Outcome Report

ACKNOWEDGMENTS

The International Telecommunication Union (ITU) has produced this report. The ITU would like to express its gratitude and appreciation to the Ministry of Transport, Information Technology, and Communication, as well as the State e-government Agency of the Republic of Bulgaria. The ITU would also like to thank all participants for their presentations and expertise that they contributed to this forum, the moderators for coordinating proceedings, as well as Ms. Rūta Jašinskienė, ITU Consultant, and Mr. Damian Kashfia, ITU for putting this report together.

1. INTRODUCTION

1.1 Background

The ITU Regional Cybersecurity Forum for Europe and CIS regions was co-organized by the International Telecommunication Union (ITU) with the Ministry of Transport, Information Technology and Communication of the Republic of Bulgaria and the State e-government Agency of the Republic of Bulgaria, on the 27-28 February 2020 at the Grand Hotel Sofia, Bulgaria.

This Forum was organized within the framework of the ITU Regional Initiative for Europe on Enhancing Trust and Confidence in the use of ICTs, and the ITU Regional Initiative for CIS on the Development and Regulation of Info Communication Infrastructure to make Cities and Human Settlements Inclusive, Safe, and Resilient, adopted by the ITU World Telecommunication Development Conference 2017 (WTDC-17).

The sessions composing the Forum were:

- Session 1: Cybersecurity Priorities for Governments
- Session 2: National Cybersecurity Strategy: A Roadmap to Meaningful Actions
- Session 3: Data Protection – Legislation and Regulations in Response
- Session 4: 5G: Tackling the Security Challenge
- Session 5: AI: Positive or Negative Impact to Cybersecurity
- Session 6: Certification Frameworks for Digital Security
- Session 7: eSIM and IoT Security Challenges
- Session 8: Incident Response and Management
- Session 9: Building Capacity in Cybersecurity
- Session 10: Cooperation in the Region and Beyond

1.2 Participation

This event brought together national and international stakeholders in cybersecurity for information exchange on trust and confidence building, enhancing awareness of the risks and constructing dialogues around the cyber-threat landscape and current safety practices. The attendees included national policy and decision makers, Computer Security Incident Response Teams (CSIRTs) managers, legislators, regulators, service providers, academia, civil society and

other relevant cybersecurity professionals from European and CIS region countries. The forum brought together 150 individuals from 28 countries representing 72 organizations.

1.3 Documentation

All relevant documentation for the forum, including the agenda, panel presentations, and background information are identifiable from the event webpage at https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2020/CSF/SofiaBG.aspx.

1.4 Opening Address

The opening ceremony of the forum started with opening remarks by H.E. Andreana Atanasova, Deputy Minister of Transport, Information Technology, and Communications of the Republic of Bulgaria, in place of the ministry's minister, H.E. Rossen Jeliazkov. The Deputy Minister. ~~highlighted the need to work in strengthening regional cybersecurity through innovation, cooperation, and knowledge sharing as well as exploring the capabilities of emerging technologies.~~ The deputy minister's speech can be read in full at the aforementioned link found in Section 1.3 of this report. H.E. Atanasova's remarks were followed by Mr. Jaroslaw Ponder, Head of the ITU Office for Europe, ~~who touched upon the cost of cybercrime reaching in the trillions of dollars by 2030, thus necessitating placing cybersecurity as a key priority for stakeholders, as well as underscoring the importance of incorporating cybersecurity in political agendas as a key objective of the ITU~~who mentioned a multitude of activities the ITU has in relation to cybersecurity. Mr. Ponder underscored the ITU's emphasis on interoperability, accessibility, and security. Mr. Ponder went on to articulate the importance of global and regional cooperation, with particular respect to the implementation of the ITU Regional Initiative for Europe and CIS on Cybersecurity.

Following the opening remarks of H.E. Atanasova and Mr. Ponder, a special address was given by Ms. Jelica Krišto, Minister Counselor at the embassy of the Republic of Croatia in Bulgaria, on behalf of the E.U. presidency being held by Croatia at the time of the forum. Ms. Krišto adressed the priority of maintaining security for EU citizens, including hybrid and cyber threats. Ms. Krišto then informed on the necessity of securing the union to foster growth, innovation, and security, as well as how implementing the EU's toolbox for cybersecurity will greatly serve to further these interests.

