

# Cooperation Model for Establishing Secure Digital Transformation in Corporations: Overview of Regulatory Issues

**Nikola Saranov** 

*Unitedlex Ltd, Sofia, Bulgaria, <https://unitedlex.com>*

## ABSTRACT:

Digital transformation is not only a one-time effort that a company wishes to go through, but an entirely new vision on the evolution of business processes in the context of inevitable movement to the information age. Having in mind the nature of this movement, organizations should work hand in hand with each other and together to cooperate with the governments worldwide in order to establish secure environment for developing and implementing new technologies and innovations. This paper is focused on the essence of such interactions and the challenges before the organizations and gives valuable examples and suggestions for ensuring on-site security, as well as the best practices which demonstrate how the business could impact the creation of cybersecurity norms locally and globally. Additionally, the paper reviews the most recognized regulations in the area of cybersecurity and industry best practices applicable to the demands of the digital transformation.

## ARTICLE INFO:

RECEIVED: 31 JUL 2019

REVISED: 10 SEP 2019

ONLINE: 17 SEP 2019

## KEYWORDS:

digital transformation, cooperation, private sector, cybersecurity, legal framework



Creative Commons BY-NC 4.0

## Introduction

Along with the opportunities of the new technologies, implementations immanently bring new risks. Therefore, in the efforts of creating a security strategy for the business, it is an imperative for the organizations' decision makers to fully understand the implications before adopting technologies. At the same

time, in order to achieve actual benefits of the fourth industrial revolution and successfully transform to smart manufacturing and smart society as interrelated components, the governments should take measures to encourage cybersecurity market growth hand in hand with and even ahead of the Industry 4.0 market.

Over the past few years, there is an exponential raise in the focus on Digital Transformation in the companies worldwide. Entirely new business modules are created through transformational innovations and many old ones become contingently improved through the use of new technologies. Then again, according to Gartner's Hype Cycle of Emerging Technologies.<sup>1</sup>

Those who innovate and develop the cyber space are the ones that are harmed at most. The organizations learn about the newest threats and vulnerabilities first. With this pointed out, it becomes clear that the only way to effective and beneficial digital transformation goes through more careful and deeper consideration of the security. And security in the context of the nature of the digital environment can only be achieved through constant interrelation and cooperation on global government, academia and industry level. Security is in interest of each and every organization, but what is more important – it is an interest of each and every citizen too. In the cyber space though, terms like 'citizen,' 'sovereignty,' and 'territory' are inapplicable. Thus, it becomes an urgency for the cybersecurity to be redefined and reconsidered for the purposes of creation of an adequate and appropriate global regulation.

## **Methods**

Both, governments and organizations face a challenge to be cyber resilient in order to adapt to evolving and disrupting technologies. Therefore, this paper uses holistic and comprehensive approach to review some of the key factors in establishing secure digital transformation as inevitable part of the journey to a smart industry and smart society. Through analysis and review of the current state of some of the essential legal frameworks, legislations and industry best practices, applicable to the cyber space, this paper focuses on the challenges before the corporations, provides valuable recommendations and proposes cooperation model to the key stakeholder groups involved in the process of digital transformation. These will be highly beneficial for the organizations' higher management in considering appropriateness of their internal policies and processes as important prerequisite of secure digital transformation, as well as the government bodies, who are gradually realizing the key role of the industry and the academia in creation of conceptually new manner of regulation – the norms of the global cyberspace.

## **New Digital Landscapes and Concerns**

Ensuring an appropriate security level of the cyber environment inevitably requires timely and accurate interrelation between the actors of such environment: individuals, academia, industry and governments worldwide. This, on the

other hand, is their greatest concern. Sharing threat information outside an organization may cause reputation loss and violates their confidentiality policies. However, good example in the area of creation of cyber norms show that it is feasible to reveal the necessary information without breaching confidentiality norms applicable to the private as well as the public sector. Without requiring confidential information sharing, the US Cybersecurity Information Sharing Act<sup>2</sup> is federal law designed to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity incidents. The act creates system for federal agencies to receive threat information from private companies.<sup>3</sup> With respect to privacy, the bill includes provisions for preventing the sharing of personal data that is irrelevant to cyber security.<sup>4</sup> These shared cyber threat indicators can be used to prosecute cybercrimes, but may also be used as evidence for crimes involving physical force.

