# SLOVAK REPUBLIC CYBER READINESS AT A GLANCE

Melissa Hathaway, Francesca Spidalieri and Anushka Kaushik

April 2019

POTOMAC INSTITUTE FOR POLICY STUDIES

GLOBSEC
IDEAS SHAPING THE WORLD

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: CyberReadinessIndex2.0@potomacinstitute.org

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

***Acknowledgements***

The Potomac Institute for Policy Studies and the authors would like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

# SLOVAK REPUBLIC
# CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

# SLOVAK REPUBLIC

## *CYBER READINESS AT A GLANCE*

| | |
|---|---|
| Country Population | 5,440 million |
| Population Growth | 0.17% |
| GDP at market prices (current $US) | $95,769 billion (ranked 64th in 2017) |
| GDP Growth | 3.4% |
| Year Internet Introduced | 1992 |
| National Cyber Security Strategy | 2008, 2015 |
| Internet Domain(s) | .cs and .sk |
| Internet users per 100 users | 81.6 |
| Fixed broadband subscriptions per 100 users | 25.8 |
| Mobile cellular subscriptions per 100 users | 130.7 |

Information and Communications Technology (ICT) Development and Connectivity Standing

| | |
|---|---|
| International Telecommunications Union (ITU) ICT Development Index (IDI) **46** | World Economic Forum's Networked Readiness Index (NRI) **47** |

*Sources: World Bank (2017), ITU (2017), and NRI (2016).*

# INTRODUCTION

In 1918 – after World War I and a long history of conflicts and occupations by neighbors, including Austria, Hungary, and Germany – Czechoslovakia became an independent country. Czechoslovakia was comprised of the Czechs and the Slovaks, two distinct communities with their respective languages, religions, cultures, and economic sources of income/growth. During World War II, Czechoslovakia suffered significant loss of life and infrastructural damage until the Soviet Army liberated them in 1945. In 1946, the country held national elections that ceded power to the Czech's leading political party. Simultaneously, Czechoslovakia became a client state of the Soviet Union. For the next four decades, they were under a one-party system and the influence of the Soviet Union as part of the Warsaw Pact.

The Czech side of the country was highly industrialized (e.g., automotive, machinery, metallurgy, textiles, etc.) and provided much of the technical talent and educational capacity to the region, including three main universities focused on math, science, and engineering. Whereas on the Slovak side of the country, the main sectors of the economy were agriculture and mining of raw materials (e.g., gold, silver, copper, iron, and salt).

During the communist period, Czechoslovakia's telecommunications network was neglected. By 1960, the Soviets had centralized the postal, telecommunication, and transport bodies into a single Ministry of Transport and Communications. The merger was dysfunctional. In 1969, two ministries were set up – the Ministry of Post Offices and Telecommunications in Prague and the Ministry of Transport, Post Offices and Telecommunications in Bratislava.[1] However, most central planners still did not consider telecom services to be a genuine form of production and did not invest in the underlying communication infrastructure.[2] Instead, investment was targeted at primary forms of production, such as industrial enterprises. Telephone services served as a stable source of revenue that was channeled to help fund the more valued entities contributing to the country's economic wellbeing. In particular, the telephone service was used to subsidize postal services, which operated at a loss. Telephone tariffs were not related to the cost of providing service. Charges for domestic calls were fairly low and charges for international calls were extremely high. The central government in power at that time also imposed substantial social restrictions and actively worked to make communication among people difficult in order to promote political stability and quell the ability to conspire against the Communist Party.

Therefore, the first Internet pioneers in the country had to overcome several operational, technical, political, and social limitations. In 1976, Czechoslovakia sponsored a state project, called "Computer Network," to enable the transfer of information from one computer to another – effectively, trying to implement an ARPANET (the experimental computer network that became the basis for the Internet). A group of researchers at the Institute of Applied Cybernetics (UAK) in Bratislava began working on a number of related initiatives.[3] By 1986, the first intra-network became operational using 16-bit mini computers[4] sold by Digital Equipment Corporation. UAK was able to transfer data between three nodes in Bratislava and one in the city of Prague.

Later, researchers at UAK started experimenting with email services that used the Unix to Unix Copy (UUCP) protocol, but the network still had both operational and technical limitations. At that time, bandwidth was still limited (only 10 telephone lines per every 100 people). This network was principally used for research and did not allow communication between individuals or businesses.[5]

In November 1989, a series of demonstrations across the country, known by the Czechs as the Velvet Revolution and by the Slovaks as the Gentle Revolution,[6] showed people's desire to end the one-party rule and embrace a market economy. Eventually, this led to the election of Czechoslovakia's first multi-party government in June 1990.

During the period between 1989 and the peaceful separation of Czechoslovakia into two independent countries in 1993, the adoption of ICTs and the development of commercial networks and email communication started increasing. In 1989, UAK had established one of the primary Internet nodes (*Iac.cs*) using BITNET (a computer network of universities, colleges, and other academic institutions that was a predecessor to the Internet) to enable email communications.[7] The University of Chemical Technology in Prague had established a similar node. In 1990, UAK transitioned its node to the Comenius University in Bratislava and became part of the European computer network (EUnet). Export restrictions on wide area network (WAN) products were gradually reduced, allowing the existing nodes in Bratislava and Prague to be connected to international networks.[8] In the early 1990s, nearly every European country had a telecommunications monopoly and in Czechoslovakia it was SPT Praha (*Sprava post a telekomunikaci Praha)* under the Ministry of Posts and Telecommunications. The market was still closed to other commercial and non-commercial telecommunications services. But the European Community's (EC) industrial policy advocated for the diversification of the market from U.S.-dominated products and services and promoted the development of next-generation European network technologies and protocols as well as incubating national "research" network operators (e.g., SURFnet and DFN).

*In 1989, the Institute of Applied Cybernetics (UAK) in Bratislava established one of Slovakia's first Internet nodes.*

Several academic institutions in Czechoslovakia started receiving financial support and technical know-how from foreign partners. This was facilitated by the EU-funded project, Trans-European Mobility Scheme for University Studies (TEMPUS), launched in 1991 with the goal of providing connections between universities in the region. The project involved the sharing of expertise with universities in the hill town of Banska Bystrica in Central Slovakia and partners like UNI-C Lyngby in Denmark, the National Institute for Nuclear and High-Energy Physics (NIKHEF) in Amsterdam, the National Technical University in Athens, and the National Science Foundation (NSF) in Washington D.C. The NSF, in particular, promoted connectivity among academic institutions to ARPANET.

In 1991, the Slovak Academic Network (SANET) was established to formalize the cooperation among experts and scientists from UAK and EUnet, as well as users of those services and representatives from a host of technical universities in Bratislava, Zilina, and Banska Bystrica. Their main goal was to create and operate a backbone network for the Slovak academic community, support its scientific, technical, and organizational needs, and adopt international standards and rules consistent with the EC industrial policy goals. SANET also helped foster cooperation with other international academic organizations, including the *Réseaux Associés pour la Recherche Européenne* (RARE), and actively participated in the establishment of the Central and Eastern European Network (CEENET), which involved academic partners from Hungary, the Czech Republic, and Poland.[9]

The first official Internet connection with the outside world took place on 13 February 1992 and was followed by the establishment of the Internet domain .cs soon after.[10]

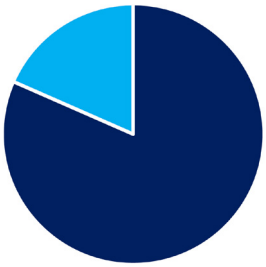
On 31 December 1992, Czechoslovakia declared a self-determined split into the Czech Republic and the Slovak Republic. The development of networks in the Czech Republic and in Slovakia took different paths. The first challenge was changing the Internet domain .cs into the two new domains .cz and .sk assigned to the two newly formed republics. The change was not easy since the .cs domain had been in use for over a year and many email addresses in both countries were jointly registered on it. It was decided that all .cs servers would remain operational for at least one more year, in parallel to the respective initialization of the Slovak and Czech domains.[11]

The second challenge was supporting additional projects to build networks in each country. Despite sharing the same Internet history and network development process up to that point, the Czech Republic was more successful in building on the work of its academics and convincing its Ministry of Education to allocate funding through large-scale government projects. Slovakia was much slower in implementing similar Internet connectivity projects and less successful in obtaining government funds right after its independence. The Slovak government struggled to define its path in the market economy and harness the value of Internet connectivity.

In 1998, Prime Minister Mikuláš Dzurinda formed a coalition government and outlined progressive political and economic reforms on the basis of a free market. His Cabinet successfully gained Slovakia's entry into the Organisation for Economic Co-operation and Development (OECD) in 2000, and accession into the European Union (EU) and the North Atlantic Treaty Organization (NATO) in 2004.[12] The accession into these important international organizations accelerated Slovakia's development, connectivity, and economic growth. The reforms also helped attract foreign direct investments and international recognition.

The Slovak government began supporting Internet uptake as a catalyst for economic growth, more efficient government operations, increased competitiveness, and the development of an information society. In 2001, the Ministry of Education launched the SANET.2 project to build out a high-speed communication infrastructure to connect with other European communication networks and provide a more robust connectivity among university centers.[13]

As a result of the increased demand for Internet services, the number of users in Slovakia has grown exponentially, from less than 10 percent in 2000, to 75 percent in 2010, to over 81 percent of the population in 2017 (or almost 4.5 million users) – above the EU average of 79 percent.[14] The availability of high-speed broadband connectivity remains lower than the EU average (32 percent versus 37 percent, respectively) because of insufficient investment in the fiber optic backbone topology. Whereas mobile broadband subscriptions have increased steadily to over 130 percent of the population in 2017, slightly above the EU average.[15]



*Slovak Republic's Internet Penetration: 81.6%*

*The number of Internet users in Slovakia has grown exponentially, from less than 10% in 2000 to over 81% in 2017.*

The ICT sector plays a very important role in Slovakia, although it is predominantly focused on manufacturing goods as opposed to delivery of services. In 2010, the country already had the 8th largest ICT sector in Europe, which constituted 4.67 percent of Slovakia's gross domestic product (GDP).[16] Slovakia's digital progress was fostered by the progressive reforms initiated by Prime Minister (PM) Dzurinda and further codified by the publication of the country's first "Information Society Policy of the Slovak Republic" in 2001.[17] This strategy declared the government's strategic intent to develop an information society and become more connected. It was reiterated in the 2004 "National Strategy for Information Society" and accompanying action plan with specific tasks and a timetable.[18]

*Slovakia's first "Information Society Policy," published in 2001, declared the government's strategic intent to develop an information society and become more connected.*

The digitization projects in the consecutive national digital strategies have been consistent with EU expectations, but have also been dependent on EU funding for their success, especially in a fiscally-constrained environment. The European Commission infused €1.2 billion (~$1.4 billion) to accelerate the "Operational Programme Information Society" (OPIS) for Slovakia for the 2007-2013 period.[19] The program, under the EU Convergence Objective framework, had a number of initiatives, such as developing electronic services, digitizing academic libraries, and improving the availability of broadband Internet access. In addition, Slovakia has received considerable financial resources from the EU Structural and Investment Funds to facilitate cross-border interoperability, provide easier access to government data, expand the government cloud, and develop electronic services for citizens and businesses. For example, in 2013, the Slovak Ministry of Interior announced that eID cards would

start being used to enable citizen access to various e-government services within the EU OPIS framework. Recently, the government announced its intentions to switch to mobile IDs and provide one unique system of identification for all e-governance, e-banking, e-health services. A new Digital Transformation Strategy is expected to be published in May 2019. The projects proposed in this strategy are consistent with previous strategies – focused on the "digital citizen" and providing free access to high-quality public services and healthcare.[20]

The new digital strategy may also be able to address the shortfalls identified in the latest EU assessment on the digital economy and society of each of its member states. In that study, Slovakia's progress in e-government participation and the integration of digital technology by Slovak businesses lagged behind the EU average (Slovakia ranked 20th out of the 28 EU member states in the 2017 European Commission Digital Economy and Society Index (DESI)).[21] Slovakia is working to improve its ability to deliver e-services (Internet use, digital skills development, e-commerce, digital public services provision, etc.) and improve broadband coverage. The government continues to pursue demand-oriented projects, consistent with EU priorities that support the construction of last-mile connections in places where the market fails and that use co-financing for broadband deployment from several EU programs.

Slovakia's awareness of the threats to its digital assets and society began in 2007. In April and May of 2007, Estonia – one of the most digitized nations in Europe – was knocked off line. Its citizen-facing services (e.g., e-banking and government services) were disrupted by a distributed digital denial of service (DDoS). Estonia requested emergency assistance from NATO for the defense of its digital assets and restoration of its citizen-facing services. It requested assistance under Article 4 (i.e., information sharing and consultation) and wanted to activate Article 5 (i.e., collective defense).[22] This accelerated the cyber discussions in NATO and resulted in NATO's first Policy on Cyber Defence that was published in January 2008. In the summer of 2008, offensive cyber techniques were demonstrated between Russia and Georgia – rendering Georgia's air defense ineffective. NATO members again realized that cyber activities were a growing component of warfare and that each country needed to take active measures to increase its defensive posture and increase the resilience of its critical infrastructures. Slovakia's Ministry of Finance noticed and took action, publishing the "National Strategy for Information Security (NSIS) 2009-2013." This first-of-its-kind document focused on an information security policy, with an outline of the institutional and organizational structure and long-term strategic objectives in the field of information security. This strategy's development was an action item from the government's 2008 National e-Government Strategy noting the country's need to protect cyberspace.[23] It also emphasized the importance of harmonizing security policies among public administration authorities and aligning them to EU and NATO's security policy.

*The Slovak's "National Strategy for Information Security" (NSIS), published in 2008, was a first-of-its-kind document focused on information security.*

The NSIS was an important first step in discussing information security policy at the national level. The NSIS defined the country's strategic goals in various sectors, including protecting critical information infrastructure (CII), raising awareness, building capabilities, developing a secure digital environment with technical, operational and strategic controls, providing effective management of information security, defending public administration information infrastructure, and engaging in national and international cooperation efforts.

