ForumEurope

Version of 12 October


**The European Security Summit**
**Connecting the dots across the security landscape**
**13 – 15 October 2020 | An Online Event**

**Tuesday 13 October**

**09:00 – 09:20** **Virtual Platform and Networking area opening**

**09:20 – 09:30** **Welcome by Forum Europe**

**09:30 – 10:20** **Summit opening keynote session:**

**João Gomes Cravinho,** Minister of Defence, Portugal
**Margaritis Schinas,** Vice President, Promoting our European Way of Life, European Commission

Moderated by **Paul Adamson**, Chairman, Forum Europe

**10:20 – 11:30** **Session 1: The Europe Cyber Security Policy Landscape – Building an integrated approach to future proof the security environment**

Cyber and digital now sits at the heart of both the challenge and the solution for Europe's approach to matters of security across the board. Societies are increasingly hyper-connected and reliant on digital technologies for every-day activities and essential services, and securing the digital eco-system is therefore a fundamental priority. In recent years, the EU has implemented several initiatives in order to develop trust and cooperation across member states. With the review of the NIS Directive expected before the end of 2020, and just over a year after the Cybersecurity Act entered into force, this session will look at the latest EU cyber policy thinking and how this will interact with other areas of the EU's Security Union Strategy.

How is the threat landscape developing and what are the latest considerations for the NIS Directive review? How can cooperation and the sharing of best practice between stakeholders across Europe be further encouraged to build a coherent approach to EU cybersecurity? What impact has the EU's Cybersecurity Act had so far in strengthening the cybersecurity features of ICT products, services, and processes? What should we expect from the Stakeholders Cybersecurity Certification Group? How are concerns related to the voluntary nature of cybersecurity certification being addressed and will mandatory certification eventually become necessary? To what extent will the European Cyber Competence Centre efficiently stimulate the European cybersecurity technological and industrial ecosystem and what more needs to be done to boost competitiveness and innovation capacities in Europe to ensure a sustainable supply in the cybersecurity sector and support Europe's drive for increased digital autonomy?

**Session opening speech**
**Juhan Lepassaar,** Executive Director, ENISA

**Panel:**
**Juhan Lepassaar**, Executive Director, ENISA
**Jakub Boratynski**, Acting Director, Digital Society, Trust and Cybersecurity, DG CONNECT, European Commission
**François Zamora**, Chief Security Officer, European Division, Orange
**Liga Rozentale**, Senior Director, Cybersecurity, Microsoft
**Volkmar Lotz,** Head of Security Research, SAP

Moderated by: **Luigi Rebuffi**, Secretary General, European Cyber Security Organisation (ECSO)

**11:30 – 12:40** **Session 2: Modern Law Enforcement in the Digital Eco-System: Encryption, lawful data access and the implications for security and privacy**

By ensuring the confidentiality, availability and integrity of data at rest, in use or in transit over networks, encryption makes connected products, services and critical infrastructures more secure against cyber incidents. Encryption is, however, also used by hostile actors (examples of which include terrorism ransomware attacks, and in the sexual exploitation of children through the exchange of videos and images) and this raises challenges to national security and law enforcement agencies in the investigation and prosecution of online criminal activity.

Calls continue for the tech industry to create 'backdoors' for exceptional access for law enforcement, which, it is argued, could in turn weaken security. Focusing on the challenges that law enforcement agencies and industry face when retrieving digital evidence, this session will discuss the technological advancements and regulatory frameworks needed to support law enforcement authorities in the investigation and prosecution of cybercrime. It will explore the need for cross-border data investigatory processes to be improved by addressing issues relating to conflicting national legislation, jurisdictions competency and procedures for mutual legal assistance. Finally, speakers will elaborate on the need for greater cooperation and collaboration within the law enforcement community, as well as with other relevant public and private sector organisations to ensure that authorities have the most innovative lawful methods of digital evidence access.

