CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

CYBERSEC BRUSSELS LEADERS' FORESIGHT 2019

KEY TAKEAWAYS

2ND CYBERSEC BRUSSELS LEADERS' FORESIGHT, 20 FEBRUARY 2019

#CSBXL19

www.cybersecforum.eu/brussels

THE QUEST FOR CYBER TRUST

> As a representative of Polish government, I couldn't start differently than by saying congratulations to the organisers, which is a Polish think tank, good job! CYBERSEC is a good opportunity to talk a bit more about cooperation, which is a crucial thing.

Tomasz Zdzikot
Secretary of State, Polish Ministry of the National Defence

> CYBERSEC is an outstanding institution, making a very positive contribution to global cybersecurity.

Ciaran Martin
CEO, National Cyber Security Centre of the UK

> Events like today will give us the necessary energy push to put more efforts in mobilising projects such as the Digital 3 Seas Highway.

Maria-Manuela Catrina
State Secretary, Ministry of Communication
and Informational Society, Romanian Government

CONTENTS

DISCLAIMER:
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.
The takeaways are based on original speeches delivered during CYBERSEC Brussels Leaders' Foresight. They have been reformulated and edited for more clarity. Only the parts accompanied by a quotation mark are quotes and reflect the wording used.

CYBERSECURITY CALL – ONE FOR ALL. ALL FOR ONE

In 2019, we are celebrating the **fifth anniversary of launching the CYBERSEC Forum.** Over that period of time we have hosted more than 400 speakers during our events in Krakow, Warsaw and in Brussels, so we already know that **great cyber minds think alike.**

But we also know that those minds need to **act** alike.

As we are rapidly moving towards a **smart world**, with everything being smart thanks to a connection to the internet, we need to introduce **smart power**. We can define it as the ability to use all tools in a flexible and agile way to build a cybersecure world and foster our interests in cyberspace. But that smart power that merges soft and hard powers may only be exercised thanks to cooperation and pooling together resources and capabilities of all stakeholders.

That is why today nothing is more important than the cybersecurity call "one for all, all for one".

We need to invest heavily in **alliances, partnerships, norms, regulations and institutions** to get the outcomes we want. We need to build resilience and deterrence together.

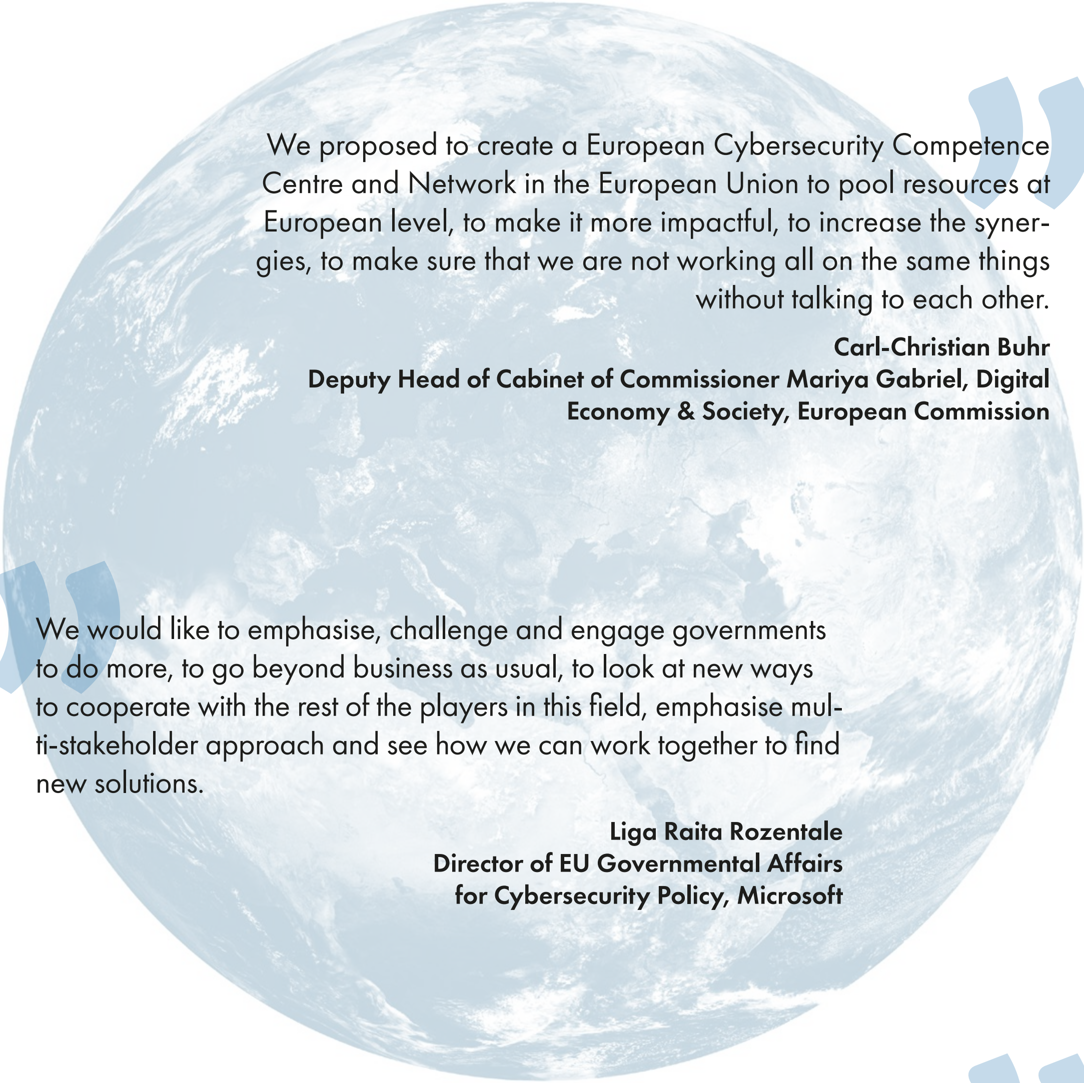
We also need to innovate and invest together in cutting-edge technologies. Because what cybersecurity in the complex smart world era per se needs is to make sure that technology would not overpower but empower us.

Enjoy the read!