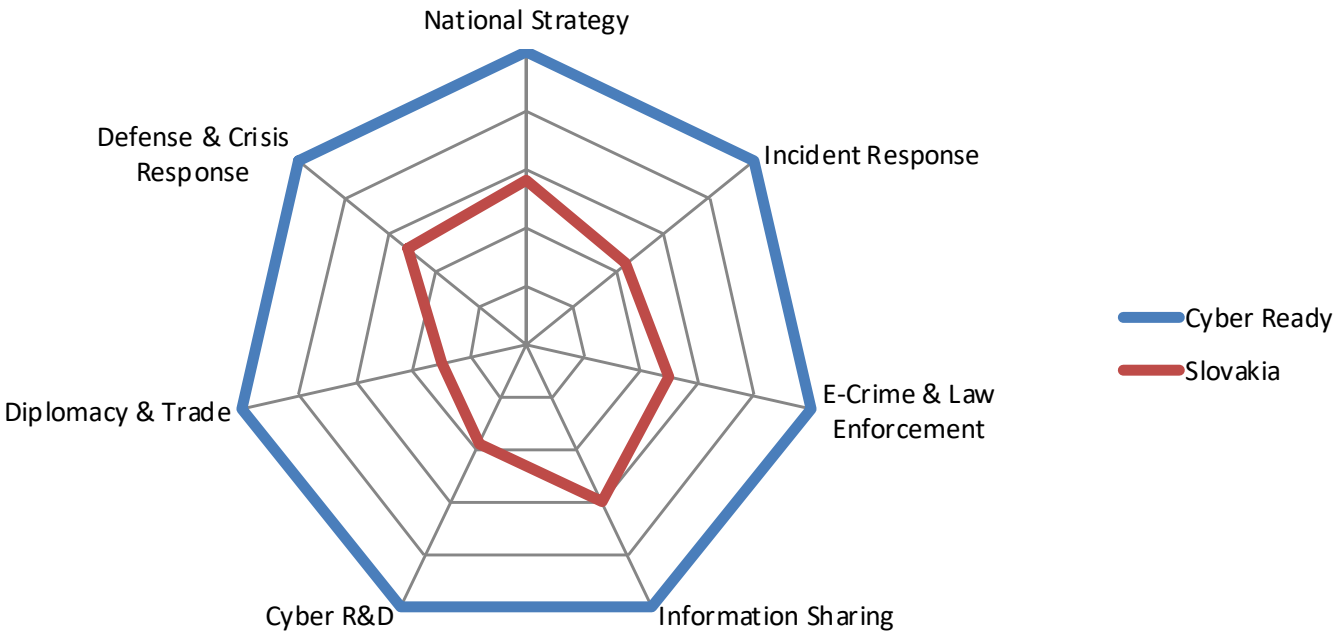
Cyber defense was introduced into NATO's Defence Planning Process in April 2012. Each Member was tasked to identify and prioritize cyber defense as part of their national and military planning processes.[24] This requirement was amplified by the EU with the publication of the "EU Cyber Security Strategy" in February 2013. The EU strategy "outlines the EU's vision on how to enhance security in cyberspace and sets out the actions required, including to drastically reduce cybercrime."[25] Taking the broader European guidance into account, Slovakia, in 2015, published a more comprehensive national cyber security strategy – the "Cyber Security Concept of the Slovak Republic for 2015-2020" – with an accompanying "Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020."[26] Both the strategy and action plan acknowledged the national security and economic risks of *cyber insecurity*. The documents delineated the roles and responsibilities of the different entities involved in national cyber security and articulated strategic and operational objectives to be implemented. In January 2016, the responsibility for coordinating the country's cyber security efforts at the state level were transferred from the Ministry of Finance to the National Security Authority (*Národný bezpečnostný úrad*, NBÚ). In March 2016, the Slovak government approved a dedicated Statute of the National Security Authority, which officially elevated NBU to be the national competent authority for cyber security.[27] All these elements were codified in the Cybersecurity Act in January 2018. The law gave the NBU additional cyber security-related responsibilities and assigned it to implement the strategy and update policies as required.[28]

The progressive reforms of the early 2000s provided the basis for Slovakia's digital economy, and the call to action from NATO and the EU has sharpened Slovakia's focus toward cyber defense. The challenge, however, is that these two sets of goals are being executed by three separate entities. The digitization of the country and the digital economic priorities (aligning Slovakia to the EU Single Digital Market) are led by the Office of the Deputy Prime Minister for Investments and Informatization, whereas the cyber security and cyber resilience priorities of the country are led by the NBU. The Slovak Military Intelligence will assume responsibility in the event of a serious national-level cyber incident, and will respond using the capabilities of the Cyber Defense Center. It is unclear how the country will align its initiatives to meet the expectations of the international institutions, and more importantly meet business needs that comprise a growing portion of the country's GDP. In order to attract foreign direct investment, Slovakia must promote its critical location in Central-Eastern Europe and its strong ICT sector. Its high connectivity, coupled with its lack of preparedness and insufficient use of the full capacity of the government entities (whole-of-government approach), has made it one of the countries in Europe that is most vulnerable to cyber

crime.[29] Moreover, because of its role in both the EU and NATO, it has become the target of state-sponsored espionage. In October 2018, the Slovak Ministry of Foreign and European Affairs was penetrated and information on the country's foreign policy and security intentions was illegally copied.[30] While the government claims to be addressing both the criminal and nation-state activity, it may be missing the nexus with other transnational cyber activities.

Slovakia economically desires to reach the same growth level of countries such as Hungary, Finland, Sweden, and Estonia, where the digital economy already accounts for 5 to 5.5 percent of their GDP, and gain an additional 2.3 percent in GDP growth from expanded broadband connectivity.[31] It also looks to these countries and Austria for inspiration on how to best align its policies to EU and NATO's strategic guidance. Slovakia needs to better understand its Internet-infrastructure dependencies and vulnerabilities and launch a concerted and coordinated effort across national stakeholders to significantly reduce cyber risk and move forward to ensure its future safety, security, and economic wellbeing.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate Slovakia's current preparedness levels for cyber risks. This analysis provides an actionable blueprint for Slovakia to assess its commitment and maturity to closing the gap between its current cyber security posture and the national capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) follows:




*Slovak Republic Cyber Readiness Assessment (2019).*

# 1. NATIONAL STRATEGY

In 2016, the digital economy already accounted for 5.9 percent of Slovakia's GDP or €4.8 billion out of €81.2 billion (~$5.4 billion out of ~$91.1 billion).[32] Then-Deputy Prime Minister for Investments and Informatization for Slovakia and today's Prime Minister, Peter Pellegrini, recognized that the digital transformation offered Slovakia the chance to regain a leadership role in the region. He also acknowledged that Slovakia was lagging behind in ICT innovation, research, and development because the country had suffered insufficient investment under one-party rule. It was not until the reforms of the early 2000s that Slovakia began to rebuild its economy and create a business environment that might attract foreign investors.[33] He conceded that Slovakia needed capital infusion to enable a digital transformation and promote innovation.

*In 2016, then-Deputy Prime Minister for Investments and Informatization Peter Pellegrini recognized that the digital transformation offered Slovakia the chance to regain a leadership role in the region.*

Since 2001, Slovakia published several national-level plans to promote the digitization of the country's government services and operations. These strategies were developed in line with EU priorities and goals set forth by many documents including: the European Information Society for Growth and Employment (an initiative launched as part of the 2000-2010 Lisbon Agenda,)[34] various iterations of the *e*Europe Plan of Action(s)[35] and EU e-Government action plan(s), the 2010 Digital Agenda for Europe 2020, and finally the 2015 EU Digital Single Market Strategy.

In 2001 – before its accession to the EU in 2004 – the Slovak government adopted its first "Information Society Policy of the Slovak Republic," which declared the government's strategic intent to develop an information society and become more connected.[36] This strategy was followed by the 2004 "National Strategy for Information Society" and accompanying action plan. These two foundational documents outlined priorities for telecommunications investments and to create the necessary technical skills to help society gain access to information and contribute to the digital economy.[37] The plan was evaluated on an annual basis, yet progress against the goals were limited likely due to inadequate funding. The government codified this strategy into law and assigned the Ministry of Finance, in collaboration with the Government Plenipotentiary for Information Society, as the responsible entity for developing an information society under the Prime Minister (i.e., state administration) and creating a stable digital economy.[38]

Over the next decade, Slovakia published a number of plans to advance the country's development. These initiatives, listed on the following page, included beginning to invest in broadband infrastructure, digitizing citizen-facing services, advancing digital literacy and inclusion, and promoting the need to protect data.

- The 2004 "Sustainable Development Action Plan for 2005-2010";
- The 2005 "Competitiveness Strategy for the Slovak Republic until 2010" adopted in direct response to the 2000 EU Lisbon Strategy;
- Two National Reform Programs (2006-2008 and 2008-2010);[39]
- The 2008 "Information Society Strategy for 2009-2013," which built upon the experience of its predecessor while considering the ongoing economic crisis that swept through Europe in the late 2000s;[40]
- The 2008 "National e-Government Strategy" and an ambitious national master plan, which called for the development of a national strategy for information security "with the aim of providing cyberspace protection" in Slovakia;[41]
- The 2008 "National Strategy of the Slovak Republic for Digital Integration";[42]
- Two national broadband strategies (one for 2009-2013 and one for 2011 with no expiration date);
- The 2012 national "Operational Program Information Society."[43]

In 2014, the Ministry of Finance released another national digital strategy – the "Strategic Document for Digital Growth and Next Generation Access Infrastructure (2014-2020)."[44] This strategy built on the seven pillars of the 2010 Digital Agenda for Europe 2020 and its 2012 revised version. It identified priorities and specific actions to help foster wider use of ICTs, ensure safe and secure access to digital services, and expand e-governance processes in Slovakia. It had four key priorities: "encouraging economic growth, boosting competitiveness, enhancing economic with a higher value added, and increasing effectiveness of public administration."[45]

It recognized that the digital economy already represented 4.6 percent of Slovakia's GDP in the first half of 2012, making the digital economy outperform other sectors such as agriculture, banking, construction, and retail. It also acknowledged that Slovakia's digital economy had a considerable potential for further growth to approach the level of such countries as Hungary, Finland, Sweden, and Estonia, where the digital economy already accounted for 5 to 5.5 percent of their GDP, and that broadband and productivity gains could contribute an additional 2.3 percent to national GDP growth.[46]

*The 2014 "Strategic Document for Digital Growth and Next Generation Access Infrastructure" acknowledged that Slovakia's digital economy had a considerable potential for further growth.*

Moreover, the 2014 national digital strategy recognized the importance of increasing the security of electronic services and systems, with an emphasis on protecting personal data and privacy, modernizing and protecting critical infrastructure, developing

processes to handle security breaches, and aligning national strategies and policies with the 2013 EU "Cybersecurity Strategy along with the draft directive concerning network and information security (NIS) submitted by the Commission. … The goal of the specific measures [was] to increase cyber resilience of information systems, reduce cyber crime, and reinforce cyber defense policy and capabilities" in line with the EU Common Security and Defense Policy (CSDP).[47] The document also identified funding and resources for specific priorities, such as providing electronic services for citizens and businesses, securing the networks of the public administration, and expanding broadband connectivity, etc.

Slovakia's initiatives have been significantly dependent on the receipt of EU funding, especially in a fiscally-constrained environment. Only 44 percent or € 2.3 billion (~$2.6 billion) of funding to implement the 2014 strategy came from the state budget. The rest came through a combination of EU Structural and Investment Funds, such as the European Regional Development Fund (ERDF), and private funding and investments. This digital strategy has since served as the basis for subsequent initiatives aimed at digitizing citizen-facing services and developing a knowledge-based society in Slovakia. A new Digital Transformation Strategy is expected to be published in May 2019. The projects proposed in this strategy will likely build on previous strategies – focused on the "digital citizen" and providing free access to high-quality public services and healthcare.[48]

*Slovakia's initiatives aimed at digitizing citizen-facing services and developing a knowledge-based society have been significantly dependent on the receipt of EU funding.*

In announcing this new digital strategy, Deputy Prime Minister Raši emphasized that citizens will also have increased transparency regarding how the government and private sector are collecting and using their personal data. The document will outline the government's priorities to transition to mobile IDs and migrate all services and platforms (banking, healthcare, social security, etc.) online. He reiterated the government's motto "*Jedenkrát a dost*" ("Once is enough"), meaning all citizens should only have to be identified with one digital ID to access all public services. As the country continues to become more digitized, however, it must also mitigate the risks resulting from its hyper-connectivity ensuring that ICT systems do not suffer from breach, disruption, or destruction.

Slovakia became more focused on the need for cyber defense in 2008 as a result of the incidents in Estonia and then Georgia. Its national leaders recognized the need to protect their digital environment by reducing the overall level of cyber security risk within and across borders. After the publication of the 2008 e-Government strategy, which had called for the development of a national strategy for information security, the Ministry of Finance published the "National Strategy for Information Security (NSIS) 2009-2013." This first-of-its-kind document focused on an information security policy, with an outline of the institutional and organizational

structure and long-term strategic objectives in the field of information security. At that time, the Ministry of Finance served as the national authority for information security pertaining to all unclassified information in public administration and the general public. The Ministry of Finance was also responsible for developing and implementing both the digital and national cyber security strategies.[49] Classified information protection, cryptographic services, electronic signatures (expanded to trust services in 2016), and cooperating with foreign national security authorities and international organizations were the responsibility of the National Security Authority (*Národný ezpečnostný úrad*, NBU).[50]

*From 2008 to 2015, the Ministry of Finance was the entity responsible for implementing both the digital and national cyber security strategies.*

The NSIS was an important first step in discussing information security policy at the national level. The NSIS defined the country's strategic goals in a number of areas, including: protecting CII, raising awareness and digital skills, developing secure digital environments with technical, operational and strategic controls, ensuring the security of and defending public administration information infrastructures, and engaging in national and international cooperation efforts. The accompanying 2010 "Action Plan for 2009 to 2013 for the National Information Security Strategy of the Slovak Republic" directly aligned the NSIS to the EU's relevant documents as well to the interests articulated in OECD and NATO's policies. The action plan and the "Report on the Performance of Tasks of the NSIS" set clear milestones and objectives for each initiative and assigned specific tasks to government agencies for implementation. For example, the Ministry of Interior was assigned responsibility to manage crises and protect CII. The Ministry of Telecommunication continued its responsibility over Internet Service Providers (ISPs). The NBU continued its role in protecting classified information and managing digital certificates. The Ministry of Justice continued to apply existing laws and combat cyber crime. It also outlined a national governance roadmap for cyber security and stated that its initiatives would be financially supported by the EU OPIS program.