### Digital Transformation and Security

George Westerman, a Principal Research Scientist with the MIT Sloan Initiative on the Digital Economy shares in one of the initiatives' webinars the following definition of Digital Transformation:

Digital Transformation marks a radical rethinking of how an organization uses technology, people and processes to radically change business performance... digital transformation is about how technology changes the conditions under which business is done, in ways that change the expectations of customers, partners, and employees.<sup>32</sup>

The digital transformation means a change, an opportunity to use the advantages of the new technologies and innovations. However, it sometimes means increased risk too. Apart from the strategic advances of digital transformation, an organization's higher management should also take into deeper consideration the new digital demands that support such initiative. The usage of personal devices, new applications, collaborations and new access to the network and digital ecosystems expand the vector for potential cyberattacks. Therefore, one of the greatest challenges for the organizations' legal teams and Chief Information Security Officers (CISOs) is the creation of a balance between protecting the organization, customers, data and employees, and fostering an environment where ideas, partnerships and strategic business advantages can grow by underlying appropriate regulatory compliant Security Strategy.

Accordingly, the smart industrial and social evolution evolves around data. Confidentiality, integrity and availability of the sensitive data are at the core values of an appropriate security strategy and that has been accelerated by the digital transformation. Traditional information security practices might provide necessary approach but might not be enough to completely protect the organizations.

Through the use of appropriate standardization norms, organizations need to be encouraged to focus and commit to a framework or strategy that:

- Provides an integrated approach to cybersecurity – holistic approach to detect threat landscape and assist proactively in cooperation to minimize its impact rather than employing security technologies in isolation.
- Develops capabilities for threat detection to respond appropriately – most recent experience with incidents caused by the unsecured digital transformation outlines dramatic lack of cyber awareness and expertise.
- Employs the use of Artificial Intelligence (AI) to recognize patterns for smart monitoring of the IT infrastructure – according to Verizon’s Data Breach Incident Report,<sup>5</sup> detection of a data breach may take from three minutes up to thirty years. AI can assist in the response activities, but cannot accurately complete all tasks around it.
- Develops strong relationships between organizations across different sectors and government bodies for sharing information, intelligence, capacity building and research.

Thereafter, one of the greatest challenges for organizations’ decision makers at this stage of transformation to the fourth industrial revolution remains the change of the general perception of security and the focus on its strategically advantageous impact on both technology and resources. From technology perspective, strategies should be business objective-driven, rather than conservative and strictly protective, since it is more likely to become burdensome for the transformation process rather than its prerequisite. In addition, as the technologies develop and scale up, education and inclusion of human resources become the cornerstone of organizations’ progress. Successful adaption of these technologies requires new skills.

More and more examples from the recent history of threats with global impact like #Petya, #WannaCry, #CloudHopper show how important it is for the industry and government actors to collaborate and communicate the incident details in reasonably timely manner. In the past the confidentiality rule was leading. Many organizations saw security as their own business, with keeping virus data and threat information within their own systems. Nowadays the organizations legal teams and CISOs realize that the best way to beat increasingly advanced and complex cyber threats is to co-operate with each other and the government and openly exchange information and intelligence to address an array of cyberspace issues.<sup>6</sup>

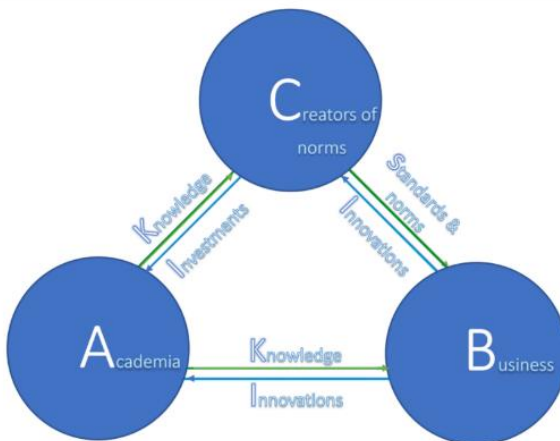
Moreover, the governmental institutions benefit from having the perspectives of the private sector, especially since the industry is the primary technology innovator and provider and has greater impact and is impacted in greater way on development of the regulatory framework.

