CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

CYBERSEC BRUSSELS LEADERS' FORESIGHT 2020

RECOMMENDATIONS & KEY TAKEAWAYS

3rd CYBERSEC BRUSSELS LEADERS' FORESIGHT, 24 MARCH 2020
DIGITAL-ONLY EDITION

#CSBXL20 cybersecforum.eu/brussels #SecureDigitalDNA

SECURING THE EUROPEAN DIGITAL DNA

CONTENTS

OPENING REMARKS

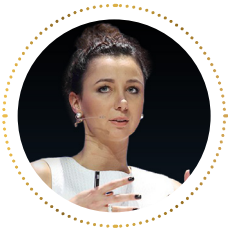
WATCH THE VIDEO
ON CYBERSEC YOUTUBE CHANNEL

Welcome remarks were given by:

- Izabela Albrycht – Chair, the Kosciuszko Institute; President, Organising Committee of the European Cybersecurity Forum – CYBERSEC
- Marek Zagórski – Polish Minister of Digital Affairs
- Casper Klynge – Vice President for European Government Affairs, Microsoft

The COVID-19 pandemic has recently changed the way we live, work, interact and engage. The emergency lockdown across Europe marks a critical moment in which the digital infrastructure of our civilisation is being put to the hardest stress-test yet, and cybersecurity becomes more important than ever before. In this exceptional moment, it is even more crucial for us to speak up about cyber challenges. Thanks to the Internet and digital technology we can remain connected and preserve some aspects of our regular way of life. Now more than ever, when we are more vulnerable to malicious activities and cyberattacks, we have to think about cybersecurity.

And for this reason, CYBERSEC Brussels 2020 was organised in a virtual form, gathering top policy and business leaders from EU, NATO, national ministries, cybersecurity organisations and the global and European tech industry as well as experts and civil society. Fostering trust-based cooperation between like-minded cybersecurity stakeholders for the period of digital disruption has always been a key aim of CYBERSEC. It is valid now more than ever and is gaining the momentum which we have not expected to see. Today's debate matters also because we are in a crucial moment of significant shifts in global soft and hard powers, both of which are driven by modern disruptive technologies. We are at the junction where we need to build a secure cyber world together – this is where our shared future is now being shaped. We all need to team up – countries, governments, experts, civil society and tech companies – to make it effective as soon as possible.



"Fostering trust-based cooperation of like-minded cybersecurity stakeholders for the period of digital disruption has always been a key aim of CYBERSEC. It is valid now more than ever and is gaining the momentum which we have not expected to see. (...) We are calling all digital actors to strengthen cooperation and speed up the adoption of all necessary measures to secure the European and world's digital DNA. We – the think tank community – are here to help and hope that in the upcoming days, weeks and months we will observe the empowerment of scientists and experts in their interactions with policy- and decision-makers."

IZABELA ALBRYCHT

"Close cooperation through cross-border projects and joint actions can contribute to ensuring an adequate level of cybersecurity essential to achieve safe and secure digital environment. That is the reason we do not want to limit this initiative only to the V4. We think it could also be a matter to be addressed using a framework of the Three Seas Initiative."

MAREK ZAGÓRSKI

"It's so evident that today we cannot do it alone, whether we are governments, whether we work in the private sector, think tanks, civil society – there is really only one way to try and fix the issues of trust in cyberspace and promoting responsible behaviour in cyberspace, and that is by working on it much closer together."

CASPER KLYNGE

INTERVIEW WITH NATO ASSISTANT SECRETARY GENERAL FOR EMERGING SECURITY CHALLENGES

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Interview was given by:

- Antonio Missiroli – Assistant Secretary General for Emerging Security Challenges, NATO

and chaired by:

- Izabela Albrycht – Chair, The Kosciuszko Institute; President, Organising Committee of the European Cybersecurity Forum – CYBERSEC

BIG PICTURE – WHY THE TOPIC MATTERS?

Never in our lifetimes have we experienced anything like the current COVID-19 pandemic. This may be one of the greatest tests of our world in this generation, and it is also showing that we should and can overcome our differences and stand united. This is the lesson that NATO Allies have learned over the past 70 years – when it matters, we stand together and we can also grow. Despite the impact of the virus, NATO's ability to conduct operations has not been undermined. As other challenges have not gone away with the virus, NATO's forces remain ready and the work goes on (including the multinational battle groups in the east of the Alliance, NATO Air Policing, the maritime deployments and the missions from Afghanistan to Kosovo). NATO is also doing everything possible to limit the spread of the virus, protect the soldiers and the communities they serve. NATO has been working with allies and partners for many years to strengthen their resilience and enhance their preparedness across the public sector including the health care. The increasing mobilisation of armed forces at the national level in the effort against that COVID-19 testifies to the good work that has been done with the allies and partners to strengthen their military in the previous years.

Also, NATO is closely monitoring the digital environment which is changing with breathtaking speed. It is up to institutions like NATO and the EU working hand in hand and with governments to ensure the proper policy frameworks to face the future with confidence. NATO cyberdefense strategy was adopted a few years ago and in fact there is a demand on the part of allies to review it, particularly in the light of the new technological developments that are on the rise.

WAY FORWARD:

- NATO is changing the way it works with industry, with technology companies, startups and traditional defence firms. Its aim is to become less prescriptive and more open to risk. The experimentation must become institutionalised to make it possible to fail early and fail small (if something does not work) and on the other hand to learn quickly and scale fast (if it does).

- In order to fulfil NATO's mission of deterrence and defence, the resilient and reliable communication, transport and energy infrastructures are crucial. Fifth-generation networks are poised to transform the military. This means that 5G will fast become vital national infrastructure and it has to be secured. Apart from 5G, there is also a need to be forward-thinking and looking in addressing vulnerabilities in other new technologies, such as quantum computing and artificial intelligence, which will impact alliance and military operations in ways that are still very hard to predict.
- NATO will probably deliver a new cyberstrategy on the occasion of the next NATO summit that is planned for 2021. Additionally, the innovation unit at the NATO headquarters will be laying out their policy foundation, to enable the Alliance to take full advantage of the opportunities arising from innovative technologies while minimising the potential risk, and also doing an important work in terms of understanding the potential implications of all these technologies. Individual allies are driving change. Therefore, it is important for every ally to contribute and do their part on national resilience, training and education, and capability development (an example of such activities is the mission of the Pentagon's Joint Artificial Intelligence Center).
- Regional initiatives among like-minded countries who share similar challenges, similar history and common future are welcomed by NATO. There is always a scope and room for mutual learning and support in this respect. Any initiative to strengthen individual and common capabilities is and will be supported by the Alliance.

"You cannot build fences that are high enough to keep cyber threats away, though you can do a lot more working with others and learning from others. This is why partnership and cooperation matter."

