FOREWORD

CYBERSECURITY A Challenge and a Responsibility for Romania

Alexandru PETRESCU
Minister of Communications and Information Society

Cyber, as a word and as a prefix appended to many concepts, has permanently entered our vocabulary, our public discourse and our policies. It reflects the reality of a society changing under the impetus of the rapid adoption of Information Technology.

By "society", I mean not only the lives of individuals, their relationships and their governing bodies, but also the fundamental substrate of technology and organizations that allow modern societies to function.

The Romanian legislation and the European Union call these critical infrastructures but, however they are termed and governed, they are nevertheless vital. The list is very long and includes finance, agriculture, food processing, transport, energy generation, energy transport, healthcare, education and many more, not just in the sense of industry, but in all aspects, including regulatory and security.

CYBER SECURITY AND CYBER RESPONSIBILITY

Cyber is for us the encapsulation of a challenge – the challenge of development. For Romania, to continue its economic growth and development, quantitatively and qualitatively, it will require the transformation of industry, society and government in ways which enable higher productivity, the creation of value, innovation, efficiency and security. These transformations, both of existing infrastructures and the development of new ones, are mediated by the digital sphere. There is no way around this, no alternative techniques or technologies.

Cyber without growth may be possible, but growth will not be possible without cyber, and it will come not as a result of government initiative, but organically, through companies, communities and individuals adopting and adapting tools that fit their needs.

Government itself must adopt and adapt these tools to provide the citizen, the consumer and the investor with the experience that they have come to expect from a modern and advanced society – digital services, rapid resolution of requests, lower bureaucratic overhead and more value created.

Therefore, I believe that the digitalization and, by extension, the cyberization of society, in all its facets (civil, economic, governments) is desirable, beneficial and inevitable.

But this does not absolve us of responsibility. Because, with the rapid adoption of cyber-everything, come new challenges, new vulnerabilities and new threats. While I write this from the perspective of a state institution, the bird's eye view I am afforded of the issues facing the cyber transition not just of our country but also of our partners in the EU and NATO, have convinced me that cybersecurity must become a responsibility for individuals, for civil society, for academia and for companies, and not just for governments.

Centralized efforts at improving cybersecurity are vitally necessary and can provide the crucial scaffolding of societal cybersecurity efforts, but they are never sufficient in themselves.

The permeation of cyber throughout our societies has transformed the users into principal agents of their own protection and that of others, and their security culture must inform tools, methods and attitudes with respect to security.

At the same time, the variety of infrastructures for which cyber provides command, control and coordination capabilities is so great that, in addition to the skillsets for defending any cyber system, there is a vast amount of necessary specific knowledge regarding the individual systems and sectors that have to be defended, making centralized safety/security/defense near impossible by itself.

Neither does cybersecurity end at the national level, since globalization has resulted in the creation of communication lines and production and supply chains which are global in scope.

Therefore, since geography becomes more or less irrelevant in the cyber sphere, the transmission of risk and the contagion of insecurity find themselves without the traditional barriers of distance and geography.

Cyber governance becomes a global issue and the cybersecurity of myriad entities abroad will impact the security of entities and individuals in Romania, whether we like it or not. As Klaus Schwab, Founder and Chairman of the World Economic Forum wrote, "we must develop a comprehensive and shared view of how technology is affecting our lives and reshaping our economic, social, cultural and human environments".

THE CYBERSECURITY MICROCOSM

The World Economic Forum developed the chart below to illustrate the numerous interdependencies and potentialities of cyber security. We have gone from oral and written communication to analog and then digital communication, not just between people, but between systems. Figure 1 is the least complex but still comprehensive breakdown of the new state of things in cybersecurity that one can produce.

Individual entities have to function as cybersecurity agents within the larger milieu administered by the government, in general, or competent authorities, in particular. These entities may be individuals managing their risk, companies, state institutions and so on and they operate in an environment beset by lone wolves, cybercriminal groups, ideological groups including terrorists and state entities. These aggressors exploit deficiencies in hardware, in software and in user behavior to achieve goals ranging from profit and sowing chaos to tactical advantages in state confrontation.

Figure 2, from the latest edition of the Cyber Handbook compiled by the company Marsh & McLennan, highlight the most important functions of a cybersecurity framework that is as relevant to a company as it is to an individual.