A special address was then provided by high-level guest H.E. Marian Murgulet, Secretary of State – Chief Information Officer of Romania. In his statement, H.E. Murgulet detailed how the Digital Europe program highlights European interest in the digital domain and the growing need for cooperation and trust to maintain cyberspace as a common good.

2. [LL1]SESSION 1: CYBERSECURITY PRIORITIES FOR GOVERNMENTS

The objective of this session was to facilitate a high-level discussion on hot issues in cybersecurity in relation to emerging technologies including blockchain, AI, and IoT.

Session moderator:

- Dr. George Sharkov, Director, European Software Institute – Center Eastern Europe Head, Cybersecurity Lab, Sofia Technology Park, Republic of Bulgaria

Panellists:

- Mr. Arnaud Taddei, Technical Director of Standards and Architectures, Broadcom Inc.;
- Mr. Jorn Erbguth, Legal Tech, Blockchain, Smart Contract and Data Protection Consultant, Head of Technology Insights, Geneva Macro labs;
- Ms. Daniela Androvic, Senior Advisor for ICT Systems Security, National CERT, Republic of Serbia.

General Findings:

There are a multiplicity of issues in cybersecurity garnering the attention of governments as priorities in the digital area. Among these, include the use of quantum key distribution, which still maintains a deficit of knowledge and awareness. Blockchain technology represents another challenge for governments through its decentralized nature that can easily create a domino effect of security dilemmas if one part of the chain is compromised, thus presenting a difficult balancing act between privacy and security. Indeed, the rise of technologies such as blockchain and AI present an array of vulnerabilities and threats necessitating cooperation and information exchange to face digital challenges.

Key points

- Quantum Key Distribution is a developing area with several countries currently exploring the subject, but there is still a lack of knowledge.

- Quantum computers already exist and is allowing us to discover what the human mind is not capable of discovering on its own.
- Blockchain security is decentralized security and this blended security approach works more effectively than traditional networks (the network continues to operate even if certain segments stop functioning)
- In a blockchain, it is not possible to manipulate transactions due to the heavy use of cryptography, but weaknesses remain:
    - Possibility to remove/steal transactions
    - Being unable to restitute lost "personal key"
- A major challenge regarding decentralized security is that a single intrusion could have a cascading effect; creating a fake certificate, it could easily multiply inside network.
- The dueling concern between transparency and privacy is another major issue.
    - A more private blockchain enhances the allure of using such technology for money laundering or other illegal activities.
    - Increased transparency could lead to the abuse of accessible data. Security should be balanced and integrated with privacy.
- Many private entities use their own blockchain infrastructure due to a lack of trust in governmental networks as well as avoiding control and regulation thus creating an attractive environment for criminal use.
- Current regulation is not technologically neutral and has friction points with decentralized systems.
- There is a strong need for AI cybersecurity, particularly in relation to behavioral analytics and vulnerability threats detections.
- Preventive security measures are not sufficient; active detection of threats and soft sports within systems should be enhanced
- Cooperation between the public and the private sectors should be encouraged as it could bring added value to awareness raising in cybersecurity issues

3. Session 2: National Cybersecurity Strategy: A Roadmap to Meaningful Action

The objective of this session was to understand how countries review their national cybersecurity strategies and what effective tools they are using to do so.

Session moderator:

- Mr. Marwan Ben Rached, Technical Officer – Cybersecurity, ITU

Panellists:

- Mr. Ruslan Abdikalikov, Vice Chairman of Committee of Information Security, Ministry of Digital Development, Innovations, and Aerospace Industry, Republic of Kazakhstan
- Mr. Arman Abdrassilov, GR Director, Center for analysis and investigation of cyberattacks (TSARKA), Republic of Kazakhstan;

- Ms. Natalija Veljanovska & Ms. Solza Kovachevska, Inter-Ministerial Working Group on National Cybersecurity Strategy, North Macedonia;
- Mr. Adel Abusara, Project Coordinator, Geneva Centre for Security Sector Governance (DCAF).

