated. In particular, the powerful can externalize their negativities such as pollution, etc.

The security implications of past, present, and future climate-related changes affect health/disease, migration, food availability, political in/stability, …, etc.

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

4. Security theories for new technologies

The realist perspective may underscore actual dangers to traditional states as national boundaries erode, whereas the traditional arms race has exploded into a technological race, including hacking, intrusion, and cyberwarfare as the fifth domain of warfare.

Liberal internationalism perspective raises the importance of technological tide that may emerge with a great deal of work and diligence on the part of many stakeholders. They would advocate international cooperation, regimes, and institutions to frame these new forces.

Constructivists ascribe the new technological developments and that our cultural and psychological projections, anticipations, and fears can turn them against our interests.

New technologies are revolutionary and baffling enough to warrant new security paradigms that traditional international relations ignored so far. Traditional boundaries break down as power concentrates on information technology and STEM.

Existing social and political structures are stretched, strained, and broken as power distribution shifts toward the complete interweaving of information as the new fabric of society. While legacy power structures remain, coevolving alongside the exploding information economy, the distribution of force ownership of conventional assets has become increasingly diluted and disrupted.

Below the interrelated aspects of our technological world:
Cyberspace threats, artificial intelligence, scientific and technological development, and the vulnerabilities of global logistical networks made possible by trade globalization and information technology. However, Malicious ideas emerge, allowing for novel forms of control via super-intelligent predictive algorithms, ubiquitous surveillance, and robotic/drone deployment. The “evolution of evolution” (Kelly 2017, 2018) may outstrip” the human ability to cope.

Generally, The New dangers lurk at the intersection of human and technological co-evolution, since the existing social and political structures are stretched, strained, and broken as power distribution shifts toward the complete interlinking of information as the new fabric of society.

4.1. Threats for cybersecurity and STEM. Digital ecosystem and critical infrastructure

Mature organizations possess key functional capabilities that allow them to run an effective security program to protect against attacks intended to penetrate the confidentiality, availability or integrity of critical information (Understanding New Security Threats - Google Books, n.d.) (Gueldry, Wei, 2016; Limba et al., 2017; Korauš et al., 2019).

The foundation of any security program is the Governance, Risk, and Compliance (GRC) area, which defines the strategy, identifies risk areas and ensures compliance with defined or mandated standards and regulations.

Security governance defines the policies and standards that apply and enforce these policies across the organization. Risk management is critical for determining the risk level associated with various threats, security control gaps, and vulnerabilities. Based on these risk levels and collaboration with governance and technical experts, priorities are set, driving a strategic roadmap for maximizing security investment to reduce or offset risk over time.

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

Compliance management involves assessing the adherence of an organization to applicable regulations, standards, and internal policies. In smaller organizations or less mature security programs, all of these responsibilities may be assumed by security management, whereas, for mature organizations, there could be a sizable team dedicated to the contentment of these responsibilities.

Vulnerability management involves scanning applications, systems, and infrastructure to find entry points where systems are inclined to attack. While security controls can stop a wide range of potential attacks, they are not a substitute for continuously finding and remediating issues that could be exploited. Risks identified by the vulnerability team are typically leveraged by GRC, engineering, and architecture to help remediate issues and harden security controls to prevent exploitation.

Incident response leverages alerts from the security controls ecosystem to identify, contain, and reverse the impact of intrusion attempts, intended to compromise the confidentiality, availability, or integrity of information assets.

Forensics performs post-intrusion analysis to help quantify, contain, and remediate a breach this function also helps inform any requirements for executive or public disclosure requirements.

Information from these two processes helps to inform the hardening of security controls by engineering and architecture, while also feeding key information into the GRC/Risk Management function.

Finally, when a full mature security program has been implemented, it is time to "Sustain" this progress. At this point, GRC processes should be reaching full maturity.