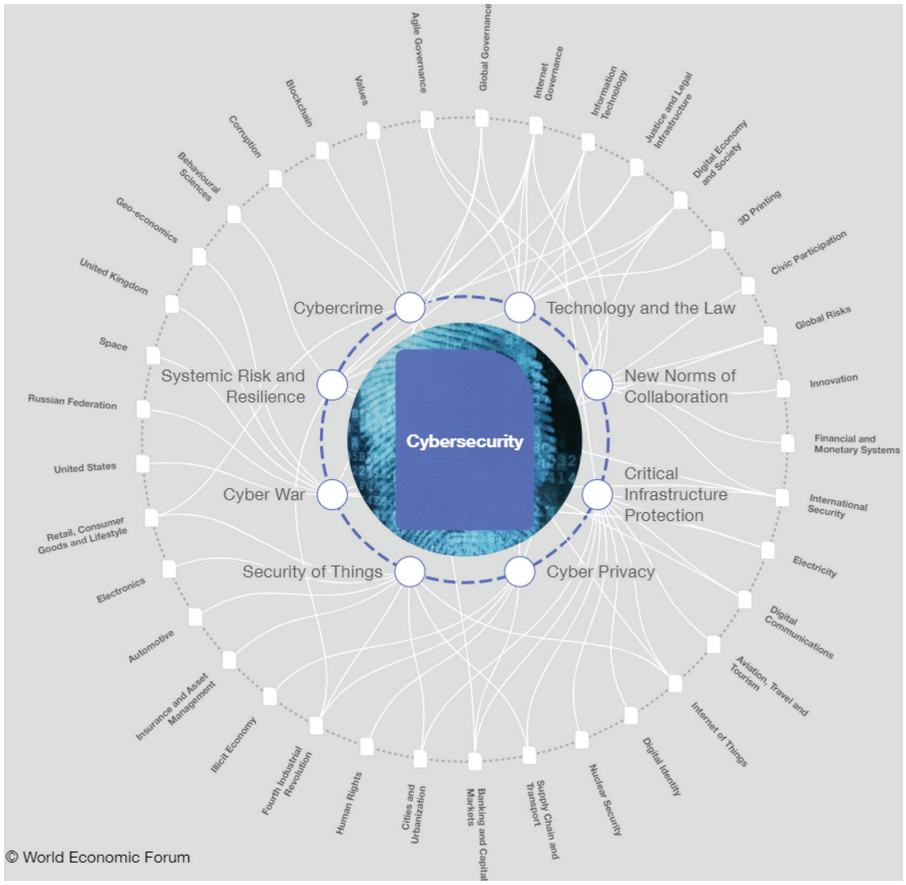

Fig. 1: *The composition of the Cybersecurity issues, according to the World Economic Forum's Center for Cybersecurity*

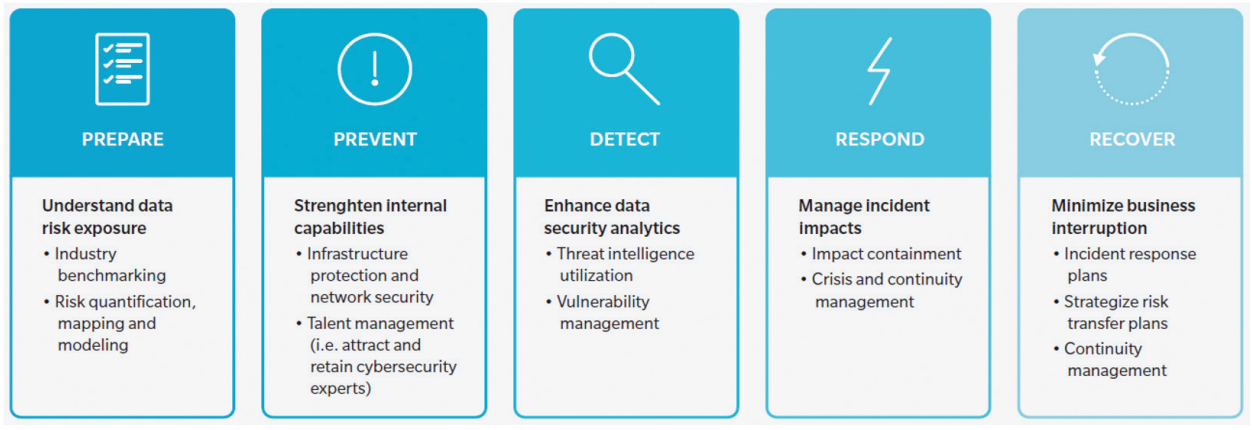

Fig. 2: *Five key functions for cybersecurity framework and key actions (source: Marsh & McLennan Cyber Handbook, 2019)*

