The New Global Challenges in Cyber Security

The 22nd of October 2020

Conference report

www.cert.ro/certcon10

Rapporteurs:

Mr. Cezar Bărbuceanu, Public Relations Specialist, CERT-RO
Ms. Alexandra-Maria Bran, Bachelor Student, Faculty of Medical Engineering, University POLITEHNICA of Bucharest
Mr. Ciprian Buzatu, Master's Student, National Defense University "Carol I"
Ms. Alexandra-Ioana Buzățoiu, Bachelor's Student, Faculty of Information Systems and Cyber Security, Military Technical Academy "Ferdinand the First"

Ms. Elliza Ciurea, Legal Advisor, CERT-RO

Mr. Adrian Diac, Bachelor's Student, Faculty of Information Systems and Cyber Security, Military Technical Academy "Ferdinand the First"

Ms. Diana Grigore, Bachelor's Student, Faculty of Mathematics and Computer Science, University of Bucharest

Ms. Ioana Tănase, Crisis and Security Manager, MSc Graduate - Leiden University

Editor and rapporteur:
Ms. Cosmina Moghior, Public Policy Expert, CERT-RO

Contents

Sessions insights

Opening Session

Head of Analysis, Policies and Cooperation of CERT-RO, Mr.Sabin Popescu mentioned the importance of strong institutions against forces that interfere with the wellbeing of mankind and added that there is a necessity for adapting CERT-RO to National Directorate of Cyber Security. Mr.Sabin Popescu also resumed the content of the conference.

Mr. Antonel Tănase, Secretary-General of the Romanian Government, begun by mentioning the challenges of 2020, the necessity of adapting to these new situations. He stressed that the current developments created a wave of digitalization which forced many people to adapt to these new conditions. Secretary-General indicated that CERT-RO has reached a certain level of maturity and at this level, there is a need to adapt the institution to the current cyber security environment. He underlined that CERT-RO is an institution that is prepared to evolve considering its experience in subjects such as implementing the NIS Directive, the topic of cyber security during the Romanian Presidency of the European Council, the rollout of 5G networks, international and national cooperation, the effort for creating a national framework for certification, cooperation with the private and academic sectors. Mr. Antonel Tănase added that Romania needs a new professional approach in cyber security and IT and consolidated the idea by illustrating a national issue regarding qualified personnel in this area.

Mr. Tănase considers that a Romanian Directorate for Cybersecurity (DNSC) is a solution for creating a proper cyber security environment that can work along with foreign ones and which will have an immediate impact on the national economy. DNSC will have an important contribution in education, by preparing the next generations of cyber security specialists and it will be offering adapted opportunities for the requirements of these professionals. He also mentioned that specific cyber developments such as the rollout of 5G networks, Artificial Intelligence, Big Data, standardization and certification require a prepared institutional framework. Romania also needs an institution that is able to assist in implementing the European Directives.

H.E. Adrian Zuckerman, the Ambassador of the United States of America in Romania started by mentioning the important role of CERT RO for keeping the online environment safe from threats and thanked the Romanian Prime Minister for prioritizing cybersecurity among other national issues such as the rule of law and corruption. H.E. stressed the importance of international cooperation and the necessity of using resources against cyber threats, underlining the importance of the partnership between Romania and US on the topic of cybersecurity.

Mr. Adrian Zuckerman indicated that the US is committed to assisting Romania's development as a regional leader by exemplifying the strong security relation between the two countries in Eastern Europe and the Black Sea Region. H.E. added that American assisted projects such as the nuclear reactors from Cernavodă and the highway and railroad from the Black Sea to the Baltic Region are an important economic boost for Romania.

The American Ambassador indicated that rule of law is paramount for freedom and democracy, mentioning that Romania made important progress in this regard.

Cyber-attacks against digital infrastructure, orchestrated by foreign actors from countries such China or Russia, will require a response from the US and steadfast partners like Romania. H.E. also mentioned that 5G will bring a range of innovations, but stressed that 5G networks provided by untrustworthy partners are a threat for national security. Considerable efforts such as the Agreement between the US and Romania on 5G will help in keeping networks safe.

Dr. Markus Richter, State Secretary at the Federal Ministry of the Interior, Building and Community and Federal Government Commissioner for Information Technology recalled that the Covid 19 pandemic accelerated the adaption of digital technologies and added that EU makes efforts for adapting those technologies, while taking note of possible vulnerabilities and threats that do not stop at national borders. He also mentioned the importance of cooperation in cyber security within the EU, adding that the European Commission is working on a new cyber security strategy. Dr. Markus Richter also stressed the necessity for a European cyber security architecture and further indicated that the European Commission is currently evaluating the NIS directive. In this context, he stressed that ENISA will have a key role in building national capacities and that the European common goal is to inspire innovation and establish EU as a leader in cyber security technologies.

Dr. Markus Richter mentioned Germany's proposal regarding the safety of IoT, considering that all devices connected to internet must have a basic level of security. He concluded by mentioning that the EU has the opportunity to develop cyber security and improve European citizens' overall quality of life in a digital and connected future.

Mr. Juhan Lepassaar, Executive Director of ENISA, welcomed the conference as an environment for strengthening cybersecurity cooperation. He underlined that cyber security attacks are increasingly sophisticated and widespread. ENISA welcomes European Commission's decision to review the NIS Directive and the plans for drafting a new cybersecurity strategy. He also added that ENISA will assist and contribute to a better understanding of cybersecurity across various fields.

Mr. Marian Murguleț, CIO of the Romanian Government, mentioned that 5G networks have a strategic relevance and the Romanian State has the duty to carefully reviewing the impact of implementing the new technology, while cooperating with relevant international partners on this subject. He also stressed the importance of adopting concrete measures to counter cybersecurity threats that are becoming increasingly complex. The European Union's initiative for reviewing the cyber security legislation must be followed by a similar effort at national level. The CIO mentioned that the Romanian national legislation regarding cybersecurity is outdated and stressed the necessity for transforming CERT-RO into DNSC, a process which is currently in progress.

Mr. Saad Kahdi, Head of CERT-EU, presented the activity of CERT-EU in defending institutions, which now protects over 80 organizations in Europe and outside the European borders. He also mentioned the importance of a close collaboration with ENISA for improving operational response, considering that APTs have severely increased in the last 3 years, from an average of 47 incidents per month in 2019, to more than 100 per month in 2020. Mr. Saad Kahdi added that there is a need for better capacity building in cyber security across Europe.

Mr. Igal Unna, **Director General at Israel National Cyber Directorate,** underlined the fruitful and helpful operational relationship between Romania and Israel in cyber security, especially in mitigating attacks on hospitals. He mentioned that the global Covid-19 pandemic brought a cyber pandemic involving malicious actions such state sponsored attacks. Mr. Igal Unna stressed that a basic solution for pushing back threat actors of all kinds is international cooperation.

Mr. Anton Rog, Director of Cyberint, welcomed Mr. Tănase and Mr. Murguleț's strong support for the creating the DNSC, adding that SRI is also supporting this process. Mr. Anton Rog mentioned that the Covid-19 pandemic created a special environment in which certain actors took advantage and increased the frequency of attacks. State actors, cybercrime groups and cyber terrorists became more involved in disrupting the online environment. He indicated that in Romania, classic cybercrime is being implemented against banking systems, through banking trojans, and against the health system, central and local administration and academia, which are facing waves of ransomware campaigns. Mr. Anton Rog also mentioned the inter-institutional efforts of improving awareness on ransomware and the Emotet campaign targeting Romania.

Dr. Guillaume Poupard, General Director of National Cybersecurity Agency (ANSSI), France, stressed that EU has to fight against malicious actors that are increasingly prepared. In this context, there is a need to cooperate with public and private sectors to establish a common view on cyber defense. He also mentioned the importance of the new NIS Directive which should enable the member states to face cyber problems adequately.

Dr. Guillaume Poupard suggested that the digital sovereignty of the EU shouldn't be marked by protectionism, illustrating the necessity of working with strong allies and private companies outside of the EU, while making sure that those external entities follow rules for creating a safe digital environment in EU.

He also stressed the importance of cybersecurity certification for service providers, which would create a white list of trusted providers. He added that the 5G Toolbox shows that EU can provide solutions and a common strategy to complex issues.

Mr. Hans de Vries, Director of National Cybersecurity Centre of the Netherlands, discussed the current global threat in cybersecurity and indicated the need to strengthen ENISA and the overall European cooperation in cyber security. He also mentioned that digital sovereignty, problems with 5G, AI and cybercrime are important topics which need our attention. Mr. de Vries stressed that cooperation is the key for combating cyber threats and proposed making efforts for an enhanced cooperation in Europe, illustrating that his country has a long history in sharing valuable information.

5G Toolbox: the instrument of the future

5G technology empowers the already existing technologies and creates a backbone for future ones as well. This generation is already in use and a lot of work has been done, but it also needs considerably attention in order to achieve best performances in terms of risk mitigation and cybersecurity.