Digital Ecosystems

A natural of the ecosystem is a complex combination of interconnected organisms and their environment, including all organic and inorganic constituents. Technology systems also organize into digital ecosystems comprised of people, ideas, and information (software and data), along with the diverse infrastructure supporting complex networks of interactions. Just as the natural and ecosystem evolves and adapts based on continuous interactions between organisms and their environment, digital ecosystems are adaptive self-organizing constructs that co-evolve toward adaptive novelty (Sebastiani et al. 2019; Vlasov et al. 2019).

STEM

Science, and **T**echnology, and **E**ngineering, and **M**athematics represents the field of emerging technology and expanding capabilities that materialize new ideas with unprecedented speed. They include, notably, artificial intelligence (AI), robotics, bio- and geoengineering, space exploration, nanotechnology, computer-aided design (CAD), additive manufacturing (3D of Printing), and massive digital interconnectedness.

Computer interactions with many technologies weave together our activities; our social interactions depend on the Internet of Things, or technologically connected material elements which the estimations for the number of internet-connected devices expected by the early 2020s range from 20 to 50 billion. Let’s think of the number of systems essential to visiting a hospital, flying across a continent, or going through typical work/school week. The level of interdependence we have formed with our technology has become astonishing, and loss of this capability would hurt our individual and collective mind, as mind now includes digital extensions of natural cognitive capability (Nordrum 2016). What happens if these technologies brought to our working job success in life then interrupted? What technologies exist on the horizon that we will simultaneously benefit from and become dependent on us or are we upon?

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

Technological substitution and the crisis of employment

The long-term aspects of STEM introduce future challenges; other pragmatic issues warrant unique, more immediate consideration because their consequences are already here.

A unique dilemma arises where countless tasks can be automated and hit critical mass, causing catastrophic job loss and degradation of status. The socio-economic implications are profound both during today's transition period and as this automation revolution further materializes.

Imagine a scenario where productivity hits an all-time high, with robots producing goods at an unfathomable rate, while fewer consumers have the resources to purchase these products due to unemployment and polarization of wealth which would lead lack in the economic system and then collapses due to lack of demand from erosion of aggregate purchasing power. The irony is if such a work market collapse occurred, it would be against a backdrop of unprecedented production (Mallozzi, Mullie, 2015).

Emerging cultural and social tensions and unrest may accelerate the use of autonomous robotic police and warriors to keep the peace. The topic of semi-autonomous killer robots and already been proposed since military drones are now widely utilized. In the existing episteme of humanity, few would argue that military projection of force is not are necessary. Elon Musk and Mustafa Suleyman have led a consortium of experts to petition the UN to ban the development, proliferation, and use of killer robots (Gibbs, 2017). Even this is the reactive effort intended to curb the impact of what is already occurring.

Awareness, preparedness, and resilience of societies emerge as key preconditions of further secure and sustainable economic development and general well-being (Tvaronavičiene, 2018), i.e., to develop ability to recognize, prevent, and, in case of disaster, to resist to consequences of critical infrastructure infringement which is the ultimate goal of fostering of leadership for critical infrastructure protection (Tvaronavičiene, 2018).

Hence, the European Commission has developed a Critical Infrastructure Warning Information Network (CIWIN) and European Reference Network for Critical Infrastructure Protection (ERN-CIP)("EUR-Lex - jl0013 - EN - EUR-Lex," n.d.), which ultimately would develop ability to share, discuss and generate novel approaches leading to fruitful outcomes related to critical infrastructure protection and enhancement of resilience of international community to the possible disasters.

5. Case studies of the impact of new technological threats on the information system in modern societies

What information systems interact with us, and how many activities in our day are technology dependent? Let's take the typical day for a progressive and technologically inclined adult, working for a large company in an urban area, after getting ready; they may ride into their cars with navigation and automation capabilities that border on self-driving. They receive updates on traffic, revise their commute to save several minutes, and avoid close calls with advanced collision avoidance features that now come standard on many models.