And more and more such targets are taking heed of the changing reality of our security environment. The Global Cyber Risk Perception Survey, last published in 2017, asked 1,300 executives in many fields what they considered their interests and means with regards to cybersecurity. 56% of responders declared that cybersecurity risks are a top 5 issue for risk management, while 6% placed it in the first spot. Only 34% placed it outside the top 5 and the number is falling continuously, as the reality of the new and highly publicized threats (data theft, data leaks, ransomware) percolate throughout the C-suite.

The way in which cybersecurity lapses can affect companies is quite varied, as seen in figure 3 below, and the clarification of issues and practices regarding liability for data loss or theft will likely be a main motivator for future investment in cyber security.

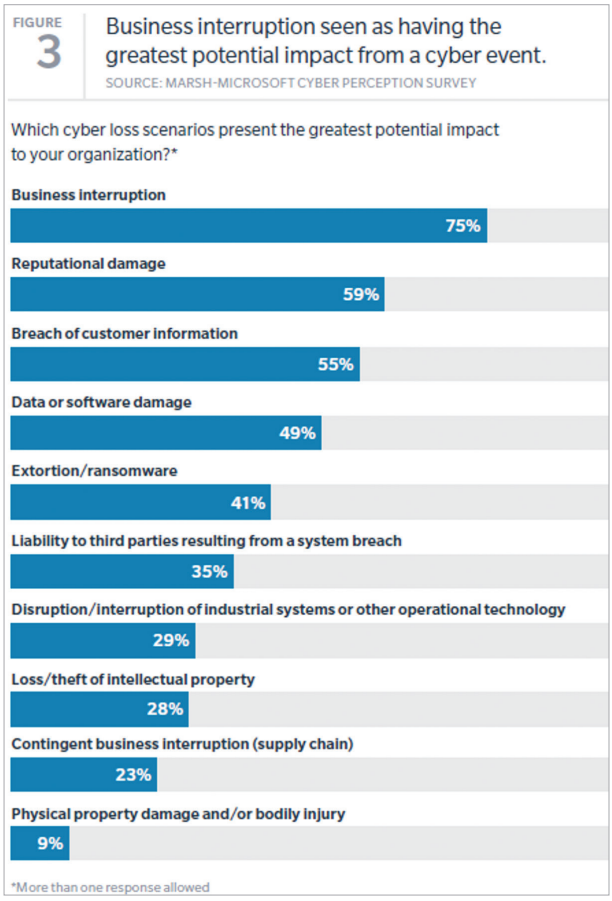

***Figure 3**: Cyber scenarios with the greatest impact on companies (source: Marsh & McLennan, Microsoft, Global Cyber Risk Perception Survey, 2017)*

This is all the more apparent in how they identify their probable attacker:

- 41% are organized crime or hacktivist groups with financial motivation;
- 16% human error resulting in the loss of devices;
- 15% are malicious entities, such as rogue employees or contractors;
- 11% a third-party with access to IT services;
- 11% operational error;
- 6% political or geopolitical threats from state actors or state sponsored groups.

This very interesting perspective shows the extent to which our institutional biases serve to enhance or diminish the perception of certain risks.

The data gathered by the survey skews in favor of the limited perspectives that companies have, as opposed to governments, as well as their limited scope for security processes. For instance, the data highlights the extent to which accidental or random threats factor into the concerns of companies.

As societies become ever more complex and intertwined through transport, finance and information, the growing complexity of the resulting system is, in itself, a source of random occurrences, unanticipated breakdowns and unpredictable behaviors.

At the same time, we notice that the executives focus the least on the threat represented by state actors or state-sponsored groups that seek to disrupt rivals as a means of hybrid warfare.