ANTONIO MISSIROLI

SPECIAL PRESENTATION: CYBERSECURITY IN THE TIME OF COVID-19

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Presentation was given by:

- Rafal Rohozinski – CEO, SecDev Group

BIG PICTURE – WHY THE TOPIC MATTERS?

The COVID-19 crisis resulting in a massive movement of people to the online world demonstrated one of the biggest advantages of the digital tools, which enable the continuity of institutions and social life despite a pandemic. However, it has also brought forward some of the basic truths about the cyber environment that many experts in the cybersecurity field have found, over the last decade and a half, difficult to communicate to decision-makers. COVID-19 has exposed cracks and insufficiencies in how we have been managing the digital infrastructure as a whole. Internal resources, previously protected and accessed through well-defended networks, have now become exposed. They are now being widely accessed through poorly secured endpoints, which cybercriminals and cyberspies are starting to take advantage of. Over the past month, Bitdefender has noted an almost 500% increase in malware related to COVID-19. Malware deployments on unprotected or lightly defended devices have established bridges that might be used in the future. Ransomware has been employed against healthcare providers and there already are several hospitals in Europe that have been hit and numerous others that are under risk because of poor cybersecurity practices. The consequences of successful large-scale cyberattacks might go well beyond those of lockdowns that we are currently experiencing during the COVID-19 pandemic.

MAIN THREATS & CHALLENGES:

- increased congestion, network strain and network failures
- lack of business continuity plans
- poor scalability of the existing tools (e.g. VPNs)
- exposure of internal assets accessible through endpoints that are not well protected
- lack of cybersecurity capabilities and increased vulnerabilities in critical sectors of the economy
- risk of surveillance

WAY FORWARD:

- There is a need of clear understanding that telecommunications and internet resources are a critical national asset, and as a result require a degree of supranational as well as national coordination.
- Regulatory tools which could force providers to be able to share bandwidth in extraordinary circumstances should be developed. However, this is a measure that has to be taken with great care and caution because it does risks a form of surveillance and control over the Internet which also would be unprecedented in democratic countries.

- Business continuity plans that would envision a large amount of employees working remotely should be considered with a greater attention by organisations and institutions. They would include both the security of employees' devices and of communications methods. VPNs do not scale easily and are computationally heavy; as a result, supporting large numbers of users very quickly reaches the physical limits.
- It is also important to mobilise the cybersecurity industry. Hospitals, municipalities and critical infrastructure providers very often do not have the knowledge or the capabilities to simultaneously deal with the stresses of operating in a disconnected environment and manage cybersecurity. Creating coordination and clearinghouse mechanisms for cybersecurity that can match the capabilities of industry with the needs of hospitals, municipalities and other institutions is a priority.
- The crisis is a wakeup call. Our economy, our political system, our institutions (from municipalities and healthcare institutions to critical infrastructure providers) are highly reliant on digital technologies and digital communications. In crises like COVID-19, that dependence becomes even more apparent as people are not able to use any other means for coordinating their activities. Digital public safety needs to become an organic component of digital transformation in all digital policies. This means building infrastructure not just for efficiency but for resilience and it means an investment in the digital hygiene. Resilient infrastructure can be addressed through money and investments while digital hygiene can be accomplished through behaviour change with the aim of creating a well-informed and well-equipped citizenry and workforce.

"Just like the awareness of basic public health and hygiene is at the end of the day what will get us through the COVID-19 crisis, digital hygiene will help prevent and ensure that we never have to face a digital public health emergency in cyberspace in the future."

RAFAL ROHOZINSKI

EU DIGITAL POLICY FORESIGHT: TOWARDS COMMON EUROPEAN DATA SPACES

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Interview was given by:

- Yvo Volman – Head of Unit, Data Policy and Innovation, DG CONNECT, European Commission

and chaired by:

- Samuel Stolton – Digital Editor, EURACTIV

BIG PICTURE – WHY THE TOPIC MATTERS?

Data is crucial for the economy, the efficiency of all the sectors and also for creating new products and new services. This is also an area where there are huge opportunities for Europe. Europe might have missed the wave with the consumer data that has been taken by the big platforms. However, the data that exists today is only a fraction of the data that will be collected in years to come. Thus, Europe still has the possibility to be at the forefront of the data-driven revolution. The Data Strategy is one of the documents the European Commission released as part of its "Shaping Europe's Digital Future" strategy in February 2020. Its aim is to fulfil the vision for a single market for data and tackle the problems identified through policy measures and funding. The strategy is structured around four main pillars: a cross-sectoral governance framework for data access and use; investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability (enablers); empowering individuals, investing in skills and in SMEs (competences); common European data spaces in strategic sectors and domains of public interest. Proposals include the creation of nine common EU data spaces across sectors (industrial manufacturing, European Green Deal, mobility, health, financial, energy, agriculture, public administration and skills) as well as the establishment of the Data Act in 2021 that could foster business-to-government data sharing for the public interest.

Amid the current coronavirus crisis, the subject of how data can be used to citizens' advantage is a question more pertinent than ever. Data analytics holds an enormous potential and impacts the decision-making processes and their efficiency.

MAIN THREATS & CHALLENGES:

- differences between sectors regarding the approach towards data
- replicating already existing solutions instead of creating innovations
- risk of creating sectorial silos
- lack of structures in EU member states that would ensure the proper reuse of data
- prioritising either privacy or public health amid crisis (mutually exclusive or two sides of the same coin?)

WAY FORWARD:

- Europe might greatly benefit from data thanks to creation of a single common European data space. There are a few prerequisites for this: there should be ample of data available for use; data flows must be ensured between countries and between sectors, for the benefit of all; European rules and values must be fully respected (in particular privacy and data protection, as well as competition law); the rules for access and use of data should be clear, practical and fair.
- Because of the differences in dealing with data in various sectors and resulting challenges, apart from the EU horizontal framework, actions in the individual sectors must be taken. At the same time, creation of new silos needs to be avoided.
- Adequate structures to support mechanisms like data altruism or data donation should be created. People should have the possibility to contribute voluntarily to the common good, sharing for example mobility data to improve transportation in the area they live in or health data to combat the disease they are facing.
- With conscious and proactive data handling, both privacy and data use for a specific purpose are achievable. Member states should set up structures and processes to handle the tension between privacy on the one hand (GDPR rules) and the enormous potential of data on the other. The example of such an organisation is Finnish Social and Health Data Permit Authority that decides what health data might be used and for what purposes.
- In order to create a level playing field for companies and cross-border products, all EU Member States must act in the same direction and at the same speed in terms of open government data and access to other sectorial data sets.

"Let's look at areas where Europe really can make a difference like low-power or green data centres. (...) Let's look at the future in terms of secure cloud in the edge. This is not about replicating what exists already to have our own thing, this is looking towards the future, to areas where actually Europe can make a difference and can have an advantage."