In contrast to the historical evolution of international law norms, the development of cyber norms should engage the private sector and even individuals. The nature of the cyber space requires much different approach than the creation of locally oriented regulations, which address relatively steadily and slowly progressing matters. The statement that only governments can create legally binding norms is not applicable anymore. The role of industry and the academia

and the experience from its digital transformations is unique. On the contrary of the traditional laws' environment, the significant amount of the infrastructure of Internet, as an object that needs to be regulated, is privately owned.<sup>7</sup>

Initiatives in the sphere of Private Sector Engagement like the ones established by UN's Secretary General's High-Level Panel (Digitalcooperation.org), UN's Security Council Counter-Terrorism Committee and ICT4Peace Foundation,<sup>8</sup> as well as the European Public-Private Partnership for Resilience,<sup>9</sup> the European Network and Information Security Platform (NIS Platform), the European Network for Cyber Security, share the unique goal to identify the emergence of norms of voluntary self-regulation amongst the private sector in their responses to terrorist use of their products and services. The highlight here is multi-stakeholder and public-private initiatives aimed at supporting efforts in this area, identify persisting challenges, and recommend further areas for engagement.

In essence, providing secure environment for digital transformation and innovations is constant process of interactions between businesses, governments and academia on local and global level that could warrant appropriate and adequate cybersecurity framework legislation. On Figure 1 below, based on a comprehensive methodology to research the main actors and issues in digital transformation process, a cooperation model is proposed to outline the main interactions between the stakeholders. The same play major role in the creation of legislation, which aims at secure cyberspace as a subject of regulation and promotes innovations in more strategic path. Incorporation of such cooperation model will lead to creation of mechanisms for observation and constant improvement of the legal enforcement in accordance with the state-of-the-art technological evolution and evolving digital transformation demands.



**Figure 1: Cooperation model for developing and maintaining regulatory framework for security in the cyber space.**

### *A. Academia*

In the proposed model of cooperation, one of the key roles is given to the Academia. The significance of the knowledge it provides has three aspects:

- Proves the applicability and the reliability of technology products created by the business

Researchers from the Academia have the ability to provide valuable experience and recommendations from the test and use of the innovations. In number of cases this model of interaction between the academia and the business is presenting valuable benefits for both stakeholders, since the business depends on the competitiveness of their products and the academia relies on innovations to enlarging the horizons of their research.

- Improvement of technology standards

In the interaction with Governments, the Academia is playing key role in recommending standards for implementations on government level. This develops new opportunities for large number of the government bodies' activities and improves the results drastically. Norway and Denmark are good examples of well working and developing digitalized state environment. Despite the successful implementations, they still lack experts – another initiative that depends on the academia-governmental interactions in its significance.

- Capacity-building

By strategic investments, the governmental bodies are able to foster initiatives in gaining awareness for the functionalities and vulnerabilities of a digital transformation and its inevitable impacts in establishing smart society and smart manufacturing. This will not only raise end users' awareness but will improve the expertise of the government as well as the business agents, which will majorly contribute to the competitiveness of the state's economy. Capacity-building means enhancement of skillsets to enable individuals as well as organizations to furnish and help keep up with new technology and its use. It is not only limited to development of skillset, but requires broader understanding of the technology, policy and threat environment too.<sup>10</sup>

Capacity building in human resources for Industry 4.0 is facing conceptually new challenges, where focus on different mindset should be developed. On the other hand, it is important for the governments to establish new skill upgrading programs of the existing man-force and ensure that the curriculum of school and universities is suitably modified to include these as core subjects in future. Such tasks could only be achieved through establishment of appropriate partnerships with all actors involved: business, government and academia.