General Findings:

Countries have highlighted the importance of investing in national cybersecurity improvements. In this light, countries have created a formalized legal structure and set up security coordination and operation centers, and national cybersecurity councils.
However, issues remain to be addressed, including lack of infrastructure, human capacity, and lack of awareness. Due to cybersecurity always being in flux, strategy must always be in constant change as well. Equally important to bear in mind is the budgeting of cybersecurity planning and coordination between relevant active stakeholders to successfully implement strategies and define KPIs involved.

Key points

- Kazakhstan has invested in national cybersecurity improvement through
    - Elaboration of regulatory legal framework that launched a national information security coordination center, operational center of information security, set up standards for some professions.
- Kazakhstan's efforts helped to raise its global cyber index significantly, but serious issues remain including insufficient infrastructure, lack of human capacity, low awareness rising.
- North Macedonian population's awareness of cyber threats is very low
    - A high number of citizens are not familiar with cybersecurity risks.
- North Macedonia created a cybersecurity strategy involving different parties, including the public sector and academia.
    - Priorities are the establishment of the National Cyber Security Council and the improvement of cybersecurity education.
- Meaningful cybersecurity will include a legal framework including the competent authority that will be involved in the drafting of such framework.
- Cybersecurity strategy must be a lifecycle due to the ever-changing nature of cybersecurity.
- Mandates should be revised at least every two years.
- Key factor for strategy and action plan development is defining the budget.
- The action plan should work parallel to strategy to not lose time for implementation.
- When donors finance actions, a compromising dependency can be formed as well as overlapping actions if donors do not coordinate actions.
- It is very difficult to estimate the budget needed for action implementation.
- It is challenging to find the responsible organization for implementation and define KPIs, especially in a timeline.
- Involve the private sector in strategy building and transfer knowledge into the public sector, is an opportunity to be tapped.

- ITU published guidance materials on how to develop a national cybersecurity strategy and countries are encouraged to make use of the guide and to connect to ITU for assistance.

4. SESSION 3: DATA PROTECTION – LEGISLATION AND REGULATIONS IN RESPONSE

The objective of this session was to develop a conversation around GDPR, ICT regulations and laws currently in place as well as examine whether such legislation is responding to current needs as well as what needs to be done better.

Session moderator:

- Mr. Farid Nakhli, Programme Coordinator, ITU Regional Office for CIS

Panellists:

- Mr. Ventsislav Karadjov, Chairman of the Bulgarian Commission for Personal Data Protection & Deputy Chair of the European Data Protection Board (EDPB);
- Ms. Nathalie Devillier, Grenoble Ecole de Management, Member of the Expert Group on Liability and New Technologies, European Commission;
- Mr. Andreas Iacovou, Security Analyst, National CSIRT-CY, Republic of Cyprus.

General Findings:

Key to successful implementation of laws and regulations regarding ICTs and data protection is education and awareness building of the public regarding the use of technology and algorithmic calculations in relation to themselves with the aim of creating a secure cyber realm.

Regulations should always ensure that, with the ever-evolving nature of technology, that privacy remain central to legislation. In line with privacy protection, the emergence of AI will undoubtedly create issues regarding privacy and civil liability in the event of attacks, thus necessitating proactive actions to be taken now.

Key points

- Personal data protection rules are fit for innovation; GDPR is technologically neutral.
- It is important to educate and explain to the public the purposes of technologies/data used and what algorithms are used.
- The goal of legislation is not to forbid or create obstacles but provide a secure digital environment and protect citizens data against abuse.
- There is a need to raise the knowledge level of the society as it is imperative for the public to understand how and why their data could be used or abused.
- Privacy is a long and continuous process. Non-EU countries improve their databases through observing EU legislation.
- EU Guidelines are applicable to national AI technologies. Some requirements increase the cost for developers.
- It is very difficult to keep a balance between technological benefits and privacy violation. The most important element – the purpose of AI use.

