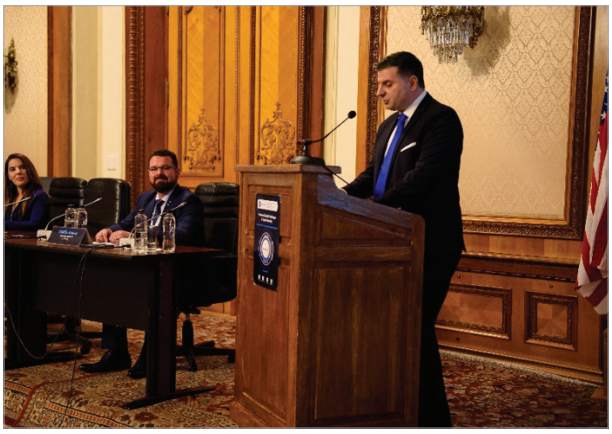
CERTCON9, a gate for new horizons in cyber-security

Cătălin-Petrică ARAMĂ
Romanian National Computer Security Incident Response Team
catalin.arama@cert.ro

Cosmina MOGHIOR
Romanian National Computer Security Incident Response Team
cosmina.moghior@cert.ro

Every year, the „New Global Challenges in Cyber Security" conference tackles the most pressing cyber security issues on the public agenda and looks at both the latest challenges in this field and ways to overcome them together with cyber security experts from private companies across all sectors and industries, government officials, policy-makers, NGOs and Academia.



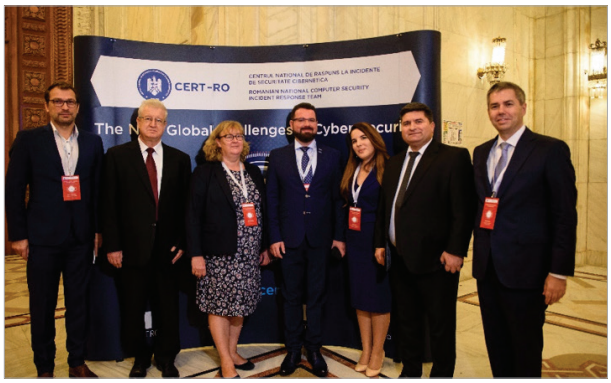
This year's edition of the CERTCON addressed some of the most critical subjects of cybersecurity, ranging from Cybersecurity of 5G Network, Cybercrime, Education & Awareness, NIS implementation, Artificial Intelligence, Research & Development in cybersecurity.

The new technologies bring to Romania new opportunities, but also new security challenges. Some of the measures that can reduce these vulnerabilities are cooperation, increasing confidence, increasing incident response capacity, developing digital skills, education and awareness, as well as updating the education curriculum to new realities.

OPENING SESSION

Mr. Alexandru Petrescu, Minister of Communications and Information Society has stressed the importance of promoting a safer digital society, an effort in which Romania plays an important role by participating in different formats of international cooperation. Cyber security affects all domains, reason why it is necessary to develop communication, cooperation and an appropriate common response to cyber threats.

Mr. Cătălin Aramă, the General Director of CERT-RO has presented the three main pillars created with the entry into force of the Law no. 362/2018 on ensuring a high common level of security of computer networks and systems. The novelty elements are the designation of CERT-RO as nationally competent authority, Single Point of Contact and CSIRT team.



Security is a vital condition for the proper functioning of a society, and cyber security is no exception. Cyber threats have a cross-border and non-discriminatory character, which is why it is necessary to develop cooperation between the parties affected by this phenomenon.

SESSION 1 - THE CHALLENGES OF 5G NETWORKS FROM CYBERSECURITY PERSPECTIVES

In terms of connectivity and expansion of services, 5G means an increased number of devices connected to the core network and to other devices at extremely large speeds with a very low latency. These aspects will generate great vulnerabilities and challenges when comes to data security. We can anticipate that some of the digital experiences will increase

in quality. The technological advancement will pave the way to new services. Edge computing will move the processing power from the core of the network towards the consumer. The main challenges that we have to solve is the widening of the attack surface that the 5G network.