Ms. Julie Ruff, Head of Sector in unit Cybersecurity Technology & Capacity Building, DG CNECT, European Commission, discussed about the 5G technology prioritisation in the view of the European Commission. There is already a framework on European Electronic Communications Code (EECC) which establishes the obligations for telecommunication operators to take security measures. The risk assessment section has been a global contribution of all the member states of EU, including the identification of the right combination, mapping the risks and finally elaboration of practical guidance regarding the components and products.

Mr. Andrew Greenough, Economic Officer, U.S. Embassy Bucharest, underlined that this new technology should be viewed in relation to military cooperation. Securing 5G networks is a collaboration between civilian and NATO forces on one hand and suppliers and operators on the other hand, which have to take all the necessary measures for digital trust standards. Relying on transparency, the created links lead to key concepts such as political government standards for data protection and business practices in form of ethical behaviour.

Dr. Tobias Mühlenbruch, Head of section, Federal Office for Information and Security (BSI), Germany, presented the main highlights of the Security Catalogue, created in 2013, updated in 2016 and 2020. The document ensures the necessary precautions and measures to safeguard data protection and telecommunications confidentiality. It contains more than 350 individual requirements and also refers to the BSI Technical Guideline on product and system certification. The Technical Guideline is based on existing standards and developed at EU level. In Germany, mandatory certification of 5G components will be introduced based on BSI 5G Certification Technical Guideline in 2021 and then will migrate to the European scheme as soon as it will become available.

Mr. Evangelor Ouzounis, Head of Unit - Secure Infrastructures and Services, ENISA detailed that 5G technology is not an update of older generation networks, but a technology on its own, because of the range of applications and functions, as well as the security implications. Strengthening the role of national authorities, assessing the risk profile of suppliers and ensuring their diversity are some of the proposed strategic measures, along with the vital technical measures. ENISA has a continuous involvement on 5G toolbox, drawing technical guidelines for telecom security authorities and studying security measures.

Mr. Pieter van der Berg, Senior Coordinating Policy Officer, Ministry of Justice and Security, Netherlands Digital Security Program, discussed about the approach of the Netherlands in securing the 5G networks. One of the issues is decreasing the dependency level on the providers of 5G components to ensure a vendor-neutral national network. The promise of 5G is immense and will be a visible impact on economy, but also cares risks that cannot be ignored. The security of this generation depends on the physical and digital infrastructure.

From a technical perspective, **Mr. Ioan Constantin, Cybersecurity expert, Orange Romania** presented the work of the private sector in establishing and implementing a more secure environment. Operators as well as end users have to identify a set of measures in order to achieve sufficient control. Objectives like ensuring strict access control, increasing the security of VNFs and reinforcing physical security occur in the frame of abundant usage of Artificial Intelligence, Machine Learning and IoT.

Certification & Standardization: need or opportunity

Mr. Philippe Blot, Lead Expert Certification, ENISA, presented the general overviews of current activities on cybersecurity certification according to the CSA and some elements on the EUCC scheme on ICT products and the EUCS scheme on cloud services. After presenting the calendar of the current activities on cybersecurity certification, he went on to discuss the main points of the two candidate schemes. The candidate EUCC scheme version 1.0 published in July received in majority a positive feedback from the SCCG, public and ECCG consultations. ENISA updated the candidate EUCC scheme and provided v1.1 to the ECCG for its opinion.

Prof. Dr. ing. Fănel Iacobescu, President of RENAR presented his institution’s perspective on the current cybersecurity developments at EU level. RENAR is the sole national accreditation authority in Romania and will have a very important role in developing the cybersecurity certification framework in our country. On this note, RENAR is a strategic partner of CERT-RO, which intends to take on responsibility of national cybersecurity certification authority.

Mr. Gheorghe Țucu, President, National Standardization Body (ASRO) underlined that certification and standardization is both a need and opportunity. He presented the main responsibilities of his institution in the area of cybersecurity standardization, including JTC 1 SC 27, CEN/CENELEC and ETSI. Cybersecurity is critical underpinning for the next wave: 'Digital Transformation, '4th Industrial revolution'. Its complex, fast changing story, with lots of inter-connected stakeholders.

Mr. Philippe Magnabosco, from ANSSI, presented the French perspective on certification and standardization. The main takeaway from his presentation is that there is an important link between standards/certification and innovation and trust. State of the art tech needs minimum trust, fairness and interoperability to reach markets. State of the art tech needs minimum trust, fairness and interoperability to reach markets. In the EU legislative framework, voluntary standards play a key role, but this is quite specific to the EU. Standardization is not only a question of innovative products on a competitive market, but one of defense against malicious actions. It is an added layer of trust between Cybersecurity stakeholders (developers, users) including public authorities and the general public. Often, a need for officially recognized standards emerges. We need a type of European standardization because the European context provides added possibilities, the EU legislation calls for it and it is inclusive, open and attracts stakeholders from around the globe. European standardization has also begun addressing the evaluation of **cybersecurity services** which will provide a better foundation for future certification schemes than international standards currently do and will do so by drawing again from the experience of national cybersecurity agencies such as ANSSI, and other stakeholders.

Mr. Matthias Intemann, from BSI presented the German experience in running a certification and standardization scheme. BSI's contribution to the digitization process spans from legal framework development to standardization and certification. Mr. Intemann gave the example of digitization of the energy sector, with details on the regulation adopted and the role of BSI in the process. He den proceeded on presenting similar actions to be taken for the mobile network security, with focus on 5G. He stressed the importance of agreeing at the EU level on security principles and security assessment methods. In addition, it would be efficient if EU member states would support global standards based on harmonized European requirements. He presented then the main benefits of certification, among which was mentioned the increase of trust, avoid duplications and increase transparency. The Cybersecurity Act systematizes the process of European cybersecurity certification framework development.

Mr. Patrik Palm, Ericsson Director Product Security presented a private sector perspective on the security of the 5G networks through global standards. To ensure that mobile networks are secure, reliable and privacy-preserving there is a need for a comprehensive life-long planning, which will include the development of the products based on standards which would ensure the security of the supply chain. The second steps is deployment and configuration, where the systems' trust function include security, privacy, resilience, reliability and safety. The last element is dynamic assurance, adjustment, transparency and compliance proofs for trust functions during operation. Mr. Palm underlined that ensuring security in deployed networks requires mitigation on all levels with processes on operation, deployment, vendor product development and telecommunications standardization. NESAS scheme developed by GSMA and 3GPP is one of the most important documents for ensuring the security of the telecommunications networks.

Mr. Florin Dragomir, Head of the Technical Regulation Department, ANCOM, Romania, presented the main activities at national and European levels on the standardization of ICT products. The most important documents in this area are the European standardization strategy, standardization Rolling

Plan, other global ICT standardization developments, as well as public-private partnerships between European Commission and private standardization organizations. Standardization is an opportunity as it increases competition and is a stimulant for innovation.

Mr. Valentin Necoară, Chief Technology Officer, certSIGN, presented the certification and standardization from an industry point of view. Certification and standardization can both be industry or regulatory driven, or both. He underlined that for security related products, standards and certification are both highly praised and dearly needed. He then presented a series of industry driven initiatives, such as Cloud Signature Consortium, Open Banking Europe and dome research projects. Standards and certification bring safety and predictability to the end users and the involvement of industry in standardisation is critical. In addition, the is a need for a culture development to contribute to the community.

Cybercrime & Social engineering

Mr. Virgil Spiridon, Head of Operations, Cybercrime Programme Office in Council of Europe presented how Council of Europe fights Cybercrime. He agreed that regulation is the way and exposed the main highlights of the International Convention for Cybercrime from Budapest. He has also underlined that only 1% from the reported cybercrime incidents end up in criminal conviction as a result of limited capacities of police agents to deal with cybercrime.

Mr. Catalin Zetu, Head of Bureau of Investigation of Crimes against Information System within the Romanian Police saluted the cooperation between CERT-RO and Romanian Police. Romanian Police focuses its efforts on non-cash of payment frauds, cyberattacks investigation, infantile pornography over the internet and digital forensic. Mr. Zetu have mentioned how the pandemic of COVID19 has influenced Cybercrime. As most of lucrative activities have moved online during the pandemic, criminals have adapted to the new environment created by COVID19. Mr. Catalin Zetu stressed that on one hand criminals exploit public’s interests for COVID19 in different phishing campaigns, but, on the other hand, they attempt on healthcare system and infrastructure, asking for exponential amounts of money in exchange.

Mr. Oleg Bondarenko, Director of International Research FireEye Intelligence spoke about the new trends of public shaming on the internet for those who refuse to pay the ransom and the current practices of vishing, which is voice phishing.

Ms. Magda Popescu, Outside Legal Counsel to Microsoft Corporation, Digital Crimes, EMEA, presented Microsoft’s latest operations against Trickbot C2, a network of servers and infected devices run by criminals. The disruption launched by Microsoft is intended to disable Trickbot’s infrastructure and make it difficult for its operators to enable ransomware attacks. Until October 18, they have worked with partners around the world to eliminate 94% of Trickbot’s critical operational infrastructure including both the command-and-control servers in use at the time their action began and new infrastructure Trickbot has attempted to bring online.