### *B. Businesses*

For the purposes of this paper and for the reason that the Business is the most active stakeholder in the aspect of digital transformation, a deeper consideration of its role is necessary in order to accurately outline the proposed methodology for cooperation in establishment of cyberspace framework regulation.

- Creation and use of state-of-art technologies

The private sector has valuable expertise in setting technical as well as performance-based standards. Thus, through assistance with the academia, it sets the criteria for the appropriate level of security of the new products, services and infrastructure that enables the digital transformation and new industry standards. Due to the constant evolution of technology and the emergence of new practices and behaviours which they enable in cyberspace, new norms and standards are needed to address challenges on the international stage between countries.<sup>11</sup>

- Experience and information about threats

The Verizon's 2019 Data Breach Investigations Report<sup>5</sup> shows significance. The FBI Internet Crime Complaint Center (IC3) contributed to this year's report with data from business email compromise (BEC) and computer data breach (CDB). Direct losses to treat actors are about \$8000 for BECs and \$25000 for CDBs. Additionally, where IC3 Recovery Asset Team acts upon BRCs and works with the destination bank, half of the money recovered or frozen; and only 9% had nothing recovered.

In the context of the threat awareness, the private sector proves to have better coverage and position than most national governments. Moreover, they are able to share timely and relevant information with appropriate public bodies across multiple jurisdictions and this would be crucial asset for many nations and their alliances in developing and maintaining regulatory framework that governs the security in cyberspace. The new perception of security requires establishment of information sharing system with direct involvement of the business and end-users. There are few initiatives in this direction, but nothing yet is unified by law and recognized by the governments. This outlines another major challenge during the already launched transformation to smart society and smart manufacturing – no responsibilities and liabilities of the actors in this process are defined.

- Partnership mechanisms and law enforcement

Meaningful partnership between public and private sector throughout implementation and development of the new industry standards are crucial in both – digital transformation and cyber regulatory endeavours. A key requirement in the development of norms is the consensus, or at least common understanding among states about the nature of the problem and the need for it to be resolved in particular way. In this context Public Private Partnerships deserve deeper consideration. This is a joint public and private initiative as it is funded and run through the government as well as a private sector or multiple private companies. Public Private Partnerships function is to provide particular information and help building and sharing the necessary expertise at the local level, which enables and facilitates the application and enforcement of the cyber norms.

A good example of such establishments is the International Telecommunication Union (ITU)<sup>12</sup> and the Organization of American States (OAS)<sup>13</sup> who have entered into partnerships with companies to disseminate information to their members on the current threat landscape with an emphasis on particular region

or issues. The objective is a common understanding among the member nations'- and organizations'- policy makers. Despite the different stages of technological maturity and legal and political cultures, an improved common understanding about the nature of cyber regulatory issues raises the likelihood of reaching consensus on common cyber norms and the need of regulation of secure environment for evolving industry processes. In the United States another interesting initiative is launched by the University of Texas at San Antonio – the National Security Collaboration Center, which has as goal to build a collaborative and impactful ecosystem engaging government, industry and academia to solve great issues surrounding cybersecurity.

The areas of cyber crime and law enforcement provide number of examples for the benefit of international collaboration. The Budapest Convention<sup>14</sup> from 2001 is regarded as the international benchmark for combatting cyber crimes. Even though, its status as a Council of Europe instrument limits its influence globally. Using the common understanding of what constitutes cyber crime that the Budapest Convention provides allows industry to collaborate across different jurisdictions with law enforcement agencies.

While nations are finding it tough to cooperate on creation of cybersecurity regulation, Microsoft is making a step forward by proposing the Digital Geneva Convention in prevention of cyber warfare.<sup>15</sup> The convention is serving as foundation for new and international cyber norms. In July 2015, governmental experts from 20 nations recommended cybersecurity norms for nation-states “aimed at promoting an open, secure, stable, accessible and peaceful ICT environment.”<sup>16</sup> In country’s government would conduct or support cyber-enabled theft of intellectual property.<sup>17</sup> This paved the way for the Group of 20th to affirm the same principle more broadly at its meeting just two months later.<sup>18</sup>

This attempt is significant and shows potential new steps ahead. Microsoft created new opportunity for vital bilateral action, pointing out that together, the governments can do more.