CYBERSEC Team

Cyber defence is a team sport. NATO cannot and should not do it alone. We are only made better the more we can share information, the more best practices we can pull, and the more we can interoperate with partners.

Antonio Missiroli
Assistant Secretary General for Emerging
Security Challenges, NATO



We proposed to create a European Cybersecurity Competence Centre and Network in the European Union to pool resources at European level, to make it more impactful, to increase the synergies, to make sure that we are not working all on the same things without talking to each other.

Carl-Christian Buhr
Deputy Head of Cabinet of Commissioner Mariya Gabriel, Digital
Economy & Society, European Commission

We would like to emphasise, challenge and engage governments to do more, to go beyond business as usual, to look at new ways to cooperate with the rest of the players in this field, emphasise multi-stakeholder approach and see how we can work together to find new solutions.

Liga Raita Rozentale
Director of EU Governmental Affairs
for Cybersecurity Policy, Microsoft

It's really now the time to act and to work together. It's about team play, it's about collaboration and co-creation. (...) Nobody is perfect, but a team can be, and I think this is really what it's all about.

Johannes Nitschke
Senior Director, EU Government Affairs, Siemens

STATE STREAM

ELECTIONS IN A DIGITAL ERA – BUILDING RESILIENCE AGAINST HOSTILE INTERFERENCE

- **Election interference** can take different forms: cyberattacks, leaks, disinformation campaigns or actions casting doubt on the integrity of the electoral process.

- **Sharing best practices** is the crucial first step to go beyond a very general level of cooperation. Responses to attempts of election meddling should not be strictly national anymore. Working together – to make sure that the two relevant institutions involved in elections, the EU and NATO, are getting the kind of information they need – is a must.

- Thinking elections – and especially European elections – in the digital era requires a shift of paradigm. Even though member states have the exclusive competence in electoral matters, a new way of thinking about the legislation and on how to treat the European elections will have to emerge. Ultimately, it needs to expand to a reflection on how we think of **democracy itself in the digital era.**

- The **level of resilience** as well as the **mindsets** and the **political willingness to take action** vary across EU member states. This makes the negotiations at the EU level difficult. The EU needs to have a **general approach on election interference** and to keep the level of attention and alert constant. It must be able to react quickly.

- EU member states have been encouraged to organise themselves into new networks so that they can exchange experience, learn from each other and take steps on cybersecurity, tackling disinformation and protecting personal data. This will also allow them to establish **rapid alert mechanisms** in order to flag disinformation campaigns.

- The European Commission designed **the Code of practice against disinformation** as a self-regulatory mechanism, but it does not exclude looking at other ways to advance the fight against disinformation if the progress is not sufficient. On other issues – for example targeting illegal content online – the Commission moved towards the regulatory environment.

- Having voluntary pieces of mechanisms like the Code of practice against disinformation helps creating a **feeling of responsibility** in the private sector as well as a more aware environment. A strong regulation could backfire.

- Creating a regulation to counter disinformation requires from legislators to be careful not to fall into censorship. For the moment, rules at the EU level centre on **transparency** and **clarity** about the provenance of materials.

- In the US, there have been cases of data breaches of voting lists, showing that the **cybersecurity dimension of the electoral process** is another crucial aspect when dealing with hostile interference. Electronic voting machines are unreliable, hackable and able to compromise the security of elections. The EU is in the process of adopting the **Cybersecurity Act** which will reinforce resilience, but it should go further. Making sure that the certification schemes – designed within the Cybersecurity Act – will cover **technologies used during electoral processes is crucial.**

- Cooperation of European public bodies – like ENISA – with the **private sector** is a good way to improve the cybersecurity level. Businesses are one step ahead of public institutions as they are able to rapidly disclose problems they encounter and to propose solutions. A solid interaction of all the layers involved in providing better cybersecurity (public and private actors) is needed.

- There is an important **skills gap** in the field of cybersecurity. First, on the side of professionals, there is a lack of people with the necessary skills to ensure the right level of security. Attracting talents and providing better training is the way forward. Second, **digital literacy** on the part of policy makers and politicians is sometimes very low. **Raising awareness** and **educating** the broader public on topics related to cybersecurity is needed.

> In the digital era we have to relook at the broader issue of what kind of elections we have. Referenda also have to be far better thought out because when you have a situation where you have two more or less equally balanced sides, those are really ripe for manipulation.

Toomas Hendrik Ilves
Former President of Estonia (2006–2016); Member of the Transatlantic Commission on Election Integrity

> It is important to point out that we all have our role to play – government, academia as well as industry.

Liga Raita Rozentale
Director of EU Governmental Affairs for Cybersecurity Policy, Microsoft

The debate around disinformation and social media platforms is a fascinating debate that motivates a lot of comments but actually quite a lot of the stuff that we have to protect is cybersecurity. It's relevant to elections obviously but it has a much wider relevance. The work that we are doing at a European level – and the work that's done in the individual member states – is an important part of mitigating risks around election.

Sir Julian King
European Commissioner for Security Union

We are as weak as the weakest part of the chain in the European Union. This means that we need to change the mindset in a consistent way and then we will be able to approach the elections in a much more resilient way.

Pavel Telicka
Vice-President, European Parliament

CYBERSECURITY OF THE DIGITAL SINGLE MARKET

- The European Union has to deal with a **risk assessment** regarding the equipment it will use when building its **5G network**, and the **Chinese 2017 intelligence law** gives legitimate reasons to be worried about Chinese software and hardware producers. The debate about providing solid evidence of these producers creating backdoors in the equipment is a different and misleading one. The EU has to act now and if it waits for solid evidence it might be too late.

- The argument of **reciprocity** is a faulty one. Whereas the European Commission purchased – after having organised an open tender – and uses Chinese laptops, using equipment or software produced outside of China is not allowed at the state level in Beijing. In the same vein, the market share of Chinese companies in 4G networks in Europe is around 40% but the market share of European companies in China is only 15%.

- The EU sets its **connectivity aims** regarding 5G development. According to those, until 2025:

  – Operators will have to start providing, on a commercial basis, 5G services in all urban areas as well as along major transport routes.

  – At least one city in each member state will have to be provided with 5G services which is important because it will enable operators to face real-life challenges and to develop the best solutions for further 5G deployment in the country.