Mr. Andrei Bozeanu, CERT-RO Expert presented a series of threat intelligence reports resulted from technical sources (darknet, honeypots), OSINT (social media) and HUMINT (open source intelligence).

Mr. Scott Kerin from International Computer Hacking and Intellectual Property Attorney Advisor, US Department of Justice presented a few statistics on the activity of FBI. There was recorded a 400% increase in cyberattacks, a 80% increase in ransomware and 49% businesses in USA faced at least a cybersecurity threat in the past 6 months. Mr. Kerin mentioned the increase of online fake pharmacy distributors. In the current psychological context, people are turning to online solutions (fake COVID19 cures, vaccines, antibiotics).

Mr. Liviu Arsene, Global Cybersecurity Researcher, Bitdefender discussed about human vulnerability. "The weakest component in cybersecurity is between the chair and the keyboard", the user. Hackers have improved "marketing" abilities of communication to target the victims. Among the tendencies, we can mention promotions from e-mails which are fake, very similar to big corporation domains, with same interface, same signatures asking for credentials or money. Criminals adapt to the nowadays context. After the COVID lockdown, the malicious actors launched campaigns with "special discounts" between June and July, after the relaxations. In September and October, when everyone was doing online shopping, there were a lot of campaigns impersonating Banks and Financial Institution.

Mr. Yoad Dvir, Cybersecurity Tech Sales Lead, Central & Eastern Europe, Microsoft, discussed the issue of paying the ramson or not. Mr. Yoad David explained that if the ransom is payed, the total prices for restauration and ransom will be higher than building everything from 0 again. In addition, if the ransom is payed, the victim enters a payers list, which brings him/her closer to the next attack.

Mr. Cristian Aflori, Technical Expert from "Gheorghe Asachi" Technical University presented a real-life perspective of a forensic technical expert. The stages of an IT forensic include understanding the case and the context, IT evidence acquisition and preservation, forensic analysis and finished with an expert opinion. The best practices in this type of activity is to respect the chain of custody, every step of the expertise must be reproducible, every type of the investigation has it's own procedures, methods and tools, integrated forensics tools are helpful (Slueth Kit, OSForensics, Caine, EnCase). A successful investigation is the ability of the expert to choose and combine the right forensics methods and tools and to interpret and summarize the partial conclusions. The challenges are the wide range of legal cases and technical domains, the lack of the formal education in IT forensics, the gap between IT knowledge level of the Courts and the IT technical complexity of the legal cases, IT legal expertise market is still young.

Education, awareness & psychology in cybersecurity

Cyberattacks increased exponentially in the current context of COVID-19, as people spend more time online and they also conduct their work from the comfort of their houses. Thus, more than always we need more cooperation between the state, private sector, and academia in order to make sure the future generation is well prepared for the emerging cybersecurity challenges.

Ms. Claudia Nicolae, general director of News Agency Agerpres, mentioned that misinformation can be a real force on social media as it is present everywhere and it plays with our weaknesses and emotions. However, a major risk in the actual context is that many people will go from trusting almost everything to not trust anything at all. Consequently, education is a major antidote to fake news, and in order to minimize the influence of misinformation within social platforms. Private actors like media, journalists particularly, can build a culture of integrity, compliance, and ethics that support accurate information. As a first step in enhancing this behavior, in 2016 Agerpres launched the Cybersecurity section which aims to make people more aware of the strategic problems of cyberspace and security. Additionally, in partnership with CERT-RO, there were organized cybersecurity courses for journalists.

Mr. Sorin Stănică, Director of Crime Research and Prevention Institute underlined that the internet is not only the source of online crimes, but it can also play an important role in prevention. By conduction partnerships with governmental and non-governmental actors, the Crime Research and Prevention Institute undertook many awareness campaigns via online platforms. Some examples of such campaigns were provided. Mr. Stănică further presented „The theft catalog", which is a set of examples of criminal activities linked to cyberspace. The document aimed to make people aware of the fact that photos and videos they post online reveal items from their houses or ways to enter their house.

Mr. Ionut Florea, Presales and Marketing Director, certSIGN stressed that as there is a general agreement that both public and private agencies that have the top expertise in the field of cybersecurity need to be involved in the training in schools and universities, more companies organize opportunities for students, for young entrepreneurs, and even for kids. CertSign launched the project C4K that aims to provide important cybersecurity lessons for primary school children and their parents as well.

Mr. Cristian Pațachia, Development and Innovation Manager, Orange Romania presented the programs run by Orange in the field of cyber education. The company is involved in academia by organizing workshops, educational programs, and masters in cybersecurity in 5 different universities. This three-level partnership is developed to foster the exchange of information and to further extend students' capacity to handle cyber threats. It is important to highlight that this cooperation between actors is mandatory when it comes to the ecosystem of Cybersecurity.

Lecturer Simona Caraiman, deputy-rector for IT, Gheorghe Assachi Technical University mentioned that there is a big gap between social needs, economic needs, and the specialized human resources. This lack comes from the way digital sector evolved, but this is also a complex topic, thus cybersecurity is not for all. Considering the dynamic evolution of cyberspace, the need for continuity and cooperation is greater than ever. Everyone needs to cooperate and to increase investments in a mix of best practices and capacity building to close this gap. Consequently, academia started to understand this need and in the past year, an increasing interest in cybersecurity has been seen among students.

Mr. Adrian Danciu, Senior Regional Director South Eastern Europe, FORTINET reminded that the risk increases as cyber threats are becoming more sophisticated. Phishing practices are tailored to leverage the covid-19 pandemic and increased up to +600% since March 2020. Thus, we still need to prioritize the cyber awareness training, to train employees, and to further extend the academic sector. User education is the key, there is important to build a human firewall, to give people knowledge about cyber threats, techniques, and security. Similarly, along with academia, the public and private sectors need to train their employers to spot cyber threats. Humans are the weakest links and everybody should receive cybersecurity training, since a small technical team of super experts is not always enough to protect institutions such as schools or universities:

Prof. Univ. Dr. Răzvan Bologa, Faculty of Cybernetics, Statistics and Informatics, Economic Studies Academy stressed that cybersecurity awareness is required. The myth of training only a few experts to protect our systems is false, as it must be designed to be used by everyone, thus there is a need to increase the awareness. Educational programs must be developed in order to ensure an average level of cybersecurity awareness.

Dr. Tal Pavel, CEO CyBureau, Israel emphasized the idea that cyberstudies in higher academic education need to move from cybersecurity to cyberspace to provide more cyber knowledge and awareness. The „Cyber" domain is more than technology and security, it needs educated people who know how to mediate the issues in cyberwar and to narrow down the digital gap. It is mandatory to invest in human capital that knows how to tackle the digital sphere.

To sum up, there is a general agreement that more cyber knowledge and awareness need to be provided among people of different ages, educational levels, and professions, in order to face the new processes, new technologies, new threats. The whole process is circular and security is a process where collaboration between actors is essential. It is important to gather forces, skills, and knowledge and to build more trust between stakeholders (NGOs, Companies, and governmental organizations). Crime prevention is well done when there is cooperation, similarly, the best results are obtained when there is trust between stakeholders.

e-Governance

Given the importance of e-governance in the daily interactions between citizens and public administration, this panel was dedicated to promoting the importance and raising awareness of the evolution and improvement of the systematization of governance processes. This panel enjoyed a wide range of presentations and speakers from CERT Estonia, University Professors, leading representatives from the Ministry of Internal Affairs and the President of the Agenda for the Romanian Digital Agency. During the discussions, the speakers presented aspects and characteristics of the e-Governance process, as well as updated information of the new services made available to the citizen through this process.

Mr. Tonu Tammer, Director of CERT-EE, presented how Estonia manages to pleasantly surprise by implementing the e-Governance process, bringing that concrete results such as 98% of administrative processes between citizens and public administration carried out through online platforms provided by the Estonian government, with a deficit of their use of only 2% that uses legal physical and bureaucratic forms. At the same time, Mr. Tonu Tammer states that the Internet in Estonia is a social right, and each resident has an electronic identity that allows him to connect to it, Sandbox for everyone through the Cuckoo platform and 100,000 Malware samples per year. Estonia places great emphasis on educating Estonian users, training to develop cyber hygiene of public employees and developing a stronger government to address the needs of citizens through e-governance.

Mr. Sabin Sarmas, Director of the Agency for the Digital Agenda of Romania, delighted the audience with a presentation on his institution's priorities for smart governance. Mr Sarmas also emphasized regulatory transparency, interoperability, electronic identity and the government cloud, reviewing the need to use electronic services.

Mr. Razvan Jiga, Director General Chief Police Commissioner of the General Directorate for Communications and Information Technology within the Ministry of Internal Affairs presented information about the service hub of the Ministry and about public electronic services that bring benefits such as obtaining an electronic identity card, electronic passport, electronic driving license and personal vehicle registration card. It also reviewed the results of projects implemented so far in terms of e-governance such as modernizing and securing public services by the Ministry of Internal Affairs, eliminating bureaucracy as much as possible, improving communications, reducing time to process citizen's request and reducing the supplies cost.

