

THE 4TH ANNUAL PUBLIC POLICY CONFERENCE
DEDICATED TO STRATEGIC ASPECTS OF CYBERSECURITY

CYBERSEC 2018

RECOMMENDATIONS

& KEY TAKEAWAYS

EUROPEAN CYBERSECURITY FORUM
8-9 OCTOBER 2018, KRAKOW, POLAND



CYBERSEC

www.cybersecforum.eu/krakow



CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

THE QUEST FOR CYBER TRUST

8-9 OCTOBER 2018, KRAKOW, POLAND

CO-FINANCING INSTITUTIONS



Ministry
of Foreign Affairs
Republic of Poland

KRAKÓW REGION
MAŁOPOLSKA
INNOVATIVE



Consulate of the United States of America

The publication presents the opinions of its authors and cannot be equated with the official position of the Polish Ministry of Foreign Affairs or any of the partners or patrons of the publication.



Ladies and Gentlemen,


Each year, the European Cybersecurity Forum – CYBERSEC becomes a platform of dialogue on the most pressing challenges of the digital world. During lively onstage discussions, thought-provoking presentations and inspiring interviews, the holistic community of professionals and experts share their insights on strategic aspects related to cybersecurity. This year, debates were once again deeply informative, constructive and delivered highly valuable content.

CYBERSEC team is honoured to present the publication containing the set of actionable and tangible recommendations that aim at shaping policies, improving strategies and boosting the quest for cyber trust. As the digital ecosystem is evolving and new global rules are arising, this quest should be a constant and ongoing process, profoundly embedded in the mindset of all stakeholders – from policy-makers to business leaders, academics and experts.

Our distinguished speakers spoke with one voice – we need trust, we need tools to provide it and we need to be agile and less hesitant to act.

We deeply hope that this set of recommendations will be an important source of inspiration and will spur cybersecurity stakeholders and decision-makers on to take bold measures aimed at ensuring safe cyberspace.

Enjoy the read!



We wholeheartedly invite you to attend the next editions of CYBERSEC family events to boost **THE QUEST FOR CYBER TRUST** even further and continue the discussion on safe, sustainable and beneficial digital future.

See you on 20 February 2019 in **BRUSSELS**
and on 19 March 2019 in **WASHINGTON D.C.**

METHODOLOGY OF THE CYBERSEC 2018 RECOMMENDATIONS

During two days of the European Cybersecurity Forum, around 150 speakers discussed how to bolster trust-based cybersecurity. The CYBERSEC team has prepared the recommendations by following closely the statements made by CYBERSEC 2018 participants. This document does not credit any particular person with any particular remark as topics explored in different debates have not infrequently been merged here. Please bear in mind that the experts on a panel were not always in agreement, thus not every assertion or recommendation reflects each participant's point of view. Should you be willing to view any of the following issues in its overall context, please see [the conference footage](#) or contact us directly.

CONTENTS

STATE STREAM



GENERAL REMARKS	4
THE DIGITAL 3 SEAS – LOOKING INTO THE FUTURE OF THE REGION	4
CYBERSECURITY MARKET IN THE 3 SEAS REGION	6
CYBER TRUST IN VALUE CHAIN	6
TOWARDS THE CYBERAUTONOMY OF EUROPE? STRONG POINTS AND BLIND SPOTS	7
ATTRIBUTION AND CREDIBLE RESPONSE AS FOUNDATIONS OF CYBERSECURITY	8
ACTIVE CYBER DEFENCE	9
INTERNATIONAL PEACE AND SECURITY IN CYBERSPACE	9
ISRAEL'S EXPERIENCE IN THE FIELD OF CYBERSECURITY	9

FUTURE STREAM



GENERAL REMARKS	10
IS THE PUBLIC SECTOR READY TO TACKLE CYBERSECURITY CHALLENGES?	10
CYBERSECURITY OF POST-QUANTUM CRYPTOGRAPHY	11
THE ROLE OF CLOUD COMPUTING IN BUILDING CYBERTHREAT RESILIENCE	11
BLOCKCHAIN – TECHNOLOGY THAT HELPS BUILD TRUST?	12
CYBERCRIMES OF THE FUTURE	13

BUSINESS STREAM



GENERAL REMARKS	14
5G AND CYBERSECURITY	14
CYBERSEC HUB: CYBERSECURITY VS INNOVATIONS	15
GDPR	15
THE INTERNET OF THINGS AND CRITICAL INFRASTRUCTURE – NEED FOR TRUST	15
LABELLING & CERTIFICATION LANDSCAPE – BUILDING A TRUSTWORTHY ICT INDUSTRY	16
CYBER TRUST IN BUSINESS	17
360° APPROACH TO CYBERTHREATS OVER CRITICAL INFRASTRUCTURES & INDUSTRIAL IOT	18
BUILDING CYBER RESILIENCE INTO CURRENT AND NEXT GENERATION ENDPOINT DEVICES	18

DEFENCE STREAM



GENERAL REMARKS	19
OPERATIONALISING CYBER DEFENCE – A KEY SHIFT IN NATO POLICY AND PLANNING	19
FOLLOWING DIFFERENT PATHS, SHARING THE SAME GOAL – EU-NATO COOPERATION ON CYBERSECURITY	20
INTELLIGENCE-POWERED SECURITY: CAN TERROR INVESTIGATION METHODS HELP CRACK CYBER INVESTIGATIONS?	21
CYBER ELECTROMAGNETIC ACTIVITIES (CEMA)	21
HARDWARE SECURITY IN PUBLIC PROCUREMENT	22

STATE STREAM



GENERAL REMARKS

- EU and NATO as well as its Member States must take bolder and more decisive actions when it comes to cyber attribution. This is the only way to establish a deterrence value.
- States should overcome the taboo of discussing the need to develop offensive capabilities and at the same time keep in mind that international law applies to offensive capabilities.
- States should come together and continue the United Nations Group of Governmental Experts (UNGGE) process. However, they must change the *modus operandi*. It has to be **open**, it has to be **transparent** and **inclusive**. Inclusive is understood in a broad sense involving multi-stakeholder approach: business, industry, civil society, academia, technical community.
- Western democracies should be much more active in promoting their understanding of the use of ICTs – how cyberspace can change countries in various sectors: economy, governance, society, education, awareness. Those actions must be based on dialogue.