Such threats are much greater than is apparent here, and involve more than just a few key sectors like public administration, energy and finance. This apparent blindspot can be explained through lack of means and lack of interest to attribute attacks to state actors (possibly for fear of business consequences), but also the limited scope the company has for resolving the issue, as opposed to the lawsuits or criminal proceedings that would deter other actors.

More and more, given the high cost and disruption of a conventional war, we are seeing the use of hybrid warfare, including through cyber-attacks, to weaken and coerce adversaries and rivals. The challenging security environment

of NATO's Eastern Flank also comes with built-in cyber risks, that have materialized before, in Estonia and even in Romania.

CYBERSECURITY FUSION

The complexity of the cybersecurity environment is also leading to a breakdown of the walls between the important categories in which we organize cybersecurity issues.

The distinctions between types of attackers are academic after a certain point and may become intricately linked. For instance, cybercriminals may assist terrorists or take on operations on behalf of a state actor. With tools developed and services rendered by cybercriminal groups, state entities may enhance their plausible deniability and may also achieve a better resourcing of their cyber operations, through outsourcing.

While security is mainly defined as a qualitative issue, there is a definite quantitative dimension to cyber insecurity. The 2019 Cost of Cybercrime report by Accenture highlights this by showing that year on year increases in the cost of cybercrime to countries are in the 10-30% range, with banking, utilities and software companies being the most affected (figure 4).

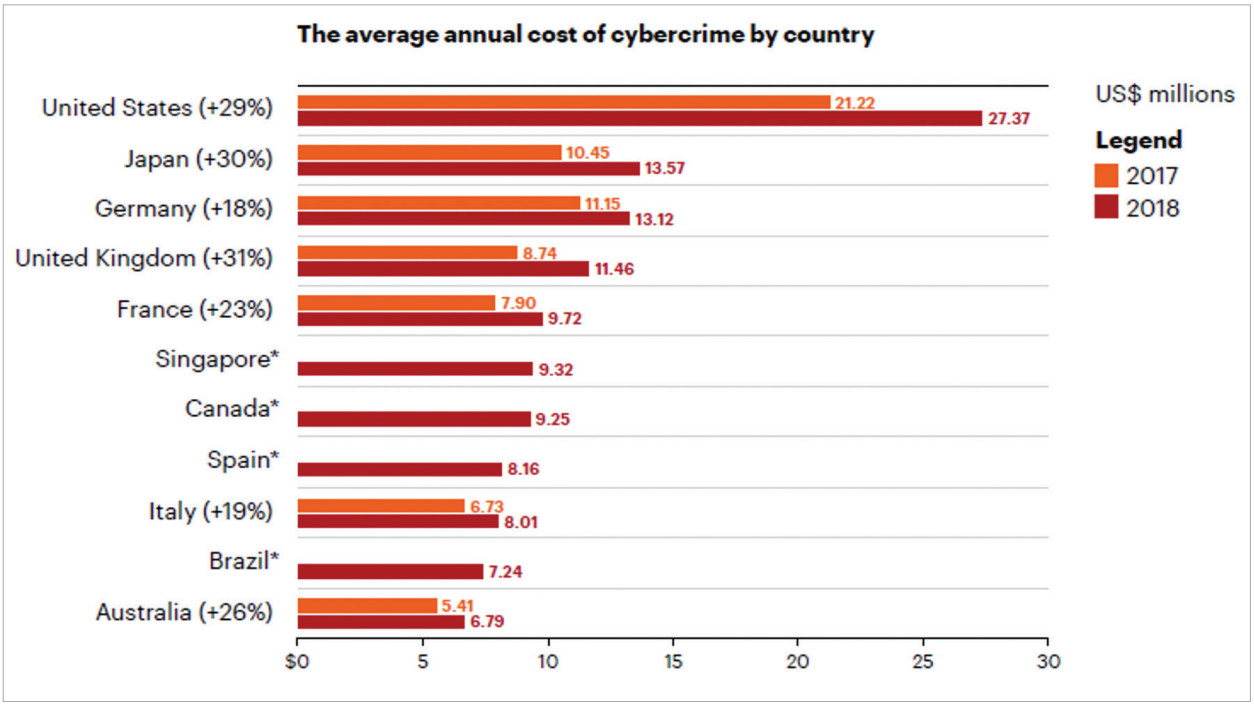

***Figure 4**: 2017 to 2018 increase in the cost of cybercrime for various countries (source: Accenture Cost of Cybercrime Report, 2019)*

Ultimately, the global value at risk from attacks is 5.2 trillion dollars, mostly from direct threats, which is over 6% of global GDP.