Mr. Cristian Ciurea, Associate Professor and head of the Department of Economic Informatics and Cybernetics from the Academy of Economic Studies in Bucharest emphasized the importance of digitizing higher education, the online admission process in high schools and faculties, online courses and seminars, online and instant quizzes or automated examinations, online library, online gradebook for studs and teachers, online secretariat support and digital e-signed diplomas.

Dr. Catalin Vrabie, lecturer specialized in IT&C for Public Administration, E-government strategies and policies and the use of Smart technologies teaching those disciplines at the Faculty of Public Administration at National University of Political Studies and Public Administration in Bucharest spoke about the symbiosis between society and technology, the interaction between citizens and Public Administration, tools that might help improving e-Governance. The lecturer also reviewed the fact that in the coming years [e-governance] will transform not only the way most services are delivered, but especially the relationship between government and the citizen. After e-commerce, the next revolution of the Internet will be e-governance.

The presentations made in this panel by the speakers who honored us with their participation were made with reference to the current situation and with a solution to the problems imposed by the COVID-19 pandemic.

In conclusion, we need e-Governance to make our day-to-day business easier and to simplify time-consuming bureaucratic processes and interactions that keep us behind huge queues.

Women in cyber

Ms. Anett Madi-Nator, President at Women4Cyber Foundation presented the main reasons why there is a need to include women in cyber. Cyber, like any other technical field, has shortcomings. Security and cybersecurity are pioneering areas, specifically they do not have a very long-standing basis and they do not have ancient traditions. It is therefore normal for the workforce to be better developed and structured than it is today, which implies the need for additional help. This discrepancy is somewhat normal, but now with globalization and the extent of cybersecurity, we should ensure that all people are able to actively participate in the establishment of a normal state of security. In cybersecurity, almost 2 million specialists would be needed, and at European level about 350,000. The lack of women is extremely visible. Out of the total number of those working in this field, about 7% are women (At CERT-RO, women represent almost 30% of the staff. In fact, a few days ago, a woman engineer became part of the IT team). When we think about how to cover this discrepancy we should start with ensuring the balance in terms of the need for cybersecurity specialists and considering the very small number of women. Two years ago, the European Commission and the European Cyber Security Organization launched the Women4Cyber initiative, which created a European-wide registry to allow all women working in this field to register. The Women4Cyber Registry was created to identify and build the community of women working in cybersecurity. The Women4Cyber initiative and the registry help women become visible and it allows experts to contact women working in this field. There is also an initiative of Women4Cyber which aims to encourage, support and promote women's participation in cybersecurity, regardless of their professional training. There are 6 main directions of action, among which we mention the sharing to the general public of the discrepancy in terms of workforce, good practices and examples of women who have managed to stand out in this world of men.

Ms. Vilma Tomco, Director General of the National Authority on Electronic Certification and Cyber Security, Albania underlined that one way is to encourage more women to become part of the culture of cyber security. Another is to give them equal opportunities to rise to senior management positions. It would be beneficial to encourage girls and women regardless of age and the professional training they have to take every opportunity to enter this field. It also seems important not to instill the idea that some sectors are for boys and others are for girls. Especially considering that globally the number of women is higher than that of men. In addition, they should take advantage of any chance that arises, for example in Albania there is a program that allows pupils and students to stay for a day to the job they want.

Ms. Liliana Musetean, IT Security Risk Management Programme Manager, European Commission discussed about communication as a needed skill when working in cybersecurity. She underlined that is there is talent, passion, keen to learn it is possible to build things. Participating in the arena of cybersecurity is about us and the will to put our service in the benefit of others. Cybersecurity is in the middle of the objectives of the current Commission. The level of threats is today wider than ever before, thus we need more talent to defend us, both men and women. The Women in Cybersecurity Training Program was organized for the first time this year, with 12 people selected. Today women should be ambitious and should express bold ideas about what could be done and encourage other women to apply to jobs in cybersecurity and other cyber-related skills.

Ms. Isabel Baptista, Head of Development and Innovation Department - Portuguese National Cybersecurity Center, discussed about the involvement of women in Portugal and worldwide. In Portugal, in 2019 only 9% of workers in the field of cybersecurity were women. The representation of women in the IT area is a matter of culture, which starts with the number of women in IT faculties and consequently is reflected in the labor market and in the decision making. For a qualified and diverse environment, it is crucial to encourage women in joining the field and provide progression capable of attracting and retaining woman capital in the area of cybersecurity. Considering inequality, it is impossible not to speak about numbers. 90% of the workers in cybersecurity in the world are male not only shows the inequality, but also the gaps in the talents within the field. The gender diversity matter because it reflects in the quality of the products resulted.

Ms. Bareket Knafo, Head of the Israeli Economic Mission to Romania and Ukraine discussed about some of Israel’s initiatives in reducing the inequalities in the IT area. Today we have the opportunity to see and hear more women in various fields. We can further promote the involvement of women in cybersecurity through education, investment and mentoring. We should start in the early age. The Israeli Ministry of Education started the project named STEM, which encourage girls in the elementary and secondary schools to develop an interest in the technological and scientific world and provide them with the appropriate theoretic and practical tools. They have identified a change in the number of women involved in scientific domains and an increase in the percentage in the technological military units. Another initiative is called "SheCodes" funded in 2013, which is a community of women in technology which aims to decrease the inequality of gender in software development domain through online coding trainings.

Ms. Manuela Catrina, Former State Secretary for Communication and Informational Society, Romania, discussed about the importance of having women involved in decision making discussions. It is important to have equality in the IT field, as these jobs assure a good level of life quality for women and for their families, even with the differences in the salaries. In addition, discussing about women in STEM should be a priority. The private companies are supporting this debate, not only because it is a fashionable, but because women are bringing talent that men might lack. Even from the childhood, most of the toys related to STEM are made for boys and we should change that.

Incidents and security measures in NIS sectors: pretending and defending

Mr. Maciej Siciarek, Head of Division from NASK and **Mr.Andrzej Matysiak, Project Manager from NASK** delivered a presentation on the Polish incident notification framework. They mentioned the Polish National Cyber Security Act, which was inspired from the NIS Directive, the project being launched as national cyber security platform called “S46”. The S46 is a platform on which users, stakeholders and participants share information, which is then analysed. They also mentioned the multiple functions of the S64 scheme and the unique and advanced tools it uses. S64 provides functions such as collecting data and response, along with analyses and risk awareness for creating a situational picture at national level. They added the benefits of joining the S64 system: possibility of reporting incidents, reporting vulnerabilities, information on risks, access to alerts, solutions in form of technical analyses. S64 contributes to building a chain of interdependence between services and operators.

Mr. Marnix Dekker, Team leader Cybersecurity Breach Reporting and Telecom Security, ENISA presented the details of reporting a cyber security breach, mentioning that mandatory reporting occurs after the effect of an attack. He stressed the benefits and challenges of incident reporting and illustrated a security incident reporting process from telecom’s point of view. Mr. Marnix Dekker also indicated factors for incidents: system failures, human errors, natural phenomena, malicious actions. He presented details about reporting under the NIS directive and the root causes categories for NISD incidents. He also referred to the CIRAS tool and its functions as a source of inspirations for institutional partners.

Mr. Aleksandar Ciric, Security Techincal Sales Specialist SEE, IBM, presented the roles of different levels of an incident response team from his company’s perspective. There are three levels in the operation: triage, investigation and response. He further detailed the work of an incident response person and the details regarding and incident response playbook, by exemplifying a malware incident response.

Mr. Eugen Popescu, Cyber Security Inspector at the National Civil Aeronautic Authority, stressed the need for developing multiple aspects such as dedicated OT sectors regulations, a coherent cybersecurity program at organizational level, implementation, understanding of hacking approaches, organizational and industrial SOCs. He also suggested that certification of a service shouldn't stop further development of new cyber security measures and stressed that an HR Department must have policies for prevention of insiders and happenings hide sensitive information from public access. Mr. Eugen Popescu also stressed that basic regulation shouldn't be avoided by specialized legislation, these being complementary, and further underlined the importance of cooperation with law enforcement authorities.

Mr. Yugo Neumorni, President of CIO Council, warned about cyber threats directed against power grids and stressed that a cyber-attack can seriously disrupt the activity of a big company, city, or country, producing significant financial damage through a power outage. He further provided relevant examples of such situations, mentioning the attack on the Ukrainian power grid on December 23, 2015. Mr. Yugo Neumorni also warned that serial converters are unsecure components and a cyber risk for critical infrastructure.

Mr. Tudor Cristea, Regional Sales Manager at Palo Alto Networks, presented the role of a Security Operation Centre focusing on the importance of prevention. He mentioned details about the Palo Alto SOC, indicating how to bring efficiency in specific processes from the company's experience.

Mr. Max Heinemeyer, Director of Threat Hunting, Darktrace, indicated the challenges of a NIS operator, such as tight deadlines, cyber security not being a core business, small teams, limited experience and complexity of threats. He mentioned the important role of machine learning in detection and investigation.