- Keeping minimal requirements and standards are vital but it is not necessary to constantly adopt new legislation for every new technology, rather it policies can be updated as needed.
- A growing issue will be privacy and civil liability in relation to AI security threats.

5. SESSION 4: 5G: TACKLING THE SECURITY CHALLENGE

The objective of this session was to understand the cybersecurity implications of rolling out 5G solutions with the presentation of use cases.

Session moderator:

- Mr. Jarolsaw Ponder, Head of the ITU Office for Europe, ITU

Panellists:

- Dr. Vassiliki Gogou, Co-Chair, 5G Cybersecurity Working Group, BEREC;
- Mr. Danijel Vlahovic, Head of Spectrum Monitoring Department, HAKOM, Republic of Croatia;
- Mr. Sergey Stefanovich, Head, Information Security Department, Beltelecom, Republic of Belarus;
- Ms. Visiola Pula, Analyst, Cullen International.

General Findings:

As 5G technology rises into prominence, the EU has created a toolbox comprising a holistic approach to mitigating risks as well as prescribing recommendations for strategic and technical measures regarding 5G security. As 5G technology is incorporated into emerging technologies, education and capacity building will be key to maintaining security in a post 5G world as human beings will be the weakest point of the security chain. Key to ensuring 5G security will also be to avoid dependencies on a single supplier for ICT services. Countries may also implement bans or restrictions on certain suppliers as another security measure.

Key points

- Currently, 10 countries have implemented 5G in their digital environment
- 5G holds benefits, especially for the health, energy, and transportation sectors.
- EU Toolbox for 5G Security published in 2020. Based on EU coordinated risk assessment of 5G-network security, the toolbox lays out a range of security measures to mitigate risks effectively and ensure secure 5G networks are deployed across Europe.
- EU Toolbox is a holistic approach comprising detailed mitigation plans for each of the identified risks and recommends a set of key strategic and technical measures, which should be taken by all Member States or /and Commission.
- Only a few countries meet the set criteria in the EU toolbox while the majority are not ready to implement[LL2] the recommended technical measures.
- Prediction of mass connectivity of machines to 5G networks in near future.

- Information sharing and communication, as well as sustainability and diversity, are key points in 5G development.
- In the security chain, the weakest point is human, while even strong cybersecurity systems can be broken or damaged by insiders.
- The most effective measures against internal risks is education; continuous learning (including assessment) is especially important to build resilience
- Support of certification for ICT services and 5G core components. It is essential to avoid dependence of one supplier.
- Common digital security measures [LL3]could help harmonize countries' initiatives and efforts.
- Recommendation for West Balkan countries: look through the EU toolbox's elaborated requirements and understand what they need and find help. Improve cooperation and information sharing.
- No common practice on 5G security measures across the world. The strongest measures could be applied in the USA (direct ban) while other countries may ban equipment from certain suppliers or require an authorization for certain equipment.
    - Italy: There is a notification system where there is an obligation to notify relevant authorities before completing agreement of purchase of specific ICT technology; this policy would only concern sellers outside of the EU.
    - Sweden: An authorization to use transfer lease for radio transmitters could be agreed if there is no danger found to national security, which would be relevant to full spectrum, not just 5G.
    - United Kingdom: High-risk vendors must be excluded from operators' networks.
    - Germany: The implementation of mandatory certification of critical components; BNetzA security catalogue.
    - United States of America: A ban on technologies posing an unacceptable risk with exception only for support of equipment that is already in the country.

6. Session 5: AI: Positive or Negative Impacts to Cybersecurity

The objective of this session was to take stock of the current use of AI in the field of cybersecurity and share perspective on the cybersecurity challenges that AI brings forward as well as how these challenges may be addressed.

Session moderator:

- Mr. Adel Abusara, Project Coordinator, Geneva Centre for Security Sector Governance (DCAF)

Panellists:

- Dr. George Sharkov, Director, European Software Institute – Center Eastern Europe Head, Cybersecurity Lab, Sofia Technology Park, Republic of Bulgaria;
- Mr. Marwan Ben Rached, Technical Officer, Cybersecurity, ITU;
- Mr. Goran Gotev, Senior Policy Manager, BSA.

