CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

THE TRANSATLANTIC QUEST FOR CYBER TRUST

KEY TAKEAWAYS

CYBERSEC WASHINGTON LEADERS' FORESIGHT, 19 MARCH 2019

#CSDC19

www.cybersecforum.eu/washington

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 Washington 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.

PREFACE

In the year of its fifth anniversary, the European Cybersecurity Forum – CYBERSEC was successfully **introduced to the other side of the Atlantic** thanks to cooperation between The Kosciuszko Institute and the Center for European Policy Analysis (CEPA).

CYBERSEC Washington Leaders Foresight featured government officials and the brightest leaders in cybersecurity from both sides of the ocean to foster the **Transatlantic Quest for Cyber Trust.**

That debate matters as we are in a crucial moment of **significant shifts in global economic and military powers**, both driven by modern disruptive technologies. We are now at the moment when we need to build a secure cyber world together – this is where our shared future is now being shaped.

The unique US global leadership can not exist without its allies. It is obvious today that a new world order is taking shape. **The Three Seas Region**, and more broadly speaking Central and Eastern Europe, seems to be emerging as a **region of pivotal importance** – a critical one in the designs of China, Russia and the US. And since the struggle for the world's leadership is now also taking place in cyberspace, the US should engage the Three Seas Region to foster the digital potential in the countries who can contribute to the future shape of shared cyber realm.

The main takeaway of the conference was that the **US and the Three Seas countries together have unique potential to protect the rules-based democratic liberal order** that is threatened by the rise of undemocratic regimes, often using powerful cyberweapons. To overcome these challenges, we must merge transatlantic soft and hard powers to work hand in hand with corporate and non-governmental partners. We need to **build cyber resilience and deterrence together**. But there will be no cybersecurity without innovation, so we need to invest in cutting-edge technologies. The US can stimulate G2G cooperation, business-driven technology transfers, strategic investments, joint R&D projects and market opportunities in the Three Seas countries. It can also help to enhance digital and cybersecurity capabilities in the region by supporting the Digital 3 Seas Initiative as well as by introducing a new Marshall Plan concerning technology.

We are proud to present you with recommendations that may facilitate achieving that goal.

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

Peter Doran
President & CEO of the Center for European Policy Analysis (CEPA)

MESSAGE FROM **MINISTER MAREK ZAGÓRSKI**

Digital transformation is and will continue to be a major factor of social and economic change. With this digital revolution, of course opportunities for new business models, investments and economic growth come. **Competition for the profits generated by digital economy is fierce.** In this technological battlefield, the stakes are as high as one can possibly imagine – **for people and our values.** Human-centricity has never been more needed than it is now. The Western civilization focuses on human beings, who are at the center of interest for science, politics and culture.

Access to tech solutions determines not only the strength of the economy, but also political power. Europe and the USA need cooperation in a new dimension. We need consolidation of resources and partnership in investments. If we want to achieve the common goal of maintaining our values, our position in the world, **we must think about the new Marshall Plan – this time concerning technology.**

If we don't do it, we are threatened with the victory of a world in which technology, instead of serving people, serves to control them. Therefore, now more than ever, we must join forces and establish strong foundations for cooperation. **We need a transatlantic partnership based on solidarity and commitment.** In practical terms, **it means moving towards the same goal.**

What Poland would like to see is not only to have access to technology. Our aim is to co-create and develop IT solutions on a partnership basis. We need experience with exchange, joint projects and joint investments. We need to build a system based on **common standards, data formats, reciprocity of participation and recognition of certificates.** But at the same time a system that is secured and resilient to cyberattacks.

One of the **latest challenges we are facing is the roll-out of 5G technology and cybersecurity of the network it operates on.** Here we see great opportunities in establishing cooperation in the development of proper security requirements. Because 5G will be used to provide a broad range of services, **a high level of trust with network operators and technology providers must be established.** It is also our view that we should ensure **diversification of trusted technology suppliers,** certification at all supply chain levels and impose strict conditions on the vendors. A good solution would be a **cooperation between the national state security authorities introducing the 5G network.**

The digital transatlantic partnership should also cover both personal and raw data, privacy policies, and data ethics. We are in military and political alliances. Today we need a **technological alliance.** If we want our model of values to prevail, we have to step up, **we need all hands on deck!**

Thank you!

Marek Zagórski
Minister of the Digital Affairs, Republic of Poland

> I would challenge the whole policy community to begin to conceive of the Three Seas Region as an area of strategic competition with our great power rivals. Perhaps there is no better way in which we are poised to compete than in the dimension of the cyber.