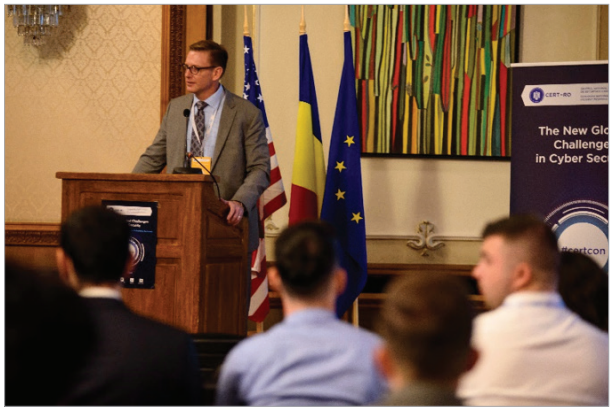
We need to create a holistic and versatile strategy to confront the ever-changing vulnerabilities characteristic to 5G network. Apart from these vulnerabilities, we have to keep in mind that 5G comes with a number of key enhanced security properties compared to earlier generations.

Mobile connections are the most vulnerable to the challenges brought by 5G.

5th generation (5G) deployment of network technologies is a major enabler for future digital services and a priority for the Digital Single Market strategy.

SESSION 2 - CYBERCRIME – ACTION & COUNTERACTION

Cyberattacks represent the common area between cybercrime and cybersecurity. Cybersecurity refers to security, trust, resilience and reliability of ICT, while cybercrime focuses on the rule of law, criminal justice and human rights. The Budapest Convention on Cybercrime (Budapest Convention), the Cybercrime Convention Committee and the C-PROC consist the basis of the needed legislation to protect the individuals and their rights in the cyberspace. The means of fighting cybercrime include reporting mechanism for criminal activities, international cooperation channels and data shared by public and private parties.



We continue to see an escalation in the volume, sophistication and impact of data breaches, which only seem to be getting worse. Among the foremost consequences are alert fatigue and too many false positive verdicts requiring far too much manual action which is time consuming. The solution is to surface the most advanced attacks with machine learning to speed up investigations.

The first challenge of security leaders is the detection of advanced threats, many of them are hidden, unknown and emerging. Cyber threat hunting is the act of aggressively intercepting, tracking and eliminating cyber adversaries as early as possible. The primary objective of threat hunting is gathering actionable intelligence, which include individuals, organizations, institutions, infrastructure and geography.

One problem with the security guards is that they might not be well equipped, they might become ineffective over time, might not be focused on the right target and they might lack process and procedures.

SESSION-3 - EDUCATION & AWARENESS

We need more cooperation between the state, private sector and academic/education in order to prepare the future generation for the current cybersecurity challenges. In this endeavor, we only need to use the real assets that Romania already has. In meeting the need for well-trained human resource, the cooperation between the three parties is the optimal choice, as they complement each other. The need for preparing the population of all ages is increasing with the development of sophistication, frequency and impact of the attacks.

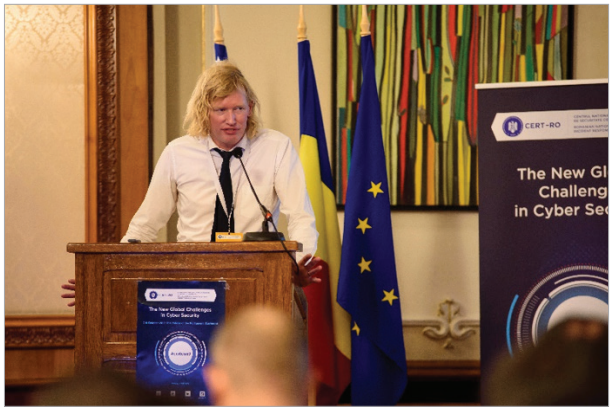
The public institutions and agencies that have top-expertise in the field of cybersecurity should be involved more in the training in schools and universities. In order to prepare the future generations for the challenges will come, we have to establish an appropriate curriculum with a vision on the future. The training program should focus on three key-elements: awareness, education and offered services.

The public-private-academia partnership should be developed in order to foster exchange of information and know-how. Furthermore, we should involve the top-level practitioners in teaching.

The employment of resources has to be done wisely to the programs with good results and stop the ones that do not perform well. In addition, we have to project strategies for no more than 3 years in order to always have a vision that matches reality.