General Findings:

The growth of AI has presented society with numerous benefits and detriments as a result of this emerging technology. Among the major issues in AI are ethical challenges related to the type and quality of data needed to train AI; however, entities such as the E.U. are implementing ethics guidelines for AI. Indeed, AI has great potential for enhancing cybersecurity through machine learning, but misuse of such capabilities could produce great damage as well. This is due to the development processes of AI for illicit purpose moving at a faster rate, due in part to a lack of legal limitations.

Key points

- Two aspects to be addressed:
    - AI for cybersecurity (how to employ AI to increase cybersecurity in general)
    - Cybersecurity for AI (how to protect AI technologies).
- The biggest challenges and discussions concern the ethics and quality of data used to train AI. Fostering AI to use anonymized data could lead to incorrect AI working (biasing decisions).
- Lack of data for machine/deep learning stops AI development.
- Ethics guidelines for trustworthy AI is available in the EU since 2018. Requirements are set up in 7 areas:
    - Human agency and oversight,
    - Technical robustness and safety,
    - Privacy and data governance,
    - Transparency,
    - Diversity, non-discrimination and fairness,
    - Societal and environmental well-being,
    - Accountability
- Use of AI and an application of neural networks could bring enormous added value for cybersecurity, but misconduct could bring huge damage.
- Currently, machine learning is used widely in translation, assistance to clients (chat boxes, call centers), and health sector for accurate diagnoses.
- Machine learning could be valuable for cybersecurity detecting spam, vulnerabilities, and increasing resilience, but could serve malevolent purposes such as DDoS attacks, site scraping, vulnerability scanning, spam, and fraud.
- Development of AI for illegal or malicious purposes is faster than legal development due to a lack of legal limitations and big financing.
- The challenge: Widespread use of IoT with different OS and low qualification in their harmonization. Development capabilities and taxonomy is urged.
- Standardization and data processing is required. Still, systems using AI are enabled to take decision independently, but human approval should be mandatory.

7. SESSION 6: CERTIFICATION FRAMEWORKS FOR DIGITAL SECURITY

The objective of this session was to explore the products and services certification frameworks playing an important role in developing trust and confidence towards a safer and more secure internet. This included examining if the adoption of the EU certification framework for ICT digital products, services, and processes could be beneficial to developing countries.

Session moderator:

- Mr. Krasimir Simonski, Deputy Chairperson of the State e-Government Agency, Bulgaria

Panellists:

- Mr. Eric Vetillard, Lead Certification Expert, European Union Agency for Cybersecurity (ENISA);
- Ms. Vilma Tomco, General Director, National Authority for Electronic Certification and Cyber Security (NAECCS), Republic of Albania;
- Mr. Alexander Metz, Partnerships & Communications & Mr. Johan Bloemberg, Software Engineer, Internet Clean-up Foundation, Netherlands.

General Findings:

Digital security certification will only grow in importance as digitalization continues to grow. The process of certification is meant to serve as a process for creating enhanced secure in the digital realm. An increasing number of countries and organizations are coming to understand the importance of digital security certification; however, gaps remain in training practices and knowledge[LL4] *that must be addressed through inter-sectoral cooperation as well as identifying upgrades to implement in digital certification.*

Key points

- EU Cybersecurity Act entered into force on 27 June 2019.
- Certification is becoming a major issue and involves not only countries that have previous experience with cyber certification, but rather includes new countries with burgeoning cybersecurity frameworks as well.
- The main debate is whether certification is more beneficial or brings limitations.
- Certification is not to create limitations or obstacles; it is about making digital services more secure to enhance the security and benefits of the citizenry [LL5]in relation to the digital sphere.
- ENISA is enabling the process of certification, by involving an array of parties, including member states, academy, and industry as well as explaining the added value of certification to stakeholders.
- Current certifications schemes require continued assurance.
- The biggest challenge arises in ensuring smooth transition from existing scheme to a new one.
- The use of e-signature and e-seal are constantly increasing in Albania.