THE DIGITAL 3 SEAS – LOOKING INTO THE FUTURE OF THE REGION

- 3 Seas countries should jointly apply for and then make use of the financial resources available in the new EU Multiannual Financial Framework to implement projects in the digital pillar. The priority project in this area is the **3 Seas Digital Highway**. Examples of funding sources are the Connecting Europe Facility and the Digital Europe Programme. In addition to European funds, it will also be important to allocate national resources for these purposes. In the near future, efforts should be undertaken to prepare specific investment plans.
- One condition for further economic growth in the region is the use of available modern technologies to solve the identified development problems. **The synergy of technology, solid digital infrastructure and the free flow of non-personal data** can propel the region forward.
- It is recommended to identify and develop “**the region’s digital specialisations**”, i.e. projects that would be hallmarks for example in the healthcare sector and industry 4.0. The growth should be firmly based on cooperation and high operational scalability.

- For modern economies the cornerstone and the engine of growth is data. In order to fully use their potential in the 3 Seas region, it is necessary to develop digital infrastructure that will enable further projects in the field of data-driven economy, including for example **“virtual data repositories”**.
 - Implementation of many modern technologies, for instance cloud computing, requires trust. Trust is built on transparency of technology and verification of security and privacy (using, among others, certifications or standards). The mechanisms of building confidence in digital technologies should be employed and promoted throughout the region.
 - An important element to build the Digital 3 Seas should be a further development of **Digital Innovation Hubs** (including those dedicated to cybersecurity) and their cooperation. In Central-Eastern Europe, their number is the lowest in the EU.
-
- **Cybersecurity has to be the cornerstone of each and every activity and project in all three 3 Seas pillars: energy industry, transportation, digital dimension (cybersecurity by design). The do-things-fast-and-fix-them-later way of thinking has to be abandoned, especially since digital solutions are today the foundation of critical processes which the socio-economic security depends on.**
-
- Within the 3 Seas region, projects that **enhance cybersecurity cooperation** ought to be given emphasis. Possible cooperation areas are:
 - R&D,
 - collaboration by CERTs,
 - cooperation among law enforcement agencies,
 - creating an early warning platform based on information exchange; joint actions against hybrid threats should be expanded in this context,
 - creating a capacity building platform built on the basis of exploiting the intra-region potential, including not only people but also cybersecurity companies,
 - integrating cybersecurity with components of broadly understood security, also in its more conventional sense,
 - active participation in the process of building norms of responsible conduct in cyberspace; establishing standards for states concerning their actions below the threshold of armed conflict is a key issue as effective legal protection in this respect seems lacking.
 - Private entities, academia and non-governmental organisations should be involved from the start in activities related to the development of the Digital 3 Seas Initiative.
 - Strengthening much-needed collaboration between public and private stakeholders, among the former **(G2G)** and the latter **(B2B)**; the Cybersecurity Tech Accord initiative and its regional dimension is a perfect example of such cooperation.
 - Regional initiatives ought to be developed in broader synergies, even transcending the initial region. For instance, the Digital 3 Seas Initiative can be linked with The Digital Agenda for Western Balkans. One possible way of integration is to transfer best practices to these countries by comparing and relating existing and planned models of digitisation, development of skills and certification.

CYBERSECURITY MARKET IN THE 3 SEAS REGION

- **Education of customers** is the prerequisite for boosting the cybersecurity market in the region. **Awareness raising** among business entities, especially SMEs, should be perceived as a crucial task for the coming years.
- The 3 Seas market is heavily dependent on public sector procurements, including public owned or controlled entities. There is an urgent need for raising the level of cybersecurity knowledge amongst public sector employees and decision-makers to make them aware about their needs, existing threats and possible solutions.
- To engage with customers, cybersecurity businesses should also cooperate between each other (**B2B**) and with public institutions (**B2G**) in areas such as cyberthreat information sharing or awareness campaigns.
- More companies from the 3 Seas region have to take an active role in global platforms of collaboration on cybersecurity issues such as the Cybersecurity Tech Accord.

CYBER TRUST IN VALUE CHAIN

- The concept of the security of the digital value chain is central to all activities in the area of cybersecurity.
- **Securing the digital value chain** is thinking about end-to-end ecosystem. It involves anyone engaged in any of the lifecycle stages of ICT technology and solutions, whether it's software, cloud service or hardware, etc.
- In the interconnected world, we are entirely interdependent. The critical issue is to identify third parties upon which we rely and to implement effective security requirements.
- **Private-public cooperation** is the key. We need to identify fundamental security requirements based on international solutions. We should think globally – not about regional or even country-specific solutions.
- While thinking about cybersecurity, we need to look at the full spectrum: physical security, logical security, operational security, behavioural security, information security and security of technologies.
- Trends for the future:
 - **enhanced intelligence** – we will observe increased utilisation of the human element of risk control enhanced by machine speed,
 - **the convergence of information technology (IT) and operational technology (OT)** – that convergence has not been fully manifested yet. What is more, the exponential rate of proliferation of the IoT devices around the world introduces new types of threats,
 - the use of **distributed ledger technologies (DLTs)** for more secure solutions.