- Reaching the **EU connectivity objectives** will require a level of investment close to **EUR 500 bn per year.** The agreement on the **new EU telecommunications code** will aim at avoiding an investment gap of EUR 155 bn that would have occurred if the previous one had stayed in place.

- All areas of the European continent have to be covered by an efficient 5G network. In **rural areas,** 5G combined with IoT and artificial intelligence will enable progress in agriculture.

- **Fragmentation of the market** is an important issue for companies, for instance in the field of certification. With a fragmented market, it can take years for a company to commercialise and certify its products on the 28 national European markets.

- Setting up **future-proof regulations** in rapidly developing areas such as the digital is a challenge. **Self-regulatory measures** are much more flexible and can help make big digital players such as social media platforms more responsible. It is in their business interest to regain people's trust and to comply with a code of practice for instance.

- Big European companies in **traditional industry** sectors have been transformed by the digital revolution, not only in their way of working but also in their preoccupations. Nowadays they are dealing with **data business** a lot. Implementing **free and secure flow of data** is not only about digital giants but also about all other, more traditional industry sectors.

- **Digital literacy** among government officials needs to increase, as the current relatively low status is making it difficult to raise the topic of the importance of cyberdefence or other important digital issues.

- **Demystifying cybersecurity** issues as well as IoT and artificial intelligence topics is important. Bringing it closer to people and decision-makers will also help raise awareness and develop **cyber hygiene.**

> National security is up to the member states, it is not up to the European Commission. But when the member states will ask us to create some kind of coordinated approach on 5G networks, then of course we will say yes.
>
> * * *
>
> Fragmentation is a real headache for all the companies acting here in European markets but also for our citizens. (...) If we continue with this fragmented Europe, we will send a very bad message to our SMEs and start-ups, equivalent to “stay at home or go to the United States where they already have this huge single market”.

Andrus Ansip
Vice-President of the European Commission in charge of the Digital Single Market

> Three years ago, when the talks about the certification schemes started, there was a trend from the engineering point of view to see it as regulatory burden. But through the course of the conversation people came to realise that this is an advantage for the industry precisely because there is so many devices and we need to do a better job not just certify the devices at point of sale but certify it over its useful life and its retirement.

John Frank
Vice President, EU Government Affairs, Microsoft

THINK GLOBAL, ACT GLOBAL: CYBERSPACE AND EMERGING TECHNOLOGY

- In the era of globalised technology, it is more important than ever that **the effort we make is global as well.** There are limitations to what Europe can do on its own in the era of American and Chinese technology domination.

- There are **two structural challenges for the future of internet security.** Both of them require the EU and non-EU European nations to act with others outside the continent:
  1. Security of the telecommunications infrastructure.
  2. Improvement of structural flaws in the wider internet environment.

- **TELECOMMUNICATIONS INFRASTRUCTURE:**
  - 5G accelerates the **pace of technological change** but there is no cliff-edge transition. Its importance is related to its **future large-scale use** in autonomous vehicles, cloud services, HD streaming or smart cities.

  - 5G requires **complex physical infrastructure** whose configuration varies from country to country and has to be built on existing telecommunications infrastructure.

  - The **supply chain** and where suppliers are from is only one issue. Networks' weaknesses and the way they are architected can be used by hostile entities (e.g. the attribution of attacks on UK networks to Russia in 2018, while UK networks do not have any Russian electronics in them). According to the incident statistics carried out by the British National Cyber Security Centre, the supplier's country of origin has not featured among the main causes for concern in how attacks are carried out.

  - There are **three technical pre-conditions** for secure 5G networks:
    1. We must have higher standards of cybersecurity across the entire telecommunications sector.
    2. Telecoms networks must be more resilient.
    3. There must be sustainable diversity in the supplier market.

- **STRUCTURAL SECURITY PROBLEMS:**
  - The Internet was not built with security in mind and the **improvement of the global digital infrastructure** is necessary.

  - **Active (automated) cyber defence programme** (launched by the NCSC) aims to provide a framework to make the Internet automatically safer for people to use. Its results can serve as an example to follow; they are mostly based on technical improvements (e.g. blocked connections to malicious sites, anti-spoofing mechanisms) and do not require legislation.

We must assume that a global supply chain will have multiple vulnerabilities, whether intentional or, more likely, unintentional. Networks are built by human beings and human beings make mistakes.
No network can be totally safe.

* * *

Whether it's future telecommunications infrastructure or digital security more generally, we want to work with everyone across Europe and beyond to push these changes, to deliver the digital world we all want to see, one that is not just free and prosperous, but safer as well.

Ciaran Martin
CEO, National Cyber Security Centre of the UK

DEFENCE STREAM

EUROPEAN DEFENCE INDUSTRY: WHAT FUTURE FOR EU CYBER DEFENCE?

- Cyber defence is clearly a priority area for **capability development and research.**

- Allied Heads of State and Government should remain fully committed to implement the important initiatives that have been set up in recent years in the field of cyber defence – i.e. NATO's **Cyber Defence Pledge** or the EU's **Digital Europe Programme.**

- All defence instruments and programmes that are being developed by the EU nowadays – i.e. Permanent Structured Cooperation (PESCO), the Coordinated Annual Review on Defence (CARD), the European Defence Fund (EDF) – have to be used in a consistent way and become the foundations for a **coherent European defence system.**

- **Duplication** can arise as a result of temporary political considerations – like temporary Transatlantic disagreements – but it has to be avoided. The broader objective of making Europe and the Western democratic alliance stronger should prevail. Moreover, in the cyber defence sector, duplication comes at a great cost – both in terms of money and in terms of human resources – and can prove harmful and counterproductive.