Romania is not immune to these trends and might, in fact, be terribly exposed to them. Firstly, the economic and social evolution of the country has always outpaced the ability of the governance mechanisms to keep pace. While there is a high degree of inequality within the population and the economy in terms of digital sophistication and usage, the country with some of the fastest Internet speeds in the world is surely experiencing rapid permeation of cyber capabilities in the lives of individuals and the business of companies and government.

A study by PwC, titled the "Global Economic Crime and Fraud Survey 2018 – A front line perspective on fraud in Romania", highlighted the fact that 65% of Romanian companies surveyed had been victims of cyber-attacks in the prior two years. Half the cases resulted in business disruptions (as opposed to 30%

globally and 36% regionally) and a quarter of the cases resulted in significant economic losses from extortion or asset theft. At 40%, cyber-attacks are close behind consumer fraud in frequency for Romanian companies, but they are first in impact. However, rapid evolution is also in place – 72% of companies reported that they have a cyber-incident response plan in place, double compared to 2016. Another 8% of the companies were undergoing the implementation of the cyber incident response plan and only 3% did not have a plan, as opposed to 16% in 2016. Meanwhile, 59% of surveyed Romanian companies had performed a vulnerability assessment to cyberattacks in the two years prior.

The chart below (figure 5) highlights the key elements of cybersecurity programs in Romania. The PwC report speaks of growing sophistication among Romanian companies. The use of new technologies, such as machine learning, AI and blockchain in the

Figure 15 - Key elements of the Cyber Security Program among Romanian respondents