YVO VOLMAN

EU DIGITAL POLICY FORESIGHT: BOOSTING EU CYBERSECURITY – TOWARDS THE NEW NIS DIRECTIVE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Presentation was given by:

- Jakub Boratyński – Head of Unit, Cybersecurity & Digital Privacy, DG CONNECT, European Commission

BIG PICTURE – WHY THE TOPIC MATTERS?

The existing NIS Directive is a pillar and a cornerstone of the EU cybersecurity policy framework. The first proposal for the NIS Directive originated in 2012 and was published together with the first cybersecurity strategy in 2013. After intensive negotiation process, the Directive entered into force in August 2016. The transposition period lasted till May 2018 and the NIS now constitutes a part of the regulatory frameworks of all Member States. It became effective six years after policy-making process had been originated, which nowadays is hard to imagine while observing the current dynamic of digital change accompanied by cyberthreats. The review of the NIS Directive is part of the new digital strategy of the European Commission (EC) and is expected to be the main element of a future cyber-package. Despite the fact that the Directive envisaged a deadline for the periodic review to be concluded by May 2021, the EC decided to accelerate this process and carry out the review in 2020. The review is a routine process where the EC looks at the effectiveness of the legislation and its practical impact. As a part of the review the EC will evaluate all aspects of the way the Directive functions, will carry out an impact assessment and indicate possible ways to address the identified gaps. The EC will also be looking into the scope of the NIS Directive and consider whether any additional areas should be subject of the rules as the practice of implementation by member states demonstrated that some countries went beyond the indicated scope and included additional sectors.

MAIN THREATS & CHALLENGES:

- discrepancies in determining operators of essential services in different countries (e.g. there are situations when companies with a similar status are not consistently recognised as OES in all countries where they provide services)
- large degree of discretion in terms of how security measures are being defined in the national law and what incident reporting thresholds are used
- the risk of fragmentation of approaches towards risk management practices

WAY FORWARD:

- The process should be carried on in an in-depth and inclusive manner involving all relevant stakeholders – member states, companies and cybersecurity industry – in an agile and fast-track policy-making process.
- The review of NIS will also give the chance to identify areas where certain measures might be taken, for which EU legislation would be useful, which can collectively reinforce cybersecurity posture of all member states.
- Sharing and comparing practices between the countries in terms of defining the security measures and the thresholds used for incident reporting is needed in order to establish a similar degree of risk management practices.
- Public consultations through online means will be organised. Also, the EC encourages the ideas on the directions of change from all stakeholders.
- It is also important to see the interplay with other parts of EU legislation, first of all with the Cybersecurity Act, but also some sectoral initiatives which are aimed at increasing the resilience, and other related measures in specific sectors. Notably, there is a consideration of an instrument that would address financial institutions in the context of cybersecurity. It's very important to make sure that there is a good alignment between important horizontal frameworks and sectoral developments.

"The review of NIS gives us clearly the chance also of looking where else we can take certain measures, for which EU legislation would be useful, which can reinforce cybersecurity posture of all of us collectively, of all member states."

JAKUB BORATYŃSKI

EU DIGITAL POLICY FORESIGHT: EUROPEAN APPROACH TO DEVELOP SAFE & LIABLE AI

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Presentation was given by:

- Kilian Gross – Head of Unit, Technologies and Systems for Digitising Industry, DG CONNECT, European Commission

BIG PICTURE – WHY THE TOPIC MATTERS?

Undoubtedly, artificial intelligence (AI) as a ground-breaking technology can benefit the economy and society in a great way. In order to compete with the major actors in this domain – namely China and the United States – Europe needs to develop its own European strategy, taking advantage of the large number of experts and existing startups. The European Commission (EC) has been working on the topic for the past couple of years, including establishing the High-Level Expert Group (HLEG) on AI. The work of the EC and HLEG resulted in a number of strategies and guidelines (such as *Communication on Artificial Intelligence for Europe; Communication on Coordinated Plan on Artificial Intelligence; Communication on Building Trust in Human-Centric Artificial Intelligence, Ethics Guidelines for Trustworthy Artificial Intelligence or Policy and Investment Recommendations for Trustworthy AI*). As part of the AI Ecosystem of Excellence, six key actions were identified that are crucial in order to improve the uptake and development of AI: working with Member States to ensure a coordinated approach, strengthening efforts in research and innovation, advancing skills (both to have sufficient workforce to develop AI and to allow the current workforce to find adequate jobs in the environment where some routine or standardised tasks will be taken over by the AI), helping SMEs in digitisation process (through Digital Innovation Hubs present in every member state), working with the private sector, promoting AI in the public sector.

Last year, the new EC President Ursula von der Leyen highlighted the importance of developing a regulatory framework on AI as part of the *Europe Fit for the Digital Age* priority. The much anticipated legislation on AI is to come out by the end of 2020 (potential delays due to the pandemic are likely to influence the schedule).

MAIN THREATS & CHALLENGES:

- appropriate protection of fundamental human rights, such as privacy, freedom of expression, or dignity
- liability allocation between the different actors in the value chain
- high-risk systems employed in various sectors
- high-risk systems existing across multiple sectors (recruitment and remote biometric identification)
- overregulation and fragmentation of the framework
- low degree of SME digitalisation

WAY FORWARD:

- The EU should work towards becoming one of the leaders in the field by developing its own approach based on European values and in tune with existing regulatory frameworks.
- The requirements included in the *Ethics Guidelines for Trustworthy Artificial Intelligence* should be respected and taken into consideration when developing and deploying new AI-based solutions. These are: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; accountability.
- The AI regulatory framework should be based on trust. In order to have trustworthy AI, the following actions are necessary: identifying high-risk systems, working on mandatory requirements and their enforcement, and assessing the impact on other systems. At the same time, overregulation should be avoided so as not to make investments or coming up with new ideas difficult for companies.
- Once a sector is identified as high risk, the question arises how to appropriately address the risks. Inspired by the work of the HLEG on AI, the EC developed some criteria that should be followed:
    - training data (it should be of high quality and respect EU rules and values; not only the data must be accurate, but also data collection should be done without violating privacy rules)
    - record keeping (the relevant data sets and the programming and training methodologies)
    - provision of sufficient information about the AI in the proactive manner
    - robustness and accuracy
    - human oversight.
- Systems that do not fall into the high-risk category are entirely subject to already existing rules such as GDPR. The EU can introduce a qualitative assessment of those systems by voluntary labels, which when obtained could help the operators promote and sell their products as ones respecting fundamental rights and values of the Union.

"On the one hand, we want to push for innovation, we want to push for uptake of artificial intelligence, because we believe it's a ground-breaking technology which can bring a lot of benefit to our economy and to our society. At the same time we acknowledge (...) certain risks and therefore we want to prepare for a solid regulatory framework, which allows us to say that artificial intelligence made in Europe is safe."