**Session opening speech**: **Edvardas Šileris,** Head of EC3, Europol

**Panel:**
**Edvardas Šileris,** Head of EC3, Europol
**Cathrin Bauer Bulst**, Head of Unit, Cybercrime, DG HOME, European Commission
**Robin Wilton**, Director - Internet Trust, ISOC
**Selene Giupponi**, Managing Director, Resecurity

Moderated by: **Vladimir Radunovic,** Director of E-diplomacy and Cybersecurity, DiploFoundation

**12:40 – 13:45** **Lunch break and virtual networking**

**13:45 – 15:00** **Session 3: Securing International Supply Chains – Cooperation, Trust and Trade**

In today's interdependent and interconnected world, the security and the resilience of supply chains are vital to the global economy, demanding strong cooperation between, governments, businesses, security technology providers, standards bodies, manufacturers and users. With systems relying on

components that are designed and built by different parties around the globe, and with cyber threats growing in number and varying in their nature and sophistication, it is crucial that collaborative initiatives and structured dialogue is increased, particularly at the global level, in order to address issues related to the resilience and vulnerability of complex supply chains, from both security and commercial perspectives. Highlighting the responsibility of all stakeholders to develop a trusted ecosystem that remains appropriate and proportionate to each potential risk, this session will explore what needs to be considered at technical, standardisation, and regulatory levels to work towards end-to-end security. Speakers will address the role that technology such as blockchain and AI can play to ensure the integrity and resilience of the supply chain and the session will debate how a common, global approach to enhance cyber security can be found and new barriers to data flows and digital trade are avoided.

What progress is being made in relation to cyber security global standardisation initiatives in cooperation with international partners in order to secure the entire supply chain? Where does the certification framework included in the EU Cybersecurity Act fit with initiatives worldwide? How can it be ensured that these schemes are not restricting data flows and imports on IT products, which create barriers to innovation and trade? To what extent can trade agreements be used to develop international standards? What role can the EU and global partners play in assisting developing countries with regards to the security of their digital infrastructure?

**Panel:**
**Jean-Francois Junger**, Deputy Head of Unit, Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission
**Scott Friedman**, Deputy Assistant Secretary for Economic Security, DHS Strategy, Policy and Plans, Department of Homeland Security, USA
**Nathalie Jaarsma**, Ambassador at-Large for Security Policy and Cyber, Kingdom of the Netherlands
**Jacques Kruse Brandao**, Global Head of Advocacy, SGS
**Paddy McGuinness**, Former UK's Deputy National Security Adviser, Senior Advisor, Brunswick Group

Moderated by: **Iva Tasheva**, Co-Founder & Cyber Security Lead, CYEN SCS

**15:00 – 15:30 Networking and End of Day 1**

**Wednesday 14 October**

**10:00** **Virtual Platform and Networking area opening**

**10:25 – 10:30** **Day 2 Welcome by Forum Europe**

**10:30 - 11:45** **Session 4: 5G Security: Building a secured ecosystem of ecosystems fit for the digital transformation**

5G will play a leading role in shaping Europe's future economy, becoming the backbone of Europe's digital and, it is hoped, green transformation. The technology has the ability to improve efficiencies at every level when combined with IoT, but also poses security challenges by widening the attack surface. Ensuring the security and resilience of the EU's 5G networks is therefore critical. Following the assessment of the EU Toolbox for 5G Security by Member States, are the recommendations published in January deemed enough to ensure the security of 5G infrastructure in Europe and is there a need for further action?

What is being done to address the increased exposure to attacks through the ecosystem of devices and applications supported by 5G networks, as well as the risks of major dependencies on suppliers and vendor lock-in problems? As 5G is being deployed, what support is available for businesses and public sector organisations to assess, and often rethink, their security strategies? How can greater collaboration between network operators and their vendors be incentivised to address the complexity of 5G networks security and resilience?

**Julie Ruff**, Head of Sector, Secure Value Chain, DG CONNECT, European Commission
**Florian Pennings,** EU Cybersecurity Policy Manager, Microsoft
**Sauli Pahlman**, Director, National Cyber Security Centre Finland
**Mikko Karikytö,** Chief Product Security Officer, Ericsson

Moderated by: **Visiola Pula**, Senior Analyst, Cullen International

**11:45 - 12:30** **Showcase Session: Global Encryption Coalition (GEC) – By Internet Society**
Encryption safeguards the personal security of billions of people and the national security of nations around the world. The Global Encryption Coalition promotes and defends encryption in key countries and multilateral gatherings where it is under threat.

The Global Encryption Coalition calls on governments and the private sector to reject efforts to undermine encryption and pursue policies that enhance, strengthen and promote use of strong encryption to protect people everywhere. With a steering committee led by the Center for Democracy and Technology (CDT), Global Partners Digital (GPD) and the Internet Society (ISOC), the GEC also support and encourage the efforts of companies to protect their customers by deploying strong encryption on their services and on their platforms.

Join us for an interactive discussion around Encryption in the EU and the activities of the Global Encryption Coalition in Europe!