Research shows that around 75% of security incidents involved a third party.

TOWARDS THE CYBERAUTONOMY OF EUROPE? STRONG POINTS AND BLIND SPOTS

- Autonomy should not be understood as an equivalent of isolationism, but as measures towards **ensuring resilience**. There is a fundamental difference between strategic autonomy and strategic autarky.
- It is important to have European capabilities to understand, analyse, assess and evaluate the risks and the level of cybersecurity of given products and services.
- The Common Criteria (ISO 15408) serve as principles of certification which may be used as an example of how the process can work.
- It is also worth underlining that standards serve as a precondition of certification process. Cooperation in choosing and developing standards is essential.
- We should not **develop standards** country by country but in close cooperation – **a common approach** at the EU level is needed.
- **EU certification framework** will have to be realistic and useful – carefully crafted to respond to real needs. For instance, we can focus first on an affordable scheme for consumer products.
- **Cyberautonomy of the EU** brings business opportunities in the form of financial proposals for various initiatives. The initiative of Public-Private Partnership (cPPP) in cybersecurity, the European Cybersecurity Competence Network – are just examples. These opportunities should be taken advantage of. They will allow technology, research community and industry to come together and bring cutting-edge cybersecurity solutions.
- EU Member States' governments should be in a position to procure these technologies in a collective manner.
- Competitive advantage of the European technologies may be related to the **trust value** they can offer, further strengthened by the EU regulations.
- **Transparency of cybersecurity industry** is the key. Finding the right balance is challenging but essential: policy-makers should outline goals and levels of transparency to be reached. However, industry should be granted some flexibility in achieving these. An additional regulatory oversight of the process is needed.
- Both global business and the public sector are sharing responsibility for making cyberspace more secure. But we need to move from declarations to actions, therefore **information sharing**, being still at the centre of discussions on cybersecurity, should be enhanced. The following actions may enhance the process:
 - developing a system of incentives for information sharing,
 - eliminating potential risks to the business,
 - improving the communication between governments and the industry (the public sector should come up with ideas of mechanisms on how to provide information that they have, for instance on vulnerabilities, to the industry) in order to improve security of their products and services.
- Better implementation of the European R&D programs is crucial. The industry should take advantage of the projects' outcomes.
- The EU should develop research capabilities in the area of cutting-edge technologies – AI, quantum computing, etc

ATTRIBUTION AND CREDIBLE RESPONSE AS FOUNDATIONS OF CYBERSECURITY

- Attribution should be treated not only as a technical challenge, but also as a political one which requires more cross-domain approach.
 - It is worth bearing in mind that **attribution has a different meaning for corporate entities and for state actors**. For the corporate entities main reasons to attribute are: to meet the criteria of compliance vis-à-vis regulators or to deal with insurance. For state actors it is mostly a matter of national interests and security.
 - Attribution is very important but it's not enough – timely and credible responses are needed for effective deterrence. Otherwise there is a risk of creating a norm of inaction.
 - Trust is a very important element of attribution – the question should be posed: how are governments going to induce more trust within their respective audiences. Developing a **consistent, high-level messaging** is the key.
- THREE MAIN TYPES OF ATTRIBUTION**

DIPLOMATIC ATTRIBUTION

CRIMINAL JUSTICE ATTRIBUTION

REMEDiating ATTRIBUTION
-
- **The development of the EU Cyber Diplomacy Toolbox should be pursued – one potential dimension for further action is to enhance community building, boost cooperation among entities that may contribute to attribution, including the private sector and non-EU states.**
-
- There is a need to balance conflicting elements in the context of attribution. Some countries require irrefutable proofs to confirm attribution but falling into an evidentiary standard trap should be avoided. At the same time there is a legitimate lack of standard or rule against which we can hold actors accountable – there is room for improvement and discussion in this area.
 - As regards possible deterrence activities, internet governance ecosystem should be completely off-limits.
 - Apart from better attribution, stronger prevention is needed. 90% of cybersecurity problems that affect most entities in most circumstances ultimately come down to preventable things. Simple measures like protective DNS, two-factor authentication, legitimate software, patching, whole disk encryption may bring remarkable change.
 - The EU can do much more in terms of reconceiving the entire cybersecurity ecosystem. It is not purely a political and military issue, but also an economic one. In this context, the size of the European market gives it quite substantial weight, and this should be treated as a tool with which Europe can shape its competitive advantage.

ACTIVE CYBER DEFENCE

- It is high time to change the approach towards cybersecurity from passive to active – which means taking steps, often small, which will increase cybersecurity posture within organisations. The UK government created the **“Active Defence” framework** composed of a set of automated and free-to-implement measures which help a user to eliminate numerous cyber risks. Similar activities could be introduced in different countries.

INTERNATIONAL PEACE AND SECURITY IN CYBERSPACE

- **Norms of responsible behaviour** in cyberspace should be developed with strong involvement of all stakeholders – coming from public and private sector and civil society.
- The process of **building norms** should go beyond like-minded countries. The point about international norms is to include everyone, even those countries that one perceives as adversaries. That is why the UN GGE process must be continued. However, it should be more open and transparent.
- Norm development process must be followed by a **deterrence strategy** intended to impose costs on those who do not follow the rules of the game.
- As they prepare a future binding treaty, policy-makers have to draft it very carefully, since some players might want to hijack this process for their own benefit.
- Undisturbed functioning of DNS is one of the key issues when it comes to internet stability.
- In the context of **multi-stakeholder approach** each actor has its own specific and individual role and should operate within its scope of responsibilities.
- While creating international processes related to cyber issues, a **step-by-step approach** should be undertaken. It ought to encompass a combination of small steps channelled into a process linking together the military, political and economic perspectives as well as human rights and technical issues. A decentralised but coordinated approach would be beneficial.