KILIAN GROSS

EU DIGITAL POLICY FORESIGHT: SECURING EUROPEAN DEMOCRACY WITH THE DIGITAL SERVICES ACT

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Panel discussion included:

- Karen Melchior – Member of the European Parliament
- Prabhat Agarwal – Head of E-Commerce and Platforms, DG CONNECT, European Commission
- Siada El Ramly – Director General, EDiMA
- Eline Chivot – Senior Policy Analyst, Center for Data Innovation

and was chaired by:

- Samuel Stolton – Digital Editor, EURACTIV

BIG PICTURE – WHY THE TOPIC MATTERS?

In her agenda for Europe (*A Union that strives for more*) the President of the European Commission, Ursula von der Leyen, has pledged to upgrade the EU's liability and safety rules for digital platforms, services and products and complete the Digital Single Market with a new Digital Services Act (DSA). The forthcoming legislation could greatly help in curbing the spread of hate speech and disinformation online by expanding the liability of digital platforms for the content they host and by setting up common rules on online advertising services in the EU, thus reinforcing European democracies in the face of increasing threats. As an attempt to harmonise the laws across the EU, the DSA should respond to the needs and demands of business stakeholders, intermediaries and citizens to ensure safe and secure use of the services through enhanced transparency and accountability rules, specific obligations for cross-border services and improved regulatory measures. The EC's new project is said to target a wide breadth of the tech sector, in particular social media platforms, search engines and collaborative economy services.

Recent trends demonstrate that digital platforms are much more cooperative with each other and more communicative towards EU institutions. The dialogue has recently become mature and the platforms are taking their responsibilities more seriously than was the case in the past. The situation thus indicates that an appropriate moment has come to take further legislative steps in this matter.

MAIN THREATS & CHALLENGES:

- material takedowns as an easier solution than the appropriate content control
- difficulty to ascertain long-term effects of short-term responses that are needed to ensure safe and secure use of the digital platforms
- the question on passive / active role of the platforms (according to the current E-Commerce Directive, platforms have an incentive not to engage with the content they host in order not to be liable for it)

- lack of clear binding procedures on how to deal with illegal content online (according to the current E-Commerce Directive)
- difficulties to define a "political advertisement" which is dependent on the national context (the situation might entail obstacles in imposing the regulations in this matter)

WAY FORWARD:

- It is essential for the European democracy to look at the platforms that EU societies are using in the democratic dialogue and make sure that their rights are protected against hate speech and discrimination with the freedom of expression being ensured at the same time. With the platforms having a dominant role in online lives of many, this is the balance that needs to be sought.
- Self-regulation, co-regulation and voluntary frameworks are a good basis to start from because they enable all parties to learn, share lessons, profit from the experience of others, while improving existing practices and developing new ones. These approaches ensure an implementation of measures that is flexible and involves the responsibility of all. At the same time, such frameworks simplify the rules and reduce legislative burden.
- There is a tendency in the regulation framework to lean towards having a lot of material takedowns as this is an easier solution for the platforms. At the same time, the platforms are not neutral networks that do not know what the content is. Platforms choose to boost certain types of content and reduce the access or the distribution of other types. This is why the regulation that will find a balanced role for platforms and an appropriate level of liability is needed.
- While creating a new legislation it must be underlined that in Europe there are not only big tech platforms but also small ones, and their objectives might differ. There is a need for a framework that will allow the smaller ones to grow and scale up.
- Clarifying the definitions of illegal information and activities is an important step forward in removing the ambiguity and confusion that can exist now. At the same time, some flexibility is needed in order to adapt to the rapidly evolving situation online.
- Being responsible is thinking about the impact of the product and service and it is part of the continued effort that should be carried on together with the regulator. The industry is nowadays actively interested in the mutual dialogue and is turning to stakeholders to seek answers on how things can be organised in a better and safer manner. The EU should take advantage of this situation and engage the online platforms in the dialogue on the forthcoming regulation.

"Platforms have a dominant role in our democracies and our online lives. That's why it's important that we have regulation that provides for protecting our rights when we're online as well as when we're offline."

KAREN MELCHIOR

"Let's really use this opportunity to potentially look at a more ambitious approach, to really deal with content moderation. (...) Let's try and think of what framework we need to have in place to do this in a better way for the long term, bearing in mind that the reality of the technology is going to be completely different by the time any piece of legislation is going to hit the ground."

SIADA EL RAMLY

"I think the EU Code of Practice on disinformation has shown that there is a possibility to work together, enact coordination with tech experts and tackle issues as complex as disinformation issues can be."

ELINE CHIVOT

STATE STREAM: SECURING THE EUROPEAN DIGITAL DNA WITH CYBERDIPLOMACY

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Panel discussion included:

- Marina Kaljurand – Member of the European Parliament; Former Chair, Global Commission on the Stability of Cyberspace
- Heli Tiirmaa-Klaar – Ambassador at large for Cyber Diplomacy, Estonian Ministry of Foreign Affairs
- Carmen Gonsalves – UN GGE member; Head of International Cyber Policy, Dutch Ministry of Foreign Affairs
- Liga Raita Rozentale – Director of EU Governmental Affairs for Cybersecurity Policy and Security of Emerging Technologies, Microsoft

and was chaired by:

- Luigi Rebuffi – Secretary General and Founder, European Cyber Security Organisation

BIG PICTURE – WHY THE TOPIC MATTERS?

The rapid increase of the usage of Internet and the connectivity is calling for clear rules on the behaviour in cyberspace not just by the governments but also by the civil society, technology providers and individual users. The international community must be ready to face the upcoming multidimensional and often unexpected consequences of the new digital world in the security, legal and ethical areas. International norms of responsible behaviour in cyberspace are still under discussion and significant advances of the UN GGE and OEWG processes are long awaited. Also, the European External Action Service introduced a Cyber Diplomacy Toolbox, setting up a framework for a joint EU diplomatic response to malicious cyberactivities, and agreed upon a framework of sanctions. Initiatives are also flourishing at bottom-up levels involving a wide range of actors from states to civil society and private companies, which offer great hopes in times of growing cyberthreat complexity and geopolitical fragmentation of the world. There is a need to further explore and design innovative solutions which will contribute to an effective implementation of cyber-norms, provide a higher level of security in cyberspace, and inspire international community.