SESSION 4 - NIS IMPLEMENTATION, LESSONS LEARNED, CHALLENGES

The NIS Directive lays down measures to achieve higher level of security for network and information systems. To achieve this goal, it was created a cooperation group with strategic role which brings together the CSIRTs of MS via CSIRTs Network. Starting with NIS national strategies, the NIS Directive's provisions also establish incident notification and security requirements for DSPs (such as cloud provides, online market players and search engines) and OES (such as transport, energy, water, health,



finance and digital infrastructure).

The NIS Directive is the first piece of the EU cybersecurity legislation. Cybersecurity is a necessity and is no longer optional. Many companies viewed cybersecurity in terms of costs and preferred to give it a low priority. This resulted in a lack of specialization to meet all the security needs. It will take time to implement all the security requirements. Risk evaluation is necessary and can be done through security audits and testing methods. In order to build this capacity, we need to see which detection and protection mechanisms are missing.

SESSION 5 - ARTIFICIAL INTELLIGENCE-CHALLENGES AND VISION

In 3 to 5 years, the technological landscape will be completely different and will have a huge impact on cybersecurity. Artificial Intelligence will play an important role, both for personal security and for organizations' security.

We are witnessing an increase in the sophistication of the instruments employed by the cyber criminals. One of the instruments used by these malicious actors is hacking the human, or social engineering.

The cyber criminals are using our lack of attention or our lack of skills to try to scam us. Machine learning and AI will help us in fighting cybercrime. The cyber criminals are using algorithms to create and spread botnets and we can use the same instrument to identify the malicious code and try to disrupt it or take legal actions against it.

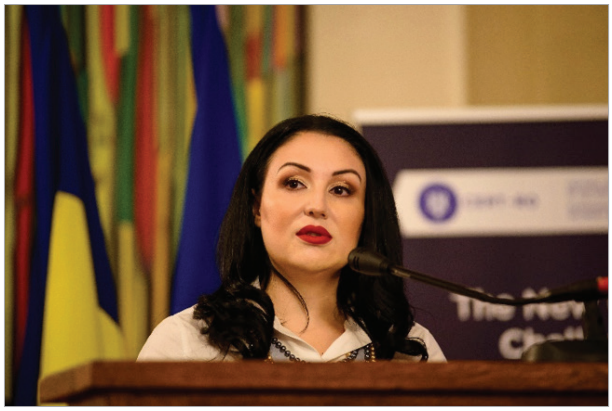
We are in the middle of an arms race in terms of cybersecurity threats.

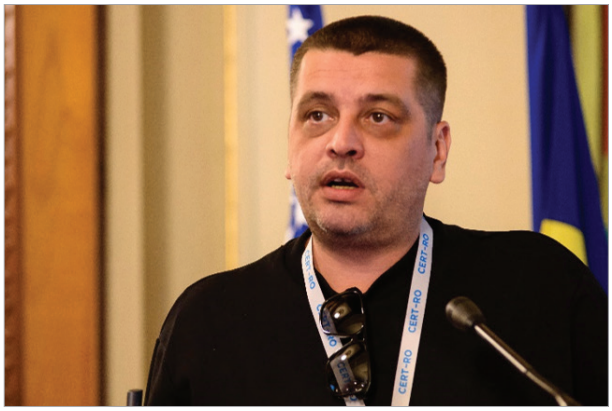
Machine learning and behavior analysis can be used to identify, at a very early stage, the patterns that are out of the ordinary. The natural language processing and image recognition can be used to recognize the methods (such as pop-ups) which are employed in the scamming activities.