### *C. Creators of Norms and Standards*

- Knowledge, information and innovations sharing for law creation

Historically, the industry and the academia have been actively involved in the creation of public policies. One of the mechanisms for that is the public consultations. Experts are regularly invited to provide recommendations as well as functional and technical expertise. Some recent examples include the EU General Data Protection Regulation (GDPR)<sup>19</sup>, the Network and Information Security (NIS) Directive,<sup>20</sup> the European cyber security strategy, the European Regulation on Electronic Identities and Trust Services (eIDAS)<sup>21</sup> and the Directive on Attacks Against Information Systems.<sup>22</sup>

Experts participate in advisory roles for state, as well as international agencies and organizations which are active in cyber security matters. For instance, the statutes of the former European Network and Information Security Agency (ENISA, currently European Cybersecurity Agency) of the European Union created the Permanent Stakeholder Group (PSG) to serve as an advisory capacity



to the Executive Director with the aim of providing feedback on ENISA's work program. ENISA's objective consists of improving the cyber security posture across the European digital single market. ENISA's model of engaging stakeholders from the onset in the decision-making process through preparation of the work program has proven to be successful. Since April 2019, in accordance with the Regulation 881/2019 of EU,<sup>23</sup> ENISA is permanent European body, which provides certification mechanism.

The European Cyber Crime Centre (EC3) that sits within the European Police Agency (EUROPOL), has adopted a similar model. The EC3 has different advisory groups which provide advice and support on the exercise of the Agency's mandate. The Internet Security Advisory Group is focused on advising on and facilitating law enforcement action against cybercrime. The EC3 has announced a number of successful operations in collaboration with the industry that have eliminated criminal infrastructure, such as botnet takedowns.<sup>24</sup>

The North Atlantic Treaty Organization (NATO) established the Cooperative Cyber Defence Centre of Excellence (CCD COE) in May 2008 and the Centre obtained the status of International Military Organization in October 2008. The Centre has recognized the compelling need to address emerging challenges on cyber with affect the ability of NATO to achieve its mission and impact the defensive capabilities of NATO nations. Its mission is to enhance cyber defence awareness and security through capability, cooperation and information sharing among NATO member nations and partners. In achieving its mission, the NATO CCD COE is partnering with the private sector in activities such as cyber defence exercises.<sup>25</sup>

During Wales Summit of 2014<sup>26</sup> NATO for first time indicated its readiness to engage with the cyber security industry. The Alliance recognized the importance of working with the private sector in order to better protect NATO and allied infrastructure and to support its ability to conduct operations. A number of activities are already underway focusing on information sharing, capacity-building and promoting technological innovation to address emerging challenges.

The proposed cooperation model is also applicable in development of standards which meet private and public sector needs. Such collaboration in the United States produced the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which stems from a Presidential Executive Order released in February 2013 titled "Improving Critical Infrastructure Security."<sup>27</sup> The NIST Cybersecurity Framework consists of guidelines and references to global standards and best practices that help organizations to identify, detect, protect, respond and recover from cyberattacks. The NIST Cybersecurity Framework also creates common language to ease internal and external communications for cyber security.<sup>28</sup>

## Challenges and Recommendations for Organizations' Decision Makers

Digital Transformation is not necessarily a choice of a particular unit in an organization – it is an inevitable process in the era of Industry 4.0. The greatest

risk to be considered at this early stage of implementation is that the move to digitally based services widens the attack surface substantially.

Using a comprehensive approach this paper tries to outline main issues related to cybersecurity in the digital transformation to smart society and smart manufacturing, whereby challenges and recommendations are associated with one of the following categories: People, Processes, and Technologies.