MAIN THREATS & CHALLENGES:

- grey zones in the international law which are taken advantage of for malicious activities
- efforts limited to certain geographic areas (e.g. European countries have a high level of cyber awareness but other developing regions don't)
- division between countries regarding the approach towards the Internet and basic concepts

- lack of commitment to initiatives such as the Paris Call from the world's biggest nations (e.g. China, Russia, or the United States)
- lack of inclusiveness and assistance in cybersecurity capacity building
- various levels of digital maturity in different countries

WAY FORWARD:

- Apart from the discussions on the security and threat issues in cyberspace, there is also a need to talk about the responsibilities of all the actors involved and about the multi-stakeholder nature of cyberspace.
- The EU has devoted serious efforts to raise awareness of its organisations and citizens on cybersecurity issues, but these actions should not be limited to the European dimension. It is important to also reach to the regions outside the EU and make sure that many more states and actors in Africa, Asia, Latin America and less digitally developed regions in the world also start to understand the challenges regarding the increasing reliance on the digital technological tools.
- An important aspect of cyberdiplomacy touches on the notion that freedom as it applies offline should apply online. It includes e.g. the freedom of expression, freedom of association or freedom to access the information. The discussions on aspects of what should be done in terms of increasing the Internet freedom globally and making sure that all the countries and citizens can enjoy the same rights online as they enjoy offline should be fostered (Freedom Online Coalition is an example of such platform).
- It is crucial to adopt a realistic approach and know what can be achieved under a specific framework of cooperation. Within the UN process it will be most probably impossible to agree upon the binding instruments or responses against those who violate international law, because countries are too divided. Thus, the UN should have roles such as awareness raising, education, capacity building. The regional level should be seen as the one where tougher issues such as attribution can be successfully addressed.
- The reason why the Paris Call is crucial is that it is the first document which is really multi-stakeholder in its nature. The UN should look into the Paris Call and take it as a basis. The group of signatories should be enlarged in order to have a global document where stakeholders agree on some concrete steps (even if they are not legally binding and they are just a political concept).
- Clarity in the international law is highly demanded as bad actors are using the vague zones of international law as a playground. Clarity might be achieved through concrete actions such as attribution or political statements.
- There is a need to address diversity in the process of finding solutions. As there is no one-size-fits-all answer to any particular problem, there is a need to look at different resources (from governments, civil society or industry) to try to find the best one.
- It is very important to collectively invest in capacity building worldwide and help countries not only defend themselves in cyberspace but also work together and ensure responsible behaviour globally.

"We should send a very clear message that our economy and our political systems depend also on the functionality of cyberspace and we won't tolerate it if this is disrupted by state actors."

AMBASSADOR HELI TIIRMAA-KLAAR

"We should all be mindful of the fact that crises sometimes require different approaches, however, we should not forget that the balance between security and fundamental freedoms should be upheld."

CARMEN GONSALVES

"There should not be difference between online and offline. If we are having sanctions or other restrictive measures for somebody who violates international law in real life – occupation of Crimea – then we should also have restrictive measures and sanctions towards those who are violating international law on the Internet."

AMBASSADOR MARINA KALJURAND

DEFENCE STREAM: ARTIFICIAL INTELLIGENCE CALLED TO ARMS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Panel discussion included:

- Giacomo Persi Paoli – Programme Lead for Security and Technology, United Nations Institute for Disarmament Research (UNIDIR)
- Antonio Missiroli – Assistant Secretary General for Emerging Security Challenges, NATO
- Lindsey R. Sheppard – Fellow, International Security Program, Center for Strategic and International Studies

and was chaired by:

- Ulrike Esther Franke – Policy Fellow, ECFR

CONTEXT – WHY THE TOPIC MATTERS?

AI in military applications may have disruptive effects, create asymmetric advantages, and therefore alter the strategic stability. Cooperation and convergence of views is essential within European and like-minded countries in order to develop future defence capabilities and to use them in a reasonable and ethical manner. The political discussion on the AI in the military seems limited among the European countries. As part of the proactive approach example, the UN has endorsed guiding principles that concern certain crucial aspects regarding the development of intelligent weapons. Among them are: international humanitarian law continues to apply fully to all weapons systems (including the potential development and use of lethal autonomous weapons systems (LAWS)), human responsibility for decisions must be retained since accountability cannot be transferred to machines, and the human-machine interaction has to be designed and implemented in such a way that throughout the entire lifecycle the weapon is in compliance with applicable international law. However, it is worth highlighting that potential military applications of AI are way broader than weapon systems themselves. They encompass among others: logistics, operation and mission planning, decision-making processes, preventive maintenance or resource allocation. In fact, if we look at the technology maturity as of today, one can argue that it is in the non-weapon category that AI could really represent a game-changer compared to current military practices.

MAIN THREATS & CHALLENGES:

- dual use nature of AI
- hampering progress or non-military uses of AI with overregulation
- non-adequate policy framework excluding some key players from the debate

- inflated expectations regarding the technology maturity (LAWS, the most extreme use case of AI in warfare, are not yet mature enough to be fully integrated into a military capability)
- concept and clear definition of the meaningful human control

WAY FORWARD:

- The AI-centred systems should be treated as an ecosystem. It requires much more than just the algorithm and the data to work. It also requires a competent workforce (from investors, senior leaders, developers to users), secure modern computing infrastructure (the software packages, the network infrastructure, the computing capability), and adequate policies and regulations.
- Any measures or initiatives that are taken in the context of LAWS should not hamper progress or access to peaceful or non-military uses of intelligent autonomous technologies.
- There is a tendency to use the term "AI" for applications that do not exist yet and are theoretical. At the same time, non-combat uses of AI are very important but tend to be understudied in the public debate. The areas like logistics, operation and mission planning, decision-making processes, preventive maintenance or resource allocation are the ones where there is a huge potential for AI to increase efficiency.
- There are many ways and frameworks in which the topic of AI in the military might and should be discussed. However, it needs to be highlighted that maintaining the discussion within a UN process is very important as it is one of the very few ways available to ensure that all key national players are involved in the discussion.
- One of the key elements of the UN work should be the clear definition of the concept of meaningful human control, namely defining what it means to exercise meaningful human control on autonomous weapon systems. Is the ultimate decision of using force only the moment where a weapon is deployed or a trigger is pulled, or are there decisions that happen before that point that can be considered as meaningful human control?
- Besides adopting guiding principles, there is also a need to further indicate the way they should be implemented. Principles should not only encompass the end use but also the technology development phase. The example of such an initiative are five principles elaborated by the Defense Innovation Board (advisory body to the US DoD) indicating that the Department should set the goal that its use of AI systems is: responsible, equitable, traceable, reliable and governable.
- One of the major challenges still valid today is the lack of workforce in the field of AI. There is a limited supply of talented researchers and it takes long to train people in-house. Another challenge is then keeping the talent within the military. Funding and other incentives are needed in this regard.
- We need more structured mechanism for multi-stakeholder engagement. The private sector is the driving force behind the development of many AI applications in the military but there is no systematic way for the technology providers, the developers and the researchers to engage in these discussions.

"'AI called to arms' evokes to some extent the risk of an arms race in this particular domain. Arms races are not inevitable, they can be controlled, they can be channelled, they can even be stopped to some extent. I think that in this particular case mitigation and limitation of the possible arms race is really what we should look at in the current strategic context."