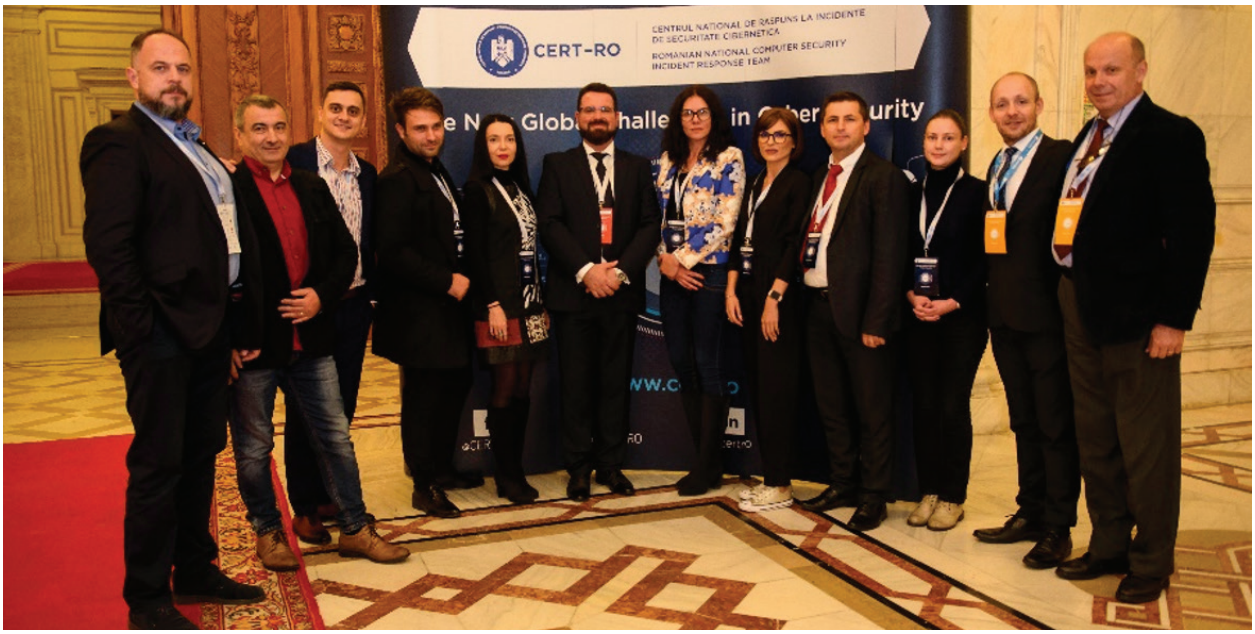
SESSION 6 - RESEARCH & DEVELOPMENT IN CYBER SECURITY

The core-elements of R&D is asking questions, building consortium and groups of interest, cooperation and exchange of knowledge and experience. The Memorandums of Understanding in the field of communications and information society with other countries is the first step in fostering cooperation. The idea of an eastern partnership would create the incentives needed to start new R&D initiatives in the future.

Cyber criminals are organized and are collaborating in sharing information. They develop and sell exploit kits on the darknet, which makes it very cheap and simple for anybody to launch a cyber-attack. The reality is







that cybersecurity remains a business activity and is often difficult to justify the investment necessary to protect.

The three biggest challenges we have to face is the high quantity of false positives and poor quality of data, lack of scalability and massive volumes of data, skills shortage and the lack of collaboration and information sharing. There are information sharing, collaboration and trust channels in place, but sharing critical information and collaborate is still hindered by the lack of trust.

CONCLUSIONS

The main take from the 9th edition of "The New Global Challenges in Cyber Security"- #certcon9 is that we have to work hard in order to keep the pace with the changes in cyberspace, none of us having the feeling that we can cover 100% the challenges that the future will bring. In this endeavor, we must consolidate the cooperation mechanisms and guarantee reciprocity with international partners in fighting these challenges.

We need to put all of our effort in adapting the legal framework, educational system, digital infrastructure and our capacity to respond to challenges brought by 5G network.

The private and public sector have different attributions and knowledge in fighting cyberthreats. This is one of the reasons why the partnership between the two should be intensified and the joint activities in cyberspace extended.

The traffic in cyberspace will continue to grow, as such we need to strictly apply the criminal law in order to protect the individuals and their rights in the cyberspace. In addition, the subsequent legislation needs to be updated in order to ensure the optimal functioning of the judiciary system in cybersecurity activities.

The NIS Directive provides member states with considerable margin of discretion, which could lead to a divergent application across the EU. One of the challenges in implementing the Directive is to define and understand which are the essential services.

The capabilities of the malicious actors to employ sophisticated attacks are developing proportionally with our readiness and capability to respond these attacks. The solution to this challenge might be the art of using Artificial Intelligence technology in our favor.

The way forward is increasing cooperation, foster thrust to stimulate the exchange of knowledge and experience and invest with a vision on the future. We should overcome the internal or systemic barriers and unite our efforts in fighting the common enemy. Cybercrime does not have borders and neither should have our endeavor in fighting it. We need to put our creativity at work in order to become stronger.