NIS Directive review: needs and vision

Ms. Raluca Ștefănuc, Policy Officer DG CNECT, European Commission presented the context of the NIS Directive, from the EU Cybersecurity Strategy in 2013, until now in the document Shaping Europe's Digital Future. The NIS Directive already showed great achievements resulted in the current review process, which will finish by Q4 of 2020. The last stage, the evaluation report and impact assessment, is now planned to be finished by end of November 2020. The information for the review is gathered from the Cooperation Group work, ENISA survey, OES report, country visits, study surveys, expert interviews and workshops. One of the observations is that the Member States use different identification thresholds, leading to fragmentations. The main fields of evaluation of the NIS Directive is the identification of OESs, role of DSPs, scope (sectors and services), security requirements, incident notification processes, national competent authorities and CSIRTs and cooperation at EU level. The objectives of the review is to prepare the document to respond to changing threats, enhance cyber resilience of all economic sectors, reduce fragmentation, be coherent with other sectorial/European legislation.

Mr. Alexandre Leite, Legal Advisor, Portuguese National Cybersecurity Center, presented the Portuguese perspective on the ongoing review process. The NIS Directive set the deadline of the revision on May 2021. Nevertheless, the Commission stated that it will review the Directive until the end of year. The scope of the new directive must consider the work in progress, the international for a and the scope of the annex 2 on the sectors of the Directive, as well as the annex 3 on digital service providers. The review must be done in a harmonized way. Portugal has adopted a national strategy for the network and information systems, as required by the Directive. From 2016 until now, in Portugal there was already a strategy, which was updated in 2018 to consider the NIS Directive.

Mr. Lucas Buthion, Policy Officer at National Cybersecurity Agency (ANSSI), France underlined that there is a positive reaction on the implementation of the NIS Directive in France. Voluntary cooperation through the Cooperation Group and the CSIRT Network helped creating a trusted ecosystem in the field of the cybersecurity all over the EU. Three main needs for the NIS Directive evolution. First is to keep as a driver the main objectives that were used so far. The second is the need to consider the evolution of the cyber threats and also the context of the booming digital transformation and the COVID 19 context which is accelerating the previous trends. The third need is to ensure consistency between the revision of the NIS Directive and the ongoing process of related documents (eg. from the financial sector). The NIS takes the legislative process with a cross sectorial implementation. The revision is structured around two objectives. The first one is to strengthen the security level of OES. The second one is to improve the cross-border cooperation schemes, to reinforce the trust between the member states and to improve the integration of the single market.

Mr. Toma Cîmpeanu, CEO of the National Association for Information Systems Security (ANSSI), Romania presented a private sector business perspective on the NIS Directive review. We have to start by considering that it is much easier to implement a directive rather than imposing a regulation. But the directive leaves room for flexibility in the implementation, which can lead to fragmentation at EU level especially in terms of application and level of sanctions. In the new Directive, the fragmentation must be decreased and increase cross-border cooperation. Furthermore, there is a need to see a progress in the development of the national legislation for the Romanian Cyber Directorate that would support the new directive.

Gl. bg. (r) Daniel Ioniță, Cybersecurity Manager CYMED offered another perspective on the NIS Directive review. One of the reasons why the Directive is difficult to be implemented in Romania is the diplomatic language in the document. Words such as “adequate” softens the urgency of some aspects which should constitute a priority, such as resources (human and financial), protection, staff. Thus, in the national interpretation of the Directive, this sense of urgency is decreased and now CERT-RO is still under-staffed and under-funded. The requirements and tasks of the CSIRTs on monitoring and responding to incidents is difficult to know if the incident is subject to the NIS Directive or to asses the level of criticality. As well, who receives the alerts is also difficult to assess.

Mr. Mihai Guranda, Head of Legal Department, CERT-RO, outlined the main challenges in implementing the NIS Directive. They are aspects such as identification of essential services and OSE, establishing a common standards and requirements, providing a proper infrastructure to CSIRTs and competent authority, human resources, the adaptability of the national NIS system, harmonization standardization, effective cooperation. There were substantial difficulties in convincing the administrative authorities from the seven sectors envisaged by the NIS Directive to sit at discussion table and to cooperate. And there was a lack of understanding regarding the importance of cybersecurity at different layers. There were no major changes identified over the last two years, but for sure there is a huge potential in this direction. Once the legislative blockages are removed, it is estimating a boosting in the implementation process.

Strategies of Cybersecurity & best practices: best strategies

Mr. Mika Kerttunen, Director of Strategy, Cyber Policy Institute, Estonia started with the definition of strategy as a balance between resources and goals in cybersecurity. Then, he continued with the idea that a good strategy should be based on 3 question: ”Where are we?”, “Where do you want to go?” , “How do we get there?”. Mr. Kerttunen said that Romania should focus on the first question and not to borrow strategies from neighbours, also gave as example Estonia who firstly focused on the main 6 problems from their country and then set their goals. Mr. Kettunen continued with the fact that for a good strategy needs exercise and highlighted the ideas that always need to take a strategy gradual and to invest resources. In the end he summarized all in two words for a good strategy: Relevant & Implementable.

Mr. Aristotelis Tzafalias, Policy Officer in the Unit 'Cybersecurity and Digital Privacy Policy' within the European Commission in Brussels (DG-CNECT) described in his presentation the main ideas about good strategies and different risks considered at more levels, including EU, National and more explicitly at NIS directive level. Mr. Tzafalias focused during presentation on the idea that policy makers have the responsibility to find the right balance between competing interest and that cybersecurity should always be an enabler for digital innovation and progress. Mr. Tzafalias also said that there should be coordinated efforts across public and private sector for improving cybersecurity. He finished his presentation with the remarks that relate the ideas wrote before.

Mr. Cătălin Iordan, Innovation Business Lead, S&T Romania presented first who is S&T Romania and then continued with the services that they offer in cybersecurity. Beginning from the main steps in cybersecurity guidance the show the “adding value” that S&T offer and in this can be found the following: high responsive to cyber-attacks, refining cyber security strategy operational efficiency.

Mr. Haider Pasha, Sr. Director & Chief Security Officer at Palo Alto Networks, Romania discussed about the impact that Covid-19 had on cybersecurity and also on society. The main ideas that he talked about was that we need to rebalance our priorities in order to recovery, about the necessity to provide guidance, to re-evaluate business continuity plans, to build a platform capability in order to secure our assets and adopt a zero-trust strategy. Mr. Pasha also said that in 10 ten years are most likely to appear major risk like cyber-attacks.

Mr. Madalin Vasile, System Engineering Manager, Fortinet identified the lack of staff and the huge amount of data the main vulnerabilities in the face of cyber-attacks. In order to resolve this, Fortinet offer technologies that reduce the risk with the use of A.I algorithms that can detect faster cyber-attacks. He mentioned that one of their strategies is to put traps for attackers and also mentioned that their product reduces false positives.

Mr. Liviu Arsene, Global Cybersecurity Researcher, Bitdefender, talked about the term “policies” and the importance of it. Because is a huge difference between reality and expectations the policies always need to be re-evaluated and well examined. In order to highlight the importance of a good policy, he offered as example the impact of Covid-19, how the employees needed to go remote and then appeared a lack of security due to a bad planning. Furthermore, he underlined the idea that strategies can only prepare us for known threats, but cannot do much against the new ones.

Mr. Ovidiu Neghina, CyberSecurity Sales Specialist, Cisco România talked about how the security does not make any easier to develop a product, how are so many vendors and takes a lot of time and people in developing a secure product. He also presented how in our days are so many threats by passing to 5G technology or working with huge amount of data. In order to prevent security threats and make it easier to secure products Mr. Ovidiu Neghina presented Cisco SecureX as a solution.

Mr. Andrei Popisteru, Security Engineer, Check Point Software Technologies talked about the developing process of a product and how the security task in the end part of process. He said that a good practice for security would be to "shift left" the security task in the developing cycle and more exactly to put the security process at every step. He presented the best practices for a secure a product through team training to develop a secure code, track security issues or inject failure to ensure that security is hardened.

Mr. Daniel Pisaru, Chief Commercial Officer, Safetech Innovations during his presentation focused on a few main ideas that are a good practice in cybersecurity namely: we need to move from existing normal to the new normal in security, we need integrated platforms and get rid of non-integrated security tools, human factors. Behavioural intelligence plays an important role in detecting and preventing cyber-attack and we need readiness for digital transformation challenges. He highlighted that we need to focus on human factor, to train and educate people to face cyber threats.

Mr. Matias Bevilacqua, Technical Manager, Mandiant, stressed that the customer fails in securing the product and he presented best practices to prevent that. Firstly, he talked about the bridges that allow security threats and the general malware. Then he continued with some of the best practice, namely to always be prepared for your strategy to fail, to focus on detection and to put more resources in security.

Emerging technologies: IoT, Blockchain, Machine learning, Cloud computing & Quantum Computing

Mr. Florin Vidu, Head of Information Security Department, ICI, presented the challenges and solutions in the field of cybersecurity, with focus on the activity of the SOC run by the Institute. The first challenge is the reduced interoperability with the national and international systems when responding to the threats. To counterbalance this issue, ICI created this SOC that can be used by various entities. The main services offered are consulting services, development of customized security procedures and consulting services such as data loss protection and insider threats.