#### *A. People*

Users or employees are crucial asset of an organization but could be the greatest threat too. The lack of awareness in the digital transformation is great challenge at this stage of moving to digitalized and smart environment. Capacity-building is necessary step before the company digital transformation endeavours start taking place. The threats are constantly showing tendencies of getting more and more sophisticated and part of the process to create a secure environment for the industry operations is to create a highly educated medium, where users will more efficiently recognize the potential threats.

Greater access and more devices, on the other hand, impose the organizations at a greater risk. The organizations' decision-makers face new challenges and the focus on traditional firewalls is no more effective. The data is now the core value for the organizations and the security strategies should be much more focused on the data centres and its perimeters.

#### *B. Processes*

With so much dependence on data flow and communication between processes, components and sub-systems, data integrity and systems integrity assume critical dimensions. Manual supervision of various processes is neither feasible nor effective. Even patching security flaws from time to time is not practical – data by itself needs to be both abstracted and secured through different tools and techniques. Following secure design principles and guidelines such as in ISO 21827 is critical to secured system design.

In the lack of centralized regulation for cyber security, organizations prefer complying with industry specific standards and best practices as International Organization for Standardization (ISO) 27k series or Payment Card Industry Data Security Standard (PCI DSS). In the age of digital transformation and new Industry demands, it is crucial for governments take initiative to assist and co-operate with private sector to detect contain, respond to and recover from cyber-attacks. Just like every other process, the digital transformation requires initial establishment, identification and clarification of the responsibilities and the liability of the actors.

In the lack of centralized regulation for cyber security, organizations prefer complying with industry specific standards and best practices as International Organization for Standardization (ISO) 27k series or Payment Card Industry Data Security Standard (PCI DSS). In the age of digital transformation and new Industry demands, it is crucial for governments take initiative to assist and co-operate with private sector to detect contain, respond to and recover from cyber-attacks. Just like every other process, the digital transformation requires initial

establishment, identification and clarification of the responsibilities and the liability of the actors.

Additionally, under a consolidated act like the Digital Geneva Convention, an independent organization is recommended to be created to span the public and the private sectors. The industry, as well as the states, need an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries. Such organization should address cyber threats in a manner like the role played by the International Atomic Energy Agency in the field of nuclear non-proliferation. In order to facilitate the needs of the individuals, industry and governments, such organization should consist of technical experts from across governments, the private sector, academia and civil society with the capability to examine specific attacks and share the evidence showing that a given attack was by a specific nation-state, so that the particular nation state would know that if they violate the rules, the world will learn about it.<sup>29</sup>

### *C. Technology*

The technology and innovations have a great impact on the economy by transforming many organizations into digital businesses and facilitating new operation models, improving efficiency and increasing capacity. The digital transformation involves utilizing data, technology, and software as a means to generate meaningful business insights and conduct operations more efficiently. When used correctly, data can trigger a meaningful shift in the capabilities of a company.

However, the most recent experience with the newest technology and innovations shows that the security concerns arise after the implementation has taken place. Having in mind the evolving complexity of the threats, which is almost as fast as the technology progress, organizations' decision makers, should much more focus on the technical and organizational measures that need to take place before implementation and optimization of processes through digital transformation. Moreover, that all the technology is interrelated in an infrastructure and this applies further risks to the data as core value of a security strategy.

### *D. Compliance and Legal Challenges*

There is also a number of legal aspects that the organizations' decision makers need to consider before creating a security strategy for their shift to smart manufacturing or smart services. From a legal aspect, the traditional organizational challenges before a digital transformation can be easily grouped in three categories: Intellectual property - facing challenges like trade secrets, which trademarks and copyrights; Contract law – related to the utilization of digital servers, cloud services and software contractors; and Compliance – now, more than ever concerning topics like Data Protection, data mining and control, data loss prevention, etc.

For the purpose of this paper, challenges like the trade-of between system performance and security level<sup>30, 31</sup> have not been considered. However, such

research directions are recognized as highly important for the technical aspects before the process of digital transformation.