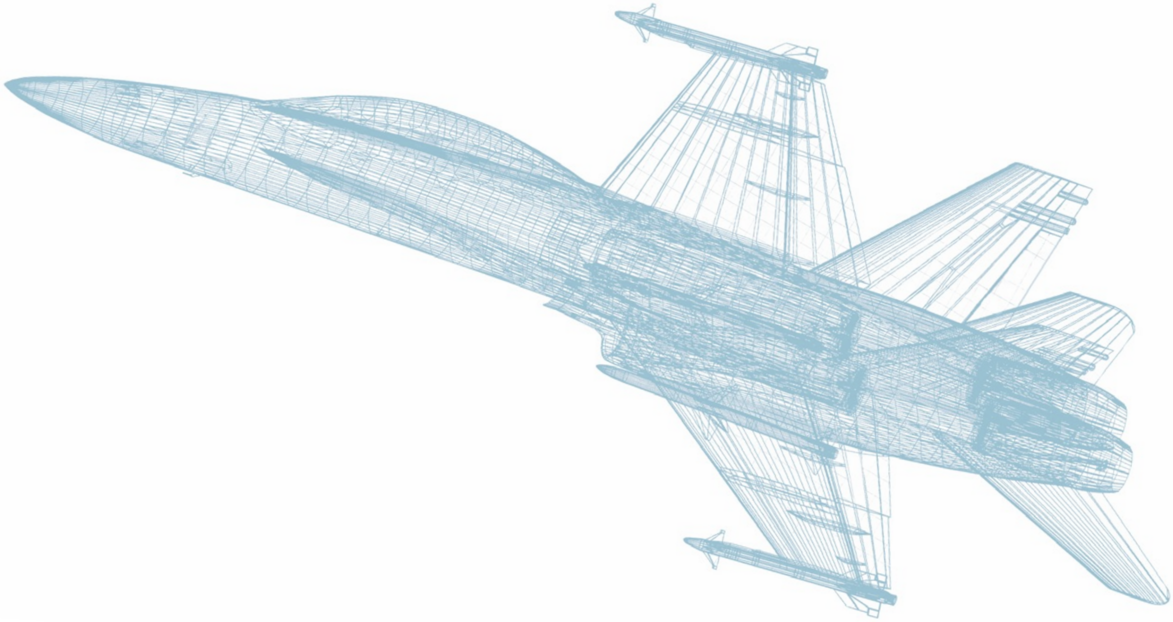
- It is crucial that companies from all over the EU, including SMEs, start-ups and mid-cap companies, have the **same access to resources and EU funding** than larger-scale companies. Geographic balance as well as scale balance principles have to be respected when it comes to funding opportunities.

- **Cyberthreat intelligence sharing** will be a crucial aspect for 2019. A relevant case involves Ukraine's presidential and parliamentary elections. The situation will have to be carefully monitored and pertinent information will need to be exchanged in order to mitigate the risks of major cyberattacks on the country's electoral process. Shared information will also help to build resilience and to be better prepared for elections taking place in the EU member states, which might be the targets of similar cyberattacks.

- **Information sharing for EU-led military operations** should be improved thanks to general provisions guaranteeing a high level of information sharing for cyber operations. Setting up common standards for information sharing will make fast-running and highly efficient operations possible.

- Public bodies have to help developers to bring their technology innovations through the "valley of death". **The European Defence Fund** can be the right instrument to utilise in order to better link the excellent academic base present in Europe with the excellent existing industry.

- **Cyber exercises** are an effective way to test and increase the level of cyber readiness of both companies and public bodies.
    - On the public side, exercises can help stock-taking and achieve the demystification of cyberspace and cyber defence for the top leadership. It is important that more of these exercises are organised and go beyond the military community boundaries to include all ministries, as well as the private sector.
    - On the private side, organisations are nowadays more and more interconnected, sometimes with elements of the national and cross-national infrastructure. This raises the possibility of cyber insecurity of one company becoming the vulnerability of the whole system. It is important to think about cybersecurity of one's own network but also to take into account the whole chain of vendors, partners, suppliers and customers. The way to test this cross-dependency is through technical cyber exercises.



@MicrosoftEU
EUROPEAN DEFENCE INDUSTRY: WHAT FUTURE FOR EU CYBER DEFENCE?

> We have to be better organised at the European level (...) and raise the question of how we spend the available budget better. We have to invest in innovation and innovative technologies like artificial intelligence and nanotechnologies because these technologies will change the battlefield of future military operations. Europe cannot stay behind.

Wolfgang Roehrig
Head of Unit Information Superiority, in the Capability, Armament and Planning Directorate, European Defence Agency

> In cyberspace we cannot afford to be counter at transatlantic relations. We are in the same cyber domain and Europe doesn’t have the same firepower alone that it would have with our like-minded allies across the globe. (...) I hope this kind of transatlantic and international cooperation will continue, also throughout the European projects.

Jaak Tarien
Director, NATO Cooperative Cyber Defence Centre of Excellence

I believe that where the primary responsibility for national security – including in cyberspace – lies is within the Member States, including the governments and the private sector. But the EU definitely can and does add value to all of this. Over the past five years, I believe that EU regulations and directives have had a really serious impact on cybersecurity of member states including both the government level and the private sector.

Merle Maigre
Executive Vice President for Government Relations,
CybExer Technologies

Developing military aspects or civilian aspects, R&D projects, intelligence services, military units, universities are very important aspects of cyber defence and a comprehensive approach is the way of developing every one of them. What we have launched in Poland with the platform cybr.mil.pl is dedicated to boost every pillar of the system.

Tomasz Zdzikot
Secretary of State, Polish Ministry of the National Defence

BUSINESS STREAM

FROM HARDWARE TO SOLUTIONS: BUILDING TRUST IN CYBERSECURITY

- Without a **cybersecurity component**, a company will never be able to earn people's trust that its products are safe and protected. People will not trust a company unless they are confident that their products and services are secure.

- Deploying **secure development lifecycle, discovering and managing security vulnerabilities** and **providing security updates** are key elements to keep IT devices safe and protected.

- The secure development lifecycle process considers **security throughout the entire life cycle** of the product and service such as initiation, design, implementation, verification, maintenance and response.

- Activities within the secure development lifecycle process include:
    - Security requirement review
    - Threat modelling
    - Open source security
    - Secure coding and code review
    - Static and dynamic analysis
    - Validation of functional and security requirements
    - Release of security advisory and updates on a monthly, quarterly, and on a needed basis

Cybersecurity is something that you earn by action. We have to show beyond a reasonable doubt that we care about cybersecurity and implement measures to ensure our products are cyber secure.

* * *

We have to think and act as one body in cybersecurity because everything is going to be connected and converged. We cannot afford to have one part having issues in cybersecurity, otherwise the entire system may be compromised. In this regard, all companies have to have the same standards, values and philosophies to ensure cybersecurity. There's no way around it.