Peter Doran
President & CEO of the Center for European Policy Analysis (CEPA)

> Poland and other Three Seas countries can contribute to the process of building a new world order with their unique innovative potential of ICT and cybersecurity experts and a flourishing digital industry.

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

> Despite all the change taking place in technology and cybersecurity, there is an important constant – we are stronger when we work together.

Piotr Wilczek
Ambassador of the Republic of Poland to the United States

ADVANCING SECURE DIGITAL TRANSFORMATION IN THE THREE SEAS REGION

PRINCIPLES:

- Free flow of data has to be aligned with the development of a **common understanding** on how to use data to **preserve fundamental human rights and core freedoms.**

- **Creativity** and what we create in cyberspace has to be protected equally for the user's safety.

- **Full transparency of software** is necessary. It is essential to have a **software bill of materials** to fully understand what is inside the systems we are depending on and how that can be affected.

IDENTIFYING KEY RISKS IN SUPPLY CHAINS:

- **Supply chains require the adoption of strategic long-term perspective** acknowledging the next 2, 3 or 5 decades rather than a focus only on low costs in a short-term perspective.

- While thinking about 5G and connectivity it is fundamental to adopt a full risk-based approach that includes **focus on the the provenance of technology and supply chains.** The political and legal system of the vendor's residential country should be taken into consideration while assessing this risk as it affects the reliability and trustworthiness of the vendor.

- We cannot only focus on the supply chain of hardware, as the technologies of the future that will come with IoT will be much more **software-defined.** We cannot only focus on the supply chain of hardware, as the technologies of the future that will come with IoT will be much more software-defined. There is much more source code involved in all of the IoT devices than in the network itself, thus the attack surface will be immensely bigger. As it is going to be much harder to verify every line of code, **the importance of having a trustworthy vendor will only increase.**

- The full spectrum of vulnerabilities and their strategic dimension is still to be grasped by decision-makers. There is a missing understanding of **where a country might have critical dependencies that should be addressed** by the stakeholders. When the Not Petya malware was released, it not only affected major companies which reduced their market share, but also disrupted the national economies those companies were part of. As a result, rival companies' market share increased, boosting the national economies of rivals.

- Currently most IoT devices are not protected against cyberthreats. This state of affairs cannot continue into a future that will be abundant with IoT-enabled drones and autonomous cars, as the results of hacking of those devices will be disastrous. **A momentous change in how we think about every single connected device is necessary** – we need to understand the full scale of their potential vulnerabilities.

DEEPENING THE SYNERGIES WITHIN THE TRANSATLANTIC COMMUNITY:

- Companies from the Central and Eastern Europe have to be treated as **trusted members of the global supply chain** by stakeholders from outside the region.

- **5G is a set of technologies and processes that need to be carefully mapped** in order to be better synchronized across countries and regions.

- **It is fundamental to create a narrative on why cybersecure interconnectivity is important**, both for the value of digital economy and for the strategic orientation in Great Power competition.

- While adopting a new cybersecurity certification regime, the European Union should ensure that it will be **compliant with international norms** in order to avoid regional blocks of standards that will obstruct international interoperability. European governments should ensure that they remain consistent with allies while adopting standards and regulations. Ultimately, their decisions shouldn't be disruptive for their current political or military alliances.

- **The Three Seas countries should incorporate international standards** in order to become more tightly woven in the international standardization and certification processes. Only then will they be able to leverage those processes. It will benefit both their public and private sectors. Initiatives such as the **Charter of Trust** or **ISO standards** related to cybersecurity should be taken under consideration.

- European and American companies should notice each other's products more often and **build on the long tradition of trust between the two economies.**

- In order to efficiently cooperate with the Three Seas Region, US companies and policy-makers need to acknowledge that the competition in the **digital market is increasingly fierce** and that they need to offer value beyond the sole acquisition of the product. They need to actively engage in the development of the region. **The region should be perceived in terms of strategic investments** rather than just commercial ties because strategic investments are how the stakeholders in the region perceive these opportunities, whether they come from the Europe, United States or beyond.

- United States can **stimulate G2G cooperation**, business-driven technology transfers, strategic investments, joint R&D projects and market opportunities in the Three Seas Region.

- Highly innovative companies from the Three Seas Region are now **rapidly climbing up the global value chain of ICT products and services.** American companies can join them in developing innovations for mutual benefit. Also, based on shared trust, the US market along with its global sales and distribution channels should open widely for the products and services coming from the Three Seas Region.