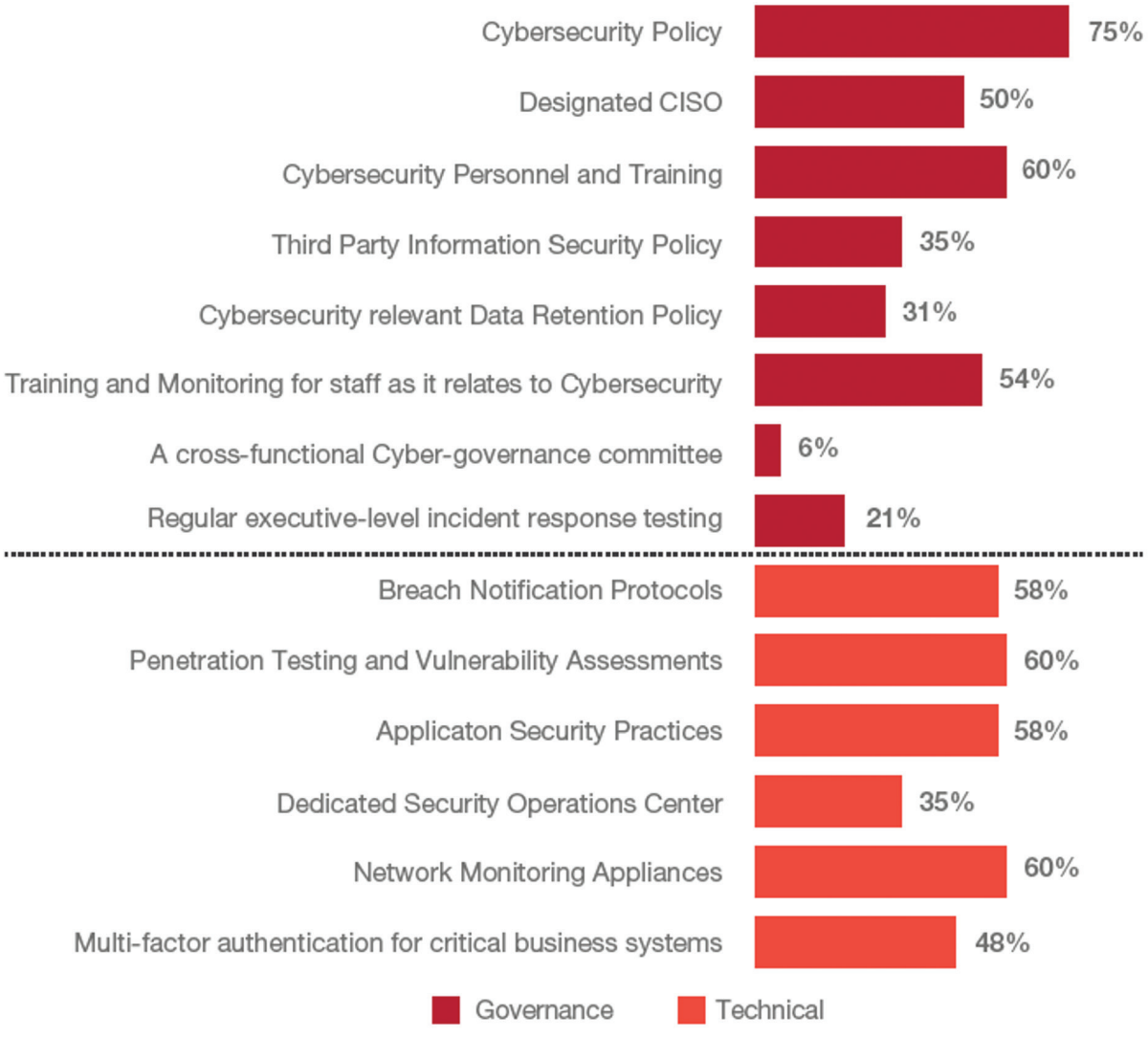

***Figure 5**: Elements of cybersecurity planning in Romania (source: PwC Report, 2019)*

digital realm will result in a more complex cyber environment, and consequently new risks, but also in a leap forward for security processes. Should Romanian companies manage to position themselves in lockstep with their peers abroad, the application of the new technologies will make up for other deficiencies, such as resource allocation and lost time. While only one company surveyed was using AI for security purposes, fully a quarter reported that they planned to use AI in their security processes, and the report also highlighted a growing use of machine learning in security processes.

ROMANIAN EFFORTS AND PARTICIPATION

The heartening developments detailed above do not manifest in a vacuum. They are, rather, the result of an organic process of diffusion of security knowledge, culture and attitudes which are driven as much by contacts and awareness raising efforts as by formal education mechanisms.

With its well-established ecosystem not only in the general IT field, but also in the realm of cybersecurity and adjunct technologies, Romania is well positioned to both promote the benefits of digitalization, as well as to manage the security risks inherent to this transformation.

The proliferation of events dedicated to technical specialists, enthusiasts, but also policy makers is an important and encouraging sign of the growing awareness of these issues. Just to give a few examples, we have the **CyberTech Conference** which took place on January 29-30 in Tel Aviv, Israel, and the European Cyber Security Challenge – ECSC 19 will take place on October 9-11 2019 at the Palace of Parliament in Bucharest.

CyberTech is the most significant conference and exhibition of cyber technologies outside of the United States. It provided attendees with a unique opportunity to become acquainted with the latest innovations and solutions featured by the international cyber community. The conference's main focus is on networking, strengthening alliances and forming new connections. CyberTech also provides an incredible platform for Business to Business interaction.

***Figure 6**: Israeli PM Netanyahu addressing the CyberTech Conference in Tel Aviv (Copyright: GPO/Haim Zach)*

***Figure 7**: Minister Alexandru Petrescu meeting with Israeli PM Benjamin Netanyahu*

CyberTech has an important component for networking between high government representatives, decision makers and industry representatives, which is why I was also present on January 30th in Tel Aviv, and had the

opportunity to interact not only with the Israeli Prime Minister, but also my counterpart leading communications, Ayoob Kara, and Yigal Unna, the General Director of the National Directorate for Cybersecurity.

Soon afterwards, on February 12th 2019, we also marked in Romania the first meeting of the Consultation Council "**Digital Romania**", which seeks to foment debate and policy discussions on the promotion of the development of the communications sector in Romania.

The period also saw active contributions on the part of Romania to the European efforts for digitization, under the heading of the Romanian Presidency of the EU Council.