**Ryan Polk**, Senior Policy Advisor, Internet Society
**Iverna McGowan**, Director, Europe Office of CDT
**Sheetal Kumar**, Senior Programme Lead, Global Partners Digital

**12:30 – 13:45** **Lunch and Networking**

**13:45 - 14:00 Keynote Speech**

**Heli Tiirmaa-Klaar**, Ambassador at Large for Cyber Diplomacy, Estonian Ministry of Foreign Affairs

Introduced by **Ruth Harris**, Research Group Director, Defense, Security and Infrastructure, RAND Europe

**14:00 – 15:10 Session 5: Hybrid Threats: International Cooperation and Diplomacy**

Hybrid threats are often discreet and are designed to be coercive and difficult to attribute, impacting critical infrastructures, jeopardising the functioning of economies and damaging confidence in democratic processes through disinformation campaigns and election interference. Given the global dimension of the issues at stake, international cooperation between all stakeholders is required to protect societies from the malicious exploitation of cyberspace and from being used as a ground for politically motivated and offensive operations led by hostile state or non-state actors.

Debating issues relating to deterrence, attribution, sanctions, respect for international law and norms for responsible state behaviour, speakers will elaborate on the role and responsibilities for stakeholders in the international cybersecurity and defence communities to ensure an open, stable and secure cyberspace where the rule of law applies.

What are the existing gaps in the global governance of cyber resilience and what needs to be done to address them? What progress has been made on the implementation of the Cyber Diplomacy Toolbox to provide useful measures for deterrence? Following the Council decision to extend the cyber sanctions regime until May 2021, what has been achieved in regard to attribution and sanctions and how can challenges regarding traceability and evidentiary standards for attribution of cyberattacks be tackled? Are sanctions efficient if they only apply to "persons and entities" and not to national governments? To what extent can norms on responsible state behaviour help prevent the use of cyber-weapons against critical infrastructure and interference in domestic affairs and how can these norms be implemented? How successful have initiatives such as the Paris Call for Trust and Security in Cyberspace or the renewed effort from the United Nations been to improve the dialogue to define cyber norms when divergent strategic visions of cyberspace exist between different regions and countries? How can concerns relating to confidence building and intelligence sharing be best alleviated? How can cross-border intelligence agencies coordination and law enforcement response be improved in line with the respect of fundamental rights and EU values?

**Panel:**
**Joanneke Balfoort,** Director, Security and Defence Policy, EEAS
**Marina Kaljurand,** Member, European Parliament
**Ben Hiller,** Lead for Partner Nations and international Organizations, Cyber Defence Section, NATO
**Samantha Seller**, Head of State Threats Deterrence, Cyber Policy Department, FCDO, UK Government
**Raj Samani,** Chief Scientist and Fellow, McAfee

**Moderated by Ruth Harris**, Research Group Director, Defense, Security and Infrastructure, RAND Europe

**15:10 - 15:40 Session 6: Cyber Skills and Awareness – The Essential, Missing Ingredient**

For all the talk of how technology can support the fight against cybercrime in all its forms, education, awareness and skills development remains an often underappreciated and underfunded part of the solutions toolbox. This fireside chat will highlight that cybersecurity is not purely a technological issue: awareness, education, skills, investments in R&D and diversity in the workforce should be a matter of much higher focus to achieve Europe's ambitions for securing the digital economy.

A conversation between:

**Janice Richardson**, CEO, Insight
**Csaba Virág**, Head of Competence Building, Guardtime

Moderated by: **Iva Tasheva**, Co-Founder & Cyber Security Lead, CYEN SCS

**15:40 - 16:10** **Networking and End of Day 2**

**Thursday 15 October**

**10:00** **Virtual Platform and Networking area opening**

**10:25 – 10:30** **Day 3 Welcome by Forum Europe**

**10:30 – 11:15** **Keynote speeches**

**Ylva Johansson**, European Commissioner for Home Affairs
**Krum Garkov,** Executive Director, eu-LISA

Moderated by **Paul Adamson**, Chairman, Forum Europe

**11.15 – 12:30** **Session 7: AI for Security: Leveraging the benefits, mitigating the risks**

AI-driven technology is a powerful tool to address new cyber threats and risks by protecting end points, detecting hidden threats and anomalies, blocking attacks before they can spread widely, and accelerating efficient response speeds to cyber incidents.