Kyu Sung Lee
Vice President & Head of European Corporate Affairs, Samsung Electronics

As we are rapidly moving towards a smart world, with everything being smart thanks to a connection to the internet, we need to introduce smart power.
We can define smart power as ability of flexible and agile use of all tools to build a cybersecure world and foster our interests in cyberspace.
But that smart power that mergers soft and hard powers may be only exercised thanks to cooperation and pooling together resources and capabilities of all stakeholders.

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

ASSESSING DIGITAL RISKS – CYBER INSURANCE ON THE RISE

- **Cyber insurance** is part of a much more global system. There is no point in only buying cyber insurance policy without understanding the risks and the ways to mitigate them. **Insurance policy** should correspond to customers' needs and to their threat exposure and should be based on mutual efforts with the insurer.

- The insurance market evolves. Some of the areas will soon disappear, like for instance motor insurance because of the expected increasing role and implementation of self-driving cars. Hence, insurers could concentrate on operators of self-driving platforms, including cyber insurance policies against cyber risks.

- Cyber insurance is going in the direction of a **dialogue and a cooperation between the insuring entity and the company** where burdens are taken together. Insurance companies will also be the ones who will need to popularise the **cyber resilience** and then insure against risks that are left. Cyber insurance is then part of a **holistic framework** including corporations, technical partners, government and insurers.

- Insurance is a mechanism of the **economics of security** which is not sufficiently developed worldwide. For instance, people are using different metrics to measure the return on investments, where data is not comparable and often poorly understood. There is also not a lot of evidence that incident data is predictive. We need **scientific method approach.** This is one of the biggest problems that hits the insurance industry.

- The approaches towards cyber insurance are very different country by country depending on the exposure, the threats, the resilience and **the level of awareness** of different players. This approach also varies by market segment – large corporations have a different self-awareness than small and medium enterprises who are also vulnerable and pose a risk to the overall society. SMEs do not often have a necessary expertise that will allow them to buy the policies that they actually need and that is why the high-quality dialogue between insurers and companies is crucial.

- The aspect that insurers are struggling with is that people probably face more risks than they're actually aware of. Therefore, there is a huge need to **increase education level**, to **exchange experience** and **good practices.**

- Cyber insurance market faces a problem with **taxonomy and language**. Different insurers explain risks using different words what constitutes a problem for consumers in the sense that it's very hard for them to compare policies. Based on ENISA studies, there is a need for a common terminology within cybersecurity field.

- **Information sharing** is very important in the cybersecurity field, and the challenge is not sharing more information but less information. The trick is to share the right information at the right time with the right person for a particular purpose – this is a basis for setting up a framework that has a chance to work.

- **Sectoral cooperation** between different stakeholders is economically efficient (for instance in pharmaceutics, aviation, banking, etc.). Gathering people in order to develop a common understanding of the **standards** that are expected in a specific sector and among the **supply chain participants** (companies within one industry very often have common suppliers) is very important. Cooperation needs to be therefore adapted to the specificity of a sector.

- There is a gap for cyber insurance between Europe and the United States. The latter are leading the way, mostly because of the huge resources and higher level of understanding of the topic among companies. **The European market is fragmented** and **less mature** and what is needed right now is the **push for common standardisation and frameworks.**

> The aspect that we are struggling with as an insurer is that people probably face more risks than they're actually aware of. First of all, you need to educate them to a certain extent which is why we get engaged in conferences like CYBERSEC.

Paweł Surówka
President of the Management Board, PZU SA

> I think the economics of security is really important and we need to understand it more. We need more studies, we need to know where we're spending money, what we're getting back, what damage is occurring and how to mitigate it.

Steve Purser
Head of Core Operations, ENISA

> As a space engineer I have to say that way – cyber insurance as such is only the last stage of the rocket. So, if you really want the satellite to be launched properly, you need to build a full rocket and not just a last stage.

Philippe Cotelle
Board Member, FERMA; Vice-President, Cyber Commission, AMRAE;
Head of Insurance and Risk Management, Airbus Defence and Space

FUTURE STREAM

TOWARDS THE SMARTER WORLD: HOW TO MAKE AI AND CONNECTIVITY "FOR GOOD"?

- Artificial Intelligence (AI) deployment will have a huge impact on international relations and on the **balance of power at the global level**. It will also affect our daily lives and the way we conduct business and ensure the necessary level of security. There is a tendency to over-estimate the short-term impact of technologies and to under-estimate their **long-term effect.**

- There are different areas in which AI can help: **improve decision-making** (both political and military), **boost the skills level** and **increase the situational awareness.**

- According to surveys, AI is seen as revolutionary by Chief Information Security Officers in addressing cybersecurity field challenges. At the same time, the big majority of AI projects (80%, according to Gartner) fail.

- AI is not only about technology. Other success factors are related to **people, skills and the good choice of data.**

- AI will be a new opportunity for attackers in terms of **threat intelligence, capability to assess a system** and **new ways to attack.** However, we need to bear in mind that basic security rules and best practices are still of huge importance. They need to be implemented even before thinking about the **AI-based cybersecurity attacks.**

- First applications of the AI need to be watched carefully. Experiments and pilot projects on actual applications – such as, for instance, connected cars – could be good examples because of **ethical and security challenges** that are related to their deployment.

- There is a need for **information sharing** and a need for **cooperation** between front-runners and those that are lagging behind in order to prevent two speeds of AI development within the EU internal market. EU legal mechanisms can be important and effective to avoid that.

- The current discussions on AI are biased towards its "dark side" and the threat landscape it presents. However, strong attention should also be paid to the **potential** and the **opportunities that AI raises.**

- When talking about building defence capabilities there is a dilemma that every state is confronted with – **national responsibility** vs **greater efficiency while cooperating with others.** The current dynamics are encouraging different entities to reach out to partners both within bilateral or multilateral frames. There is acute awareness that there is a need to cooperate.

- Security is often perceived as a cost for business and it is not easy to sell it. That is why **regulations** and **roadmaps** are necessary in certain areas, including AI. There is a need to build together (with regulators, with industry and with data scientists) a framework in order to be able to **certify systems based on AI**. Working together will also enable various parties to identify where the regulations are needed the most. On the other hand, regulating new technologies on a multilateral level usually takes time. It is a slow process that waits for the technologies to mature.