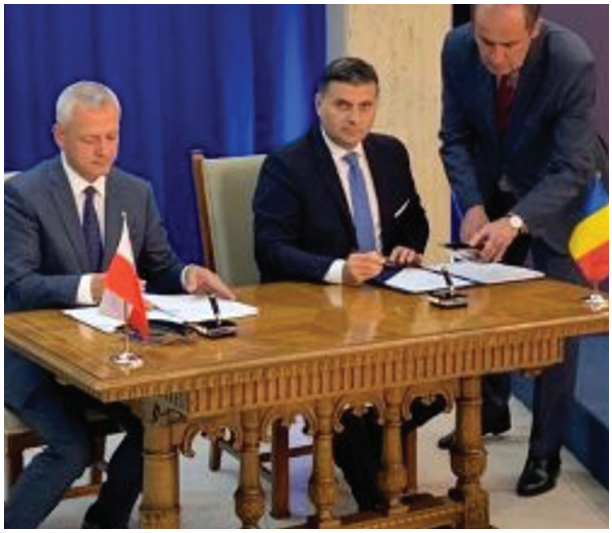

***Figure 8**: Minister Alexandru Petrescu and Minister Marek Zagórski signing Memorandum of Understanding*

***Figure 9**: Minister Alexandru Petrescu after the government approval of the 5G Strategy for Romania*

A priority for us was the negotiation of **The Digital Europe Programme**, which aims to develop and consolidate the strategic digital capabilities of the EU, while also ensuring investment in Artificial Intelligence, cybersecurity and others, in order to maintain European competitiveness in the field over the backdrop of intense global development.

We advocated for a European Center for Cyber Security of Industry, Technology and Research, along with the creation of a **European Network of National Coordination Centers on Cybersecurity** to ensure homogeneous development, during the informal meeting of the communication ministers of the EU which I hosted on March 1st, 2019.

We continued our efforts to work with academia, industry and civil society, by organizing the **Bucharest Cyber Drill 2019** exercise in partnership with the "Politehnica" University of Bucharest on 27-31 May 2019, and the Romania **Blockchain Summit**, one of the largest events of its kind in Europe, on June 21-22, while also continuing the consolidation of contacts abroad, also in countries outside the EU.

An example was the Romanian participation in the 9th **Cyber Week** event organized by the University of Tel Aviv, Israel, on 24-26 June 2019.

Another example was the signing of a Memorandum of Understanding with the Minister of Digital Affairs of the Government of Poland, Marek Zagórski, to promote resilient communication networks and development in the context of the consolidation of the Strategic Partnership with the United States that both countries have.

We reached a landmark in development with the launch into operation of the 1911 special number for reporting **cyber incidents**, which saw heavy use right from the first few days, with 87 confirmed incidents, a quarter of which were in Bucharest.

On June 20th 2019, we also launched the **5G Strategy** for Romania, which charts a development path over the next few decades.

IN LIEU OF CONCLUSIONS

These opportunities to interact with decision makers, experts and companies from other countries or from our own will be invaluable to the future safe development of Romania in the cyber-contingent environment.

We need to step up our efforts to participate, to contribute, to create and to coordinate in the realm of cyber, because the greatest challenges are still ahead of us, such as the development of 5G communications, the omnipresence of the Internet of Things and the development of Smart Cities.

In this context, I want to express my immense satisfaction that **ICI-Bucharest** launched a new scientific journal this year, the **Romanian Cyber Security Journal** (ROCYS), dedicated to a very current topic.

I am also glad to see that the vision of the Journal is to increase the knowledge of the cybersecurity field, to expand awareness of the cybersecurity domain and to support a community of theorists and practitioners in developing the Romanian security culture in this field.

REFERENCE LIST

Center for Cybersecurity, World Economic Forum, https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications

Marsh & McLennan Cyber Handbook 2019, https://www.mmc.com/insights/publications/2019/mar/mmc-cyber-handbook-2019.html

Marsh & McLennan with Microsoft, Global Cyber Risk Perception Survey 2017, https://www.marsh.com/us/insights/research/global-cyber-risk-perception-survey.html

Accenture, Cost of Cybercrime Report 2019, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

PwC, Global Economic Crime and Fraud Survey 2018 – A front line perspective on fraud in Romania, https://www.pwc.ro/en/services/advisory/forensic-services1.html

https://www.comunicatii.gov.ro/comunicate-de-presa/