After the publication of the NSIS strategy, Slovakia began reorganizing its institutional and organizational structures. It began to update laws and regulations to address the growing threat of cyber crime and increase capacity to address other cyber threats. Understanding that ISPs could and should undertake more responsibility in national defense, the country began to address the regulatory shortfalls in the security of information and communication systems. Through its national Computer and Emergency Response Team (SK-CERT), Slovakia began building the capacity to implement measures to manage cyber incidents.

In 2013, other national security entities began discussing the dangers of Slovakia's cyber insecurity. The Slovak Ministry of Defense (MoD) published its "White Paper on Defense of the Slovak Republic,"[51] noting that Slovakia must take the necessary steps to prevent

threats that could cause significant or irrecoverable damage that could undermine the credibility of the state. The Security Council of the Slovak Republic began adding the topic of cyber threats to its annual reports on the security risks to the country. Even so, Slovakia recognized that its approach to cyber security was still fragmented. In 2015, with the publication of the "Cyber Security Concept of the Slovak Republic for 2015-2020," the government entities responsible for cyber security were reorganized yet again.[52] In January 2016, NBU was elevated to become the national competent authority with the responsibility for managing national cyber security.[53]

*In 2016, after the publication of the "Cyber Security Concept of the Slovak Republic," NBU was elevated to become the national competent authority for cyber security.*

At the same time, the Committee for Cyber Security[54] was established within the Security Council of the Slovak Republic. Together, they confirm Slovakia's national security priorities including those related to cyber. These priorities, reflected in the 2015 strategy, also took into account Europe's cyber priorities as reflected by both the 2010 NATO Defence Strategy and the 2013 EU Cyber Security Strategy. Slovakia's strategy also incorporated many of the requirements of the forthcoming EU Directive on Network and Information Security (NIS Directive). Slovakia had a critical assessment of its cyber security posture and noted many shortfalls that the strategy intended to address. These included "the field of cyber security in the Slovak Republic [was still] not integrally and consistently regulated at a national strategic level."[55] The document explains that "cyber threats [were still] not generally seen as a sufficiently urgent problem," and that the country was still lacking a national framework for "systematic, coordinated, and efficient collaboration" among its key stakeholders.[56]

In 2016, the government released an "Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020."[57] The two documents taken together constitute a broader approach to cyber security "creating the conditions to build up national cyber capabilities" and ensuring "adequate protection (and security) of state cyberspace from potential threats."[58] Both the strategy and action plan acknowledged the national security and economic risks of cyber *insecurity*. The common strategic goal was to "establish an open, secure, and protected national cyberspace." The strategy laid out seven strategic areas to adequately address cyber risks and threats, including:

1. Building of institutional framework for cyber security administration, which emphasizes the establishment of a National Incident Resolution Unit and several incident resolution units;

2. Creating and adopting a legal framework for cyber security;

3. Developing and applying basic mechanisms to secure the administration of cyberspace;

4. Supporting, formulating, and adopting an education system in the area of cyber security;

5. Defining and adopting a risk management culture and communication system between stakeholders;

6. Actively participating in international cooperation; and

7. Supporting cyber security science and research.

The strategy also addressed the importance of cooperation with the private sector, especially in regard to the development of a risk management culture and information sharing framework. It noted the importance of collaboration between its government ministries, public and private sectors, and national and global institutions.[59] It also called for the creation of a formal platform for collaboration and cooperation, especially on education and training.

The high-level goals in this strategy were further detailed in its accompanying Action Plan.[60] Each task was assigned to the sector-specific agency/ministry (e.g., interior, economy, finance, and defense, and the National Incident Resolution Unit) for implementation.[61] Early successes of the plan include: assigning NBU the mission for national cyber security; establishing a National Cyber Security Incident Response Team (National SK-CERT); implementing an alert, incident reporting, and information exchange system (i.e., the Cybersecurity Single Information System); promoting *ad hoc* legislation and regulations in line with EU policies and other international obligations; and establishing mechanisms for the protection of CII.

The implementation of the action plan was funded through EU operational programs, ministry funding programs, and the NBU budget, but exact allocations were unspecified.[62] NBU's 2018 funding was €9.051 million (~$10.2 million) for the broad spectrum of its existing missions including cyber security. It is unclear how the funds will be divided by mission area.

The recommendations and action plan, as well as the key components of the NIS Directive, were codified in the 2018 Cybersecurity Act, which served as the foundation for "the subsequent creation of regulations, standards, methodical instructions, rules, security policies and other instruments necessary to provide for cyber security."[63] The law officially elevated the role of NBU (Articles 4 and 5).[64] NBU's responsibilities for national cyber security now include:[65]

- Assessing the effectiveness of the national cyber security strategy and, in cooperation with the respective state authorities, producing an annual report on the country's state of cyber security that is submitted for approval to the Committee for Cyber Security of the Security Council (which functions as an advisory body to the Prime Minister);[66]

- Developing cyber security-related national policies, regulations, standards, action plans, and methodologies, and directing and monitoring their implementation;

- Formulating incident response policies, plans, and procedures to handle national-level cyber security incidents, issuing alerts and warnings about serious cyber security incidents, accrediting incident resolution (CSIRT) units, and supervising their activities;

- Serving as the national point of contact (POC) for cyber security and defense for foreign entities and ensuring cooperation with the respective POCs at the EU and NATO;

- Representing Slovakia in international fora dedicated to cyber security and coordinating the execution of tasks to fulfill international cooperation agreements;

- Monitoring the national cyberspace by gathering, analyzing, and evaluating information on current and potential cyber threats;

- Administering and operating the Cybersecurity Single Information System – the country's national information sharing platform.

Slovakia has made significant progress since the early 2000s to advance its digital economy and shore up its cyber defense. From 2008 up until the publication of the 2015 national cyber security strategy, the Ministry of Finance was in charge of both the digital agenda and small components of information security. In 2015, the missions were separated, and the country began a new focus on cyber defense. Today, the Office of the Deputy Prime Minister for Investments and Informatization leads the digitization of the country and the economic priorities (aligning Slovakia to the EU Single Digital Market), whereas the NBU leads cyber security and cyber resilience. In the event of a major cyber incident, the Military Intelligence will assume responsibility for defending the country.

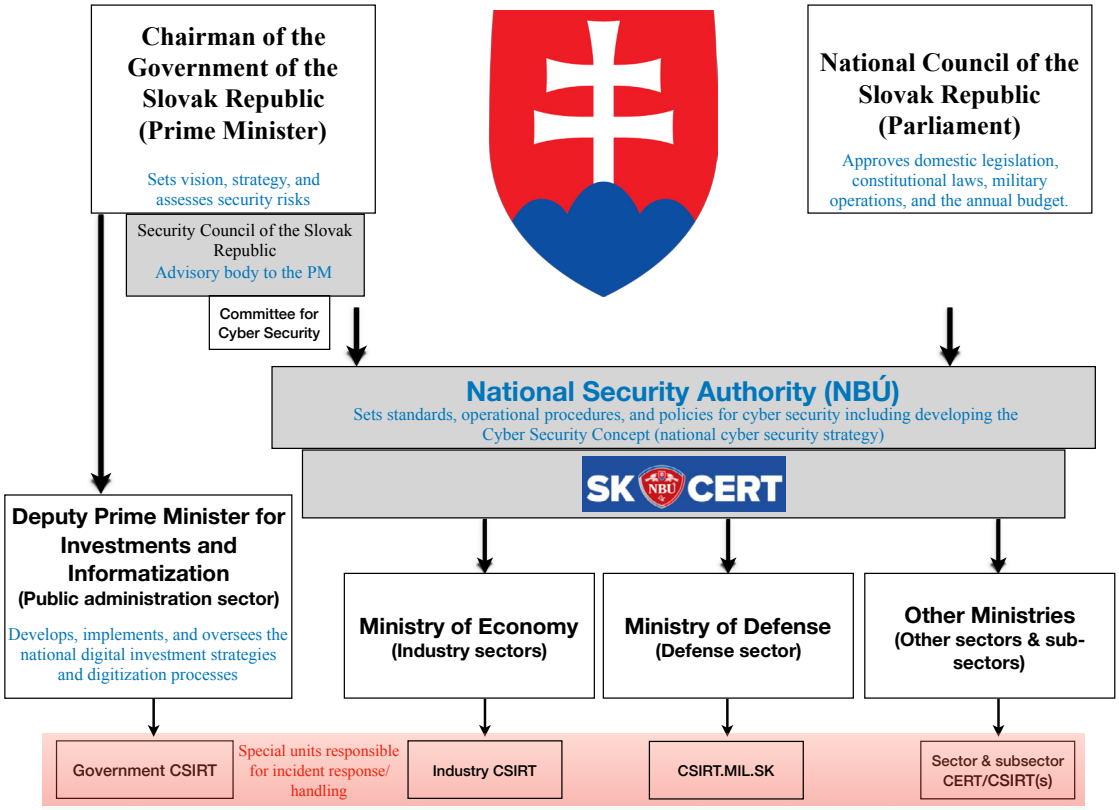



*Figure 1: Slovakia Cyber Security Organizational Chart.*

It is unclear how Slovakia is aligning its short and long-term priorities for the country. Effective risk management requires the country's leadership to understand what it values most, outline what is most important to protect (e.g., companies, services, infrastructures, and assets), and demonstrate that it is willing to invest the political capital, executive time, money, and resources needed for this protection. Slovakia continues to enumerate economic and security aspirations without clearly ensuring that they build on each other and can mutually be realized (operationalized). It is unclear if both the economic and national security considerations are addressed in the Security Council – or even in the Prime Minister's (state administration) office.

Slovakia is already one of the more vulnerable countries to cyber crime in Europe. Moreover, because of its role in both the EU and NATO, it has become the target of state-sponsored espionage. NBU must champion the cyber security and resilience considerations as part of the country's planning process. Slovakia cannot afford to slip in the execution of its 2015 national cyber security strategy's risk reduction measures.

Slovakia has set high expectations for itself, including ensuring that its digital economy grows to the proportions of northern European countries (e.g., Sweden). There are also growing expectations from international institutions that it will commit to and meet the requirements set forth by the EU, NATO, and OECD. Communicating what is at stake and improving overall risk awareness is important at every level – from government leaders to every citizen. NBU will have to put cyber security in context by explaining why each initiative will help reduce economic and societal risk. Establishing clear lines of accountability and responsibility, and successfully achieving each milestone will begin to establish credibility and foster confidence in Slovakia's ability to defend its digital future. As international institutions, businesses, investors, and citizens gain their confidence, Slovakia will likely see the much-needed infusion of capital to continue to accelerate its economic growth and innovation.

## 2. INCIDENT RESPONSE

The 2018 Cybersecurity Act detailed the processes and competent bodies responsible for cyber security incident handling, but Slovakia does not have a consolidated, single national incident response plan. The 2018 law assigned NBU the overall responsibility for handling domestic cyber security incidents, coordinating response activities at the national level, producing reports on cyber security incidents, issuing alerts and warnings about serious cyber security incidents (through the Cybersecurity Single Information System), and cooperating with international organization and authorities to handle cross-border cyber security incidents. Different entities are operationally responsible, including the national Computer and Emergency Response Team (SK-CERT, under NBU), the government CSIRT unit (under the Office of the Deputy Prime Minister for

*The 2018 Cybersecurity Act assigned NBU the overall responsibility for handling domestic cyber security incidents and coordinating response activities at the national level.*

Investments and Informatization), the industry CSIRT under the Ministry of Economy, and the CSIRT.MIL.SK (under the Military Intelligence of the Slovak Republic within the MoD). NBU is also tasked with establishing preventive measures to prevent and mitigate cyber incidents before they occur.[67]

Moreover, the 2018 Cybersecurity Act (Article 27) clarified the mission and tasks of the Cybersecurity Single Information System.[68] This system is a platform intended to manage, coordinate, and inspect the activities of state administrations and CSIRT units in the field of cyber security. It is administered and operated by NBU and is not fully operational yet. This platform will also gather, process, and evaluate information so that the state of cyber security in Slovakia can be assessed. Operators of essential services and digital service providers are required to report cyber security incidents via this system. In the event of a serious cyber security incident, NBU can issue urgent alerts both through the Cybersecurity Single Information System, the mass media, and the Central Portal of Public Administration. NBU then decides which CSIRT unit and/or operator of essential service or provider of digital service is responsible for handling the actual incident and directs specific reactive measures to be carried out by those entities. If NBU exhausts all manners of handling a serious cyber incident, it must then submit information about the perceived impacts of the event on the security of the country to the government's Security Council as part of the procedure for crisis situation handling. Depending on how grave the threat is, NBU will contact and inform the Military Intelligence.

Assessing the severity and impact of malicious cyber activity on individuals and organizations in Slovakia has been somewhat difficult in the past because of the lack of official statistics outside of the public sector and the propensity of victims not to report incidents or notify authorities. According to several studies and data collected by EU agencies, Slovakia is one of the countries most vulnerable to cyber crime in the EU, along with Malta, Greece, Spain, and Lithuania.[69] In 2018, SK-CERT reported around 1,500 denial of service attacks and 5,000 cases of malware in the country.[70]

SK-CERT, as it is known today, was established in 2016 under NBU.[71] However, Slovakia has had a national CSIRT-type unit since at least 2009, when it established the Cyber Protection Department of Information Security and Electronic Signature within the NBU's organizational structure. This department included a Department of Computer Security and Incident Response, which was renamed the Computer Security Incident Response Center (CS-CSIRC) in 2011.[72] CS-CSIRC also served as the national POC for the NATO Cyber Protection and the European Warning System, NSIAM (which expired on July 1, 2017). The unit kept developing its operational activities and, in 2014, NBU established a Security and Operational Monitoring Center (SK-CSIRC) and expanded its activities to include "the role of guarantor for cyber security in the National Security Analytical Center." In 2016, NBU established a new specialized national unit SK-CERT. The original CS-CSIRC unit has dissolved by incorporation into SK-CERT.