Assoc. Prof. PhD. Eng. Gabriel Raicu, Vice-Rector for Scientific Research & Innovation Constanța Maritime University presented the versioning for massive scale information integration as a paradigm shift in cloud computing resilience. The Constanța Maritime University is the first in Romania to consider the urgency of cybersecurity in maritime industry. There is a need to develop lectures for the maritime cybersecurity related. The university partnered in 2017 with the IMO Maritime Safety Division, Romania Naval Authority and other relevant entities and drafted the first outcome of the Black Sea Maritime Security Conference, where the main topic of discussion was the measures to increase the maritime security. They started in 2017 because there was a trigger in urgency of the operational and research activity on cybersecurity. The University published a study on the cyber security risks related to the novel coronavirus COVID 19, which explores and discusses some of the current events. The Constanța Maritime University uses the MISP platform to share knowledge for students training and interinstitutional cooperation. Mr. Raicu also conducted a research on the evolutionary cyber threats in energy security, which is considered the base for economic, environmental and social pillars of sustainability.

Mr. Cristian Roșca, Senior Sales Executive, Public Sector, Google, presented the way AI has helped entreprises adapt quickly to moments of change. The current trends in economy are showing significant shifts in demand, increased costs pressures, supply chain uncertainty, spike in customer support cases, virtual work for continuity of operations and accelerated digital transformations. The pandemic is impacting how industry is conducting business, in some industries AI spend will actually increase. Some of the most affected industries are retail , financial services, manufacturing, healthcare and life sciences, media, entertainment and gaming, as well as public sector. Mr. Roșca suggested in his presentation that AI can be the solution to all these problems.

Mr. Adrian Badea, CyberSecurity Business Development Manager, S&T Romania presented the emerging security technologies for the Romanian market. Some of these technologies are cloud security, operational technology security, IoT security, ML and security and automation response. Mr. Badea further underlined that the perspectives are different between operational technology and information technology. While the first manipulates physical things, is specialized and maintains the safety and availability, the second has a different order of priorities, the most important being the confidentiality. He further underlined that the threat actors are innovating, with AI-based malware creation, self-learning for malicious actors and automated malware delivery.

Mr. Cătălin Mironeanu, Lecturer, "Gheorghe Asachi" Technical University of Iasi, delivered a brief presentation on the understanding the attack chain, because smarter security starts with understanding how cyber criminals think. There are seven steps in a cyber-attack: recon, weaponize, deliver, exploit, control, execute and maintain. Today, the security teams are trying to cope with the continuous development of the technology, such as multi-cloud, virtualization, IoT. Meanwhile, the cyber criminals underwent their own technological development, making the attacks faster and more difficult to detect. In this current environment, the security teams are required to work smarter rather than harder. Traditionally, the security teams were focused on a handful of attacks, but now they have spread to all the elements of the system. The research in the university is focused on the first step, namely the recon. He then presented a diagram of the attacks and threats. Manual threat correlation includes an analyst who identify manually the attacks. The objective is to mitigate the attacks. There are four types of correlation approached: field comparison, rules-based matching, fuzzy matching and machine learning. No cybersecurity approach is completely safe. Investing in a more advanced threat correlation approach wil increase the level of effort required for threat actors to evade detection.

Prof. dr. Udo Helmbrecht, former executive director of ENISA, delivered a short presentation on the quantum computing and cybersecurity. A realistically usable quantum computer will be available in 10-15 years at the earliest. Quantum computing will not replace classic computing and there are still a number of physical and technical problems to be solved, including error correction. Companies, governments and academia already have to deal with quantum technologies today.

Mr. Adrian Aron, Technical Security Architect, Cisco România, offered a presentation on how CISCO uses machine learning. One practical way to apply machine learning is at the endpoints, on laptops, mobile devices, anything that runs a software. Detecting threats with industrial networks requires understanding of both IT attacks and industrial control system processes.

Mr. Derek Middlemiss, Head of Security Solutions, Engineering EME Check Point Software Technologies, presented a few ideas on security of the cloud. Prior to COVID-19, cybersecurity was a top 5 global concern, with 46% of companies affected and 36% of consumers globally lost their data. Post COVID-19, our cybersecurity challenge will only get harder for a series of reasons. First, the detection mentality which is not compatible anymore with the speed of attacks. Secondly, we are not protected against current attack levels. Most enterprises are using Gen 3 solutions focused on intrusion prevention, while the attacks are now at Gen 6 on nano security. Thirdy, there is too much complexity in our systems, with great amount of data and an exponential increase in the alerts. Fourthly, we now have to secure the cloud, an entirely new realm.

Mr. Radu Stanescu - CEO Sandline, discussed about the psychology in cybersecurity and AI. Cybernetics was defined in 1948 by Norbert Wiener as “the science of control and communication. In the animal and the machine”. Humans create further levels of cyberspace as we know it today as an extension of their own cybernetic system.

Information Sharing and Analysis Centers (ISACs): necessity or opportunity

Information Sharing and Analysis Centers (ISACs) provide an important resource for gathering information on cybersecurity issues (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis. European legislations like the NIS Directive and the Cybersecurity Act nourish the creation of sectoral ISACs and PPPs within the EU. The NIS Directive among others separates the operators of essential services in sectors and tasks the operators to implement requirements on incident reporting. Creating ISACs at national level could further assist with the implementation of these provisions.

Speakers in the ISAC panel were, Mr. Cristian Cucu, Strategic advisor on IT and cybersecurity, NUCLEARELECRTICA, Romania, Mr. Jeffrey Bonvicin, Senior Advisor with the Pacific Northwest National Laboratory, Washington DC, USA, Mr. Dan Tofan, Security Program Manager at Secureworks, Ms. Lucie Usher, Intelligence Officer, FS-ISAC, Mr. John Morgan Salomon FS-ISAC Regional Director for Continental Europe.

Following the presentations made by representatives of FS-ISAC on the ISACs and Information Sharing, Sector Resilience Building via Information Sharing and Collective Defense, discussions continued on the opportunity to create an ISAC on the energy sector in Romania.

Mr. Cucu expressed the interest of creating an ISAC on the energy sector at the level of SN Nuclearelectrica SA. Discussions and debates took place on the fundamental mechanisms and ideas underlying a sectoral ISAC as well as the exchange of good practices and useful information for the realization of a national ISAC.

This panel created the necessary organizational framework for the exchange of expertise and experience, which helped to accumulate new information useful for the development of national interests in the field of information sharing and analysis centres.

Special Session: Cooperation between state, private and academia: the US models

The special session was built around the experience that the speakers have gathered in the endeavor to make the cybersecurity ecosystem in their area a place of cooperative and problem-solving, where bright ideas and the means to implement them come together in a highly-productive manner.

Mr. Sabin Popescu, Head of Analysis, Policies and Cooperation at CERT-RO started by underlining that the main goal of change in the way different entities interact with and support each other would be keeping Romania's technology professionals from leaving the country at such a high rate. The successful model of the United States has both enough similarities and differences to help create a unique perspective on what Romania's approach should be.

Mr. Shawn P. Murray, Chief Academic Officer at Murray Security Services, emphasized the importance of the partnership between the United States and Europe and shared that the idea of collaboration is what defines the strategy that they contribute to the Cyber Security ecosystem with. Non-formal meetings between professionals, roundtables where leaders can learn about Government grants, events for academia, all encourage people to reach their full potential by communicating and solving real-life problems.

Mr. Vinnie Persichetti, Director of Cybersecurity Programs for the Colorado Springs Chamber of Commerce and Economic Development Corporation presented a unique way of igniting a change in the community of Cyber Security. The case of his city, whose Governor learnt from the cooperation between the Government and specialists in Israel, has a lot to teach us. By duplicating the model, they managed to align ecosystem organizations to ensure resources and initiatives are optimized, to attract investors and professionals in order to help with economic growth and to augment regional capacity by creating a secure and vibrant cyberspace for residents, businesses and the public sector.

A different perspective was introduced by **Mr. Jason Pennington, Executive Director of the Indiana IoT Lab**, who presented the way a suburb started growing in 1999 and became a smart, liberal and entrepreneurial center of technology in Indiana. His organization was created as a public-private partnership that tried, together with academia, to build an ecosystem that would improve the city. The IoT Lab is an innovation-driven environment that provides access to equipment and a modern workspace for the emerging Internet of Things sector. Entrepreneurs and start-up companies are helped to evolve their ideas with resources such as marketing or HR coaches, bigger organizations or young student talents.

Further, the point of view of an educational institution was highlighted by **Mr. Bill Tomeo, Cybersecurity Instructor, Odyssey Early College and Career Options**. He stated that no one woke-up deciding to work in cyber, so attracting the students by picturing the diversity of jobs and early exposure to opportunities in the field are needed in order to create a "cybersecurity workforce pipeline". The objectives of the career pathway at his college are improving the economic futures of the students and offering options for career placement and post-secondary education with the help of the industry in the area by providing opportunities such as workshops and internships.