ANTONIO MISSIROLI

"Right now, it's a very polarized debate with some countries really pushing for an overarching ban and others having the opposite view. The reality is, there are many shades of grey in between and we need understanding of what should really be banned versus what could be beneficial to reduce harm."

GIACOMO PERSI PAOLI

"One of the biggest things that we're going to see tackled is thinking about how we start laying the foundations for building up the workforce. This is one of the few areas where I think we actually do see true arms race dynamics, because there is a limited supply of talented researchers, it takes so long to actually train those researchers and to get that talent in-house."

LINDSEY SHEPPARD

BUSINESS STREAM: DATA: SOVEREIGN AND SECURE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Panel discussion included:

- Miapetra Kumpula-Natri – Member of the European Parliament
- Cecilia Bonefeld-Dahl – Director General, DIGITALEUROPE
- Pierre Chastanet – Head of Unit, Cloud & Software, DG CONNECT, European Commission

and was chaired by:

- Paul Timmers – Research Associate, Oxford University; Former Director, Sustainable & Secure Society Directorate, Content and Technologies Directorate General (DG CONNECT), European Commission

BIG PICTURE – WHY THE TOPIC MATTERS?

All sectors of the European economy are going to undertake the digital transformation which will lead us to the era of the data-based economy. A success of this process essentially depends on the availability, but also the uptake of data processing capacities and data processing services. The importance, value and amount of data are growing exponentially. Properly managed, it will result in high-quality information and knowledge which will be applied to business models and decision-making processes. As the consequence, it might be extremely powerful and transformative, allowing the technology leaders to gain critical competitive advantage with geopolitical and geoeconomic consequences. Also, the increased interest in cloud computing technology as well as resulting international data transfers entail major challenges regarding compliance, security and privacy requirements. Laws, regulations and strategies differ by countries and are complemented with international policies which, overall, create a complex and demanding ecosystem for all cloud service providers. For all of these reasons data sovereignty and security is a top issue on the European agenda.

MAIN THREATS & CHALLENGES:

- market fragmentation resulting from the development of multiple national data and cloud strategies
- possible attacks on data services infrastructure, especially in the critical sectors of the economy
- sectoral data fragmentation (e.g. health industry)
- small market share of the European providers in the global cloud market
- insufficient level of investments in the European digital market
- potential environmental cost of the digital transformation process

WAY FORWARD:

- Data should be treated as a resource which, properly processed and used, will result in bringing real benefits for the economy. Therefore, as part of the national assets, it needs to be secured. At the same time a discussion about data ownership is a must.
- As we are at the beginning of the data economy and there is still time for many technology providers to get involved in the process, the newcomers should be incentivized in order to gain the competitive advantage in the global market (especially as part of the so-called second wave of data which will mostly rely on the industrial data).
- The proactive approach from the European policy-makers is strongly needed in order to take advantage of the second wave of data.
- One of the most important things in creating data ecosystem is infrastructure, which should be trustworthy, resilient and highly energy-efficient. It should not be built from scratch but rather rely on existing capacities. The already existing cloud initiatives in the Member States (the GAIA-X project is one example) might be built upon and there is a need to foster necessary synergies at the EU level in order to avoid fragmentation.
- It is necessary to bring European capacities together to build a cloud service offering. The offering, to be successful, must respect the rules of the market and be competitive with the existing services.
- While developing data economy strategies, the European values must be always kept in mind: privacy, democracy and open society.
- In order to respond to the societal challenges of these times, the preconditions for the successful digital transformation are: affordability, energy-efficiency and trust that data processing is secure.
- An inversion of the trend between centralised computing infrastructure and edge computing is going to be observed. Currently 80% of the data is stored and processed in a centralised manner, while in 5–10 years 80% is going to be stored and processed at the edge. The opportunities as well as security challenges associated with this change of paradigm have to be carefully considered.

"Data protection is a familiar issue for all of us in the field of data and we need to get the real benefits from it. It's almost like a natural resource."

PAUL TIMMERS

"The public debate is needed as European values are something that we politicians and regulators need to keep in mind and see that privacy, democracy, open society are still respected in the data economy when we go for the digital Europe."

MIAPETRA KUMPULA-NATRI

"Data infrastructure and technologies are really at the heart of the digital transformation that is going to develop in the current decade. The past decade was very much focused on consumer data, the next decade is going to be about industrial data, and that's really a revolution that Europe cannot miss."

PIERRE CHASTANET

"There is a big need for Europe to take the lead in actually coordinating data spaces across Europe in key areas of their responsibility for public sector and to be able to advance public services in a range of areas where we should be much less dependent on where we live."

CECILIA BONEFELD-DAHL

FUTURE STREAM: TECHNOLOGY ALLIANCES: RESPONSE TO GEOPOLITICAL TENSIONS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Panel discussion included:

- Baroness Pauline Neville-Jones – Member, UK House of Lords; Former Minister of State for Security and Counter Terrorism of the UK
- Robert L. Strayer – Deputy Assistant Secretary for Cyber and International Communications and Information Policy, U.S. Department of State
- Sir Julian King – Former Commissioner for the Security Union (2016-2019), European Commission
- Marta Pośład – Director, CEE Government Affairs, Google

and was chaired by:

- Joanna Świątkowska – Senior Research Fellow, The Kosciuszko Institute; CYBERSEC Programme Director (2015-2019)

BIG PICTURE – WHY THE TOPIC MATTERS?

Technology is an essential ingredient of our politics, economics, societal reality, and a strong factor that influences the whole global order. It is fair to state that geoeconomic and geopolitical shifts of our times driven by digital technologies are unprecedented in their nature. Technological supremacy and sovereignty in the digital value chain is increasingly influencing the overall economic and political situation of countries. The digital domain is not only bringing an entire panoply of cyberthreats but also creating space for global struggle for influence and domination. Increasing strategic competition between global powers, especially in the area of emerging technologies, such as 5G, AI, and high-performance computing and quantum computing, can have a tremendous impact on the future of the world. In this context, it seems crucial for like-minded countries and stakeholders to work closely together in order to ensure that further digital development is based on shared values with respect for security, privacy and human-centric approach at its core. What is more, the unprecedented challenges related to the pandemic outbreak will redefine political relations, roles and responsibilities of various players and tech actors. Also, the COVID-19 crisis will inevitably revolutionise the global architecture of supply chains, including the digital one, from rare earths to semiconductors and all that are in between. The international community will have to face very difficult questions regarding how to organise the system all over again and what models to adopt.

