REGIONAL CYBERSECURITY SYMPOSIUM

14–15 NOVEMBER 2023

Chisinau, Republic of Moldova

www.rcs.md

#rcs2023

Co-funded by the European Union — EUROPEAN UNION

COUNCIL OF EUROPE — CONSEIL DE L'EUROPE

Co-funded and implemented by the Council of Europe

Cybersecurity EAST

GFA CONSULTING GROUP

ACTION GLOBAL COMMUNICATIONS

EU-Moldova Stronger Together

eGA e-governance academy

TUESDAY, NOVEMBER 14th, 2023

Location: Radisson Blu Leogrand Hotel, Mitropolit Varlaam St 77, Chişinău 2012

The Regional Cybersecurity Symposium (RCS) is an important event that aims to enhance national security by strengthening the resilience and security of critical infrastructure against cyber threats. It brings together regional experts, policymakers, industry leaders, and security professionals to address the unique challenges faced by critical infrastructure sectors in the region. It serves as a platform for regional dialogue, knowledge sharing, and coordinated efforts to strengthen national security in the region.

Our vision is to establish a strong and collaborative security environment where regional stakeholders have the necessary knowledge, skills, and resources to effectively combat and manage cyber threats against critical infrastructure and national security.

The primary goal of the Regional Cybersecurity Symposium is to enhance our collective defense capabilities. This event aims to unite the cybersecurity community from different regions, promoting global collaboration. The symposium will emphasize the vital role of national and other relevant Computer Security Incident Response Teams (CSIRTs) in promoting cyber resilience and protecting critical information infrastructures.

The Regional Cybersecurity Symposium, under the theme "**Ensuring Cyber Resilience: Securing Our Connected Future**" focuses on the critical importance of fortifying cybersecurity measures in an increasingly interconnected world. This Symposium brings together experts, policymakers, and stakeholders to discuss strategies and collaborative efforts for enhancing cyber resilience. A key aspect of this event is the role of Computer Emergency Response Teams (CERTs) within the region. These teams play a pivotal role in coordinating responses to cyber threats, sharing vital information, and implementing best practices to safeguard digital infrastructures. The collaboration among regional CERTs is essential in developing a unified and robust defense against the evolving landscape of cyber threats, ensuring a secure and resilient digital future for all.

Objectives:

- **Foster Regional Collaboration**: Encourage the sharing of knowledge, strategies, and best practices among neighbouring countries to bolster regional defense against cyber threats.
- **Increasing awareness** and **preparedness** among participating nations.
- **Advancing international collaboration** for a unified approach to cyber defense.
- **Enhance Understanding of Cyber Risks**: Highlight the latest cyber threats, vulnerabilities, and trends affecting critical infrastructure and national security.
- **Develop Robust Cybersecurity Frameworks:** Assist in the creation and implementation of effective cybersecurity policies, standards, and protocols tailored to the needs of critical infrastructure.
- Improving the efficiency of **incident response** and communication between Member States
- **Build Capacity and Skills**: Provide training and workshops to develop the technical and strategic skills necessary for defending critical systems.

Key Themes:

- **Policy and Governance**: Examining regulatory frameworks, national cybersecurity strategies, and public-private partnerships.
- **Threat Landscape and Intelligence Sharing**: Understanding regional cyber threats and the importance of intelligence sharing for pre-emptive defense.
- **Technological Innovations**: Exploring cutting-edge cybersecurity technologies and their application in protecting critical infrastructure.
- **Incident Response and Recovery**: Best practices in responding to and recovering from cyber incidents to ensure continuity of critical services.
- **Challenges** in **Cybercrime** and Financial Fraud
- **Workforce Development and Education**: Strategies for cultivating a skilled cybersecurity workforce to meet the growing demands of the sector.

Format:

- **Presentations**: From leading cybersecurity experts and regional policymakers.
- **Panel Discussions**: Involving a diverse group of stakeholders discussing specific challenges and collaborative strategies.
- **Interactive Workshops:** Hands-on sessions focusing on specific skills, tools, and methodologies.
- **Networking Opportunities**: Facilitated sessions for building connections and sharing experiences among participants.

Target Audience:

- Government officials from national security, defense, and IT departments.
- Executives and security professionals from key sectors like energy, telecommunications, finance, and transportation.
- Cybersecurity solution providers, academic researchers, and policy analysts.