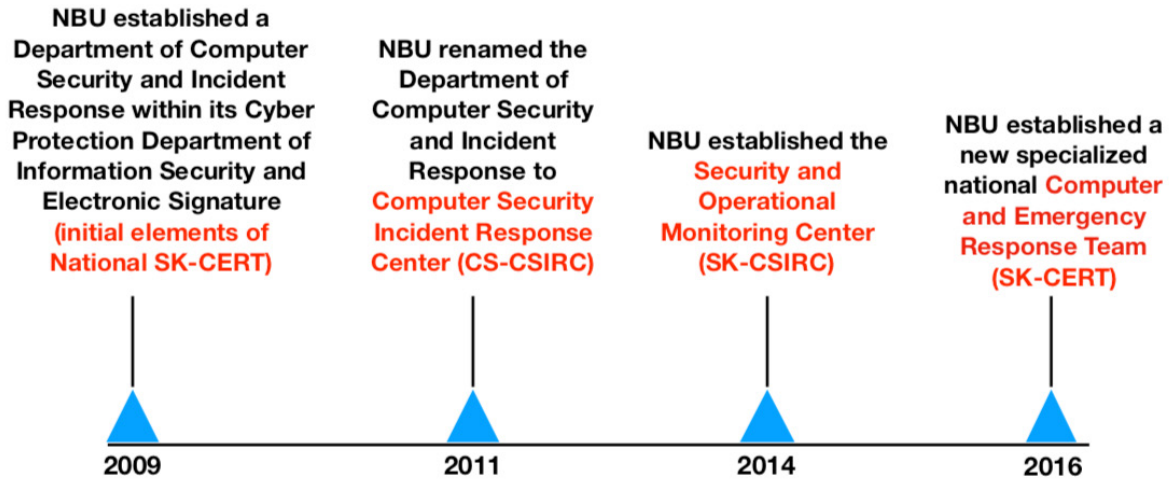



*Figure 2: Evolution of national CSIRT-type unit in Slovakia.*

Today, SK-CERT is responsible for a series of proactive, reactive, and educational services, including the following:

- Monitoring adherence to security standards in public administration information systems and determines the status of security;
- Providing services associated with the actual handling of incidents for their constituency and different levels of support depending on the type and severity of a particular event;
- Coordinating national security incident resolution and restoration of information systems in cooperation with the owners and operators of the systems concerned;
- Issuing security bulletins and alerts containing information on cyber threats, product vulnerabilities, cyber security incidents, and other cyber-related information;
- Conducting regular analysis and assessments of incidents, vulnerabilities, malware, and threats at the national level;
- Promoting cyber security awareness by publishing articles, promoting best practices, providing advice and delivering recommendations;
- Serving as an active member of the Forum of Incident Response and Security Teams (FIRST) and shares information with national and international partners; and
- Offering cyber security education and training.[73]

*The national SK-CERT is responsible for a series of proactive, reactive, and educational services.*

With the passage of the Cybersecurity Act in 2018, NBU was officially defined as "the National CSIRT Unit," in line with the requirements of the 2013 EU strategy for "An Open, Safe and Secure Cyberspace" and subsequent EU Cyber Security Directive. However, the specific tasks of a national CSIRT continue to be performed by SK-CERT. It now has a broader mandate and must perform the following tasks:

- Fulfill notification and reporting obligations to the competent authorities of the EU and NATO;
- Cooperate with central authorities, other state administration bodies, CSIRT units, basic service providers, digital service providers, and international partners;
- Impose specific obligations over service providers and digital service providers to react in the event of an incident and approve the provider's security measures;
- Receive national and international reports on cyber security incidents and cooperate with international organizations and authorities of other states in handling transnational cyber incidents.[74]

The 2015 national cyber security strategy did not identify the country's critical infrastructures, services, assets, or companies. After the publication of the 2016 NIS Directive, Slovakia was required to identify the critical providers in the following categories: banking, transportation, digital infrastructure, energy, financial services, postal services, electronic communications, healthcare, and public administration.[75]

The obligations for providers of CII services were codified in the 2018 Cybersecurity Act, as required by the NIS Directive. Slovakia created a national registry and each key operator or provider is entered in the register along with the competent authority responsible for overseeing them. Articles 8, 24, and 25 of the 2018 Cybersecurity Act detail duties and responsibilities of operators of essential services and digital service providers, and rules and obligations for reporting and responding to specific cyber security incidents.[76] They use the Cybersecurity Single Information System to report, manage, and share information, receive alerts and warnings, and when required, coordinate cyber security incident response.[77] There is a non-public, invitation-only part of the platform reserved exclusively to operators of essential services and providers of digital services that is accessed by government agencies including accredited CSIRT units, the National Bank of Slovakia, the Office for Personal Data Protection, and other government entities upon approval of the NBU.

In addition, there is a public administration CSIRT that was created under the Ministry of Finance in 2009. In 2016, it was transitioned to the Office of the Deputy Prime Minister for Investments and Informatization and was renamed to government CSIRT unit (CSIRT.SK).[78] This unit is responsible for handling cyber security incidents in public administration information systems and for providing preventive and reactive services, including the publication of monthly reports of cyber security incidents in Slovakia and around the world.

In September 2018, the Deputy Prime Minister's Office announced a new project – the "National System for Cyber Security Incident Management in the Public Administration." It was proposed in cooperation with the National Agency for Network and Electronic Services (NASES), the Slovak Information Service, and NBU. The project received €45 million (~$51 million) first to focus on the security of the government's operations and then to concentrate work on other national priorities. The money will be used to build out a government's Security Operation Center (SOC) and create a department for IT auditing within the DPM Cybersecurity Division. It will also be used to help the government CSIRT.SK implement preventive measures to thwart security incidents.[79] The new government SOC, audit team, governance, and CSIRT.SK will be staffed with about 60-70 employees.

Within public administration, the Deputy Prime Minister's Office is also transitioning to electronic means of communication across all departments as well as standardizing Service-Level Agreements (SLAs) and contracts to move toward better IT governance.[80] As the country continues to become more digitized, however, it must also understand that its hyper-connectivity may lead to ICT system breakdowns and breaches of confidentiality, accessibility, and data integrity. Slovakia has yet to develop a plan for the potential degradation of its various national digital services and especially its eID system, which will soon become the mobile ID system.

In 2002, in line with EU data protection requirements, Slovakia established a Data Protection Authority – the Office for Personal Data Protection. This office is an independent state authority tasked with supervising compliance by both governmental and non-governmental entities with all Slovakian data protection and privacy laws. It has the authority to summon data controllers or processors to investigate alleged legal infringement of data protection obligations and can force organizations to release the information concerning the breach of protection of personal data.[81] It also acts as the national regulator for the implementation of the EU General Data Protection Regulation (GDPR) requirements. The Office is one of the five competent authorities that can access information in real time via the Cybersecurity Single Information System.

Finally, SK-CERT has conducted national cyber security exercises – mostly focused on technical aspects – in 2011 and 2013 (Slovak Information Security Exercise) organized in cooperation with the Ministry of Finance and aimed at critical infrastructure protection.[82] Both the government CSIRT.SK and the national SK-CERT regularly participate in multi-national cyber security exercises organized by the EU (e.g., Cyber Europe), NATO (e.g., Cyber Coalition), the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) (e.g., Locked Shields), the EU Agency for Cybersecurity (ENISA) (e.g., CyberSOPEX), and many others.[83]

Slovakia is improving its capability to detect, repel, and contain sophisticated threats to its networked infrastructures and services. The NBU is beginning to field the latest technologies to improve the country's situation awareness of emerging threats. Finally, Slovakia has just begun to develop the necessary national capabilities to increase its preparedness by conducting continuity planning and response preparation for large-scale cyber crises.

## 3. E-CRIME AND LAW ENFORCEMENT

In 2005, Slovakia signed – and in 2008 ratified – the Council of Europe Convention on Cybercrime (commonly known as the "Budapest Convention"). While Slovakia has amended and strengthened its domestic legislation and regulations to include computer crimes, "cyber crime is not treated by law as a special category of crimes, which is also why statistics on cyber crime cases are not fully available."[84] The term "cyber crime" has not been explicitly defined in the Slovak Penal Code or in a similar normative legal act. However, the Penal Code does recognize and stipulate the facts of individual criminal offense for "unauthorized access to" or "unauthorized intervention in" computer systems or computer data, or for using, procuring, or possessing a computer to commit a criminal offense. Taken together, these provisions form the normative framework on cyber crime in Slovakia.

*In 2005, Slovakia signed – and in 2008 ratified – the Council of Europe Convention on Cybercrime.*

The methods to combat cyber crime have also been incorporated in other strategies and action plans, such as the "Strategy on the Prevention of Crime and Other Antisocial Activities in the Slovak Republic for the years 2012-2015." This strategy stated that the seriousness of cyber crime and incident rate reduction was a national priority. This is probably due to the fact that several studies have ranked Slovakia as one of the most vulnerable countries to cyber crime in the EU, along with Malta, Greece, Spain, and Lithuania.[85]

In order to meet EU expectations, Slovakia has transposed the 2013 EU Parliament and EU Council "Directive on Attacks against Information Systems" and extended the legal regulation under its Penal Code to identify a wider complex of cyber crime acts. It has also made the legal regulation of criminal liability of legal entities more precise under a separate law.[86] Collecting statistics on computer crimes and e-crime remains cumbersome. Statistics in the Prosecution Service are compiled separately from the statistics of the Police Force, Slovak courts, SK-CSIRT, or the private sector, and there is no common database to show all the criminal offenses related to computer crime. However, efforts have been made to upgrade the accuracy and interoperability of relevant public databases and to use a common taxonomy as suggested by the EU as a basis to collect data on cyber crime.

In 2014, the Constitutional Court of Slovakia issued a resolution that included a non-preservation of data clause, which had a negative impact on the detection, investigation, and prosecution of computer crimes in the Slovak Republic. It also slowed cross-border law enforcement exchange of information because there was no requirement to report incidents or retain data. This, in turn, also hampered international legal assistance in some cyber crime cases.[87] In that same year, Slovak prosecutorial authorities had to develop a special process with the U.S. authorities to request expedited preservation of computer

data and accelerate cooperation. In 2017, the law on data protection was amended making incident reporting mandatory for certain categories of businesses (in line with the NIS Directive) and allowing for the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offenses.[88]

The Slovak data retention law was also updated in line with the EU Data Retention Directives (DRD). The law requires ISPs and telecom companies to retain users' data for a certain period of time. This data must be accessible by law enforcement authorities to combat crime, terrorism, and other domestic issues. Slovakia now requires ISPs and telecom services to keep a check on the communications of all citizens – even those citizens who are not suspected or convicted of a crime – and law enforcement officials can demand access to the data for any reason. Moreover, in line with European requirements, ISPs are expected to store data of other service providers, data locations, and six months of communication parties' data in cases of email, Internet, and voice over IP (VoIP) communication, or one year of information for other communications.[89] Critics fear that these measures violate privacy, data protection, and freedom of expression in Slovakia.

While Slovakia has not established specialized units in the Police or Prosecution Service dedicated specifically to carrying out investigations or prosecutions of cyber crime, it did set up a Cybercrime Unit within the Criminal Police Bureau at the Presidium of the Police Force in 2015. The unit is responsible for criminal intelligence activities. In addition, the Ministry of Interior received over €220,000 (~$246,960) from the European Commission under the 2013 "Illegal Use of Internet" call for proposals to set up this specialized cyber crime unit and to fulfill the objectives laid out in the Slovak Police Strategy for the 2014-2020 programming period.[90] The objectives included setting up an integrated national system for reporting and monitoring illegal content on the Internet, modernizing methods and tools, and procuring technical equipment for detecting and investigating computer security related to criminal activity. The strategy also calls for the development and implementation of new programs for police training and education in the field of prevention and fight against crime, with an emphasis on radicalism and terrorism in connection with cyber crime.

The Cybercrime Unit has been growing in terms of capacity and missions since 2015 and it supports local authorities in their investigations of cyber crimes by promoting exchange of information, monitoring illegal activities on the Internet, ensuring the collection of lessons learned from casework, and facilitating training in this field. However, Slovakia has generally lagged behind other EU countries in the establishment of specific training and capacity building programs for enabling court judges, prosecutors, lawyers, law enforcement officials, forensics specialists, and other investigators to better fight cyber crime. The 2016 Action Plan that accompanied the 2015 national cyber security strategy emphasized the need to strengthen education in the area of information and cyber security within judicial authorities, and proposed the introduction of a minimum level of education for all judges and prosecutors at all levels.[91] More recently, Slovak authorities have launched various training and capacity building activities for practitioners, which are organized by various academies. They have also put forward different efforts

to prevent and raise awareness about cyber crime, including supporting the activities of the non-profit organization *e*-Slovensko that operates the Slovak Awareness Center under the EU Safer Internet Programme. *E*-Slovensko's goal is to raise awareness about cyber security among the public, especially children and youth, in order to teach them how to behave responsibly when using new online technologies. The Slovak Awareness Center performs various activities, hosts social events, and produces promotional materials to raise awareness about safer use of online technologies.[92]

*The e-Slovensko's mission is to raise awareness about cyber security among the public, especially children and youth.*

In 2014, the Slovak Ministry of Interior launched a project in collaboration with the University College in Dublin (UCD) and *e*-Slovensko to support capacity building efforts and to deliver effective and appropriate cyber crime training programs for Slovakian law enforcement personnel.[93] The project was co-funded by the EU Prevention of and Fight against Crime Programme. As part of this project, UCD organized a number of study visits for various representatives of the Slovakian Police and delivered specialized training for professionals, investigators, and technical experts. It also produced a report that reviewed current provisions for law enforcement training in digital forensics and cyber crime investigations, identified best practices in these areas, provided recommendations for cyber crime capacity building in the country, and developed a competency framework to deliver additional educational programs to Slovakian law enforcement personnel.

Slovakia cooperates closely with the European Cybercrime Centre (EC3) and Europol, and has an Interpol national bureau operating from Bratislava that serves as a 24x7 contact point, as per the provisions of the Budapest Convention. The General Prosecutor's office and the International Law Department within the Ministry of Justice regularly send their representatives to the European Judicial Cybercrime Network, including the kick-off meeting held in 2016. They also take part in other initiatives promoted by the Council of Europe on Criminal Justice in Cyberspace and the Organisation for Security and Co-operation in Europe (OSCE).