Once at work, tasks and meetings are organized and presented by personal productivity and automation software, with a speed and precision that eclipse anything that a human assistant may provide. A team of people spanning three continents uses telepresence software that allows everyone to collaborate on the same project, update design schematics, and share ideas in real-time. Lunch is ordered and paid for via apps. Workers text messages, use FB Messenger, Viber, WhatsApp, Skype, or Zoom with spouses, friends, and fellow workers all over the world. Dinner is ordered on apps while the smart-oven is preheated remotely during the commute to be at the right temperature to cook the meal exactly when the family arrives home. After dinner, the kids enjoy a video web

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

session with friends, before having their goodnight song delivered via grandparents retired abroad. (Vance, Ashlee, 2017).

This is our world now; practically every aspect of our daily life has the potential for augmentation and enrichment by powerful information systems.

What security controls have been implemented for each of these capabilities? How might an attacker manipulate these capabilities for financial gain, damage, or disruption?

Consider the following simple and ubiquitous scenarios:

- Purchase gas on the way to work.
- Drive in a vehicle with many networked computer systems.
- Transfer funds, withdraw cash, or accept payment for goods or services.
- Swipe your badge to enter the office and start work.
- Consume power, water, or gas from utility companies.
- Visit a physician, dentist, or hospital.

What type of technology systems are involved in even the simplest of jobs? How many technology systems have you interacted with today?

What would happen if some or all of these systems were unavailable or manipulated to benefit the agenda of any given attacker? Reflect on the number of tasks that are dependent on information systems or technology that could be either grossly or subtly manipulated. What is the impact potential?

What would happen if the power were unavailable for an extended period for a cold or hot area? How many times in a typical day could credit card or banking information be leaked or intercepted? What information collected about the daily activities we take for granted, which could be used for nefarious purposes? Could malicious threat actors also be peering through the looking-glass of our numerous webcams?

The infamous Stuxnet program against Iran's nuclear program development allowed for a covert technological solution to this perplexing problem. This advanced joint effort involved a malware payload designed to self-propagate rapidly while remaining dormant until certain very specific conditions were met. The malware propagated via a variety of methods, including removable media, to allow it to cross networks with an Air Gap to protect critical SCADA/industrial control systems. When the malware detected it was running on a Siemens industrial control system, consistent with those used in the centrifuges used to enrich uranium gas by the nuclear program for Iran, it engaged a subtle malicious payload. This malicious payload subtly altered the rotational speed of the centrifuges while reporting normal conditions to the operators of the machinery, with dramatic effect. This caused the costly and difficult-to-obtain devices to wear out rapidly, without a clear explanation or attribution (Zetter, Kim, 2014).

WannaCry (Fruhlinger, 2017) was known as a massive ransomware outbreak that paralyzed entire nations. This attack is believed to have impacted more than 200,000 systems in more than 150 countries, using a Microsoft vulnerability known as Eternal Blue that allowed for exploitation of the Server Message Block (SMB) protocol to allow attackers to execute commands on the host system (Vulns Tagged Entries - (CGISecurity.com), n.d.)(Grossman, 2017).

ISSN 2669-0195 (online) http://jssidoi.org/jesi/
2020 Volume 2 Number 1 (March)
http://doi.org/10.9770/IRD.2020.2.1(3)

This attack crippled the railways of Germany, universities in China, and the telecommunications infrastructure of Spain, among countless others. This attack denied access to a massive range of information systems, creating a global impact.

Debate continues on the topic of the true motive for this attack was it for financial gain, or was it a test case for how to leverage ransomware for massive global disruption? What if an attack like WannaCry was implemented in a more targeted manner against critical infrastructure as part of a complex and multifaceted military strategy? Based on these scenarios, what are the practical implications of confidentiality, availability, and integrity and how can we expect them to play out in the future?

Today's threats: Trade war between China and the USA for the sake of National Security. Trump ban Huawei communication networks and equipment.

Huawei is one of the biggest telecommunications companies in the world that is abandoned in some countries, including the US, they banning the use of Huawei networking equipment, and therefore Huawei phones are virtually invisible in these countries comparing around the world.