THREE MAIN PILLARS OF CYBER STABILITY

APPLICATION OF INTERNATIONAL LAW

RULES OF RESPONSIBLE STATE BEHAVIOUR

CONFIDENCE BUILDING MEASURES

ISRAEL'S EXPERIENCE IN THE FIELD OF CYBERSECURITY

- The Israeli example shows that **governmental resources and determination** are strongly needed to create a successful cybersecurity framework at the national level involving academia, industry, etc.
- The public sector may provide its assistance in many innovative ways. For instance, it can create a system of **mobile incident response teams** that may help the entities who are victims of cyberattacks.
- Having an agency, a person or a body responsible for cybersecurity placed in the system and reporting straight to the Prime Minister is very beneficial.

FUTURE STREAM



GENERAL REMARKS

- **Bug bounties** undoubtedly bring some benefits to the cybersecurity ecosystem, but are actually not the solution for the future.
- **Secure development and maintenance** are the launching pad for the vulnerability prevention and the safeguarding of the ecosystem. We need to have more secure coders and we need to start looking at the labour market as a whole.
- Destruction should not be incentivised. Instead, there is a need to build **more resilient creators** and to **support and celebrate the maintainers**.
- Over-romanticisation of the hunting element within the bug bounties initiatives risks missing the entire workforce that needs to be prepared for the future.

IS THE PUBLIC SECTOR READY TO TACKLE CYBERSECURITY CHALLENGES?

- What can be observed in the area of cybersecurity is a “**cybersecurity rhetoric gap**”. It means that on the one hand, governments and private sector vocally commit to strategic cybersecurity decisions (investments, strategies, etc.) and declare actions. On the other hand, it is not reflected in their everyday activities, like for instance in public procurements.
- To improve their cybersecurity posture, countries should include security criteria in procurements for the basic IT infrastructure, and price should not be a decisive factor. Cybersecurity can and must be strengthened through public procurements.
- It is strongly recommended that public sector and public procurement bodies talk more to their IT security agencies and implement cybersecurity strategies through public procurements.
- Secure public procurements should carefully look at action plans, targets, specific procurements criteria, and specific certifications, to really help national procurement bodies tackle existing challenges.
- There is an important piece of legislation – the EU public procurement directive – that is going to be reviewed. Taking an example from the chapter called “green public procurements” for instance, which sets out a requirement to procure in an “environmentally friendly way”, a chapter called “**secure public procurements**” should be included.

- It must be underlined that a lot of the security solutions that are software based rely on the fact that the device itself is secure. Therefore, **security should be perceived in a holistic way**.

CYBERSECURITY OF POST-QUANTUM CRYPTOGRAPHY

- Europe must speed up building its own quantum machines. Also, apart from quantum hardware, there is a need to develop quantum software.
 - The **European crypto policy** should be created and implemented.
 - Governments should invest in the research to build quantum repeaters.
 - The problem with quantum computer hacking is that the victim may not even know that the attack is happening. Quantum computers will be able to hack into encryption systems by forging the network route and certificate authority. It is therefore crucial to address this problem.
 - It is recommended to integrate classical and quantum technologies and benefit from the advantages of quantum.
 - It is absolutely crucial to secure routing on the internet in order to prevent potential network traffic takeovers.
 - There are three areas we need to focus on:
 - **Lack of proof of trust** – how to update older devices and older encryption methods in order to protect users.
 - **Setting standards** for crypto agility within organisations.
 - **Entities must keep in mind that the encrypted data they store today might become readable in the foreseeable future due to the quantum developments. There is no time like the present to begin to think about the various methods of protecting data against potential decrypting operations in the future.**
-

THE ROLE OF CLOUD COMPUTING IN BUILDING CYBERTHREAT RESILIENCE

- **Highly reliable cloud solutions allow their users to increase security** while saving budget on cybersecurity specialists. Many companies cannot afford to hire employees with high cybersecurity expertise. Cloud providers are capable of providing clients with secure solutions regarding data management.
- The cloud often brings a better level of resilience. For instance: denial-of-service attacks succeed rather poorly in cloud environment compared to an enterprise environment. It also enables quicker patching conducted on the core infrastructure.
- Implementing cloud solutions is much faster than creating private environment.
- In a cloud environment, **interoperability** is key. It helps to mitigate the vendor lock problem and potential loss of visibility. Interoperability also helps to be able to work in multi-cloud environments.

- **Security of the cloud** should be differentiated from **security in the cloud**. When it comes to the latter, there is still a lot of responsibility that must be taken by the user. For instance, how one manages data and applications.
 - It is advised to discuss security needs with the cloud provider and get assurance in the written contract. Things that can be specified include for instance: location of the data, access rights (super user rights), data transit to the cloud, data portability, encryption, etc.
-
- **European cloud security certification scheme**, which will be built on existing solutions and which will define common technical controls for cloud security at the European level, can significantly increase trust and transparency. Security can be sector-oriented and in the future we should move towards sectoral guidelines and requirements for cloud services.
-
- **Cloud Controls Matrix** provided by Cloud Security Alliance is a useful tool in the context of security. It is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.
 - Security of cloud services should be designed by merging the standard products approach and custom-made products approach.

BLOCKCHAIN – TECHNOLOGY THAT HELPS BUILD TRUST?