THE THREE SEAS REGION'S AUDIT OF ASSETS AND RECOMMENDATIONS:

- Decision-makers should **not think about cyber as a nationally-contained problem.** Digital connectivity and cybersecurity threats do not stop at political or geographic borders.

- The Three Seas countries should develop strategic agreements **to act and think as a like-minded region** about what technologies they want to embrace and how. They should adopt and implement joint or unified plans to develop or enhance investment in the key areas.

- **Regional consensus on 5G is critical.** It should determine which technologies to use, how to interconnect national 5G networks and develop common policy framework in order to avoid fragmentation and patchworked network landscape.

- It is fundamental to enhance uninterrupted connectivity between the communication systems in the Three Seas Region along **the North-South axis.**

- **A Three Seas Region-wide audit of assets is urgently needed** to understand how governments and companies could work together for **better resiliency and redundancy avoidance.** Existing gaps should be identified in order to plan efficient strategic investments in those areas.

- **A pan-regional consensus** on the overall value coming from **localized solutions** should be a base for cooperation. Investments in the **remote parts of the region** should be perceived as comprehensively beneficial for all stakeholders.

- **Smaller-scale cross-border infrastructure projects** that will ease existing communication bottlenecks or create new connections are vital as they **contribute to overall big-picture connectivity.** It is important to invest in these short-term local solutions as they will provide much-needed benefits and stability.

- **More ICT talent** should be educated, supported and kept track of as they advance throughout their careers.

THE 3 SEAS DIGITAL HIGHWAY:

- Digital infrastructure should be **built along existing and planned highways** as has been done in the United States. The extent of main roadways should limit neither the reach nor the utility of the infrastructure and the connectivity ought to penetrate into more remote areas.

- **A regional audit of the infrastructure layout in the 12 countries of the Three Seas Region** will also help determine the existing infrastructure that needs to **be interconnected to complete the 3 Seas Digital Highway.**

- Completing the 3 Seas Digital Highway will require the governments to build a **much stronger narrative around the value proposition to invest for industry and business partners.** They have to be attracted and convinced to invest money by a commercial value proposition in order to maintain their competitiveness, which will drive the digital economy and the digital growth of the Three Seas countries.

- The digital infrastructure in the Three Seas Region should be built focusing not only on commercial value but also on **strategic value.** Fiber optics and telecommunication antennas can be built along highway infrastructure, which is relatively easy in terms of regulations.

THE IMPORTANCE OF PUBLIC-PRIVATE PARTNERSHIPS:

- A significant amount of infrastructure is in the hands of the private sector. It is fundamental to **ensure that private sector is involved in a truly multi-stakeholder discussions** about regulations and about Internet-related policies.

- 3rd Generation Partnership Project (3GPP) showed that industry-led standards are crucial. **The industry should be in the driver's seat for setting standards for the future.**

- In the context of the entire lifecycle cost, the need to produce patches and updates is very expensive. Decision-makers should be encouraged to consider the entire cost of having a certain product that despite being cheap on the front requires intensive further maintenance. It is also important to **disaggregate the actual cost of equipment and the financing terms that go with it.** Executive decision-makers from both public and private sector should talk to each other about possible reasonable ways of financing this equipment and infrastructure in the long term.

- **Initiating multi-stakeholder processes** will strengthen the immune system of networks. Policy-makers **should encourage business and hackers to come together to identify and remedy flaws** or to create norms in coordinated vulnerability disclosures.

- CERTs should connect experts from different sectors, as only the people who know their sector can efficiently spot anomalies. **The public sector should think about how to expand the threat assessment with the help of the private sector**, as well as building up the capabilities to anticipate threats sooner.

Cybersecurity is about governing the risk. If you don't understand that your entire country is digitally dependent and without key services you can't actually deliver citizen-facing services, and your corporations won't be able to work, then you haven't really embraced the cybersecurity conversation.

Melissa Hathaway
President, Hathaway Global Strategies, LLC; Former Cybersecurity Advisor, George W. Bush and Barack Obama administrations; Expert of the Kosciuszko Institute

Photo Credit: The Kosciuszko Institute

We should change our paradigm to not think about low cost as a key value in creating cyberspace, but towards strategic, economic and other goals in the very long-term: 20, 30, 50 years.