In January 2019, US Justice Department unsealed indictments that included 23 counts about the suspected theft of intellectual property, obstruction of justice and fraud related to its alleged evasion of US sanctions against Iran (Huawei ban: Full timeline on how and why its phones are under fire - CNET, n.d.)

The core issue that Huawei ease with the Chinese government, which creates fears with some countries such as the US that Huawei equipment could be used to spy on their country and companies.

The US banned companies from using Huawei networking equipment in 2012, and the company was added to the US Department of Commerce's Bureau of Industry and Security Entity List on May 15, Trump signed an executive order essentially banning Huawei because of national security concerns that the company is too closely tied to the Chinese government and that its gear could be used to spy on other countries and companies (Huawei ban: Full timeline on how and why its phones are under fire - CNET, n.d.).

Conclusions

What is to be sustained and what is to be developed should follow with what is to be secured since Sustainability and Security have goals equal in importance and linked together. Sustainable Security integrates critical all of the state, human and environmental security, and parallels the three linked pillars of society, economy, and nature central to the field of sustainable development. New technologies are revolutionary warrants new security standards that traditional international relations ignored so far because these threats have trans-state nature and become vulnerable to regional security and then to regional development. Most of the trans-state threats depend on networking which enables them to attack regions economically, socially, also threaten ecological security**,** which deals with the threats, disruptions, and degradations that social systems impose on ecosystems and other forms of life. Societies have to keep aware of the consequence of new technologies by analyzing and monitoring their impacts and to be ready for the new threats, whether novel threats or new impacts of old threats and to be resilience with the international community for the possible disasters since the new technologies and globalization create new. Further research areas could be the focus on the study of how to forecast, measure, and manage these trans-state threats to security that came from new technologies. Issues of regional development can be solved by taking into account a wide array of threats to security.

References

Burger, J. R., Allen, C. D., Brown, J. H., Burnside, W. R., Davidson, A. D., Fristoe, T. S., … Zuo, W. (2012). The macroecology of sustainability. PLoS Biology, 10(6). https://doi.org/10.1371/journal.pbio.1001345

Buzan, B., & Hansen, L. (2009). The Evolution of International Security Studies. Cambridge: Cambridge University Press. http://doi.org/10.1017/CBO9780511817762

Case Studies | 2015 UN-Water Annual International Zaragoza Conference. Water and Sustainable Development: From Vision to Action. 15-17 January 2015. (n.d.).

Cha, V. D. (2000). Globalization and the Study of International Security. Journal of Peace Research, 37(3), 391–403.

Chandler, D. (2007). The security-development nexus and the rise of "anti-foreign policy." Journal of International Relations and Development, 10(4), 362–386. https://doi.org/10.1057/palgrave.jird.1800135

CHAPTER 3 CONCEPT OF REGIONAL DEVELOPMENT AND ITS MEASUREMENTS. (n.d.). Retrieved from http://shodhganga.inflibnet.ac.in/bitstream/10603/52566/11/11_chapter 3.pdf

Cherchyk, L., Shershun, M., Khumarova, N., Mykytyn, T. Cherchyk, A. 2019. Assessment of forest enterprises' performance: integrating economic security and ecological impact. Entrepreneurship and Sustainability Issues, 6(4), 1784-1797. http://doi.org/10.9770/jesi.2019.6.4(17)

Cherchyk, L., Shershun, M., Khumarova, N., Mykytyn, T., Cherchyk, A. 2019. Assessment of forest enterprises' performance: integrating economic security and ecological impact. Entrepreneurship and Sustainability Issues, 6(4), 1784-1797. http://doi.org/10.9770/jesi.2019.6.4(17)

EUR-Lex - jl0013 - EN - EUR-Lex. (n.d.). Retrieved August 25, 2019, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0013

Faridi, M.F., Sulphey, M. M. 2019. Food security as a prelude to sustainability: a case study in the agricultural sector, its impacts on the Al Kharj community in The Kingdom of Saudi Arabia. Entrepreneurship and Sustainability Issues, 6(3), 1336-1345. https://doi.org/10.9770/jssi.2019.6.3(34)

Fruhlinger, Josh. 2017. What is WannaCry Ransomware, How Does It Infect, and Who Was Responsible? https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Gibbs, Samuel. August 20, 2017. Elon Musk Leads 116 Experts Calling for Outright Ban of Killer Robots. The Guardian.