- The current cybersecurity paradigm, frameworks and controls are antiquated. The array of vulnerable things has significantly expanded and so has the attack surface. Blockchain could potentially be **the ledger to keep track and to monitor the identity** of those things. Unlike most cybersecurity solutions – which reduce functionality, increase cost, limit interoperability – blockchain has a cybersecurity value proposition.
- Blockchain's promise is to turn the big data problem into **big data opportunity**. Hashing and storing the "who, what, when and where" data enables to use that data while protecting users' privacy.
- The challenge is that there are some real-world use cases, but it is still at a nascent stage. To explore possibilities of technologies there is a need for **pilot projects, research**, and the increase of real-world use cases. About 90% of the early-stage projects will probably fail, but it is the successful 5 or 10% that will completely disrupt the ecosystem and will create major changes.
- There is a need for **the workforce development** and for **the multidimensional approach**. Education, awareness raising, and skills creation are essential.
- At the end of the day, it is all about trust. Blockchain has the potential to disintermediate many third parties that are creating inefficiencies in the current system. Banks, aggregators, distribution system operators are there because trust is not a commodity. The exciting promise of blockchain is that it can help get closer to the commoditisation of trust.
- Blockchain has the potential to increase **the trustworthiness and integrity of critical infrastructure** and is a good solution for critical assets in four areas:
 - identity management,
 - asset management,

- configuration management,
- supply chain security.
- From the policy and regulatory point of view blockchain is still a nascent topic and needs to be defined. The way experts, politicians, stakeholders describe and comprehend blockchain is very different. The **challenge is therefore outside cybersecurity** – there is a lack of policies, lack of definitions, lack of standards, lack of regulations, and lack of uniformity. If a global infrastructure based on blockchain is to be built, a common terminology is a crucial element.
- There are certain areas that need to be regulated (even if it is light-touch regulation) to avoid a fragmented approach. Three **main principles in the blockchain regulation** process on the EU level are:
 - business neutrality,
 - innovation principle,
 - horizontal approach.
- If there is a risk of overregulation (some industries are overregulated), the concept of **regulatory sandbox** should be considered. There is a need to make sure that the problem being solved is the one worth solving.

CYBERCRIMES OF THE FUTURE

- Private-public cooperation is developing vividly in the area of combating cybercrimes. **The cooperation between law enforcement and intelligence services** is also expected to increase.
- There are strong expectations towards regulating the IoT. Such regulations could help to effectively tackle cybercrimes.
- While thinking about preventing cyberattacks, one needs to remember that in many cases basic security actions may significantly contribute to the overall level of security.
- It is recommended to complete the legislative process related to the **Regulation on European Production and Preservation Orders** for electronic evidence in criminal matters.
- Countries should enter bilateral agreements with the USA on the grounds of **the CLOUD Act**.
- In the cyberthreat landscape, it is clearly visible that the threat actors are moving up the value chain, especially in the financial sector. The change should also be reflected in the counteractions.
- The focus of the attacks is also shifting from the individual user towards the commercial banking sector. A lot of corporate banks are affected. Criminals are spending increasing amounts of time on getting into the core banking infrastructure and they are getting increasingly more professionalised in their efforts. In addition, cryptocurrencies are probably going to be consistently targeted.
- In the future we might observe **cyberattacks impacting overall markets**, either by causing significant disruption or by altering the data.
- Erosion of trust in cyberspace can be strictly related to **the security of the value chain**. This is an area of activities where we should put in a lot of effort.

BUSINESS STREAM



GENERAL REMARKS

- We need to start introducing trust into the computational infrastructure. Product liability should apply to software providers and service providers. Accountability is needed in order to make the infrastructure trusted and trustworthy for future users.

5G AND CYBERSECURITY

- **5G development must be indispensably correlated with security activities** and for instance integrated within the national cybersecurity strategies.
- For the 5G development it is crucial to take down some legal barriers. All stakeholders must make sure that prerequisite conditions (related to the investment process for instance) are met in order to develop the 5G network in the planned time frame.
- While developing 5G it is recommended to keep in mind that **customer-oriented needs cannot undermine the security aspects** – security and functionality need to be advancing in parallel.
- The problem of spoofing, creating fake access points should be addressed. **Monitoring security** and **creating rapid response tools** are essential.
- Security responsibilities of the producers of devices connected to the network should be underlined.
- In the security context it is necessary to **increase the users' awareness**. All users (private and public) should feel responsibility for their behaviour when it comes to cyber hygiene.
- **Capacity building** is the key. More developed countries should work closely with countries which do not have enough resources and capabilities and help them develop national cybersecurity strategies which incorporate 5G security. This should prevent the occurrence of gaps.
- **5G infrastructure operators and owners should build their business models on a public-private scheme that would increase trust and provide increased efficiency and security.** Infrastructure operators and owners will have the greatest impact on cybersecurity; therefore, the decision how and with whom to act is absolutely crucial.
- Artificial intelligence and a new model of machine learning must support the analysis and prevention in the context of 5G security.

CYBERSEC HUB: CYBERSECURITY VS INNOVATIONS

- Hackers are innovative and use novel, disruptive technologies. To face that challenge, companies have to be open to cooperation with more agile service and product providers, including start-ups.
- Cybersecurity **start-ups need local partners** to scale-up and expand internationally. Breaking the glass wall between big players and young companies is a must for the competitive cybersecurity sector in the 3 Seas region.
- Start-ups have to build their credibility by cooperating within **cybersecurity ecosystems** such as local digital innovation hubs or clusters.
- To make the most of a competitive advantage provided by high supply of developers and industrial engineers in the 3 Seas region, Poland and other countries should **support the development of smart specialisation** of their start-ups ecosystems, for example in the fields of Industrial Control Systems Security and Software Security.

GDPR

- Conducting **regular reviews or assessments of GDPR implementation** (as Commissioner Věra Jourová proposed) is necessary in order to ensure the longer-term perspective and evaluate the progress.
- Ensuring a linkage and consistency between future regulatory pieces on cybersecurity and privacy is crucial.
- The need for **collaboration and consistency of GDPR at the international level** is pressing. Regarding extraterritoriality of GDPR, a massive work ought to be done by the European Data Protection Authorities and their counterparts in the rest of the world to assess the practical dimension of law application.
- **Cyber-diplomacy** is a good tool to promote GDPR globally.