Despite recent efforts to reduce the rate and risk of computer-related crimes, Slovakia continues to be plagued by higher cyber crime activities than most of its neighbors. This is caused by a combination of lack of awareness of the threats to the country's digital infrastructures and services, an inadequate investment to provision secure and resilient products and services, and a high rate of infection of Slovakia's digital devices and infrastructures. These infections and intrusions enable illicit and illegal activities. Slovakia's maturity and commitment to reducing criminal activities that affect the country and to combating transnational crime need acceleration. In order to bring the country in line with European and global expectations and to meet the needs of a healthy digital economy, Slovakia may need to increase its efforts with law enforcement agencies, ISPs, and international partners to reduce the pathways for cyber crime.

## 4. INFORMATION SHARING

As stated in the 2015 national cyber security strategy and its action plan, Slovakia recognizes that an efficient and secure system for the exchange of information between the public and private sectors, as well as with other relevant actors in the national cyberspace, is necessary to ensure the protection of cyberspace.[94] The action plan included practical recommendations to create an effective, national-level model of cooperation among relevant entities within the national cyber security architecture, and to implement a system for reporting, responding to, and exchanging relevant information about cyber security incidents. These recommendations resulted in the development of the Cybersecurity Single Information System. In 2018, with the passage of the Cybersecurity Act, Slovakia formally established the Cybersecurity Single Information System (Article 8).[95] The Cybersecurity Single Information System is administered and operated by NBU, the entity responsible for incident response coordination and information sharing during crisis and emergencies, as well as other functions. This online platform "ensures systematic gathering, concentrating, analyzing, and evaluating of cyber security incidents information," while the central early warning system promises the "timely exchange of information on the threats, cyber security incidents, and risks related thereto" between NBU and other entities involved in incident response handling.[96] Depending on the urgency of a cyber incident or threat warning, NBU can issue alerts both through the Cybersecurity Single Information System and the mass media, and on the Central Portal of Public Administration (Article 27).

*The Cybersecurity Single Information System facilitates the collection, evaluation, and exchange of information.*

The system consists of public-facing and non-public parts and access is free of charge. The public section contains a registry of competent bodies, operators of essential services, and providers of digital service. It also includes a repository of cyber security incidents, the list of accredited CSIRT units, alerts and warnings, and other information for minimizing, averting, and remedying the consequences of a cyber security incident. As well, it contains methodologies, guidelines, standards, policies, and announcements pertaining to industry and country best practices. The 2018 Cybersecurity Act specifies who qualifies for inclusion in the register of service providers or operators (e.g., banking, transportation, digital infrastructure, energy, financial services, postal services, key areas of industry, electronic communications, healthcare, and public administration).[97] Each key operator or provider of the individual sectors is entered in the register along with the competent authority responsible for their oversight.

The non-public part of the Cybersecurity Single Information System can be accessed directly in electronic form in real time, and is reserved to specific bodies within the government, accredited CSIRT units, operators of essen-

tial services, providers of digital services, the National Bank of Slovakia, the Office for Personal Data Protection, and other public administration authorities as determined by the NBU.

As mentioned in the incident response section, SK-CERT plays an important role in information sharing. It actively cooperates with other national and foreign CSIRTs and is a member of two important organizations, Trusted Introducer and FIRST. These organizations are particularly important for the sharing of information among recognized CSIRTs around the world as well as other security teams. Membership to these organizations is based on trust and professional cyber security ethics, which have a significant impact on receiving relevant cyber security information and exchanging experiences around the world. SK-CERT also publishes monthly reports with information on cyber threats, product vulnerabilities, cyber security incidents, and other cyber-related information. In addition, SK-CERT participates in the information exchange project called the "CyberExchange." It was launched in 2018 by the Czech CSIRT team and co-financed by the EU Connecting Europe Facility (CEF) as a reaction to the increase in cyber security threats and the need for cross-border defense cooperation. It is intended to strengthen mutual cooperation of national and government CSIRTs/CERTs and grow the expertise of their respective staff members. Security teams from Austria, Croatia, the Czech Republic, Greece, Latvia, Luxembourg, Malta, Poland, Romania, and Slovakia participate in the CyberExchange.

Under the Office of the Deputy Prime Minister, the government CSIRT.SK provides cyber information and alerts to other government agencies. It regularly performs penetration tests with the involvement of other public and private sector entities. In addition, it is the central contact point for other Public Administrations' European-level CSIRTs for the exchange of information and agreed upon procedures.

Slovakia is also a key member of the Central European Cyber Security Platform (CECSP), which plays a role in facilitating information exchange among the Visegrad (V4) countries (i.e., Czech Republic, Hungary, Poland, and Slovakia) and Austria. CECSP was established in 2013 by the Czech Republic and Austria, and consists of representatives of government, national, and military CSIRT teams along with the representatives of national security authorities. Slovakia is represented in the CECSP by NBU. The aim of the platform is to foster cooperation among neighboring countries in the area of cyber security, especially to promote the exchange of information; share tactics, techniques, and procedures for handling cyber threats; and work together to prevent future cyber attacks.

Finally, Slovakia participates in the NATO's Malware Information Sharing Platform (MISP) and collaborates with its Alliance members in the areas of cyber defense, cross-border cyber security incidents, and the exchange of technical information on threats and vulnerabilities.

Slovakia is beginning to promote its critical location in Central-Eastern Europe and its strong ICT sector. Yet, its high connectivity coupled with its lack of preparedness has made it an attractive target for cyber crime and state-sponsored espionage. Slovakia's businesses and critical services need actionable information and advice to help shore

up their defenses and increase resilience. The CECSP can be an excellent platform to facilitate information sharing and increase situational awareness and resilience. It will be important to ensure that the necessary incentives are in place to accelerate the timely and actionable exchange of data.

## 5. INVESTMENT IN RESEARCH AND DEVELOPMENT

While Slovakia does not have an officially recognized national or sector-specific research and development (R&D) program dedicated to cyber security or advanced technology development, the 2015 national cyber security strategy stated a clear intent to support cyber security R&D and innovation.[98] It also focused on the need to incorporate cyber security education at the primary and secondary educational levels; develop specialized educational systems for secondary schools, universities, and professionals; and create an internal market for cyber security products and services.[99] The 2015 strategy and many of the national digital plans have also emphasized the need to raise cyber security knowledge and awareness and develop digital literacy and skills among the public. The 2016 Action Plan tasked the National Agency for Network and Electronic Services (NASES), the Ministry of Education, Science, Research and Sport, and NBU with additional measures. These included: building new specialized workplaces to better protect the country's major information assets; supporting the development of knowledge and know-how in cyber security science and research; and creating forensic labs to collect and evaluate digital evidence and conduct analytical activities during responses to security incidents or attacks.[100] However, all these strategies did not clearly state how the government would support, advance, and sustain these efforts.

The Slovak system of innovation ranks below the EU average and support for R&D is the lowest among the Visegrad Group (i.e., Czech Republic, Hungary, Poland and Slovakia).[101] In comparison, the total share of R&D investment in GDP in the Czech Republic was more than twice that of Slovakia in 2017 (1.8 percent vs. 0.9 percent).[102] Corporate funds account for only a quarter of the total Slovak funding for R&D and the country is still mostly dependent on EU money to fund R&D projects, education, and training programs. In 2015, Slovakia was the fifth biggest recipient of EU funding for government and higher education R&D, benefitting from over €470 million (~$528 million).[103] In 2014, Slovakia received €2.2 billion (~$2.5 billion) from the European Structural and Investment Fund (ESIF) to implement the Horizon 2020 priorities and country-specific recommendations for policy reforms under the European Semester in education, employment, and social inclusion.

The EU funds are allocated through a series of programs, including the Operational Programme for Research and Innovation (OPVaI), the Human Resources Operational Programme, the Youth Unemployment Initiative (YEI), and the 2014-2020 ERDF. In particular, OPVaI intends to boost competitiveness of small and medium-sized enterprises, support sustainable economic growth, and promote research and innovation. This program supports R&D in a variety of fields as part of the EU 2014-2020 Intelligent Specialization Strategy. In Slovakia, these fields include environmental issues, technological development and innovation, research in science and technology (S&T),

and the promotion of increased efficiency and performance of the R&D system.[104] The Slovak Ministry of Education, Science, Research and Sports, in collaboration with the Ministry of Labor, manages all EU funds, including OPVaI. However, by the end of January 2018, Slovakia had only spent 4 percent of the €2.2 billion it received from the OPVaI and other EU programs.[105]

In recent years, the Slovak Ministry of Education, Science, Research and Sport, established a Scientific Grant Agency, called VEGA (*Vedecká Grantová Agentúra*), in partnership with the presidium of the Slovak Academy of Sciences (SAS), to serve as an advisory body for the implementation of S&T policies, financing of basic research, and evaluation of research projects.[106] VEGA is dedicated to selecting projects from institutional finance resources under two sub-chapters of the state budget: university-based S&T research and SAS. Its average annual budget is €14 million (~15.7 million).

The ICT sector plays an important role in the Slovak economy and employment in this sector has grown exponentially between 2008 and 2017 (47 percent increase). In 2018, the ICT sector contributed to 4.6 percent of Slovakia's GDP and employed about 3 percent of the overall labor force (about 24 percent of the labor force works in the private sector).[107] Given the importance of the manufacturing sector in Slovakia – which commands some of the highest manufacturing's employment shares in the EU – workers need to be trained to make sure they remain employable in an increasingly digital workplace. To respond to this need, in 2016 the Slovak Ministry of Economy established the Smart Industry Initiative for Slovakia. This initiative supports digital transformation in a variety of areas, including developing smart factories and manufacturing; raising awareness and collaboration; promoting research; and providing access to finance, labor market, and education, etc.[108] The Smart Industry Initiative was inspired by similar German and Dutch initiatives and emphasizes R&D cooperation with industry and the deployment of more advanced technologies like Internet of Things (IoT) throughout the economy. Key stakeholders from government, industry, academia, and the technical community participate in the Smart Industry Platform. Funds for this initiative, however, remain limited and mostly dependent on existing industry funding pools and the EU funds.[109]

*Slovakia has the highest manufacturing's employment shares in the EU – underscoring the need to train and retain a digital workforce.*

While the government has not developed a unified program or set of incentives to encourage cyber security education and applied research at universities and academic institutions, it does support and fund all public universities and national laboratories – some of which have developed their own research projects in this field. In particular, the Cyber Security Lab at the Pavol Jozef Šafárik University focuses on network intrusion detection, honeypots, and privacy issues; the Department of Computers and Informatics at the Technical University in Košice has an ongoing collaboration with Siemens, IBM, and Microsoft; and

the Faculty of Informatics and Information Technologies of the Slovak Technical University (STU) has recently launched a Centre of Excellence for Artificial Intelligence (AI). The Ministry of Education, Science, Research and Sport, the Deputy Prime Minister's Office for Investments and Informatization, and NBU all play a role in promoting cyber security education, knowledge creation, and skills development. The Slovak government recognizes that a cyber-literate workforce would help Slovakia in tackling cyber threats in the long run, and is trying to address its shortage of cyber security talent by incentivizing the younger population to study and work in the cyber security field.[110] In 2017, the Slovak government invested 3 percent of its GDP on bettering the overall quality of education in the country, including cyber security education for public administration employees.[111]

The Slovak government is also providing scholarships and grants through the Official Development Assistance (ODA) program to national and international students for education at technical universities, like the STU.[112] However, the ODA program is not specifically focused on cyber security education.

Different governmental entities and private sector companies are individually and more directly involved in strengthening digital skills and literacy, supporting the development of a knowledge-based society, and further increasing the number of ICT students in Slovakia. For example, in 2016, the Ministry of Education, Science, Research and Sport in partnership with the ICT industry, academia, and other partners launched the IT Academy project.[113] This project aims to increase the numbers as well as the level of digital skills of ICT students, equip IT laboratories at schools, and set up new IT-related educational programs. It also intends to train elementary and secondary school teachers to use digital technology and innovative pedagogies to teach STEM subjects, including mathematics, informatics, and natural sciences. The IT Academy project is scheduled to run from 2017 to 2020 and aims to reach 24,000 students from at least 300 elementary schools, about 9,000 students from at least 200 secondary schools, and 3,000 students from 5 technical universities. It plans to create additional informatics courses and new IT labs in 60 elementary schools, 30 secondary schools, 4 state organizations, and 8 universities. Courses already incorporated in school programs include troubleshooting and computer programming, computer systems and networks, information security, and programming of mobile devices, etc. The EU Human Resources Operational Program – part of the €2.2 billion EU Operational Program funding stream – is supporting the IT Academy project. From 2015 to 2018, the Ministry of Education, Science, Research and Sport has allocated more than €131 million (~$147 million) through this program.

In 2015, ESET – one of the world's largest IT security companies headquartered in Bratislava – established the ESET Research Centre in collaboration with the STU and the Comenius University in Bratislava. The research center aims to effectively connect the academic and business sectors and increase research activities and capacities in cyber security.[114] Other IT industry associations, such as the Košice IT Valley and the IT Association of Slovakia (ITAS), facilitate cooperation, innovation, and education in the ICT sector and support innovative start-ups and small IT companies in the

Eastern Slovakia region through incubators, financing, venture capital, entrepreneurship education, rubber training, mentoring, etc.[115] One of the main aims of the Košice IT Valley is to motivate youth to study and work in IT and robotics. Its "IT Valley 2012+" project seeks to create a communication platform for stakeholders in the ICT cluster in Eastern Slovakia including government, research and development institutions, universities, and secondary schools focused on ICT education.

*The ESET Research Centre connects the academic and business sectors and serves to increase research activities and capacities in cyber security.*

In July 2016, the EU launched the European Cyber Security Organisation (ECSO) – a contractual public-private partnership in cyber security (cPPP) that supports initiatives and projects focused on developing, promoting, and encouraging European cyber security.[116] The main objective of the partnership is to foster cooperation between public and private actors at the early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (e.g., ICT products, services, software). The partnership also aims to stimulate the cyber security industry by allowing it to elicit future requirements from end-users and sectors that are important customers of cyber security solutions (e.g., energy, healthcare, transport, finance), thereby helping to align the demand and supply sectors. NBU is one of founding members of ECSO and is involved in its organizational structure, particularly in the National Public Authorities Committee (NAPAC); the Working Group 1 (WG1) focused on certification, standardization, labeling, and supply chain management; the WG5 focused on education, training, cyber range, and awareness issues; and the WG6 focused on strategic research and the EU innovation agenda.