Gueldry, M., Wei, L. June 2016. China's Global Energy Diplomacy: Behavior Normalization through Economic Interdependence or Resource Neo-Mercantilism and Power Politics? *Journal of Chinese Political Science*, 21(2), 217–240.

Huawei ban: Full timeline on how and why its phones are under fire - CNET. (n.d.). Retrieved August 26, 2019, from https://www.cnet.com/news/huawei-ban-full-timeline-on-how-why-its-phones-are-under-fire/

Iorio, M., Monni, S., Brollo, B. 2018. The Brazilian Amazon: a resource curse or renewed colonialism? Entrepreneurship and Sustainability Issues, 5(3). 438-451. https://doi.org/10.9770/jesi.2018.5.3(2)

Kelly, Kevin. 2017. The Inevitable: Understanding the 12 Technological Forces that Will Shape Our Future. New York: Penguin.

Kelly, Kevin. 2018. The Technium: Technology, or the Evolution of Evolution. Kk.Org. http://kk.org/thetechnium/technology-or-t/

Khagram, S., Clark, W., Raad, D. F. (2003). From the Environment and Human Security to Sustainable Security and Development. Journal of Human Development, 4(2), 289–313. https://doi.org/10.1080/1464988032000087604

Knight, Frank H. 2006 (1921). Risk, Uncertainty, and Profit. Mineola, NY: Dover Publications.

Korauš, A., Gombár, M., Kelemen, P., Polák, J. 2019. Analysis of respondents' opinions and attitudes toward the security of payment systems. Entrepreneurship and Sustainability Issues, 6(4), 1987-2002. http://doi.org/10.9770/jesi.2019.6.4(31)

Limba, T., Agafonov, K., Paukštė, L., Damkus, M., Plėta, T. (2017). Peculiarities of cybersecurity management in the process of internet voting implementation , Entrepreneurship and Sustainability Issues, 5(2), 368-402. https://doi.org/10.9770/jesi.2017.5.2(15)

Mallozzi, Joseph, Mullie, Paul. 2015. Dark Matter. Toronto: Prodigy Pictures.

Martinovsky, Petr. 2011. Environmental Security and Classical Typology of Security Studies. The Science for Population Protection, 3(2), 1–16. http://www.population-protection.eu/prilohy/casopis/11/81.pdf

Moumen, Z., El Idrissi, N. E., Tvaronavičienė, M. 2019. Water security and sustainable development. Insights into Regional Development, 1(4), 301-317. https://doi.org/10.9770/ird.2019.1.4(2)

Moumen, Z., El Idrissi, N.E.A., Tvaronavičienė, M., Lahrach, A. 2019. Water security and sustainable development. Insights into Regional Development, 1(4), 301-317. https://doi.org/10.9770/ird.2019.1.4(2)

Muniz, J,; da Gloria, M., de Melo, G., Liberato, M., A., R., Wahnfried, I.; Vieira, G. 2018. Towards sustainability: allowance rights for using water resources in Amazonas State of Brazil, Entrepreneurship and Sustainability Issues 5(4): 761-779. https://doi.org/10.9770/jesi.2018.5.4(5)

Njaramba, J, Chigeza, P, Whitehouse, H, 2018. Barriers and challenges experienced by migrant African women entrepreneurs in North Queensland, Australia, Entrepreneurship and Sustainability Issues 5(4): 1054-1068. http://doi.org/10.9770/jesi.2018.5.4(25)

Nordrum, Amy. August 18, 2016. Popular Internet of Things Forecast of 50 Billion Devices by 2020 is Outdated. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

Paleri, P. (2008). National security: imperatives and challenges. Tata McGraw-Hill Pub. Co.