- The European Union considers it very urgent to create a **European Cybersecurity Network and a Competence Centre** – a community that will bring together private sector, academia and the public sector to work on projects, investments, to advise where **procurements** are necessary and how they should be carried out. Another point for deep multi-sectoral cooperation in the field of cybersecurity is the **skills shortage** that is observed in Europe. Creation of a community with different backgrounds, education and experience (from the public sector, industry and academia) will allow the industry to gather the best experts who will work together in order to increase the level of cyber resilience.

- The way to define and to prove the trust is **evaluation**. The main goal of the evaluation framework is to define a trusted ecosystem that is not just a matter of products, but a matter of the whole supply chain and the whole system based on complex interconnections.

The big challenge for organisations like NATO is the fact that in order to use AI for good and effectively you need a lot of data. And when you have to deal with data, there are a number of political and legal issues that have to be dealt with at the beginning.

Antonio Missiroli
Assistant Secretary General for Emerging Security Challenges, NATO

You cannot have a digital society without security and privacy. These are the two fundamental components and basic values for how we operate in the internal market and we should not forget it in the discussion on AI.

Despina Spanou
Director, Digital Society, Trust & Cybersecurity Directorate,
DG CONNECT, European Commission

Panel Discussion:
TOWARDS THE SMARTER WORLD: HOW TO MAKE AI AND CONNECTIVITY "FOR GOOD"?
EST FOR CYBER TR

Our job is to secure digital transformation and digital transformation needs trust. It is very important to keep in mind that there is no digital transformation without cybersecurity.

Stanislas de Maupeou
VP Strategy and Marketing, Critical Information
Systems and Cybersecurity, Thales

FLAGSHIP INITIATIVE – THE DIGITAL 3 SEAS

#D3SI

THE DIGITAL 3 SEAS – TOWARDS SECURE DIGITAL TRANSFORMATION OF THE REGION

CONTEXT

The Three Seas Initiative (3SI) is a political and economic intergovernmental project developed and launched by the Polish president, Andrzej Duda, with the president of Croatia, Kolinda Grabar-Kitarović, in 2016. It was oriented towards boosting cooperation and interconnectivity between the 12 CEE countries which are located between three seas – meaning the Baltic, Adriatic and Black Sea, focusing on transportation, telecommunication and energy sectors. The aim was to make sure that CEE countries will be more valuable members of the EU and will better contribute to Single Market. Another goal was also to enhance cooperation between the region and the US.

Whereas the two pillars – energy and transport – were rather well developed, the initiative lacked progress in the digital one. The Kosciuszko Institute together with partners – Globsec from Slovakia, the New Strategy Centre from Romania and IRMO from Croatia (later on joined also by Center for European Policy Analysis, Antall József Knowledge Centre and International Centre for Defence and Security) – launched in 2018 a project called **The Digital 3 Seas** in order to boost cooperation and upgrade it with concrete digital projects, infrastructural, technological, educational – as well as to include the cybersecurity component within all the three pillars: energy, transportation and digital.

The Digital 3 Seas Initiative has **two main goals:**
– Enhance cooperation within the digital pillar of the 3SI
– Make sure that cybersecurity is established as a prerequisite for all work undertaken in the projects deployed within three pillars.

The **Digital 3 Seas Highway** is one of the most important projects put forward by the Digital 3 Seas Initiative. Its aim is to develop a secure digital infrastructure running from North to South, connecting member states and composed of two elements: optical fibre along with technologies which will help create a 5G connection between the countries. The true success came when the Ministry of Digital Affairs of Poland, together with Chancellery of the President of the Republic of Poland, officially submitted this project during the Three Seas Summit in Bucharest in September 2018 and it was officially accepted and put on the list of "priority interconnection projects".

On cybersecurity:

- No application in the field of energy or transport can exist without the **relevant cybersecurity component.** The digital runs across all three themes of the Three Seas Initiative.
- Having the digital component crossing other fields such as energy or transportation brings a chance to build **secure-by-design networks** and to include a cybersecurity component from the very beginning of each project.
- When talking about digital transformation, the emphasis should be refocused. Infrastructure and platforms are not the only things needed. Three crucial elements to make the digital transformation happen are **the people, the processes and the policies.**

On the implementation of the projects:

- **Commercial partners** will play a crucial role in the success of the Digital 3 Seas Highway project. They have to be identified in each and every country.
- The smooth implementation of the Digital 3 Seas projects could be ensured thanks to a **consortium** that would coordinate the activities of participating countries. In addition, a work schedule could synchronise the processes and guarantee that the standards and cybersecurity requirements are set out from the very beginning.
- **Three milestones** can be identified in order to monitor the advancement of a project:
  1. Synchronisation of schedules between the infrastructure and the digital parts.
  2. Selection of parties/operators at the national level.
  3. Establishment of a plan to foresee the pace of project implementation.
- Keeping the right level of competences on both sides – consumers and producers – and in all sectors is important. On the side of the producer, making sure that the right level of quality and security is delivered – based on legislation – is a must.
- As their scope of application is becoming so vast, the **certification schemes** will have to be much more specialised than they are now. A common application for all electronic devices will not be efficient enough.

On the next steps and the future of the initiative:

- The digital factor of the Three Seas Initiative can be considered a starting point for some other initiatives that will benefit the whole region with its citizens and companies. Keeping the **broad perspective** is crucial.
- The **snowball effect** should not be underestimated. Every single initiative can add some value and boost several other projects, leading to the creation of a significant **momentum** in the whole region. It is important not to concentrate on one single project but to look at the holistic framework of increasing markets connectivity in terms of IoT.

- Following the construction of a secure digital infrastructure, **next steps** should consist in delivering services to companies and citizens that use the digital infrastructures as well as implementing further projects that will help **build digital economies** and **data-driven industries** within the region.
- To ensure the lasting success of the Digital 3 Seas Initiative, it has to be **apolitical**. Contact points in government should be established and reachable regardless of the political changes in all countries.
- The third sector, namely non-governmental organisations, also has a vital role to play in keeping the topic of Digital 3 Seas Initiative alive and on the agenda of each country.