In September 2017, then-Deputy Prime Minister for Investments and Informatization and today's Slovak PM Pellegrini launched the Digital Coalition (*Digitálna Koalícia*) – in line with the priorities of the EU Digital Skills and Jobs Coalition initiative.[117] This initiative promotes cooperation among public and private entities and the professional community. It includes projects to foster digital literacy and skills development, train ICT experts, and prepare Slovaks of all ages for work and life in the digital economy and so-called Industry 4.0. Among the founding members of the Slovak Digital Coalition are the ministries of Education, Economy and Labor, Social Affairs and Family, as well as secondary and higher education institutions, ITAS, the Association of towns and municipalities (ZMOS), and major tech companies like T-Systems, Microsoft, Cisco, and Orange.[118] In 2018, PM Pellegrini stated that the Digital Coalition project has been successful primarily due to the great commitment and enthusiasm displayed by its participants.[119] The coalition has attracted over 65 members from different sectors and established 218 measurable commitments, including a series of scholarships for foreign students to study ICT in Slovakia. Members of the Digital Coalition have also supported the development of the Center of Excellence for AI at STU.

Among its activities, the Digital Coalition carries out "IT fitness tests" to gauge the level of digital literacy and IT skills of students and teachers in primary schools, high schools, and colleges across Slovakia.[120] After the relatively poor results from the latest iteration of the IT fitness tests – the average test success rate for middle and high schools dropped from 42 percent in 2017 to 36 percent in 2018[121] – the government recognized the need to increase investments for education in computer science, critical thinking, and cyber security. Deputy Prime Minister for Investments and Informatization Richard Raši stated that focusing on cyber-literacy will be a priority going forward, especially given the 2018 cyber attacks on Slovakia.[122]

During remarks delivered at a Conference on AI and Data Science at the American Chamber of Commerce in Slovakia in September 2018, Deputy PM Raši stressed the importance of creating an attractive business environment in the country for companies focused on AI and directing the economy toward higher value-added enterprises.[123] He emphasized three specific areas of focus for the near future: 1) forming international research partnerships, 2) transferring expertise from labs to the market, and 3) following current best practices in decision-making. In February 2019, his office also announced a Memorandum of Cooperation with the United Arab Emirates to establish consensus for digital ecosystems and AI, in line with the recent push for developing smart cities.[124] Deputy PM Raši's office also released a call for projects focused on digitizing city administrations, public services to residents, transport management, and public safety.[125]

The new Slovakia Digital Transformation Strategy, expected to be released in May 2019, will also include a renewed focus on digitizing services, promoting cyber security education, and attracting foreign investments in the ICT sector.[126] Since the early 2000s, Slovakia has recognized that it needs to invest in research and education in order to realize its economic goals. Every digital and innovation strategy published underscores these aspirations. Yet, Slovakia still faces a significant shortage of cyber security professionals able to protect its critical services and infrastructures, companies, and digital assets. Moreover, most of its R&D initiatives and cyber security education and training programs are still heavily reliant on EU funding to operate. The government must find new mechanisms to encourage the development and retention of ICT talent and the creation of a vibrant startup community underpinned by increased public and private sector investments. The government's limited implementation and funding to advance its digital and innovation strategies, combined with its dependence on EU funding, may not be enough to accelerate the digitization of public and private activities while at the same time reducing the country's cyber insecurity.

## 6. DIPLOMACY AND TRADE

The 2015 national cyber security strategy and the 2014 national digital strategy both identified ICT and cyber security as important elements of Slovakia's national security and economic prosperity, and stressed the importance of promoting "active international collaboration."[127] However, Slovakia has not recognized cyber security as a Tier One priority of its foreign policy or its foreign trade and international commerce negotiations.

*The NBU is responsible for cooperating with the Ministry of Foreign and European Affairs to develop international cooperation in the field of cyber security.*

According to the 2018 Cybersecurity Act, NBU is responsible for cooperating with the Ministry of Foreign and European Affairs to develop international cooperation and monitoring activities in the field of cyber security on the foreign policy interests of the country.[128] Both the 2015 national cyber security strategy and 2016 Action Plan reiterated that, as a member of NATO and the EU, Slovakia intends to participate in the formulation of international strategic and conceptual documents, prepare and implement EU legislative and non-legislative initiatives involving cyber security, and support NATO collaboration in the area of cyber defense. In line with the objectives described in the national cyber security strategy, Slovakia regularly participates in international discussions on cyber security, cyber crime, CSIRTs cooperation, and cyber defense (although the country has rarely initiated regional agreements in these matters). In addition to its EU and NATO membership, Slovakia is a member of other major international bodies addressing cyber security-related issues, including the Council of Europe, OECD, V4, ENISA, the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE), the Digital 3 Seas Initiative, and the Network and Information Security Public-Private Platform (NIS Platform) – established as part of the 2013 EU Cybersecurity Strategy.[129]

Moreover, Slovakia currently holds the Chairmanship of OSCE, and one of the priorities it set is cyber security. Specifically, Slovakia is focusing on the protection of critical infrastructure by furthering the dialogue and implementation of the 16 confidence-building measures (CBMs) that the OSCE 57 member states adopted.[130] These measures are aimed at reducing the risks of conflict that stem from the misuse of ICTs. In March 2019, the Ministry of Foreign and European Affairs' representatives discussed possible common procedures to protect critical energy infrastructure and ways to promote multilateralism in cyber diplomacy during the Vienna Cybersecurity Week. Slovakia has an important opportunity to intensify efforts to operationalize the CBMs and promote initiatives to drive cyber resilience for the region.

*Slovakia currently holds the Chairmanship of the Organisation for Security and Co-operation in Europe (OSCE) and will work to implement the 16 confidence-building measures to drive cyber resilience for the region.*

Besides its collaboration in international organizations and structures, Slovakia also works to cultivate relations and engage in bilateral cooperation with specific countries in the area of cyber security. For example, in 2018, PM Pellegrini and French President Emmanuel Macron agreed to deepen cooperation in cyber security by facilitating information sharing between Slovak and French experts.[131] Similarly, the Slovak government has held talks with Azerbaijan and offered its expertise in regards to the adoption of measures aimed at securing networks and information systems.[132] The same year, in 2018, Serbia and Slovakia agreed to exchange experiences and expertise in the development of national innovation infrastructures, and national regulations on innovation, digital transformation, and technology transfer. Slovakia has also joined the "Paris Call for Trust and Security in Cyberspace" – a high-level declaration on developing common principles for securing cyberspace, launched by the French government in November 2018.[133]

Prime Minister Pellegrini has personally taken part in some of the global debates on cyber security issues, such as the provision of 5G technology from Chinese telecommunications manufacturers and its importance to national security. PM Pellegrini took a divergent stance from his Polish and Czech counterparts and many other NATO allies when he declared that Slovakia does not consider Chinese technology a security threat and that Slovakia will not impose any restrictions on their market entry at this time.[134]

Finally, Slovakia is beginning to support Europe's broader initiatives to address the exposure of citizens to large-scale disinformation, including misleading or outright false information. The Ministry of Foreign and European Affairs has developed a strategic communications unit that looks at the spread of disinformation and fake news. This unit is the contact point for the election cooperation network by the EU to ensure safe and secure elections. However, the MFA is more focused on confronting cyber threats coming from Russia, including influence and disinformation campaigns, than establishing a broader focus and contingent of dedicated and trained personnel whose primary mission includes active engagement in cyber security diplomacy or trade negotiations.

Indeed, the subject of cyber diplomacy exceeds just the rules of engagement and constraining behaviors. It also concerns promoting trade through the free, cross-border exchange of information, goods, services, and capital – especially within the EU. Balancing economic prosperity and national security requires establishing a refined diplomatic corps and increasing the country's regional leadership to realize its vision and goals. Slovakia has an important opportunity as it leads the OSCE on cyber issues.

## 7. DEFENSE AND CRISIS RESPONSE

In the late 2000s (after the cyber incidents in Estonia and then Georgia), the use of military grade weapons against national critical infrastructures and the use of cyber in military operations catalyzed Slovakia's MoD to undertake initiatives to start training and equipping its Armed Forces and to align domestic efforts to NATO's cyber defense requirements.

The 2005 National Security Strategy of the Slovak Republic neither mentioned information security nor cyber security. However, starting with the 2013 White Paper on Defense of the Slovak Republic, the country recognized the need to take necessary steps to prevent threats that could cause significant or irrecoverable damage to Slovakia and that could undermine the credibility of the state.[135] Also in 2013, the Slovak Military Defense Intelligence (VOS) and Military Intelligence Service (VSS) were merged into one service called Military Intelligence (VS) within the MoD. The Military Intelligence is responsible for "acquiring, collecting, and analyzing information significant for securing defense and defense capabilities of the Slovak Republic," including activities and threats in cyberspace. Its primary mission in this domain is to "protect the defense and critical infrastructure and information systems essential to secure the state functioning."[136]

The 2016 White Paper on Defense acknowledged that cyberspace was now the fifth domain of warfare, in line with the declaration made by NATO member states at the 2016 Warsaw Summit. It also recognized the influence that asymmetric security threats, including cyber attacks and hybrid warfare, could have in the future, and called for the Military Intelligence to strengthen and develop capabilities in cyber security.[137] It placed emphasis on the protection of communications and information technology infrastructures within the MoD and on ensuring support for the Slovak Armed Forces (AF SR) in cyberspace.[138]

*The Cyber Defense Center was created in 2018 as a special department within the Military Intelligence, tasked with the cyber defense of national critical assets.*

In response to this call and the 2015 reorganization of the government entities responsible for cyber security, the Cyber Defense Center was created in 2018 (based on the Cybersecurity Act) as a special department within the Military Intelligence, tasked with the cyber defense of national critical assets. The center collects, aggregates, analyzes, and evaluates information critical for cyber defense, informs affected parties about existing and potential threats, and suggests appropriate measures.[139] In addition, the center hosts the military computer security and incident response team (CSIRT.MIL.SK). CSIRT.MIL.SK oversees monitored infrastructures, provides early detection of systems vulnerabilities and malicious activities on the network, responds to serious cyber security incidents of national importance (like the 2018 attack on the Ministry of Foreign Affairs), and offers education and awareness programs for its constituency. In February 2018, CSIRT.MIL.SK was accred-

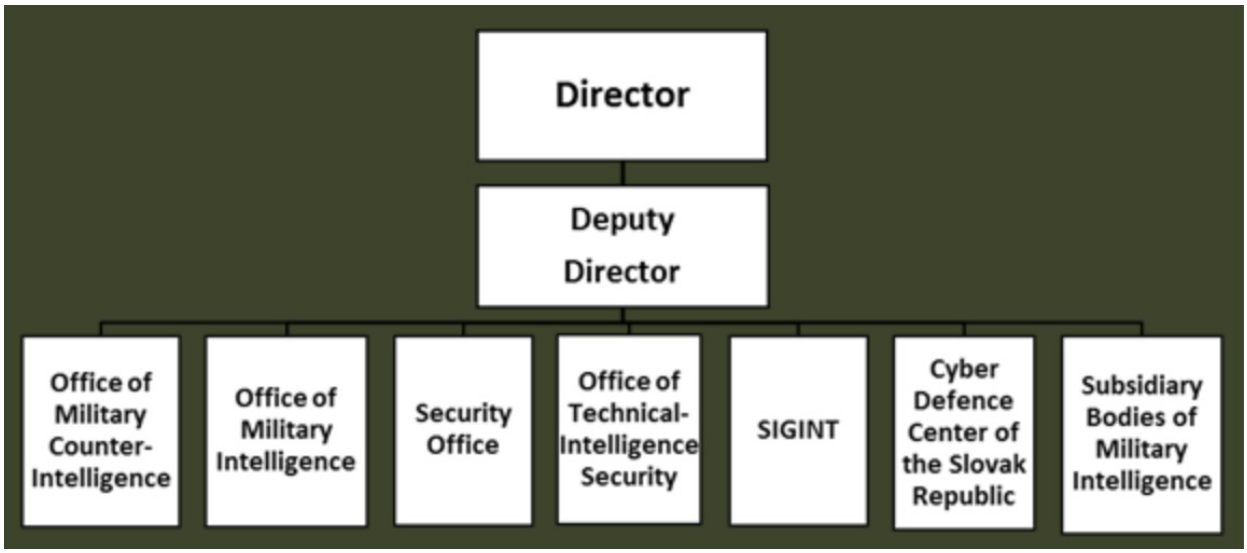



*Figure 3: Organizational structure of the Slovak Military Intelligence, http://csirt.mil.sk/75689.*

ited by the Trusted Introducer certification authority, and became a full member of the international Task Force of Computer Security Incident Response Teams (TF-CSIRT).[140]

The 2018 Cybersecurity Act codified the role and responsibilities of the Cyber Defense Center (Article 35). It also gave it the authority to "require compliance from the owners and operators of facilities of special importance and critical infrastructure elements, as well as information to the extent necessary to ensure the cyber defense of the country."[141] In order to fulfill the tasks assigned to it, the center has direct and full real-time electronic access to the Cybersecurity Single Information System. In the event of a serious cyber security incident that "exceeds the specified degree of severity" or that involves a case of "cybernetic terrorism," NBU must inform the Military Intelligence and provide all necessary information "to ensure cyber defense."[142] The Military Intelligence will then perform its incident response tasks through the Cyber Defense Center and CSIRT.MIL.SK.

*The Cyber Defense Center has direct and full real-time electronic access to the Cybersecurity Single Information System to ensure the cyber defense of the country when needed.*

The 2016 White Paper also recognized the importance of improving the training of the Slovak Armed Forces. The Armed Forces Academy of Milan Rastislav Štefánik, for example, is investing in the long-term development of university-level education and vocational training and exercises in line with the AF

SR requirements, including the training of professional soldiers in the area of cyber security. The Paper also called for training of commanders focused on the ability to plan high-intensity joint operations to defend the homeland and/or provide collective defense to NATO allies in a complex operational environment, including hybrid, cybernetic, and terrorist threats.

Slovakia regularly participates in cyber training and exercises with international partners, including the CCD CoE-led Locked Shields exercise – won by Slovakia in 2016 – and the NATO-led Cyber Coalition exercise, in order to test its abilities and reactions to cyber attacks and demonstrate cooperation through information exchange and assistance.[143] The country also contributes to the EU Cyber Europe and CyberSOPEX exercises, both organized by ENISA, and participated in the 2018 SecOps Europe exercise in Budapest. In 2018, the Slovak team that participated in these exercises consisted of representatives from the NBU, the national SK-CERT, the MoD (only in the Locked Shields exercise), and the government CSIRT.SK unit.