## Conclusion

The legal and information security experts within the company are facing entirely new challenges in terms of implementation, ongoing processes related to the security and on the other hand – policy and legislative advisory.

From security aspect though, there is much more to be considered. Since the technology helps development of drastically new industry and society environments, it is absolutely necessary to be regulated before implementations. However, in reality the companies and the governments go for implementations without taking into account the vulnerabilities behind that. This is why it is crucial for the organizations' decision makers and strategy developers to take active part in states' initiatives for cooperation and moreover, take such initiatives themselves. Cooperation is seeming to be the only way to guarantee secure environment for digital transformation and the interdependence of data driven technology requires the organizations to be more opened in sharing threat information and details.

More platforms for government, business and academia cooperation need to be established in order to speed up the consensus building around what cyber norms and cyberspace regulations should be. This depends at most on the business as being at most exposed to the cyber threats, on academia as having capacity for development of best security standards and the governments as creators of binding legal norms.

Entirely new concept of terms like norms, security and space should be created. Instead the traditional focus on building walls and blocking access as hard as possible, the new concept requires much more awareness, interrelation and readiness for cooperation. The only way to achieving this is through set of new standards by establishing legal framework and network of supervisory consultancy bodies on local, as well as international level.

## References

- <sup>1</sup> Gartner Inc., "Hype Cycle for Emerging Technologies," 2018 [www.gartner.com/document/3885468](http://www.gartner.com/document/3885468).
- <sup>2</sup> "Cybersecurity Information Sharing Act," CISA S.2588 - 113th Congress, S.754 - 114th Congress, 2016, <https://www.congress.gov/bill/114th-congress/senate-bill/754>.
- <sup>3</sup> Mitchell Kominsky, "The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress," *Harvard Law School National Security Journal* (February 2014).
- <sup>4</sup> Andy Greenberg, "CISA Security Bill: An F for Security But an A+ for Spying," *Wired*, Jul 31 2015.
- <sup>5</sup> "Verizon Data Breach Investigation Report 2019," *Verizon business ready*, 2019, <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf>.


- 6 Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," *Tallinn Paper* No. 5, Special Expanded Issue, 2014.
- 7 Microsoft Corporation, "Five Principles for Shaping Cybersecurity Norms," 2013.
- 8 "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust," Security Council, Counter-Terrorism Committee, 2018, [www.un.org/sc/ctc/focus-areas/information-and-communication-technologies](http://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies).
- 9 EU Agency for Network and Information Security, "European Public Private Partnership for Resilience," E3PR, 2014.
- 10 Mark Philips, Jennifer Cole and Jennifer Towers, "Cyber Norms of Behaviour: Executive Summary," Royal United Services Institute 2018, [https://rusi.org/system/files/Cyber\\_norms\\_of\\_behaviour\\_report\\_-\\_Executive\\_Summary.pdf](https://rusi.org/system/files/Cyber_norms_of_behaviour_report_-_Executive_Summary.pdf).
- 11 "Capacity Building in Cyberspace: Taking Stock," Event Report, EU, Institute for Security Studies, A seminar organized in the framework of the EUISS Cyber Task Force, Brussels, 19 November 2013, <https://www.iss.europa.eu/content/capacity-building-cyberspace-taking-stock>.
- 12 International Telecommunication Union, "Global Partnerships with Industry Players," 2018, [https://www.itu.int/en/ITU-D/Cybersecurity/Pages/symantec\\_and\\_trend\\_micro.aspx](https://www.itu.int/en/ITU-D/Cybersecurity/Pages/symantec_and_trend_micro.aspx).
- 13 Organization of American States, Press Department, "OAS and Symantec to Present Cyber Security Report on June 2<sup>nd</sup>," ACI-100/14, May 28, 2014, [https://www.oas.org/en/media\\_center/press\\_release.asp?sCodigo=AVI-100/14](https://www.oas.org/en/media_center/press_release.asp?sCodigo=AVI-100/14).
- 14 "Convention on Cybercrime," Council of Europe, Budapest, European Treaty Series, No. 185, November 23, 2001, [https://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf).
- 15 "The Need for Digital Geneva Convention," February 14, 2017, <https://www.blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.
- 16 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, United Nations General Assembly, July 22, 2015, [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/70/174](https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).
- 17 "Fact Sheet: President Xi Jinping's State Visit to the United States," The White House, Office of the Press Secretary, September 25, 2015, <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>
- 18 At paragraph 26. The G-20 provision affirmed the same provision agreed to by the U.S. and China, stating "that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." Available at <http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/>.