MAIN THREATS & CHALLENGES:

- dependency on high-risk vendors and rare earths
- price as a main driver influencing the choice of the supplier
- subsidy models of foreign countries in order to provide cheaper technology

- confusion of two terms: autonomy and autarchy
- difficulties to translate high-level words like "open", "free" into concrete actions
- temptation to abuse the technological tools that will compromise the fundamental rights and democratic values (especially in the times of extraordinary circumstances like COVID-19 crisis)
- pressure for activities like reshoring and relocalisation (steps back from globalisation)

WAY FORWARD:

- With the development of 5G, more and more data is going to be generated and processed. AI solutions will empower certain kinds of critical infrastructure from autonomous vehicles, distribution of energy and water, telemedicine, diagnostics to even, in future, remote surgeries. As more and more personal data is involved in these processes, people are going to demand that their fundamental individual liberties are protected. This is why, when it comes to safeguarding those individual liberties, it is important that the suppliers be headquartered in countries that have the rule of law system and where there is an independent judiciary.

- Transparency about how providers operate is of utmost importance. One of the ways to get transparency is to cooperate with a company that is publicly traded, that has a public board of directors, that has to follow transparent rules about its financial activities, about its compliance with intellectual property protection laws as well as about anti-corruption practices.

- There is a need to remember about the differences between autonomy and autarchy in the public discourse. Autonomy is about having the capacity to act in accordance with your own objectives and your own norms, not to be coerced and under pressure or influence. That is not the same as autarchy, which means cutting off completely, seeking to have total independence from interaction with other partners. That is neither realistic nor desirable. We have to look at ways of being independent of unwelcome outside influence, while still maintaining a network of contacts and cooperation with our allies and partners.

- Even though there are many uncertainties ahead of us, one thing that we can be sure of regarding the COVID-19 pandemic is that the role of technology will only increase and it will have a tremendous impact on the emerging new global order. One of the consequences of this crisis will be even faster, even more intense digital revolution.

- The current COVID-19 crisis will inevitably revolutionise the global architecture of supply chains. On the one hand, it can become an opportunity to invest in new solutions and new alliances that will put security and trust at the heart of technology. But on the other hand, as various actors will struggle heavily with the upcoming economic breakdown, they might want to look for more affordable and sometimes maybe less secure solutions.

- There is a need to think about diversification. If there is a crisis in one area, we have to make sure we have other sources that we can draw on and also channels of cooperation with our allies and partners.

- One of the consequences of the COVID-19 pandemic is the increasing role of the nation states. However, global problems need global solutions and working together on resilience along with supporting other actors through capacity building are among the key elements to succeed.

"Even though there are many uncertainties ahead of us, I think there is one thing that we can be sure of: the role of technology and its impact will in only increase and it will have a tremendous impact on the emerging new global order."

JOANNA ŚWIĄTKOWSKA

"We're also at the time of discovering new ways of how we can work together while recognising the regulatory boundaries that are out there, and as much as that debate wasn't resonating in the past weeks, I think that's gonna be the focus of this week and the following and the week after: how do we value various ideals attached to the free flow of information online."

MARTA POŚLAD

"As we try to tackle some of these issues, and 5G is one example, but there will be lots of other issues that will come up quickly, we have to look at ways of being independent of unwelcome outside influence, while still maintaining a network of contact and cooperation with our allies and partners and like-minded countries."

SIR JULIAN KING

"I think globalisation is going to be under pressure. (...) There will be pressure for reshoring, there will be pressure for relocalisation of activity, there will be pressure for actually drawing back from where we are in globalisation."

BARONESS PAULINE NEVILLE-JONES

SIDE SESSION: 5G NETWORK SECURITY – STATE OF PLAY AND STEPS AHEAD

BIG PICTURE – WHY THE TOPIC MATTERS?

The critical importance and geopolitical significance of 5G paved the way for complex but genuine debates on its secure deployment and implementation. The EU took a leading role in this endeavour and made a strong political statement, e.g. in the Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G (December 2019), and as a result of joint work with Member States put forward a toolbox of risk-mitigating measures, supplemented by supporting actions, to provide a high level of cybersecurity of 5G networks across the EU. The whole process also positively influenced and activated the efforts at the nation-state level concerning the local laws, licensing conditions and the discussions with telecoms. Cybersecurity is crucial to ensure the technological sovereignty of the EU and at the same time mitigate the concerns linked to the rising technological presence of third countries who do not comply with fundamental rights and obligations upheld within the Union. Given the increasing role of suppliers and the complexity of the value-chain interlinkages, the degree of dependency on individual suppliers and cooperation with trustworthy partners have become two of the main security challenges and topics of international debates. The way Member States are going to balance the security and economic dilemmas of 5G deployment within the EU toolbox framework will determine the future of the Union's cybersecurity and prosperity. Therefore, it still needs to be debated during formal and less formal dialogues to make sure it will be as homogeneous as possible.

MAIN THREATS & CHALLENGES:

- balancing economic gains resulting from 5G with appropriate risk management measures
- expanded attack surface area because of the increased amount of connected devices and greater network capacities
- greater importance of software in the 5G architecture and security challenges regarding update procedures (potential insider threat)
- budget pressures (potentially reinforced given the current crisis) and the question whether governments are in a position to afford the security

WAY FORWARD:

- The current COVID-19 crisis demonstrates the criticality of the telecom networks and how essential they are for the business continuity. At the same time, it shows vulnerabilities and dependencies in the global supply chains (also regarding the 5G infrastructure) exposing the need to invest more in technology in Europe and rethink supply chains.

- The current crisis should not be a pretext for governments to spend less on security measures while resorting to the argument that in times of crisis other investments are more urgent.

- It is important to make sure that Member States can compare what respective measures from the EU toolbox are being taken at the national level and what practical impact they have. Member States should also join efforts in standardisation policy to work towards rolling out relevant certification schemes. The dialogue is led by the EC and should be continued remotely even in the difficult pandemic times. At the same time, the role of the EC is broader in terms of looking at the long-term implications such as:

foreign direct investments from adversarial actors, trade instruments and competition policy aiming to ensure technological autonomy.

- In addition to the toolbox principles, some objective criteria could be developed and implemented with regard to how the telecoms should operate, how they should purchase 5G equipment and what policy should be in place.
- Because of the increased importance of software in the 5G network, the trust in the software provider should be a priority. The questions of who produces the code, who is controlling and who is updating it must be a central point of attention for decision-makers. It is also the reason why the certifications schemes which are currently being developed should encompass not only products and services but also processes.
- While talking about the increase of the surface for cyberattacks that the new network architecture brings, it is important to stress that it entails not only additional risks but also potential solutions to address it. For example, in the context of network slicing, it allows to isolate critical functions of the economies. Also, the application of AI might improve anomalies detection and predictions regarding the maintenance requirements.
- Considering the geopolitical strategic importance of next-generation networks, the EU should be more active and also involve and support Balkan countries and Eastern Partnership countries to work together on the 5G implementation.

SIDE SESSION: ON THE ROAD TO THE THREE SEAS SUMMIT 2020 – HOW SHOULD THREE SEAS COUNTRIES SURF THE WAVE OF DIGITAL GROWTH?