Moreover, the government has held at least three national-level exercises in 2011, 2012, and 2013 to demonstrate (technical) national cyber defense readiness. The Slovak Information Security Exercises (SISE) were aimed at CII protection. The primary goal of SISE 2012, for example, was to test the technical response of participating institutions to large-scale ICT incidents, including data exfiltrations, DDoS attacks, and ripple effects on the provision of public services.[144] The 2013 exercise tested the security incident and technical security processes within participating organizations, including their ability to mitigate incidents and identification of employees' security awareness levels (e.g., against phishing attacks and online scams). The Ministry of the Interior, the Prime Minister's Office, the Telecommunications Office, and the Ministry of Finance were all actively involved in the 2013 exercise.

In 2017, the Slovak government published a new draft national security strategy, which recognizes the ubiquity of cyber attacks and argues that the consequences of such attacks can reach the level of a conventional armed attack. The document also reiterates NATO's definition of cyberspace as a new domain of operations and stresses that collective defense in this sphere is critical.[145] The draft strategy states that its "aim is to develop cyber defense and create a protected cyberspace for Slovakia." It also affirms that "the Slovak Republic will create an institutional and legal framework aimed at enhancing the security and resilience of cyberspace. The result will be a comprehensive system of cyber security, including international cooperation, cooperation with the private sector and the academic community."[146]

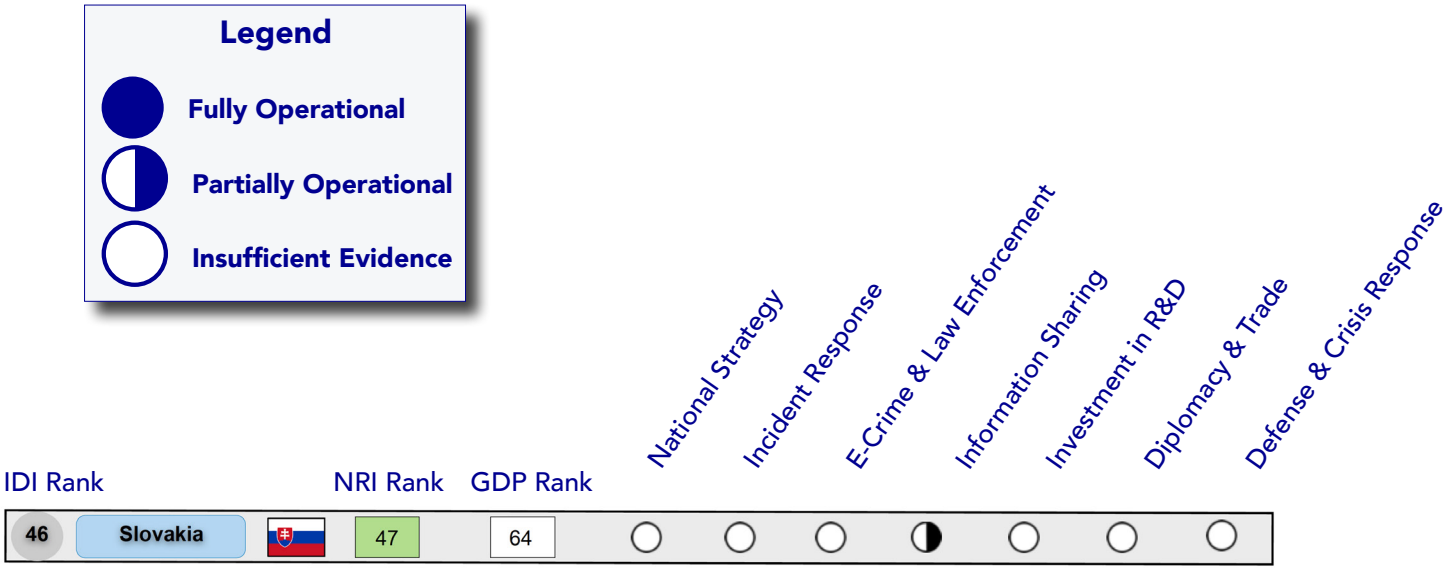
While there is a clear emphasis on scaling cyber defense systems in Slovakia, exact allocations of funding are unclear. In 2017, the Military Intelligence department spent €54 million (~$60.6 million) for all its activities.[147] MoD's overall expenditures in 2018 amounted to €1 billion (~$1.1 billion), but the specific funding for military intelligence activities and the Cyber Defense Center is not publicly available.[148]

## CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, Slovakia is still in the early stages of developing a path toward cyber resilience and cyber readiness, and is currently partially operational only in one of the seven CRI essential elements.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As Slovakia continues to develop and update its economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path toward a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: *http://www.potomacinstitute.org/academic-centers/cyber-readiness-index*.



## ENDNOTES


1. Česká pošta, "Czechoslovak and Czech Post's history," https://www.ceskaposta.cz/en/o-ceske-poste/historie.

2. Česky Telecom, "History," http://www.fundinguniverse.com/company-histories/cesky-telecom-a-s-history/.

3. Stefan Kohut, "15 years of SANET Association," http://www.sanet.sk/buletin_sanet_en.pdf.

4. The group of researchers at the Institute of Applied Cybernetics (UAK) in Bratislava who developed the first intra-network used SMEP computers (systém malých elektronických or small electronic computer systems).

5. Jaroslav Bobovsky, "History of the Internet in Slovakia," http://kit2015.aos.sk/proceedings/pdf/beset.pdf.

6. Most historians refer to this period as the Velvet Revolution, maintaining the Czech's nomenclature for this event.

7. "History of the Internet," 1.

8. Karol Fabian, "SANET Network: Evolution and Services," https://www.researchgate.net/publication/303665227_SANET_Network_Evolution_and_Services_Proc_INET'93_San_Francisco_CA_USA_1993.

9. "History of the Internet in Slovakia," 5-6.

10. Karol Fabian, "Distribuovane mikropocitacove systemy a pociatky slovenskeho Internetu v UTK SAV a UAKOM SAV."

11. "History of the Internet in Slovakia."

12. "Slovakia's Dzurinda Gets a Second Chance as Prime Minister," EURACTIV, 7 October 2002, https://www.euractiv.com/section/elections/opinion/slovakia-s-dzurinda-gets-a-second-chance-as-prime-minister/838279/.

13. SANET, "About the SANET.2 project, http://www.sanet.sk/en/oprojekte.shtm; Government of the Slovak Republic, "Resolution n° 383/2001."

14. World Bank, "Individuals using the Internet (% of population)," 2000, 2010, and 2017, https://data.worldbank.org/indicator/IT.NET.USER.ZS.

15. European Commission, "Europe's Digital Progress Report: Slovakia," (2017): 3, https://ec.europa.eu/digital-single-market/en/scoreboard/slovakia, and World Bank, "Fixed broadband subscriptions (per 100 people)," 2017, https://data.worldbank.org/indicator/IT.NET.BBND.P2?end=2017&start=1998.

16. Eurostat, "Percentage of the ICT Sector on GDP," https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00074&plugin=1.

17. Lea Hriciková and Kadri Kaska, "National Cyber Security Organizations: Slovakia," NATO Cooperative Cyber Defence Centre of Excellence, (2015): 5.

18. Slovak Republic, Ministry of Finance, "Information Society Strategy for 2009–2013," (2009): 6-16 http://www.informatizacia.sk/ext_dok-information-society-startegy-for-2009_2013/6497.

19. European Migration Network, "Ad-Hoc Query on Identity Documents issued to EU Member States citizens," November 2009, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/residence/161._emn_ad-hoc_query_identity_documents_issued_to_eu_ms_citizens_2oct2009_wider_dissemination_en.pdf, and European Commission, "Operational Programme 'Information Society'," (2007), https://ec.europa.eu/regional_policy/en/atlas/programmes/2007-2013/slovakia/operational-programme-information-society.

20. Deputy Prime Minister's Office website, 11 March 2019, https://www.vicepremier.gov.sk/aktuality/informatizacia/rasi-mame-pripravenu-strategiu-digitalnej-transformacie-slovenska/index.html.

21. European Commission, "Europe's Digital Progress Report: Slovakia," 1.

22. Melissa Hathaway, "Toward a Closer Digital Alliance," SAIS Review of International Affairs, Johns Hopkins University Press, Volume 36, n. 2, (Summer-Fall 2016): 57-67.

23. "The National Concept of eGovernment," 53.

24. NATO, "Cyber Defense," https://www.nato.int/cps/en/natohq/topics_78170.htm.

25. European Commission, "EU Cyber Security strategy: An open, safe and secure Cyberspace," February 2013, https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en.

26. National Security Authority, "Cyber Security Concept of the Slovak Republic for 2015-2020," (2015): 9, 11, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1.

27. National Security Authority, "Statute of the National Security Authority. Resolution No. 92/2016," 2 March 2016, https://www.nbu.gov.sk/urad/pravne-predpisy/statut/index.html; Jaroslaw Adamowski, "Slovak Finance Ministry drafts country's first cyber-security law," SC Magazine, 18 October 2016, https://www.scmagazineuk.com/slovak-finance-ministry-drafts-countrys-first-cyber-security-law/article/1476115.

28. National Council of the Slovak Republic, "Act on Cybersecurity and on Amendments and Supplements to certain Acts," January 2018, http://www.nbu.gov.sk/wp-content/uploads/legislativa/EN/Act_Cybersecurity.pdf.

29. Tom Watts, "Which EU Country is most vulnerable to cybercrime," November 2018, https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/.

30. "Cyber-attack hits Slovak Ministry of Foreign Affairs," 18 October 2018, Remix, https://rmx.news/slovakia/cyber-attack-hits-slovak-ministry-foreign-affairs.

31. Ibid, 9, 72.

32. Jurika Novak et al., "The rise of Digital Challengers: Perspective on Slovakia," McKinsey, (November 2018): 4, https://digitalchallengers.mckinsey.com/files/The-rise-of-Digital-Challengers_Perspective-on-SK.pdf.

33. Peter Adamovsky, "Pellegrini: Slovakia can become a testing space for bold ideas," The Slovak Spectator, 21 December 2017, https://spectator.sme.sk/c/20721988/digital-transformation-offers-the-chance-to-be-a-leader.html.

34. European Parliament, "The Lisbon Strategy 2000-2010," http://www.europarl.europa.eu/document/activities/cont/201107/20110718ATT24270/20110718ATT24270EN.pdf.

35. In 2000, the European Commission launched its first "eEurope – An Information Society for All" strategy, which proposed the ambitious goals of turning the EU into the most competitive and dynamic knowledge-based economy by 2010, and "bringing every citizen, home and school, every business and administration, into the digital age and online" while guaranteeing that "the whole process is socially inclusive, builds consumer trust and strengthens social cohesion." For more, see: "eEurope – An Information Society for All," EUR-Lex, (2000), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24221.

36. "National Cyber Security Organizations: Slovakia," 5.

37. Slovak Republic, Ministry of Finance, "Information Society Strategy for 2009–2013," (2009): 6-16.

38. Government Resolution No. 139/2013 (20 March 2013), Act No. 575/2001 Coll. on the organization of the government activities and the organization of central government administration, and European Commission position paper, http://www.nsrr.sk/sk/programove-obdobie-2014---2020/pozicny-dokument-europskej- komisie-k-partnerskej-dohode-a-programom-sr-na-roky-2014---2020/.

39. The two documents were approved by Government Resolution No. 522/2001 and by Government Resolution No. 43/2004 on 21 January 2004, 4-6.

40. Slovak Republic, Ministry of Finance, "Information Society Strategy for 2009–2013," (2009): 6-16.

41. Slovak Republic, Ministry of Finance, "The National Concept of eGovernment," (February 2008).

42. Slovak Republic, Ministry of Finance, "The National Strategy of the Slovak Republic for Digital Integration," (November 2008): 3-4.

43. Office of the Government of the Slovak Republic, "Operational Programme Informatisation of Society," Version4.0, (2012), http://www.opis.gov.sk/data/files/2448_8949.pdf.

44. Slovak Republic, Ministry of Finance, "Strategic Document for Digital Growth and Next Generation Access Infrastructure (2014-2020)," http://www.informatizacia.sk/index/open_file.php?ext_dok=16622.

45. Ibid, 3.

46. Ibid, 9, 72.

47. Ibid, 74, 111-112.

48. Deputy Prime Minister's Office website, 11 March 2019, https://www.vicepremier.gov.sk/aktuality/informatizacia/rasi-mame-pripravenu-strategiu-digitalnej-transformacie-slovenska/index.html.

49. Slovak Republic, Ministry of Finance, "National Strategy for Information Security 2009-2013," (2008): 6, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Slovakia_National_Strategy_for_ISEC.pdf.

50. National Security Authority, "Authority."

51. "National Strategy for Information Security," 8; and Slovak Republic, Ministry of Defense, "The White Paper on Defence of the Slovak Republic," (2013): 49, 127, http://www.mosr.sk/data/WP2013.pdf.

52. "National Strategy for Information Security," 6, 11-12.

53. "Statute of the National Security Authority," (2016).

54. The Cybersecurity Committee is a permanent working body of the Security Council that advises and recommends policy measures for protection in cyberspace, and the head of NBU is also on the committee.

55. National Security Authority, "Cyber Security Concept of the Slovak Republic for 2015-2020," 8.

56. Ibid, 9.

57. National Security Authority, "Cyber Security Concept of the Slovak Republic for 2015-2020," and "Action Plan of Implementation of Cyber Security Concept of the Slovak Republic for years 2015-2020."

58. "Action Plan of Implementation of Cyber Security Concept of the Slovak Republic for years 2015-2020," 3, 17.

59. "Cyber Security Concept of the Slovak Republic for 2015-2020," 17.

60. "Action Plan of Implementation of Cyber Security Concept of the Slovak Republic for years 2015-2020," 4, 34.

61. National Security Authority, http://www.nbu.gov.sk/en/authority/index.html.

62. Ibid, 17.

63. "Cyber Security Concept of the Slovak Republic for 2015-2020," 5.

64. "Cybersecurity Act 2018," Articles 4 and 5.

65. National Security Authority, "Authority," http://www.nbu.gov.sk/en/authority/index.html, and "Cybersecurity Act 2018," Article 5.