  - 64 services offered by the Albanian Government and numerous financial services provided by banks and other private financial institutions involve e-signature and e-seal, decreasing the load of paperwork and increasing the quality of services.
- Currently Albania has two accredited Qualified Trust Services Providers (QTSP), operating since 2012 and 2013, supervised by National Authority on Electronic Certification and Cyber Security.
- This year Albania is planning to introduce the Law on Remote Authentication aligned to EU standards as well adopt the National Strategy and Action Plan on Cyber Security.
- Awareness-raising campaigns and training on cyber must be developed; unfortunately, the public sector suffers from a lack of qualified staff.
- Strong cooperation between the private and public sectors increases digital security of society.
  - "Web security map" is a free tool that presents how secure public infrastructure is (services provided are scanned, government voluntary gave additional URL) visualizing data on the map.
  - The mission: make the Internet more secure for everyone by adding transparency and public accountability. Exposing vulnerabilities publicly stimulates authorities to react swiftly to correct and improve the situation.

8. SESSION 7: ESIM AND IOT SECURITY CHALLENGES

The objective of this session was to examine whether eSIM could be a solution to recent attacks on IoT, which continues to have a significant impact on industries around the world.

Session moderator:

- Mr. Farid Nakhli, Programme Coordinator, ITU Regional Office for CIS

Panellists:

- Mr. Rossen Naydenov, Expert on Network and Information Security, European Union Agency for Cybersecurity (ENISA);
- Mr. Stiepan Kovac, ITU-T SG17, Administrator, QRCrypto SA;
- Mr. Yuri Kargapolov, CEO of Ukrainian Numbering, Naming and Addressing Operation Center, Consortium, Ukraine.

General Findings:

The fast pace growth of IoT has presented numerous challenges related to IoT security due to the vast digital space of IoT, device interconnectivity, as well as a deficit of expert knowledge on the subject, creating incongruences in security standards and practices. Equally pressing is the inherent hole in security left by IoT developers who tend to be more focused on the competitive aspect of innovation, focusing primarily on functionality. To address security issues, a multiplicity of factors should be engaged, including cryptography and educating stakeholders to enhance resistance to cyberattacks.

Key points

- IoT use is fast growing and assurance of IoT security has become a challenge due to widespread coverage of IoT technology, interoperability of devices, increased connectivity and cascading, lack of expertise (including secure development), unclear liabilities, and fragmentation of good practices and standards.
- The problem is that for developers of IoT, security is not a top priority.
    - The competitive nature of the industry creates a focus on functionality first. Convenience always goes hand-in-hand with increased risk. The biggest risk is IoT without encryption being used for critical activities.
- The minimum standards requirements of certification of IoT security standards are in favour and highly encouraged. This can enable developers to introduce more security solutions and ENISA is seen as the right organisation to contribute to it.
- ENISA provides baseline IoT security measures: policies and organizational measures as well good practice.
- The need to integrate cryptography techniques urges.
- The most important element in assurance of IoT security is education of all involved groups; end-users to stakeholders.
- The goal is to increase the resistance of IoT to cyberattacks, as emerging use of AI will cause more attacks and attempts at decryption.
- Security problems arise when deployment is not well settled.
- Identity management is another problem that is not well addressed in the current functional architecture model proposed by ENISA. Non-resolved identity management issues could cause more illegal access or intrusions.

9. SESSION 8: INCIDENT RESPONSE AND MANAGEMENT

The objective of this session was to explore the good practices that are and can be used in responding to cyberattacks.

Session moderator:

- Mr. Farid Nakhli, Programme Coordinator, ITU

Panellists:

- Mr. Vasil Grancharov, Director of Network and Information Security Directorate, Head of CERT Bulgaria, Republic of Bulgaria,
- Mr. Sharifjon Gafurov, Head of Department, UZ-CERT, Republic of Uzbekistan;
- Mr. Egons Bušs, Executive Vice President, LMT, Latvia;
- Mr. Arman Abdrassilov, GR Director, Center for analysis and investigation of cyberattacks (TSARKA), Republic of Kazakhstan.