AI and Machine Learning create additional risk however, with cybercriminals taking advantage of AI systems to analyse networks, find vulnerabilities, compromise the data used to train the AI, potentially leading to disastrous consequences.

When considering the interplay between artificial intelligence and security, it is therefore essential to take all potential effects in any regulatory, technical, commercial or operational decision-making process, into account. This session will explore how stakeholders can work together to develop specific measures and processes ensuring that AI systems are, and remain, secure and trustworthy.

How is AI changing cybersecurity developments? Are the provisions in the European Data Strategy and the White Paper on Artificial Intelligence released by the European Commission earlier this year appropriate in order to allow access to the right datasets for risk and threat evaluation? How can AI and machine learning be used to stay ahead of security threats, and what solutions are available to mitigate the possible security risks of using AI systems?

**Panel**
**Edward Hunter Christie**, Deputy Head, Innovation Unit, Emerging Security Challenges Division, NATO
**Zsuzsanna Felkai Janssen**, Head of Sector for Migration, DG Home, European Commission
**Dr. Ioannis Askoxylakis**, Cybersecurity Policy Officer, DG CONNECT, European Commission
**Svenja Hahn**, Member, European Parliament
**Mark Smitham**, Head of EU Public Affairs, Huawei

**Moderated by: Luke Huxtable**, Associate Director, RAND Europe

**12:30 – 13:30** **Lunch Break and Networking**

**13:30 - 13:45** **Presentation: Social media: a tool for terrorism in Africa**
**By Kate Cox**, Senior Analyst, RAND Europe

**13:45 – 14:45** **Session 8: Terrorism and Radicalisation in Europe: The public security and information architecture challenge**

Tackling terrorism sits at the heart of the European Commission's internal security policy. The EU already has several initiatives, whether building law enforcement and information sharing architectures that support cooperation - crucially across borders – or the focus on the prevention and removal of terrorist content online. However, as new threats emerge and as internal and foreign policy dynamics change, the ability and agility of public protection agencies to respond to such change, is key. Speakers will analyse how information is currently shared amongst member states and public security agencies, how to step-up public-private cooperation to combat threats and crime and where improvements are necessary.

This session will take stock of the work completed to date by the Commission and its agencies, and what we can expect of this new executive, whose work has been somewhat disrupted by the Covid-19 pandemic. It will focus on the changing threat landscape, and how the EU, member states and EU agencies can deepen cooperation internally and with its neighbours in order to bolster public safety.

**Session Opening Speech**: **Wil van Gemert**, Deputy Executive Director of Operations, Europol

**Panel**:
**Wil van Gemert**, Deputy Executive Director of Operations, Europol
**Laurent Muschel,** Director, Law Enforcement and Security - DG HOME, European Commission
**Éric Freyssinet**, Head of the National focal point for the fight against cyberthreats, Gendarmerie Nationale
**Rob Wainwright**, Partner, Deloitte

**Moderated by: Stijn Hoorens**, Director, RAND Europe Brussels

**14:45 - 16:00** **Session 9: Border Management, Migration & Customs: The New Information Architectures**

Many of Europe's security concerns originate from instability in its immediate neighbourhood. This panel will elaborate on the current challenges faced at the EU's external borders, how the new information architectures, once in place, can strengthen border security in the European Union and tackle organised crime. This panel will also discuss the proposal for a 'New Pact on Migration and Asylum', including the revision of the Eurodac regulation.

Since EU-LISA was launched in 2011, the EU has made significant progress in a number of areas relating to interoperability of its information systems. 2020 will see upgrades to existing systems and new services expected to come on stream by the end of 2021. How will these new architectures benefit EU law enforcement and those protecting Europe's external borders?

This session will also take a step further by looking at the adoption of a Customs Single Window that reinforces the protection of borders and how the use of technology can help simplify administrative procedures for companies.

**Session Opening Speech: Fabrice Leggeri,** Executive Director, EBCGA (Frontex)

**Panel:**
**Fabrice Leggeri,** Executive Director, EBCGA (Frontex)
**Matthias Oel,** Director of Borders, Interoperability and Innovation, DG HOME, European Commission
**Uku Särekanno**, Head of Cabinet, eu-LISA
**Dr. Juha Hintsa**, Founder, Executive Director and Board Member, Cross Border Research Association
**Christine Bradley**, Programme Manager, United Nations Counter-Terrorism Centre

**Moderated by: Dr. Raphael Bossong**, Senior Associate, German Institute for International and Security Affairs

**16:00 – 16:30** **Networking and End of Event**