On financial instruments:

- In European programmes, more and more calls target projects related to cybersecurity or connected and autonomous mobility. Under the **new Connecting Europe Facility proposals**, there is a project specifically for cross-border 5G corridors which will bring together transport infrastructure overhaul and new modern communication technologies allowing autonomous driving, seamless communications throughout a transport path and smart energy technologies with power grids operating on a regional basis.
- A number of **European financial instruments**, some of which can be blended together, will address specifically the infrastructure and investment gaps to tackle issues in transport, in energy but also in the digital realm.
- Creating a **Digital 3 Seas investment fund** would help put some projects into practice and reveal the full potential of the initiative.
- The **Digital Europe Programme** has been the first of many European Commission's proposals under the next Multiannual Financial Framework to reach a political agreement. The Digital 3 Seas Initiative is very much aligned with the areas of the Digital Europe Programme and has to be considered by governments while developing the details regarding the funds allocation.

On cooperation within the region:

- The CEE region has many strengths:
  - A very good education level – almost the same as the Scandinavian "digital frontrunners" (over 230 000 graduates in ICT and related academic fields for 2016–2017).
  - A well-functioning and very affordable 4G infrastructure.
- The **opportunity** in the Three Seas Initiative is that countries work together – both businesses with governments (B2G) and governments among themselves (G2G).
- In the Digital 3 Seas Highway project, cross-border segments – particularly with the 5G element – are going to be crucial because they **prevent siloed or national-based solutions** and allow for seamless cross-border logistics, transport and a non-interrupted, equally high level of cybersecurity associated with digital infrastructures.
- The difference in the pace of digital transformation between countries should not be seen as a problem. Some players can miss an opportunity in the development of a technology but spring a surprise later on.

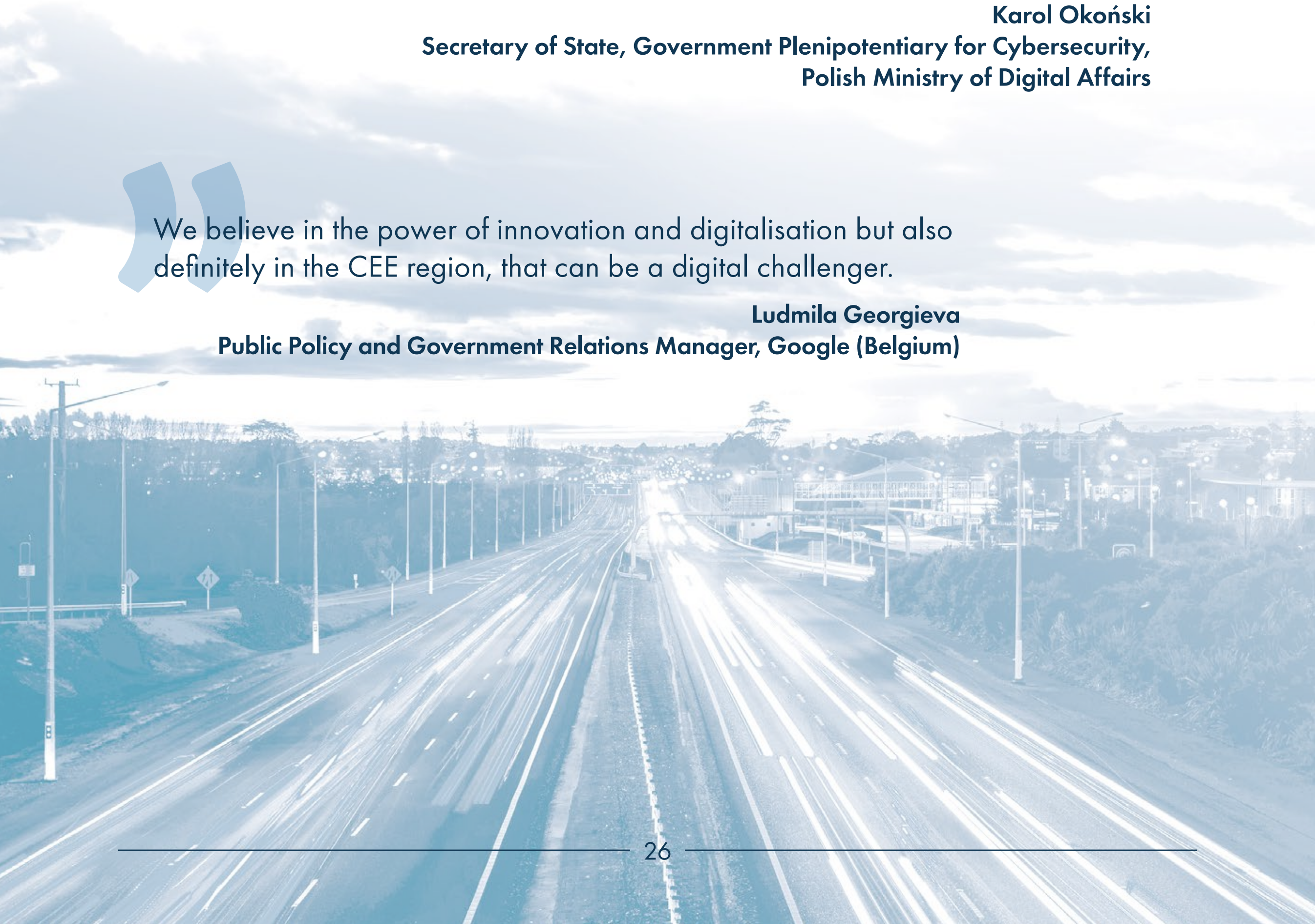
On public-private cooperation:

- **Public-private collaboration** will be indispensable for further advancements in the digital field.
- **Public and private sectors** have to work hand in hand. The private sector needs engineers and innovators to fully contribute and build digital services and products. It is not possible without a government which provides a good educational system, empowers digital tools for businesses, start-ups, and for e-government.