- <sup>19</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, [https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.ENG](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG).
- <sup>20</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>.
- <sup>21</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG).
- <sup>22</sup> Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>.
- <sup>23</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.
- <sup>24</sup> Europol, “Botnet Taken Down through International Law Enforcement Cooperation,” 2019, <https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation>.
- <sup>25</sup> NATO Allied Command Transformation, “Lock Your Shields and Brace for Impact,” 29 October 2013, <https://www.act.nato.int/article-2013-2-3>.
- <sup>26</sup> NATO, “Wales Summit Declaration,” Issued by the heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales (5 September 2014), [https://www.nato.int/cps/en/natohq/official\\_texts\\_112964.htm](https://www.nato.int/cps/en/natohq/official_texts_112964.htm).
- <sup>27</sup> The White House, “Office of the Press Secretary, Executive Order — Improving Critical Infrastructure Cybersecurity,” 12 February 2013, [www.whitehouse.gov/the-press-office/2013/02/12executive-order-improving-critical-infrastructure-cybersecurity](http://www.whitehouse.gov/the-press-office/2013/02/12executive-order-improving-critical-infrastructure-cybersecurity).
- <sup>28</sup> PricewaterhouseCoopers LLP, “Why You Should Adopt the NIST Cybersecurity Framework,” May 2014, [www.pwc.com/us/en/increasin-it-effectiveness/publications/assets/adopt-the-nist.pdf](http://www.pwc.com/us/en/increasin-it-effectiveness/publications/assets/adopt-the-nist.pdf).
- <sup>29</sup> Heidi Tworek, “Microsoft Is Right: We Need A Digital Geneva Convention,” Opinion, 9 May 2017, <https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/>.
- <sup>30</sup> Stoyan Poryazov, Dmytro Progonov, Emiliya Saranova, and Zlatogor Minchev, “Performance Prediction in Secure Telecommunication System with Quality of Service Guarantees,” *The 9th International Conference on Business Information Security (BISEC-2017)*, 18th October 2017, Belgrade, Serbia, <http://bisec.rs/files/2017/09-s-poryazov-d-progonov-e-saranova-z-minchev-bisec-2017.pdf>.
- <sup>31</sup> Stoyan Poryazov, Dmytro Progonov, and Emiliya Saranova, “Quality of Telecommunications as a Composition of Qualities of Subservices, Including Security and Trusted Third Parties,” *2017 25th Telecommunication Forum (TELFOR)*, Belgrade, Serbia, 21-22 Nov. 2017, <http://ieeexplore.ieee.org/abstract/document/8249275?reload=true>.

- <sup>32</sup> As quoted by Clint Boulton, “What is Digital Transformation? A Necessary Disruption,” *CIO*, May 31, 2019, available at <https://www.cio.com/article/3211428/what-is-digital-transformation-a-necessary-disruption.html>.

### About the Author

Nikola **Saranov** obtained his LLM in 2011 from Sofia University “St. Kliment Ohridski.” Since then Nikola gained broad experience in the IT Industry in companies such as Ingram Micro and Atos. During this period, he deepened his interest in the areas of Trade Compliance, Export Control and Legal issues in the IT Industry. Having contributed to various projects within the Compliance, Legal and Data Protection Departments, Nikola is now preparing his proposal for a PhD thesis in “Cybersecurity Legal and Compliance Issues.” Along with his work as a Data Protection Legal Counsel for UnitedLex Corporation Ltd., he does active research in the field of cloud and cybersecurity implementations and the related business and legal requirements.

 <https://orcid.org/0000-0003-4836-0606>