General Findings:

Cybersecurity requires a multitude of elements working together to ensure efficient security, including trusted communication nationally and internationally, relevant information, and cooperation between entities at the domestic and global levels. Countries increasingly

understand the strategic need of placing cybersecurity as a priority and focusing on capacity building to create a more secure digital space; regional and international guidelines aid in this effort. Equally important is to proactively search for threats in order to address weaknesses before an attack can take place. Growth in cooperation between the private and public sectors will also play a key role in building the security of public networks.

Key points

- The key elements of successful cybersecurity are timely exchange of relevant information and trusted communication at national and international levels, including international cooperation with the different working groups as well as qualified staff.
- According to statistics, the cybersecurity level in Bulgaria has increased, although some threats such as phishing attacks and malicious code have increased but decrease DDoS and intrusion attacks have also been noted.
    - Bulgaria has implemented multiple European projects that improved services provided by Bulgarian CERT across the country, increased CERT staff capacities, and built components of the national cybersecurity system.
- Among several achievements done in strengthening cybersecurity in Bulgaria recently, the country set the rules regarding reporting of incidents.
- Cybersecurity is recognized as a national priority in Uzbekistan. Accordingly, the legal base was updated and improved, strengthening public sector responsibility for cybersecurity. As a result, the country's cybersecurity index increased significantly.
- National UZ CERT provides practical support for sectorial CERTs, for instance, by detecting and informing about the vulnerabilities in governmental networks and training.
- A strong incident handling process and secure network are crucial elements for mobile operators while CIIs use it or while electronic payments are being made through such networks.
- Enhancement of security and alignment with GDPR grows as operators possess more big data.
- One of the operators' tasks, together with stakeholders, is to explain to customers how new technologies work to provide objective information, to help customers make the right product choices.
- It is important to raise people's awareness that IoT can greatly ease their lives, but it can also be used to engage in illegal activities against them if they are incorrectly configured or purchased from unreliable vendors or suppliers.
- Proactive threat hunting aids in building a more secure digital environment for government organizations as well as for society.
- Private and public sectors' mutual understanding of the problem could lead to perfect results helping in increasing the security of public organization networks and systems.
- The most common risks are use of unlicensed software, lack of updating programs and apps, use of piracy software, and simple ignorance of cyber threats.

10. Session 9: Building Capacity in Cybersecurity

The objective of this session was to examine who are the professionals that need to have enhanced cybersecurity skills as well as the actions being undertaken for the emerging skills that will be needed.

Session moderator:

- Mr. Kamen Sapssov, Head at e-Government Laboratory, Bulgarian Academy of Science, Republic of Bulgaria

Panelists:

- Mr. Kristo Põllu, Deputy Head of EU CyberNet, Ministry of Foreign Affairs, Republic of Estonia;
- Ms. Rūta Jašinskienė, NRD CyberSecurity, Lithuania;
- Dr. Plamen Russev, Executive Chairman of the Board, Webit.Foundation Goodwill Ambassador for Digital Affairs, Republic of Bulgaria;
- Ms. Albena Spasova, CEE Multi Country Industry Solution Executive Education, Microsoft.

General Findings:

Building capacity in cybersecurity requires a multi-pronged approach, which is what the E.U. is striving towards. This approach includes providing technical assistance, incorporating international norms and legislation into capacity building structures, and the protection of rights and freedoms, among others. Indeed, the successful development of capacity building skills will require multi-stakeholder action as cybersecurity is a horizontal issue that affects everyone at every level of society.

Key points

- New technologies boost our lives and we are obliged to continuously learn.
- UE CyberNet was created to
    - Strengthen global delivery, coordination, and coherence of the EU's external cyber capacity building projects;
    - Reinforce of the EU's capacity to provide technical assistance to other countries in the areas of cybersecurity and countering cybercrime.
- EU policy stipulates that cyber capacity building must be based on applicability of existing international law and norms in cyberspace, including
    - Protection of fundamental rights and freedoms.
    - Promotion of a democratic and multi-stakeholder internet governance model.
- Successful development of cyber skills must involve partnership between public and private sector.
- Practical training courses including lessons learned and advanced approaches to teaching methods are welcomed.
- Cyber skills, especially awareness raising and resilience to cyber threats, need to start developing from a young age.