Outcome: Participants will gain a comprehensive understanding of regional cyber threats, improve their skills, establish stronger networks, and develop actionable strategies for their organizations and sectors. The symposium's objective is to foster a unified and well-informed regional approach to combating cyber threats to critical infrastructure and national security.

08:30 – 09:00 **Registration**

09:00 – 09:30 **Strengthening cybersecurity and resilience in region**

- H.E. Mr. **Vladimir CUC**, Secretary of State of the Ministry of Foreign Affairs and European Integration of the Republic of Moldova
- H.E. **Laura HRUBY**, Deputy Chief of Mission of the U.S. Embassy in Chisinau, Republic of Moldova
- H.E. Mr. **Cristian-Leon TURCANU**, Ambassador of Romania to the Republic of Moldova
- H.E. Mr. **Tomasz KOBZDEJ**, Ambassador of the Republic of Poland to the Republic of Moldova
- Mr. **Stanislav SECRIERU**, National Security Advisor, Presidential Administration, Republic of Moldova
- Mr. **Alexandru COREȚCHI**, Director of Information Technology and Cyber Security Service, Republic of Moldova
- Mr. **Hannes ASTOK**, Executive Director and Chairman of the Management Board at e-Governance Academy, Estonia

Moderator: Mrs. **Epp MAATEN**, Team Leader of the Moldova Cybersecurity Rapid Assistance Project (EU), e-Governance Academy, Estonia

09:30 – 10:30 **Panel 1 | Promoting Cybersecurity Cooperation in the Region: Strategies for International Collaboration and Resilience**

In today's ever-changing cyber-threat landscape, it is crucial to prioritize international cooperation alongside technical solutions. Cybersecurity goes beyond individual organizations and has a significant impact on industries and nations due to our interconnected digital world. This panel emphasizes the importance of transparent communication, diverse perspectives, and partnerships across sectors in building a resilient cyberspace. We will explore effective collaboration mechanisms among industries, governments, and technology innovators to address widespread cyber challenges.

- Mr. **Anatoli GOLOVCO**, Cyber Security Adviser to the Prime Minister, Republic of Moldova
- Mrs. **Epp MAATEN**, Team Leader of the Moldova Cybersecurity Rapid Assistance Project (EU), e-Governance Academy, Estonia
- Mr. **Jaïr H. van der STELT**, Foreign Affairs Officer at U.S. Department of State
- Mr. **Valentina STADNIC,** ITU Office for Europe
- Mr. **Tadeusz CHOMICKI**, Ambassador for Cyber & Tech Affairs at the Polish Ministry of Foreign Affairs
- Mrs. **Yuliia VOLKOVA**, Director of the International Cooperation Department, State Service of Special Communications and Information Protection, Ukraine

Moderator: **Mr. Endrit DEMI**, Senior Coordinator for Energy, Cybersecurity and Economic Development Assistance at U.S. Department of State

10:30 – 10:50 **Presentation | Governments and institutions face the challenge of maintaining cybersecurity without compromising individual freedoms**

Privacy is a crucial aspect that requires careful consideration to maintain the delicate balance between national security interests and fundamental human rights, specifically the right to privacy. In today's digitally interconnected world, governments and institutions must navigate the challenge of ensuring cybersecurity while also respecting individual freedoms. This presentation will explore the complex intersection of privacy, national security, and cybersecurity, analyzing legal frameworks, technological advancements, and policy considerations that can achieve a harmonious equilibrium between these critical elements. The aim is to tackle urgent issues concerning surveillance, information sharing, and individual liberties in the face of contemporary security challenges. It ultimately promotes inclusive solutions that safeguard national security interests while upholding the human rights of citizens.

- Mr. **Alar AMBROS**, Adviser to Chancellor of Justice of Estonia

10:50 – 11:10 **Coffee break**

11:10 – 12:10 **Panel 2 | National Security through National Cyber Crisis Response Strategy**

In today's digital age, national security extends beyond physical borders and military capabilities. It now includes the realm of cyberspace, where threats can originate from anywhere and have far-reaching consequences on critical infrastructure, financial systems, and society. To effectively tackle these challenges, it is crucial to have a strong and comprehensive National Cyber Crisis Response Plan (NCCRP) that promotes intersectoral coordination. Valuable insights can be gained from studying the best practices of countries such as the Republic of Moldova, Ukraine, Georgia, Armenia, Romania, the Netherlands, and the United States.