Dr. Marc Rogers, Executive Director of Cybersecurity Programs at Purdue University presented the effects of a collaboration between a university and law enforcement: students see a new possible pathway in life and law enforcement institutions secure future workforce-ready employees. A few of the challenges that his organization had to deal with where convincing faculty members to participate, building trust with partners, covering costs for development and delivery, being agile enough to move at the speed of industry or law enforcement and dealing with ambiguous, as well as standardizing training. **Mr. Joel Rasmus, Managing Director of CERIAS** from the same university completed the picture by saying that cybersecurity is not the domain of a single discipline and it requires diversified education, thus classes are taught in 8 different colleges and weekly seminars for observing cases are a way of permanent exposure to industry.

Mr. Jamil Jaffer's institution, the National Security Institute at George Manson University's Antonin Scalia Law School proposes providing policy recommendations for decision makers by hosting events, publication production and media representations as a way of academia involvement. America's most pressing national security challenges are the rise of China and preserving US technology innovation leadership and by featuring a series of events, papers and policy engagements centered on these two imperative challenges, they helped contain them. A judicial training program consisting in educating judges on addressing the threats posed to US national security and the American economy are also an innovative way of engagement.

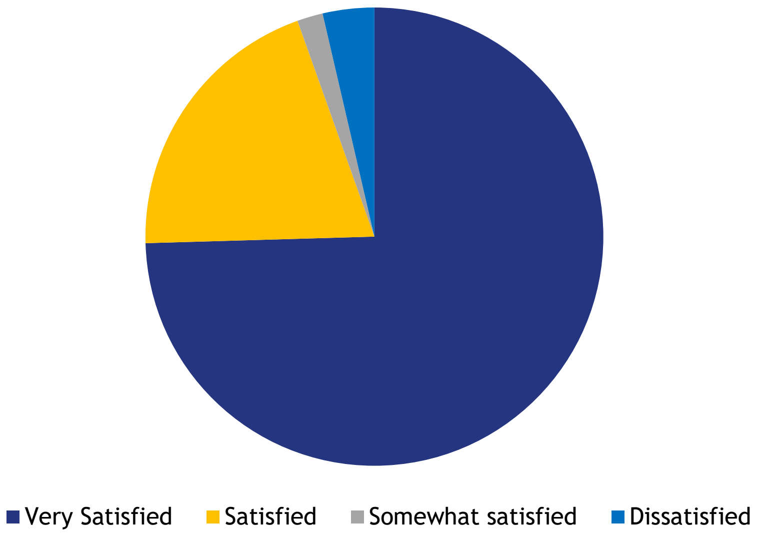
Professor Anupam Joshi, Director of Center for Cybersecurity and The Cyberscholars Program of University of Maryland, Baltimore County talked about how the issue of underrepresentation of women in cyber is handled by partnerships with corporate support. They received a $3.5M grant for their work on the matter and have a strong relation with the National Security Agency that includes research and teaching collaboration, student mentoring and ongoing recruiting activities.

Transforming former militaries into cybersecurity professionals, having in mind the similarities between the fields, was an idea proposed by **Mr. Jerry Chappee, Defensive Cyber Operations Strategist, Air Force Satellite Control Network.** His institution holds meetings for cybersecurity enthusiasts where people of different backgrounds and interests come together to exchange information and find solutions. Capture the flag events where the Space Force competes and local companies compete against high-schoolers are a way of not only identifying potential talent, but also empowering the youth, as they realize what their potential is and that a career in the Cyber Security field can be an option for them. This is in Mr. Chappe's mind, a trait of good leaders: they need to groom the ones coming from behind to be able to replace them, or they failed.

In conclusion, similarities between EU and USA were identified by some of the speakers with regard to the approach in the cyber field: the lack of CSEC workers, the increase in attacks and that the government cannot handle the issue alone. These should be viewed as a motivation to try and implement the success stories that have been presented in order to obtain a solution to the problems we all face.

Participants' feedback

The overall satisfaction with the conference



General comments

"Well chosen presentations! Congratulations!"

"Great event."

"Like most of the panel's findings, the need for cybersecurity education is vital. Good look to all, it was a pleasant and very useful conference."

"There should be time reserved for Q&A."

"The models from the US are applicable in Romania, but we need funding."

"Prolonged schedule, more marketing than technical, only general things not very specific details on important topics like NIS."

"The use of parallel session is not the best, given that the audience might be interested in multiple sessions, and the parallel running prevents us from listening to other sessions we are interested in."

"It would have been great if more time was assigned for Q&A. Maybe less topics but with more time assigned to each?

"Very interesting sessions with a lot of useful info."

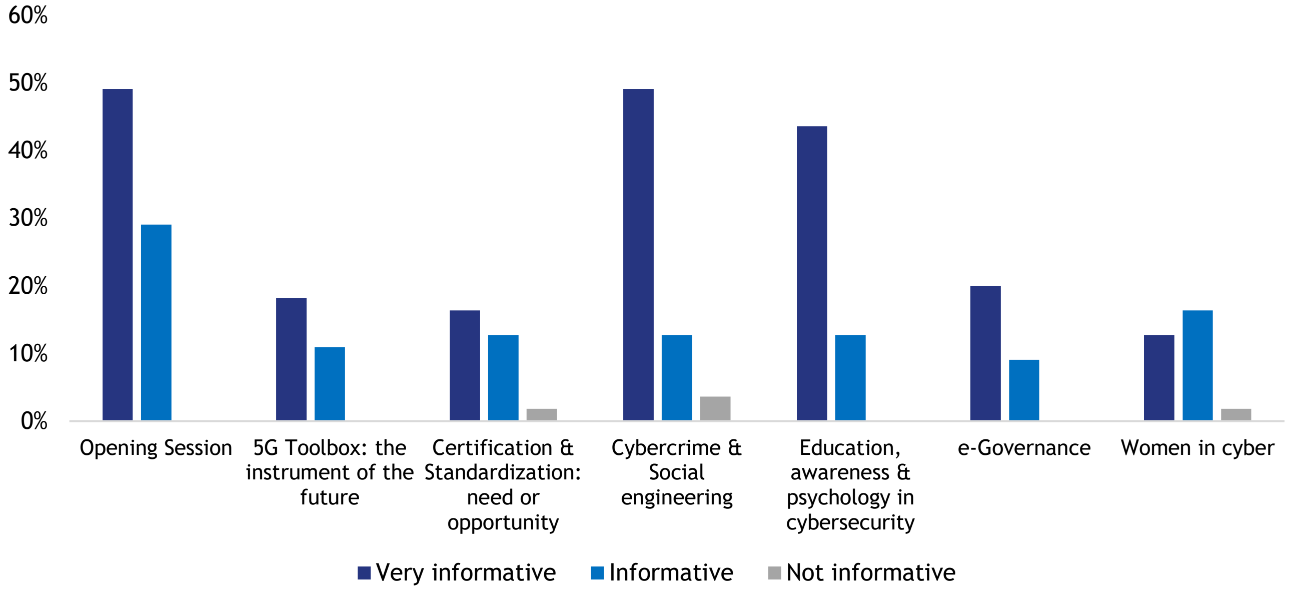
"The sessions were very informative. The presented topics were up to date and interesting."

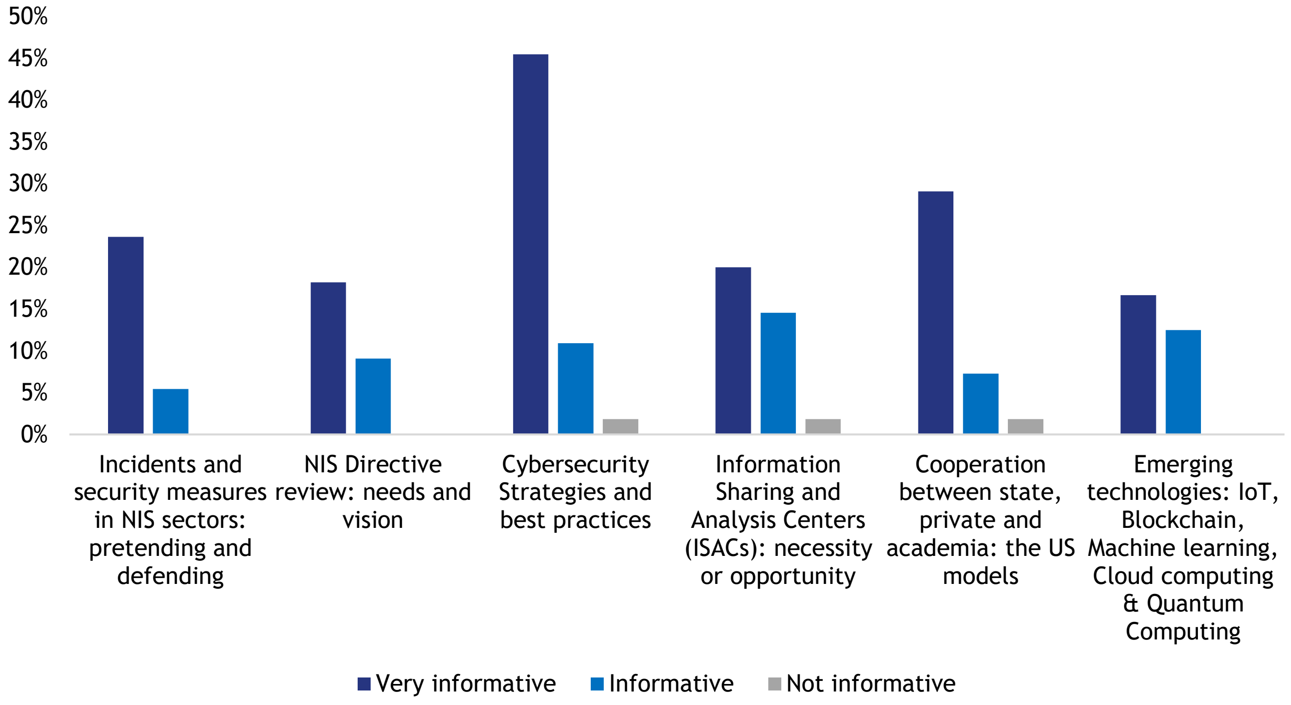
"Great sessions in the online terms."