BIG PICTURE – WHY THE TOPIC MATTERS?

The Estonian chairing of the Three Seas Initiative Summit in 2020 is a real opportunity to transform political statements and conclusions regarding the digital pillar and the cybersecurity dimension of cooperation into practical and concrete actions, addressing especially the digital infrastructure gaps that still exist between western and eastern part of Europe. The Kosciuszko Institute – as the initiator of the Digital 3 Seas Initiative – remains fully committed to working in this direction to secure the digital development of the Three Seas region and to build the digital pillar of the Initiative.

Through the development of its digital economy the Three Seas region has a unique opportunity to leapfrog other regions in the ongoing struggle for the global value chain position. The current situation and the crisis we are experiencing should not be seen as a halt or a threat to this development, but the digital sector can instead use it as an engine to restart and rebuild the economy. Looking at the projects on the table, the 3Seas1Ocean idea (concept initiated by Exatel) – which consists of fibre optic lines from the Three Seas region to the US – is necessary from a strategic point of view. Business factors as well as geopolitical and military ones are confirming this idea. Indeed, fibre optic lines will improve signal latency by at least 10% and therefore give faster access to continental US from all over the region as well as Ukraine. This will furthermore lay the foundations for the building of the 3 Seas Digital Highway, cloud infrastructure and data centres in the region, which could take this chance to become a champion in providing state-of-the-art infrastructure and services.

MAIN THREATS & CHALLENGES:

- delays in investments in digital infrastructure because of the COVID-19 crisis and unfolding economic depression
- insufficient level of support for regional SMEs
- fragmentation of the market and lack of coordination in capacity building and ecosystem building activities
- research results not sufficiently translated into concrete market solutions and projects addressing regional needs

WAY FORWARD:

- To meet the opportunity, investment in the digital infrastructure of the region has to be boosted. This will allow multiple parties to build foundations for a strong and secure infrastructure and to provide a high-level of digital services.
- The support for regional SMEs should be increased. They have a huge expertise and innovative potential to lead the region towards its digital transformation and help to tackle post–COVID-19 economic crisis.
- Working in synergy with ongoing initiatives – such as the Central European Cyber Security Platform or the V4 – and extending others, more global ones, to the Three Seas region can be an effective way of quickly moving forward.
- Establishing an integrated network of cyber attachés from the 12 countries of the Three Seas region as well as a dedicated secretariat could constitute the basis of a structure dedicated to help in carrying out digital and cybersecurity-related projects.
- It is now the duty of the digital community to support cooperation, innovation and the emergence of creative ideas to, step by step, move the whole Three Seas Initiative forward. Supporters of the initiative should encourage political and business leaders from their countries either to engage in specific projects that are already on the table or to propose new ones and build a synergy with national digitalisation agendas in the EU's new Multiannual Financial Framework.

CSBXL20 TWITTER WALL

#CSBXL20 EARNED +64K IMPRESSIONS

Marina Kaljurand MEP
@MarinaKaljurand

https://twitter.com/MarinaKaljurand/status/1242422933684916225

Thank you #CSBXL20 @CYBERSECEU for keeping the dialouge going! Using communication technology to discuss the technology related challenges. International cooperation – building alliances and shaping the online environment we operate is more paramount than ever.

ECSO
@ecso_eu

https://twitter.com/ecso_eu/status/1242828329121710080

Congratulations to @CYBERSECEU Team for organising yet another great #cybersecurity event, which was all-virtual this time! For those who missed #CSBXL20, check out the jubilee video & save the date to attend the upcoming 6th #CSCEE20 edition this autumn.

Oana Lungescu
@NATOpress

https://twitter.com/NATOpress/status/1242478584821735425

Antonio Missiroli, Assistant Secretary General for Emerging Security Challenges, gave a virtual keynote address at @CYBERSECEU today. He spoke about the importance of innovation & digital technologies and #NATO's strong cyber defence. http://bit.ly/2UhXgSa #CSBXL20

Samuel Stolton
@SamuelStolton

https://twitter.com/SamuelStolton/status/1242504004552310788

Really impressive conference @CYBERSECEU #CSBXL20 today. Everything ran very smoothly. Shows we can all maintain a sense of 'normality' amid these uncertain times. This is the future of Brussels policy events!

Francesca Spidalieri
@Francesca_cyber

https://twitter.com/Francesca_cyber/status/1242558466276962306

Interesting concept on "data donation" or "data altruism" so that people can choose to donate their own personal #data for science or other purposes — no structure exists for people to do this in the #digital realm. But need to build structures and processes - Yvo Volman #CSBXL20

ETNOAssociation
@ETNOAssociation

https://twitter.com/ETNOAssociation/status/1242436821113585667

Our @grassia_paolo is joining @CYBERSECEU's discussion today. His key messages: "in a #5G era we can tackle cyberthreats by using #AI & end-to-end #encryption. Also, telcos embrace multi-vendor strategy as key to security & competitivennes alike" https://m.facebook.com/cyberseceu #CSBXL20

EconDiplomacy@State
@EconAtState

https://twitter.com/EconAtState/status/1242804712119906304

@EconAtState's DAS Strayer participated in @CYBERSECEU virtual Cybersecurity Forum & emphasized the need to ensure communications networks are secure. That security starts with using only trusted equipment vendors in #5G networks. #CSBXL20

Poland in Nato
@PLinNATO

https://twitter.com/PLinNATO/status/1242560121840046080

Congratulations to @ialbrycht, @IKosciuszki & the entire Team for organizing the first fully virtual @CYBERSECEU
Expert discussions on emerging technologies & #cybersecurity in times of #COVID19 crisis are more important than ever.
Thank you, ASG Missiroli for your input.

G. M. Poznański
@G_M_Poznanski

https://twitter.com/G_M_Poznanski/status/1242499849477644289

Thanks for a great conference! As always insightful and inspiring! All appreciation goes to @ialbrycht @j_swiatkowska @BSztokfisz and all @IKosciuszki team and all the #CSBXL20 speakers.

Johannes Nitschke
@jonitschke

https://twitter.com/jonitschke/status/1242472031943155714

Following this year's great digital-only edition of the @CYBERSECEU conference safely from home. Can't help but echo all these great panellists who are stressing the need for #digital hygiene. These measures from #CharterofTrust are as simple yet effective as washing your hands.

CYBERSEC
EUROPEAN CYBERSECURITY FORUM

CYBERSEC BRUSSELS 2020 PARTNERS

MAIN PARTNERS

Microsoft

SAMSUNG

PZU

Google

PARTNER

aws

SAVE THE DATE FOR THE

FIRST GLOBAL EDITION OF CYBERSEC

ONLINE ONLY CYBERSEC

Binge-conferencing experience

on **28-29 SEPTEMBER 2020**