> Digital revolution can serve as an engine of growth for the economy within the region.
>
> **Joanna Świątkowska**
> **CYBERSEC Programme Director; Senior Research Fellow,**
> **The Kosciuszko Institute**

> We have to make sure that the Three Seas Initiative is not left without its digital component.
>
> **Karol Okoński**
> **Secretary of State, Government Plenipotentiary for Cybersecurity,**
> **Polish Ministry of Digital Affairs**

> We believe in the power of innovation and digitalisation but also definitely in the CEE region, that can be a digital challenger.
>
> **Ludmila Georgieva**
> **Public Policy and Government Relations Manager, Google (Belgium)**



The question is not what can the EU do for the Three Seas Initiative but rather: what will the Three Seas Initiative bring to the EU? Nearly half of the EU member states working together on a regional cross-border cooperation project is exactly what we need in order to fulfil the EU objectives with regards to digital transformation, the rollout of digital infrastructures and all the things that come through that, including digital skills, equality, development of rural areas.

Pearse O'Donohue
Director, Future Networks Directorate, DG CONNECT, European Commission

Microsoft
@MicrosoftEU
#D3SI
Panel Discussion:
THE DIGITAL 3 SEAS – TOWARDS SECURE DIGITAL
TRANSFORMATION OF THE REGION

Our citizens need success stories. We have to show the citizens and businesses that there is an added value in the Three Seas Initiative and that it is important to work together on that issue.

Maria-Manuela Catrina
Ministry of Communication and Informational Society, Romanian Government

CYBERSEC BRUSSELS LEADERS' FORESIGHT 2019

IN NUMBERS

1 Quest for Cyber Trust

1 day of high-level discussions

2 accompanying events

4 thematic streams

1 flagship Digital 3 Seas Initiative

6 significant announcements & statements

9 keynote presentations, panel discussions, fireside chats

30 speakers

27 journalists

10 partners & patrons

>250 likeminded cybersecurity enthusiasts

42 represented countries

>50 publications in media

62,7K twitter impressions

>267K of social media reach

STRATEGIC PARTNERS

SAMSUNG

PZU

Microsoft

Google

INSTITUTIONAL PARTNERS

NATO
OTAN
SINCE DEPUIS 1949

ECS
EUROPEAN CYBER SECURITY ORGANISATION

FERMA
Federation of European
Risk Management Associations

theLisboncouncil
think tank for the 21st century

IRMO
Institut za razvoj i međunarodne odnose
Institute for Development and International Relations

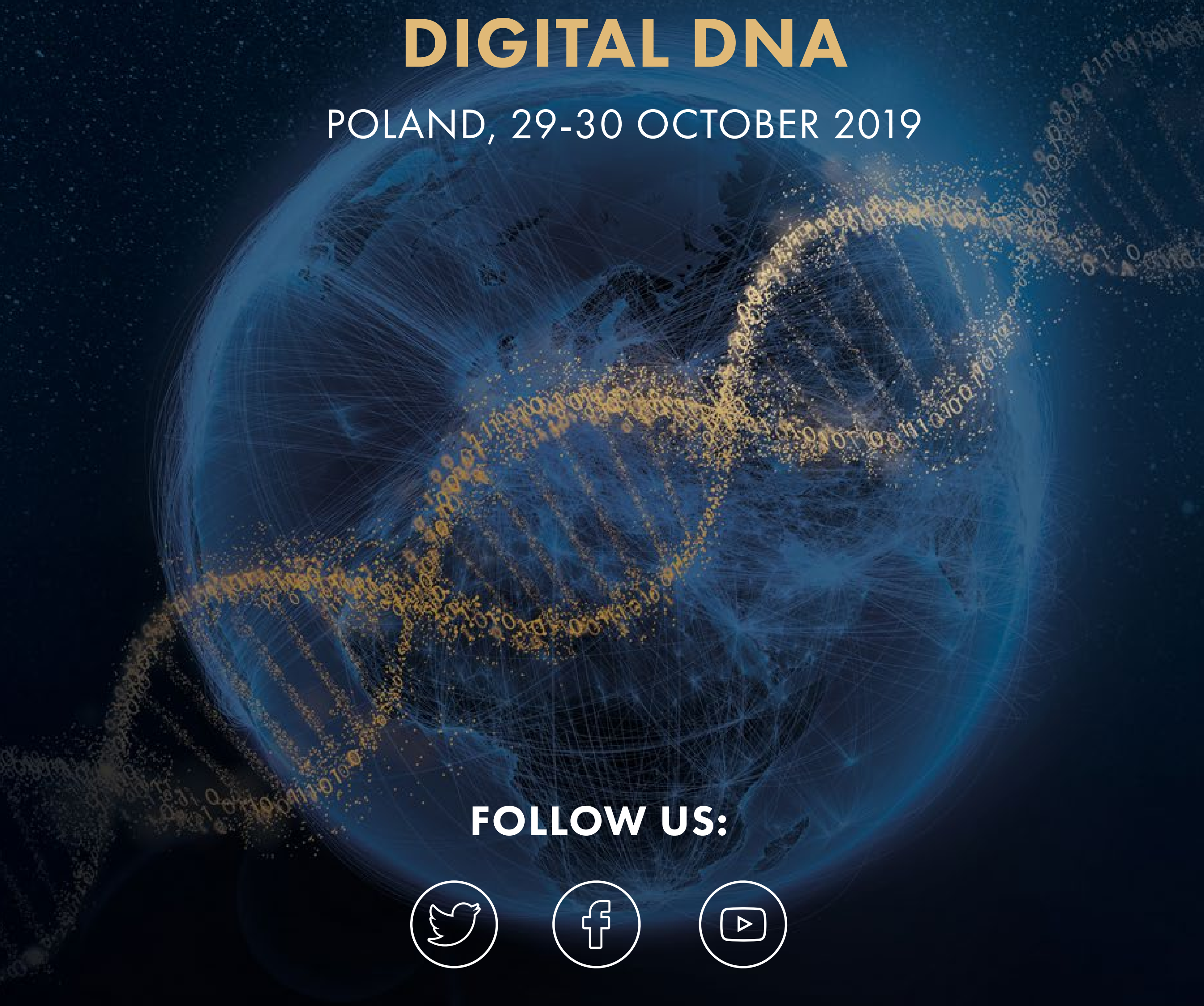
ANTALL JÓZSEF
KNOWLEDGE CENTRE

CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

SAVE THE DATE

SECURING THE WORLD'S DIGITAL DNA

POLAND, 29-30 OCTOBER 2019



FOLLOW US:

www.cybersecforum.eu