"Good orchestration of presentations, each adding up to the previous."

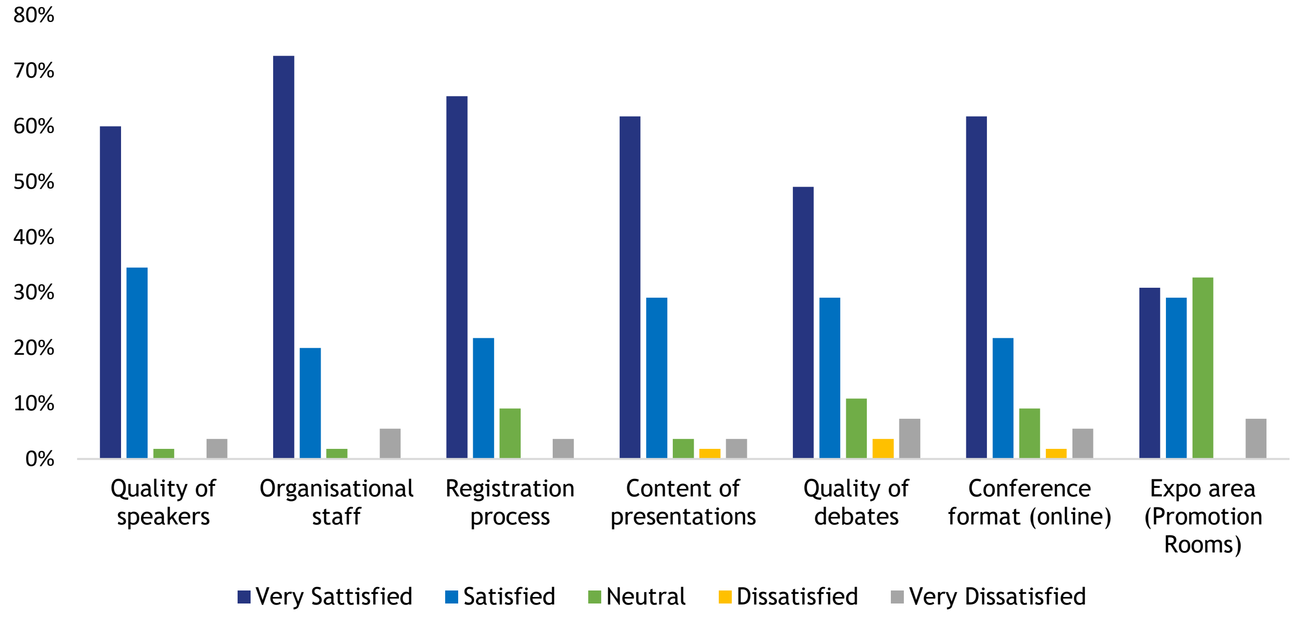
"Some discussions were very interesting and would have required a section on their own. Maybe do more of these sessions?"

The most informative sessions





Level of satisfaction with the organization



Comments on the organization process

“Amazing panels.”

“Great event, even online!”

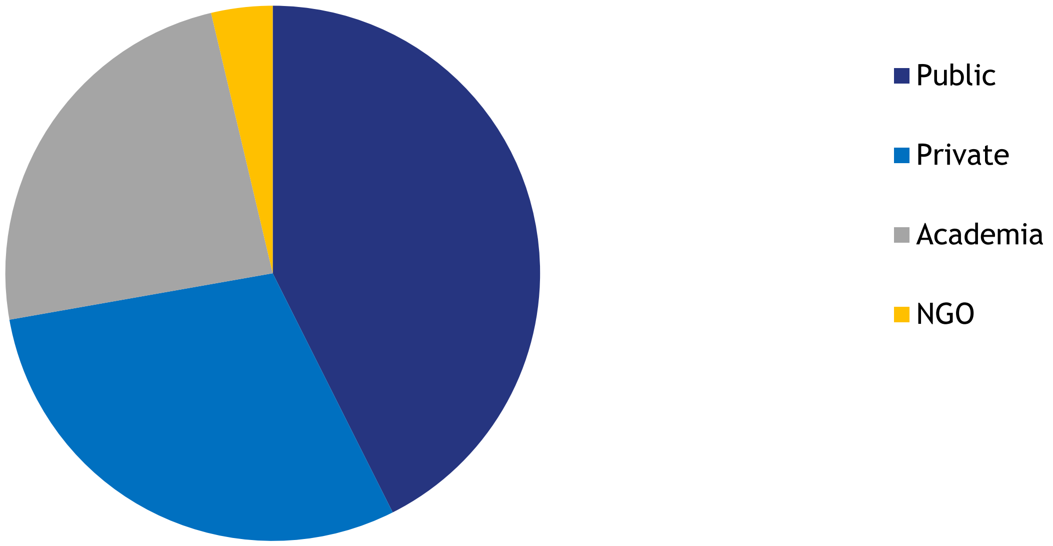
“The conference was good, but I would like the classical format in the future.”

“I rather prefer the personal contact than online, but I understand the reason of organizing on this way. You did a great job.”

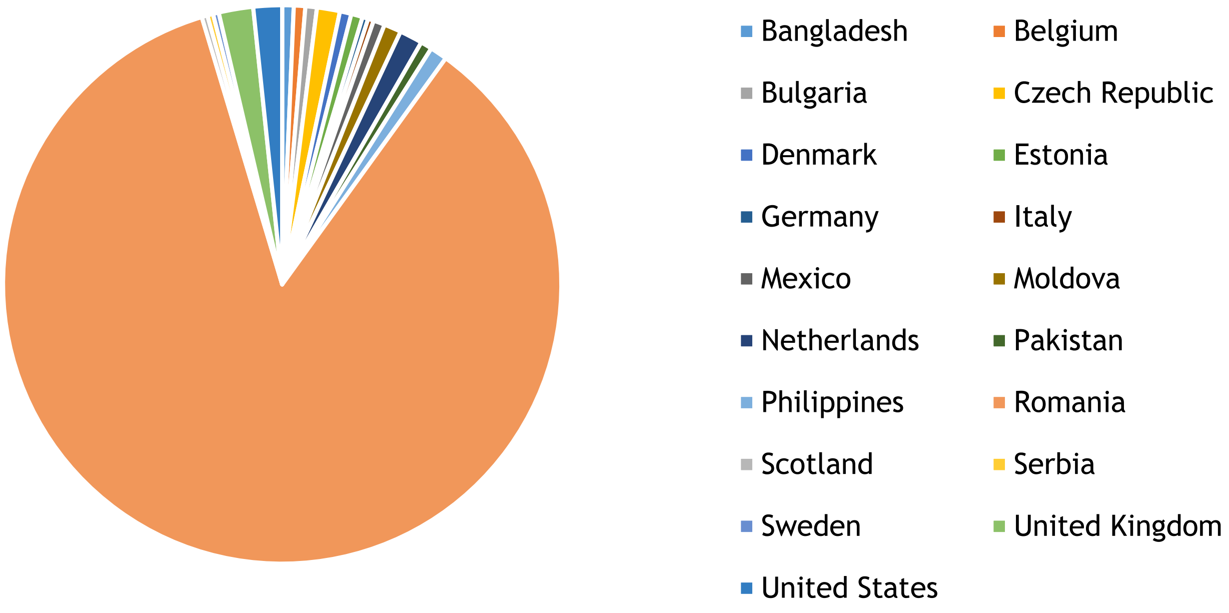
“Great people with great ideas.”

Attendee stats

Sector of activity



Country



Our Partners

paloalto®
NETWORKS

RaISA
Romanian Association
for Information Security Assurance

Check Point
SOFTWARE TECHNOLOGIES LTD.

Bitdefender®

safetech
Your trusted security partner

Business
Services
orange™

s&t
25
TWENTY FIVE Years
of IT EXCELLENCE

www.cert.ro

☎ +40 316 202 187

cooperation@cert.ro

8-10 Mareșal Averescu Blvd., 011455 Bucharest, Romania
22 Italiana Str., 020976 Bucharest, Romania