THE INTERNET OF THINGS AND CRITICAL INFRASTRUCTURE – NEED FOR TRUST

- **NIS directive** should have a wider scope, covering not only services provided by essential services operators but also those within the whole supply chain.
- Security should be considered a **shared responsibility**, starting from manufacturers to consumers of IoT devices.
- Key players, including public bodies, need to take a **proactive approach** and lead the way in adopting a **responsible behaviour** as a contracting party. Any supplying IoT company should meet some prerequisite conditions in order to be able to sign a contract.

- **Incentives** coming from the public procurement may significantly boost the security market. They would also contribute to shifting the governments' image from bodies which are only imposing legislation to responsible actors in the secure network and information systems value chain.
-
- **Product liability and responsibility** should be imposed on the manufacturers of IoT devices.
 - The **European cybersecurity certification framework** should be completed on a specific sectoral basis (industry-specific or device-specific).
 - Setting up **public-private partnerships** is essential to carry out various projects, for instance dedicated to security of industrial control systems. In order to put those types of projects in motion it is recommended to have government resources. It would be beneficial to create a laboratory able to run complete tests for private companies or new research projects for academics. Activities of this kind could contribute to overall security and mobilise different actors to engage in this process.
 - **The security of supply chain** should be addressed by:
 - conducting intensive national or international testing,
 - setting the achievement of end-to-end security as an objective,
 - increasing the level of transparency by creating conditions under which detection and reporting of vulnerabilities would be easier.
 - All regulations ought to be designed in such a way that they will boost the **culture of risk management** rather than simple "checklist" behaviours.
 - Israeli example of "lean regulation" needs to be considered. Regulation should describe what needs to be achieved rather than prescribe detailed measures. In the meantime, government should actively engage as a partner in activities such as advising and recommending.

LABELLING & CERTIFICATION LANDSCAPE – BUILDING A TRUST-WORTHY ICT INDUSTRY

- Trust is essential to accelerate the take-up of fragmented retail marketplace across the 28 EU Member States. There is still a lot to do to encourage users to trust services across Digital Single Market – 47% of Europeans who have been online never buy goods and services from outside their nation-state.
- Despite effective progressive policy regime within Europe in recent years, initiatives such as GDPR and the NIS Directive are not a shield for trust. They are a good move but they don't guarantee trusted services – therefore, looking at other **ways to encourage trust, via certification or labelling**, is a must.
- Countries should cooperate on the practical side. "**Blueprint for rapid emergency response**", a measure proposed by the European Commission, is a soft policy recommendation, stating that in case of large-scale incident there is a need to be prepared to work together from the technical/tactical level to strategic level up to the political level. Such actions need to be exercised. Today's policy says to be proactive, namely, to be prepared for threats and also to have a backup policy that encourages engagement, for example in the form of exercises and staff training.

- Challenges in building the **European-wide system for certification**:
 - It is fundamental to get together the public and the private sectors to start a dialogue. When talking about cybersecurity, all the sectors (from components, processes, services) and various kinds of products need to be considered.
 - The interconnection of digital services must be increased. If more services were integrated on the national level and regional level, more and more citizens would be using them.
 - It is important to determine what is helping the academics to commercialise the research. There is still a gap in this area and further steps in this direction would help to build the capabilities.
 - There is a need to think about the security of IoT before designing it and even before having certain kind of certification.
 - There is a need to discuss the question about the sense of repeating the evaluation, certification or labelling independently for different countries. It is true that they vary in terms of maturity or skills but challenges and threats remain similar.
 - Over time the threats evolve and, given that cyber environment is changing, what was correct yesterday is not necessarily correct today. Certification only holds for one particular moment of time.
- The industry needs to focus on **detection of the penetration** in four major areas:
 - how to **protect identity** – identity is the most targeted area right now,
 - how to **build secure ecosystem** and how to **protect supply chain** – how to protect application between a vendor and implementation environment,
 - how to effectively **monitor networks**,
 - how to **protect the data** – validation of the data when it is entering into the system and process.

CYBER TRUST IN BUSINESS

- Trust requires building an **innovative security framework** in devices on all layers – hardware level, application layers and throughout the whole development lifecycle.
- Trust requires **compliance with standards**.
- Security posture is needed while creating products and should include:
 - implementation of security development lifecycle, meaning that security and privacy are addressed from the very beginning (including risk analysis),
 - usage of automated vulnerability scanning systems – vulnerability identification should be immediately followed by patching,
 - rigorous testing before releasing products,
 - constant monitoring and product maintenance.

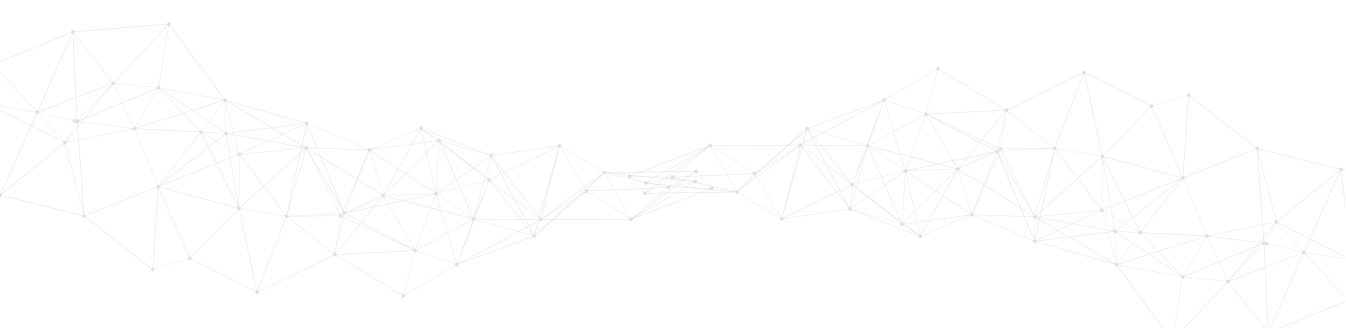
If you fix a security flaw or vulnerability in the operation and maintenance phase, the cost is 30 times bigger than when you discover the potential risks in the planning phases.