66. Role and scope of the Cybersecurity Committee within the Security Council of the Slovak Republic, https://www.vlada.gov.sk/data/files/6351_rp-vyborkb.pdf.

67. "Cybersecurity Act 2018," Article 5.

68. Cybersecurity Single Information System, http://www.nbu.gov.sk/en/cyber-security/cybersecurity-single-information-system/index.html, and "Cybersecurity Act 2018," Article 8.

69. "Which EU Country is most vulnerable to cybercrime."

70. SK-CERT, "Detected Events," https://www.sk-cert.sk/en/statistics/detected-events/index.html.

71. SK-CERT, "RFC2350 – CSIRT Description for SK-CERT, National CSIRT of the Slovak Republic," January 2016, https://www.sk-cert.sk/en/about-us/rfc2350/index.html.

72. SK-CERT, "About Us," https://www.sk-cert.sk/en/about-us/index.html.

73. Ibid.

74. Ibid.

75. NIS fully transposed in Slovakia - https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-slovakia, and Service providers under the Cybersecurity Act 2018, https://www.slov-lex.sk/pravne-predpisy/prilohy/SK/ZZ/2018/164/20180615_4883164-2.pdf.

76. "Cybersecurity Act 2018," Articles 24 and 25.

77. Cybersecurity Single Information System, http://www.nbu.gov.sk/en/cyber-security/cybersecurity-single-information-system/index.html, and "Cybersecurity Act 2018," Article 8.

78. Ibid, Article 11 & 15.

79. Office of the Deputy Prime Minister for Investments and Informatization, "Kybernetické hrozby sú reálne, Slovensko budú chrániť 4 jednotky CSIRT," 21 September 2018, https://www.vicepremier.gov.sk/aktuality/informatizacia/kyberneticke-hrozby-su-realne-slovensko-budu-chranit-4-jednotky-csirt/.

80. Interview with Deputy Prime Minister's Office representative, 12 March 2019.

81. Office of Personal Data Protection, https://dataprotection.gov.sk/uoou/en/content/procedure-personal-data-protection.

82. CSIRT.SK, "National level cyber exercises," https://www.csirt.gov.sk/news-7f7.html?id=66.

83. SK-CERT, "About us," https://www.sk-cert.sk/en/about-us/index.html; NBU, "The Slovak Republic Again This Year Participated in the International Exercise of NATO Cyber Defence – Cyber Coalition 2018," December 2018, http://www.nbu.gov.sk/news/the-slovak-republic-again-this-year-participated-in-the-international-exercise-of-nato-cyber-defence-cyber-coalition-2018/index.html.

84. Council of Europe, "Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of European policies on prevention and combating Cybercrime' - Report on Slovakia," 22 September 2015, http://data.consilium.europa.eu/doc/document/ST-9761-2015-REV-1-DCL-1/en/pdf.

85. "Which EU Country Is Most Vulnerable to Cybercrime?" 2018.

86. "Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of European policies on prevention and combating Cybercrime' - Report on Slovakia," 11.

87. Ibid, 5 and 19.

88. Ministry of Interior, "Data Subjects' Rights," https://www.minv.sk/?Data-Subjects-Rights.

89. Rebecca James, "Mandatory Data Retention in Slovakia," Privacy Sniffs, 24 September 2018, https://privacysniffs.com/data-retention-law/slovakia/.

90. European Commission, "ILLEGAL USE OF INTERNET TARGETED CALL FOR PROPOSALS," 2013, https://ec.europa.eu/home-affairs/sites/home-affairs/files/financing/fundings/pdf/isec/isec-grants-awarded-2013_en.pdf.

91. "Action Plan of Implementation of Cyber Security Concept of the Slovak Republic for years 2015-2020," June 2016, http://www.nbu.gov.sk/wp-content/uploads/cyber-security/Action-Plan-for-the-Implementation-of-the-Cyber-Security-Concept-of-the-Slovak-Republic-for-2015-2020-_3_.pdf.

92. E-Slovensko, https://diaspora-engagement.eu/org/eslovensko/.

93. University College Dublin Centre for Cybersecurity & Cybercrime Investigation, "Cyber Crime Training (Slovakia)," 2014, https://www.ucd.ie/cci/projects/current_projects/cyber_crime_training_slovakia.html.

94. "Cyber Security Concept of the Slovak Republic for 2015-2020," 17.

95. "Cybersecurity Act 2018," Article 8.

96. Ibid.

97. NIS fully transposed in Slovakia - https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-slovakia, and Service providers under the Cybersecurity Act 2018, https://www.slov-lex.sk/pravne-predpisy/prilohy/SK/ZZ/2018/164/20180615_4883164-2.pdf.

98. "Cyber Security Concept of the Slovak Republic for 2015-2020," 10.

99. Ibid, 29.

100. "Action Plan of Implementation of Cyber Security Concept of the Slovak Republic for years 2015-2020," (June 2016), areas 7.1 and 7.2.

101. Peter Adamovsky, "How does Slovakia support innovations?" The Slovak Spectator, 15 November 2018, https://spectator.sme.sk/c/20961939/how-does-slovakia-support-innovations.html.

102. OECD, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm.

103. OECD, "Highlights from the OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation: Slovak Republic," (November 2017): 1, http://www.oecd.org/slovakia/sti-scoreboard-2017-slovak-republic.pdf.

104. Research Agency of the Ministry of Education, http://www.vyskumnaagentura.sk/en/opvai.

105. "How does Slovakia support innovations?".

106. European Commission, Scientific Grant Agency VEGA, https://rio.jrc.ec.europa.eu/en/organisations/scientific-grant-agency-vega.

107. Slovak Statistical Office 2017, and Vladislava Gubalova, "Tackling Unemployment by Upgrading People's Skills: New Skills for New Jobs and the EU Support," GLOBSEC Policy Institute, 1 December 2017, https://www.globsec.org/tackling-unemployment-upgrading-peoples-skills-new-skills-new-jobs-eu-support/.

108. European Commission, "Europe's Digital Progress Report: Slovakia," 8.

109. Slovak Industry Initiative, https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Slovakia_FINAL.pdf.

110. GLOBSEC round-table, https://www.globsec.org/news/investing-in-human-resources-emerges-as-top-priority-at-globsec-chateau-bela-round-table-on-cybersecurity-in-slovakia/.

111. Ministry of Finance, spending reviews https://www.finance.gov.sk/en/finance/value-money/spending-reviews/.

112. Slovak Technical University, https://www.stuba.sk/buxus/generate_page.php?page_id=10887.

113. IT Academy - Education for the 21st Century, September 2016, http://itakademia.sk/zakladne-informacie/.

114. ESET Research Center, https://www.stuba.sk/english/science-and-research/other-research-centres-and-laboratories/eset-research-centre.html?page_id=11886.

115. Košice IT Valley, http://www.kosiceit-valley.sk/en/about-kosice-it-valley/ and http://www.kosiceitvalley.sk/inovacie/.

116. European Cyber Security Organisation, https://ecs-org.eu/activities.

117. European Commission, "Digital Coalition launched in Slovakia," November 2017, https://ec.europa.eu/digital-single-market/en/news/digital-coalition-launched-slovakia.

118. IT Association of Slovakia, "Digitálna koalícia na výročnom zasadnutí ocenila najaktívnejších členov za rok 2018," 14 February 2018, https://itas.sk/digitalna-koalicia-na-vyrocnom-zasadnuti-ocenila-najaktivnejsich-clenov-za-rok-2018/.

119. News report from TASR https://newsnow.tasr.sk/economy/it-digital-coalition-swells-by-16-new-members-to-37/.

120. Digital Coalition, "IT Fitness test 2018: prekročili sme hranicu 30 000 otestovaných!," https://digitalna-koalicia.sk/fitness-test-pred-ukoncenim-certifikacnej-casti-testu-29-500-otestovanych/.

121. Digital Coalition website https://itas.sk/vysledky-it-fitness-testu-2018-ziaci-maju-problemy-s-kybernetickou-bezpecnostou/.

122. Ibid.

123. Remarks by Deputy Prime Minister for Investment and Informatization Richard Rasi, American Chamber of Commerce, Slovakia, 15 May 2018, http://www.amcham.sk/download.pl?hash=A9wvUoiwiXim5dsUj4QLNy9Digrr1lvl&ID=4983.

124. Touch IT article dated 10 February 2019 https://touchit.sk/vicepremier-rasi-podpisal-memorandum-o-spolupraci-v-oblasti-umelej-inteligencie-a-smart-cities-so-spojenymi-arabskymi-emiratmi/217962.

125. Deputy Prime Minister's Office for Investment and Informatization, 28 August 2017, https://www.vicepremier.gov.sk/aktuality/regionalny-rozvoj/smart-cities-chcete-hodnotit-projekty-za-milion/index.html.

126. Deputy Prime Minister's Office for Investment and Informatization, 11 March 2019, https://www.vicepremier.gov.sk/aktuality/informatizacia/rasi-mame-pripravenu-strategiu-digitalnej-transformacie-slovenska/index.html.

127. "Cyber Security Concept of the Slovak Republic for 2015-2020," 10 and 18; and "Strategic Document for Digital Growth and Next Generation Access Infrastructure (2014-2020)," 86 and 112.

128. "Cybersecurity Act 2018," Article 5(h).

129. ENISA, "NIS Platform," https://resilience.enisa.europa.eu/nis-platform.

130. OSCE, "Programme of the Slovak OSCE Chairmanship 2019," https://www.osce.org/chairmanship/408353?download=true.

131. "Slovakia and France to Deepen Cooperation in Field of Cyber Threats," News Now, 16 October 2018, https://newsnow.tasr.sk/foreign/slovakia-and-france-to-deepen-cooperation-in-field-of-cyber-threats/.

132. NBU, "The National Security Authority shared its experience with Azerbaijan on cybersecurity," November 2018, http://www.nbu.gov.sk/news/the-national-security-authority-shared-its-experience-with-azerbaijan-on-cybersecurity/index.html.

133. French Government, "Paris Call for Trust and Security in Cyberspace," 12 November 2018, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf?wpisrc=nl_cybersecurity202&wpmm=1.

134. Tatiana Jancarikova, "Slovakia has no evidence of Huawei security threat - prime minister," Reuters, 30 January 2019, https://www.reuters.com/article/us-usa-china-huawei-slovakia/slovakia-has-no-evidence-of-huawei-security-threat-prime-minister-idUSKCN1PO1TO.

135. "National Strategy for Information Security," 8; and Slovak Republic, Ministry of Defense, "The White Paper on Defense of the Slovak Republic," (2013): 49, 127, http://www.mosr.sk/data/WP2013.pdf.

136. Military Intelligence, "About us," http://vs.mosr.sk/o-nas/#poslanie.

137. Slovak Republic, Ministry of Defense, "White Paper on the Defense of the Slovak Republic," (2016), https://www.mosr.sk/data/WPDSR2016_LQ.pdf.

138. Ibid.

139. Cyber Defense Center of the Slovak Republic, "About Us," http://csirt.mil.sk/75689/?mne=3146.

140. Cyber Defense Center of the Slovak Republic, "CSIRT.MIL.SK," http://csirt.mil.sk/75688/?mne=3149.

141. "Cybersecurity Act 2018," Article 35.

142. Military Intelligence, http://vs.mosr.sk/nova-legislativa-pre-oblast-kybernetickej-obrany/eng.

143. "Cyber Security Concept of the Slovak Republic for 2015-2020," 9.

144. National exercise on critical information infrastructure protection SISE 2012, November 2012, https://www.csirt.gov.sk/aktualne-7d7.html?id=53.

145. "Draft Security Strategy of the Slovak Republic," (2017), https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2017-627.

146. Ibid.

147. Military Intelligence's budget for 2017, http://vs.mosr.sk/sprava-o-cinnosti-vs-2017/.

148. Ministry of Defense's budget for 2018, https://www.mod.gov.sk/data/files/3574.pdf.

# ABOUT THE AUTHORS

**Melissa Hathaway** is a leading expert in cyberspace policy and cyber security. She served in two US presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. Today, she is a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies. She is also a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs, a Distinguished Fellow at the Centre for International Governance Innovation in Canada, a non-resident Research Fellow at the Kosciuszko Institute in Poland, and she is President of Hathaway Global Strategies LLC, her own consultancy. Melissa developed a unique methodology for evaluating and measuring national levels of preparedness for certain cyber security risks, known as the Cyber Readiness Index (CRI). The CRI methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is being applied to 125 countries. The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, Saudi Arabia, the United Kingdom, and the United States can be found at the following link: *http://www.potomacinstitute.org/academic-centers/cyber-readiness-index*. Having served on the board of directors for two public companies and three non-profit organizations, and as a strategic advisor to a number of public and private companies, Melissa brings a unique combination of policy and technical expertise, as well as board room experience to help others better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field. She publishes regularly on cyber security matters affecting companies and countries. Most of her articles can be found at the following website: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

**Francesca Spidalieri** is the co-principal investigator on the Cyber Readiness Index Project at the Potomac Institute for Policy Studies. She is also an Associate for Hathaway Global Strategies LLC, and serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, as a cyber security subject-matter expert for the UN International Telecommunications Union (ITU), as a Distinguished Fellow at the Ponemon Institute, and as a non-resident Research Fellow at the Kosciuszko Institute in Poland. Her academic research and publications focus on cyber leadership development, cyber risk management, comparative organization analysis, and cyber security workforce development. In 2015, she published a report, entitled State of the States on Cybersecurity, that applied the Cyber Readiness Index 1.0 at the US state level. All her additional studies and academic articles can be found at the following link: *http://pellcenter.org/cyber-leadership/*.

**Anushka Kaushik** is a research fellow at GLOBSEC, a think-tank based in Bratislava, Slovakia, where she drives the organisation's research efforts in cybersecurity policy. She has published papers on attribution of cyber attacks and policy implications of end-to-end encryption. She has previously worked on data protection policies and internet governance at the International Chamber of Commerce and was a Research Associate at the Centre des Recherches Internationales (CERI). While at the Indian Ministry of Electronics and Information Technologies, her research activities were centered on national e-governance advocacy plans.

*For more information or to provide data to the CRI 2.0 methodology, please contact:*

CyberReadinessIndex2.0@potomacinstitute.org

*The CRI 2.0 methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is currently being applied to 125 countries.*

*The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, Saudi Arabia, the United Kingdom, and the United States can be found at the following link:*

http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org