- Cybersecurity is a horizontal issue; it affects everybody.
- Cybercrimes are becoming the most profitable illegal activities, necessitating everyone in the private and public sectors, at the management level and at the lowest position to receive tailored training on cybersecurity.
- Organizational cybersecurity must be empowered, and its level is directly dependent on stakeholders' maturity.
- ITU Centers of Excellence Network (CoE) is a programme aimed at supporting capacity development in ICTs by offering continuous education to ICT professional and executives in the public and private sectors.
- In the European region, there are 6 CoE and in CIS, 2. [LL6]All CoE must meet strict criteria of quality in order to be able to provide specialized training courses.
- CoE covers different topics and cybersecurity is among their priorities. All course material are aligned with ITU policy and standards, meaning that all courses are of high quality and relevant to the new and emerging trends.

11. SESSION 10: COOPERATION IN THE REGION AND BEYOND

The objective of this session was to explore the collaboration and coordination components of cybersecurity incident response as well as examining the sub-areas of cybersecurity that need enhanced cooperation.

Session moderator:

- Mr. Jaroslaw Ponder, Head of the ITU Office for Europe, ITU

Panellists:

- Mr. Farid Nakhli, Programme Coordinator, ITU Regional Office for CIS;
- Mr. Radovan Nikcevic, Expert on Connectivity, Regional Cooperation Council;
- Ms. Cosmina Moghior, Public Policy Expert, CERT.RO, Romania.

General Findings:

Cooperation has and will continue to serve as a key component in enhancing security and preparedness both regionally and globally. In this light, the ITU organises numerous regional and inter-regional forums, trainings, workshops and conferences as well as bringing stakeholders together for collaboration in the name of safe and secure technological advancement for all. Other entities, such as the Regional Cooperation Council also aid countries in the facilitation of regional dialogue and identifying key areas of weakness for development stronger cybersecurity. However, much room for collaboration remains, particularly as it relates to the development of national cybersecurity strategies, information exchange, and trust building between stakeholders.

Key points

- ITU creates numerous regional and interregional events as well as initiatives and projects in the name of technological advancement for all nations

- Examples of ITU's work include cyber drills, facilitation of relevant stakeholders as ITU members, capacity building, and institutionalization of frameworks
- ITU also creates country reports and guidelines as well as coordinating with other stakeholders for a more interconnected world
- Regional Cooperation Council supports economies from Southeast Europe on their path towards the EU; one of the pillars is digital transformation in West Balkans (WB) region. Special focus is placed upon cybersecurity, trust services, and data protection.
- Special efforts are dedicated to the identification and protection of critical infrastructure, an initiation of a regional dialogue among CSIRTs, and establishment of regional dialogue among national authorities.
- The biggest input is set under education and capacity building as these actions are recognized as the initial point of security improvement.
- Sustainable process of capacity building is necessary.
- Majority of CERTs in the WB region are affected by lack of qualified staff, advanced technologies, and a fluctuation of labor force.
- Countries in the WB region are missing national strategies on cybersecurity as well as effective working national CERTs.
- Closer cooperation, willingness of information exchange, building the trust among CERTs, and other bodies is urged.
- ICT development requires stable budget.

12. CLOSING SESSION: KEY TAKEAWAYS

In a brief closing to the two-day long forum, concluding remarks were given by H.E. Andreana Atanasova, Deputy Minister of Transport, Information Technology, and Communications of the Republic of Bulgaria as well as Mr. Jaroslaw Ponder, Head of the ITU Office for Europe (to see read the speeches in full, please refer to the link in Section 1.3). The rapidly growing relevancy of enhanced cooperation and understanding of cybersecurity was underscored by both Mr. Ponder and H.E. Atanasova as society progresses further into the 21st century.