360° APPROACH TO CYBERTHREATS OVER CRITICAL INFRASTRUCTURES & INDUSTRIAL IOT

RECOMMENDATIONS FOR GOVERNMENT:	RECOMMENDATIONS FOR PRIVATE SECTOR:
<ul style="list-style-type: none">• Identify the most valuable assets at the national level.• Provide guidance for different actors within the system.• Regulate and supervise business but at the same time act as a partner.	<ul style="list-style-type: none">• Rely on standards but adjust them to the culture and characteristics of an entity.• Identify critical assets and analyse risk.• Perform intelligence activities to know the threats.• Manage supply chain security.• Test, verify and implement solutions.

BUILDING CYBER RESILIENCE INTO CURRENT AND NEXT GENERATION ENDPOINT DEVICES

- Endpoint devices must be constructed in a **cyber-resilient way**. It will require thinking about security throughout the whole value chain. It is crucial to be able to protect the device, detect potential breaches and find mechanisms for a quick recovery.
- Resilience requires also the implementation of **new security approaches**, for instance implementing state-of-the-art AI.



DEFENCE STREAM



GENERAL REMARKS

- Building cybersecurity means **taking care of technology, workforce and processes**. These elements need to be strengthened.
- Workforce should be trained with the **use of cyber ranges**.
- Strengthening the **trust-based collaboration** is crucial. It involves, among others, standardised cybersecurity processes and streamlining the training and organisation of the cyber workforce.
- Building **cyber-resilience** for mission purposes will be one of the most challenging tasks in the future.
- **Cyberthreat intelligence capabilities** must be significantly increased.

OPERATIONALISING CYBER DEFENCE – A KEY SHIFT IN NATO POLICY AND PLANNING

- Effective deterrence requires more **acts of public attribution**. Solidarity between EU member states and NATO allies is the key in this area.
 - Regarding the usage of offensive tools for defensive purposes, more focus should be put on rules on engagement, political control, and legality.
-
- **The nature of offensive cyber actions is unique and will require new areas of planning. Cyber actions are usually one-time use. This causes NATO member states to be reluctant to disclose their capabilities and methods. They will focus on providing effects rather than tools. This creates new needs for mechanisms of cooperation, especially in the multinational context.**
-
- Usage of offensive capabilities requires close analysis of potential consequences, proportionality, potential collateral damages. Their deployment must be seen from the broad perspective of all cross-domain tools.
 - NATO must be very agile when it comes to cybersecurity. Doctrinal and operational decisions must be quickly adjusted to the constantly changing environment. This will also be very closely connected with procurement mechanisms and ensuring that security is provided throughout the value chain.

- Achieving **deterrence at the NATO level** requires:
 - working together to establish a framework to impose costs upon the attacker,
 - sticking to the rule of deliberate ambiguity,
 - increasing resilience,
 - better attribution,
 - getting to know the enemies – mainly identifying what is important to the other side; only by affecting that element will one be able to change the behaviour of the rival,
 - the effect of deterrence by entanglement which may appear in the future.

FOLLOWING DIFFERENT PATHS, SHARING THE SAME GOAL – EU-NATO COOPERATION ON CYBERSECURITY

- A common **European toolkit for EU Cyber Rapid Response Force teams** using EU funds ought to be created. It is recommended to enhance the activities undertaken within the **PESCO** framework. Joint actions are much more cost-effective than having each and every country spend money separately. Aggregation of the human and financial resource from the very beginning will help in this process. As NATO is creating its own NATO Cyber Rapid Reaction Teams, there is room for cooperation.
 - The EU and its institutions should engage in a **public-private dialogue** in the field of defence and cyber-defence and see the full potential of the industry in this regard. The role of private sector in this process should be upgraded and go beyond simple information sharing.
 - Private actors' experience in crisis management and prevention could serve as a basis for the dialogue, especially while developing blueprints at the EU level.
 - It needs to be underlined that the same questions on the EU-NATO level of cooperation will arise with other actors (e.g. Japan, Australia). The **cooperation should be therefore extended** beyond the EU-NATO framework to a broader level, following John McCain's idea of a "League of Democracies" in cyber that would form "the core of an international order" in cyberspace.
-
- **A common doctrine for NATO and the EU** in the field of cyberdefence has to be embraced as well as a common terminology and set of concepts to ensure the EU and NATO speak the same language and understand each other quickly.
-
- **Bottom-up activities** are required: working at the field level, aligning people in order to use cultural commonalities, sharing training and education concepts.
 - The EU may help to overcome NATO's limitations and vice versa. For instance, NATO can learn more from the EU in the area of asymmetric response. The EU has developed a wide range of available responses what might help to multiply NATO's options.

INTELLIGENCE-POWERED SECURITY: CAN TERROR INVESTIGATION METHODS HELP CRACK CYBER INVESTIGATIONS?