- Mr. **Alexandru COREȚCHI**, Director of Information Technology and Cyber Security Service
- Mr. **Radu STĂNESCU**, Adviser to the Director of Romanian National Cyber Security Directorate
- Mr. **Justin NOVAK**, Senior Security Operations Researcher at Software Engineering Institute, Carnegie Mellon University
- Mr. **Rob HUBERTSE**, Deputy Head of the Netherlands Defense Cyber Security Center
- Mr**. Nerses YERITSYAN**, National Cyber Security Agency, Armenia

Moderator: Mr. **Klaid Mägi**, Team Lead of EU4Digital Project "Cybersecurity East"

12:10 – 13:10 **Panel 3 | Building Cyber Resilience: the prism of the EU Normative**

The panel will discuss the assurance of cyber resilience and continuity of critical services within the EU frameworks. The new EU Directives highlight the importance of conducting comprehensive risk assessments, proactive planning, and implementing resilient designs to ensure the security of critical infrastructure assets. This panel aims to explore the fundamental principles, methodologies, and best practices used to protect critical infrastructure across different sectors. The discussion will emphasize the significance of cross-sector collaboration and public-private cooperation.

- Mr. **Klaid Mägi**, Team Lead of EU4Digital Project "Cybersecurity East"
- Mr. **Magnus JACOBSON**, Senior Cybersecurity Adviser, Swedish Bankers' Association
- Mr. **Silver LUSTI,** Head of Legal Department, Estonian Information System Authority
- Mr **Vitalie VARANITA**, Legal Expert, Moldova Cybersecurity Rapid Assistance Project (EU)

Moderator: Mrs. **Elsa NEEME,** Senior Cybersecurity Expert at the e-Governance Academy, Estonia

13:10 – 14:10 **Networking Lunch**

14:10 – 15:00 **Panel 4 | Workforce Development, The Power of Training, Education, Certification and Empowerment of the Companies Cyber Skills**

Research in cyber workforce development aims to identify effective methods and technologies for organizations to cultivate the necessary knowledge and skills in their cyber workforce. With cybersecurity becoming a fundamental concern, the demand for cybersecurity professionals has significantly increased. Obtaining a Cybersecurity certification is crucial in gaining the essential skills, knowledge, and experience needed to advance one's career in this field as technology continues to advance.

- Mr. **Jan Pieter SPAANS**, Managing Director, Mainland Europe SANS Institute
- Mr. **Todd SPIRES**, Director, Cyber and Digital Resilience Programs at CRDF Global
- Mr. **Gabriel RAICU**, Vice Rector, Maritime University of Constanta
- Mrs. **Cynthia WRIGHT**, Principal, Cyber Strategy & Policy at the MITRE Corporation

Moderator: Mr. **Priit VINKEL,** Senior Expert at the e-Governance Academy, Estonia

15:00 – 16:15 **Panel 5 | The emerging trends and future in cybersecurity**

The panel discussions will explore the evolving landscape of cybersecurity. This session will delve into the latest trends, technological advancements, and shifting dynamics in the digital security realm. Experts will discuss predictions and insights about the future direction of cybersecurity, focusing on new threats, innovative defense strategies, and the impact of emerging technologies. The panel aims to

provide a comprehensive understanding of what lies ahead in cybersecurity, preparing participants for upcoming challenges and opportunities in protecting digital assets and information.

- Mrs. **Gratiela Magdalinoiu**, President at ISACA Romania, Romanian Chapter
- Mrs. **Magda (Andreianu) JIANU**, South Eastern Europe District Manager at Palo Alto Networks
- Mr. **Dragos IONICA,** Manager in Cyber Risk Advisory, Deloitte Romania
- Mrs. **Ivana ARAPU**, Head of Corporate Security, Orange Moldova
- Mr. **Alex CALISTRU,** Adobe Cyber Security, Romania

Moderator: Mrs. **Merle MAIGRE**, Programme Director of Cybersecurity, e-Governance Academy, Estonia

16:15 – 16:30 **Coffee Break**

16:30 – 17:30 **Panel 6 | The New Reality - Cybercrime and financial fraud-related challenges**

Cybercrime is primarily motivated by the desire for illegal financial gains. A growing area of concern is the need to combine cybercrime investigations with financial probes and intelligence. This is important for tackling issues such as online crime proceeds, financial fraud, money laundering, virtual currencies, and Darknet activities. The panel will discuss the importance of collaboration between criminal justice authorities and private sector entities in addressing these challenges. Partnerships between financial institutions and law enforcement agencies are vital in safeguarding society from sophisticated criminal threats, particularly in the realm of cybercrime. These collaborations are crucial in the intricate dance of financial investigations. The panel's objective is to address the challenges related to fraud, money laundering, and tracking online crime proceeds. It emphasizes the importance of joint efforts in tackling these issues and aims to explore strategies for creating a more secure digital financial world.