Pike, A., Rodríguez-Pose, A., & Tomaney, J. (n.d.). Handbook of Local and Regional Development. Retrieved from http://www.regscience.hu:88/record/418/files/DEMO-BOOK-2017-055.pdf?version=1

Prause, G., Tuisk, T., Olaniyi. 2019. Between Sustainability, Social Cohesion and Security. Regional Development in North-Eastern Estonia. Entrepreneurship and Sustainability Issues, 6(3), 1135-1154. http://doi.org/10.9770/jesi.2019.6.3(13)

Rogalev, A., Komarov, I., Kindra, V., Zlyvk, O. 2018. Entrepreneurial assessment of sustainable development technologies for power energy sector. Enterpreneurship and Sustainability Issues, 6(1), 429-445. http://doi.org/10.9770/jesi.2018.6.1(26)

Sebastiani, J., Sanchez, J., Manrod, M. 2019. Understanding New Security Threats, Routledge Published March 6, p. 254.
Security and development | SIPRI. (n.d.). Retrieved January 3, 2019, from https://www.sipri.org/yearbook/2015/08

Stewart, F. (n.d.). CRISE Working Paper Development and Security Development and Security. Retrieved from https://assets.publishing.service.gov.uk/media/57a08cd140f0b652dd00159c/wp3.pdf

Tireuov, K., Mizanbekova, S., Kalykova, B., Nurmanbekova, G. 2018. Towards food security and sustainable development through enhancing efficiency of grain industry. Enterpreneurship and Sustainability Issues, 6(1), 446-455. http://doi.org/10.9770/jesi.2018.6.1(27)

Tung, L. T. 2019. Role of Unemployment insurance in Sustainable development in Vietnam: Overview and policy implication, Entrepreneurship and Sustainability Issues, 6(3), 1039-1055. http://doi.org/10.9770/jesi.2019.6.3(6)

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)

Understanding New Security Threats - Google Books. (n.d.). Retrieved May 14, 2019, from HTTPS://BOOKS.GOOGLE.LT/BOOKS?HL=EN&LR=&ID=FH6JDWAAQBAJ&OI=FND&PG=PT16&DQ=REGIONAL+DEVELOPMENT+SECURITY+THREATS&OTS=RDN-NEKQPE&SIG=QPIFK80M7KU7WANB6QDGHHOT26Q&REDIR_ESC=Y#V=ONEPAGE&Q=REGIONAL DEVELOPMENT SECURITY THREATS&F=FALSE

Vance, Ashlee. 2017 (2015). Elon Musk: Tesla, SpaceX, and the Quest for a Fantastic Future. New York: Harper Collins.

Vlasov, A.I., Shakhnov, V.A., Filin, S.S., Krivoshein, A.I. 2019. Sustainable energy systems in the digital economy: concept of smart machines, Entrepreneurship and Sustainability Issues, 6(4), 1975-1986. http://doi.org/10.9770/jesi.2019.6.4(30)

Vulns Tagged Entries - (CGISecurity.com). (n.d.). Retrieved August 25, 2019, from https://www.cgisecurity.com/vulns/

Zetter, Kim. November 3, 2014. An Unprecedented Look at Stuxnet, The World's First Digital Weapon.Wired. Accessed March 30, 2018. https://www.wired.com/2014/11/countdownto-zero-day-stuxnet/

Acknowledgement

This research was partly supported by the project, which has received funding from the European Union's Horizon 2020 research and innovation programme European Research Council (ERC) (Grant Agreement Number 830892)

Mohammed R. CHEHABEDDINE
https://orcid.org/0000-0001-5059-9048

Manuela TVARONAVIČIENĖ
http://orcid.org/0000-0002-9667-3730

Register for an ORCID ID
https://orcid.org/register