- A major paradigm shift in the way organisations approach cyber is needed. We should move from a cybersecurity mindset to a **cyberdefence mindset**.
- Tools and strategies are needed and should encompass:
 - **Intelligence** – this involves situational awareness of yourself, your enemy and surroundings from tactical and strategic perspectives.
 - **Technology** – seen from the holistic perspective.
 - **Operational capability** – focus should be put on the set of skills, active ways to outsmart the attacker. Reactive approach will not work.
- An important element of the strategy is to **cover the kill chain**. Strategies should be built adding another layer – buffer – that will help organisations to identify the relevant threats, mitigate them and stop the attack before it reaches the network.
- Having too many tools in place may lead to confusion. An organisation must be able to understand its assets and to control them. Technology producing holistic coverage for visibility and control focuses on three elements:
 - a combination of web intelligence technology with expert services for monitoring network and providing valuable cyberthreat intelligence from external sources,
 - holistic kill chain coverage using multiple side detection engines that monitor both endpoint and network activities,
 - automation of the hunt for cyberthreats – multiple detection engines feed the security events into the system, attack patterns from external sources are added and forensic information is gathered, providing a history of the network and endpoint activity. This makes it possible to proactively hunt for threats.
- **Intelligence augmentation** is needed, with humans and machines (AI) working together.
- It is recommended to invest in the prioritised areas and keep in mind that defending everything means defending nothing.

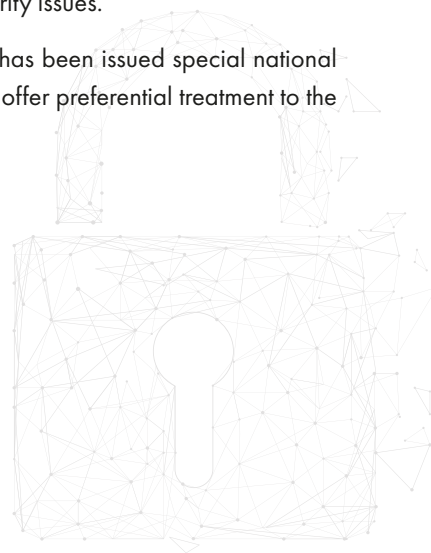
CYBER ELECTROMAGNETIC ACTIVITIES (CEMA)

- Military services must better **integrate space, cyber, and electronic capabilities** together. Synchronisation and coordination of offensive and defensive activities across electromagnetic environment and cyberspace should be observed. CEMA is about effective management and about the application of the owned resources against the threat that you face.
- Synergy between disparate capabilities is urgently needed. This may enable specific types of strategic information operations expected to be decisive in future wars.

- **Doctrines to integrate cyber and electromagnetic activities** are needed as guidance for operational commanders. They should enable them to take fast decisions and actions and to exploit the already existing tools with agility.
- Increasing hardness and resilience against various forms of electronic or full spectrum CEMA attacks is imperative, especially in the light of the fact that rivals are investing in the capabilities in this area.

HARDWARE SECURITY IN PUBLIC PROCUREMENT

- To develop and implement state recommendations concerning both legal matters and technical security measures constitutes a common challenge for the state and the private sector.
- There is a need for constant education and raising awareness of civil servants as regards the issues of cyberspace security, especially about adequate and effective protection against cyberthreats.
- It is recommended to set out particular guidelines adhered to by state administration in tenders for and in public procurement of electronic hardware which involve cybersecurity issues.
- Public administration should only use that electronic hardware which has been issued special national security certification (e.g. the national cybersecurity system act should offer preferential treatment to the devices that possess an appropriate national security certificate).



Recommendations for the Three Seas countries on the Digital 3 Seas Initiative are included in the Kosciuszko Institute's report entitled „The Digital 3 Seas Initiative – Mapping the challenges to overcome”.

Report is public task co-financed by the Ministry of Foreign Affairs of the Republic of Poland under the competition 'Support for the civil and municipal dimension of Poland's foreign policy 2018'.

The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the position of the Polish Ministry of Foreign Affairs. Responsibility for the information and views set out in this publication lies entirely with the authors.

The publication is available under license Creative Commons Uznanie autorstwa 3.0 Polska. Some rights are restricted to Stowarzyszenie Instytut Kościuszki. The content was created under the competition 'Support for the civil and municipal dimension of Poland's foreign policy 2018'. It is allowed to use the content under condition of non-disclosure of the above-mentioned information, including information about the license, rights holders and the 'Support for the civil and municipal dimension of Poland's foreign policy 2018' competition.



Ministry
of Foreign Affairs
Republic of Poland

STRATEGIC PARTNERS



MAIN PARTNERS



PARTNERS



LOGISTICS PARTNER



ORGANIZER



HONORARY PATRONS



Ministry
of Digital Affairs



Republic of Poland
Minister
of Foreign Affairs



Ministry of Science
and Higher Education
Republic of Poland



Ministry
of Finance



Minister
of the Interior
and Administration



MINISTRY
OF INFRASTRUCTURE



MINISTRY
OF INVESTMENT
AND ECONOMIC DEVELOPMENT



MINISTRY
OF ENTREPRENEURSHIP
AND TECHNOLOGY



MINISTRY OF ENERGY



Polish Investment
& Trade Agency
PIT Group



The National Centre
for Research and Development



WOJEWODA
MAŁOPOLSKI



Kraków



Cracow University
of Technology



AGH
UNIVERSITY OF SCIENCE
AND TECHNOLOGY



Wrocław
University
of Science
and Technology



JAGIELLONIAN UNIVERSITY
IN KRAKÓW

Warsaw University
of Technology



Office of Electronic
Communications



INSTITUTIONAL PATRONS



MEDIA PATRONS





CYBERSEC

SAVE THE DATE

FOR THE NEXT CYBERSEC EVENTS

BRUSSELS

20 FEBRUARY 2019

WASHINGTON D.C.

19 MARCH 2019

www.cybersecforum.eu/krakow



/cyberseceu



@cyberseceu