- Mr. **Hein DRIES**, Cybercrime Programme Office at Council of Europe
- Mr**. Giorgi SHERMAZANASHVILI**, Payment Systems and Information Security, National Bank Georgia
- Mr**. Goran JANKOSKI,** Cybercrime Programme Office at Council of Europe
- Mr. **Mircea Constantin SCHEAU**, President Cloud Security Alliance Romania Chapter

Moderator: Ms. **Kim ZOETBROOD**, CIO Office, Royal Netherlands Army

17:30 – 17:40 **Closing remarks and Practical Takeaways**

DAY 2 Workshops

Location: Tekwill, 9/11 Student Street

WEDNESDAY, NOVEMBER 15th, 2023

09:00–17:00

SANS Institute Workshop “Blue Team Fundamentals: Security Operations and Analysis”

This hands-on workshop (sampled out of SANS’s “SEC450: Blue Team Fundamentals, SecOps and Analysis” training course) tackles threat intelligence, discusses who is out there to target us and then follows up by delving deeper into more technical aspects which are part of the daily tasks of security analysts.
It gently starts by going into technical aspects so that everyone is aligned as we progress to more challenging aspects, focusing on building the skills and knowledge that can generate quick wins to be leveraged by any analyst for fast answers in most incidents.

In recognition of the fact that phishing is still the top initial delivery vector for attackers, the workshop will end with a look at what we can do to not only prevent phishing using our organization's domains but, more important in case of government and critical infrastructure organizations, how we can actually find out if/when someone tries to use our domains for phishing attempts against others.

Prerequisites:
A basic understanding of TCP/IP and general operating system fundamentals and basic entry-level security concepts.

Requirements:
Laptop with 64-bit Intel i5/i7 (8th generation or newer) or AMD equivalent, 8GB of RAM or more, 50GB of free storage space, ability to run VMware Workstation Pro 16.2.X+ or VMware Player 16.2.X+ (for Windows 10 hosts), VMware Workstation Pro 17.0.0+ or VMware Player 17.0.0+ (for Windows 11 hosts), or VMWare Fusion Pro 12.2+ or VMware Fusion Player 11.5+ (for macOS hosts). Linux hosts are known to work but will be unsupported due to their numerous variations and limited time available for troubleshooting.

08:30–09:00 Welcome coffee

09:00–11:00 **SANS Workshop "Blue Team Fundamentals: Security Operations and Analysis"**

Mr. **Cristian Mihai VIDU**, Certified SANS Instructor

11:00–11:30 **Coffee Break**

11:30–13:00 **SANS Workshop "Blue Team Fundamentals: Security Operations and Analysis"**

Mr. **Cristian Mihai VIDU**, Certified SANS Instructor

13:00–14:00 **Lunch Break**

14:00–14:30 **SANS Workshop "Blue Team Fundamentals: Security Operations and Analysis"**

Mr. **Cristian Mihai VIDU**, Certified SANS Instructor

14:30–15:00 **Coffee Break**

15:00–15:45 **Lecture and Demonstration on the Fundamentals of Cyber and Electromagnetic Activities (CEMA)**
CEMA operations are used by military forces to seize, preserve, and exploit dominance over hostile adversaries in both cyberspace and the electromagnetic spectrum (EMS).

Mr. **Operator Mike**, Royal Netherlands Army

15:45–16:30 **Workshop Threathunting**
Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find malicious actors in your environment that have slipped past your initial endpoint security defenses

Mr. Colonel **Pawel DONIEC**, H-CSIRT, Polish Cyber Command

16:30–17:15 **Triage of Cyber Incidents**
With threats on the rise, organizations must take steps to guard against cyber incidents and minimize damage when they do occur. This is where cybersecurity triage comes into play. Triage involves prioritizing incidents by severity level so that the most dangerous threats can be contained quickly.

Mr. **Rob HUBERTSE**, Deputy Head of the Netherlands Defense Cyber Security Center