Nikodem Bończa Tomaszewski
CEO, Exatel

There's no source code review, no laboratory test that is going to tell us that we have got every last line of source code correct. And if you have patches and updates to those systems, that means you need to rerun the whole test all over again. It's fundamental that you have a trustworthy vendor involved in the process.

Robert L. Strayer
Deputy Assistant Secretary for Cyber and International Communications and Information Policy, US Department of State

Photo Credit: CEPA

> We live in a democracy where, quite frankly, all of us must acknowledge that the technology exists to serve us – humanity. Not the other way around.

Edna Conway
Chief Security Officer, Global Value Chain, Cisco Systems

> In the Three Seas Region, in the cybersecurity initiatives, we need to work and not be hostage to our geographical or political borders because cyber doesn't stop there, digital doesn't stop there, it flows right on through and that's both for business opportunities but also for threats.

Tony Housh
Chairman, American Chamber of Commerce in Poland

> We need to understand what is inside our systems. This is the notion of the software bill of materials. When you buy an engine, it's going to come with a bill of materials, every single nut and bolt that it's sold with is on this list so that you can do maintenance, so you know what you are buying. We don't have this with software that is now running all of the engines that we care about.

Allan Friedman
Director of Cybersecurity Initiatives at the National Telecommunications and Information Administration, US Department of Commerce

BUILDING CYBER DETERRENCE IN THE THREE SEAS REGION

STRENGTHENING THE REGIONAL AND TRANSATLANTIC ALLIANCE:

- The 2018 National Cyber Strategy of the United States **underlined the importance of alliances and collective actions in cyberspace,** the so-called **Cyber Deterrence Initiative.** It is vital now to explain, define and operationalize the assumptions and aims of this initiative.

- **As Central and Eastern Europe emerges as a region of pivotal importance** in the global power struggle, **the United States has to strengthen its engagement in the Three Seas Region** to balance the growing political and economic presence of Russia and China. For the last 30 years the US has always kept its edge over its rivals in Central and Eastern Europe, but this state of affairs has to be **constantly sustained and reinforced to endure.**

- Three Seas countries are in a unique position to **develop a common stance and code of conduct** as they are similarly situated, face the same threats and can share their best practices as well as their shortfalls to achieve better overall resiliency. This should be done with the **active support of the United States and other allies.**

- More transparency between the allies is needed as they can **mutually enhance their ecosystems** if they are aware of each other's strengths and weaknesses.

- The United States and other allies that have their **military forces deployed in the Three Seas Region** should **coordinate their efforts** concerning the cyber defenses of the region. They have to understand that their soldiers rely on an infrastructure that is under heavy pressure from cyberattacks that their adversaries mount.

- The United States **enhanced cyber resilience posture** in Central and Eastern Europe will improve **American situational awareness.**

COMMON RULES FOR DETERRENCE:

- **Cooperation and allied conduct in cyber defenses** leads to greater efficiency and legitimacy.

- **Imposing costs** on perpetrators and malign actors is crucial. If they are ever to be respected, laws and rules in cyberspace have to be followed by sanctions for their violations. **An accountability mechanism** has to be introduced.

- **Consistency** is necessary as the leaders have to be united not only in naming the responsible actors, but also in implementing sanctions.

- Credibility is essential. Partners have to be responsible for their actions and their posture in cyberspace. **The applicability of international law in cyberspace** should be constantly affirmed.

- **Deterrence** can be seen as consisting of three elements: 1) having capabilities; 2) acknowledging this fact to others and 3) having the ability to use them.

- Deterrence in cyberspace is difficult to showcase and **capabilities are inherently not transparent** as they are linked to sensitive intelligence. Therefore, effectiveness should be assessed relying on cyber defense capabilities and successes.

MODELS TO ADOPT, POLICIES TO IMPLEMENT:

- Deterrence can be built in two ways that should be developed simultaneously. **Deterrence by denial** should be achieved by prioritisation of resilience. Regional cooperation can be especially efficient here, as it allows for information exchange, sharing platforms, training, education and joint exercises. The other way **is deterrence by retribution**, which relies on punishment of bad behavior – with at least an equal and opposite reaction - to persuade the potential attacker not to act.

- A wide spectrum of **sanctions should be agreed upon** by regional governments, as well as the rules on how and when to use them.

- Countries in the Three Seas Region should act more cohesively **and join their allies in attribution.** It is a measure of building trust that can positively affect future joint cyber defense efforts.

- It is a task for every member state to contribute to the Alliance; **meeting the NATO defense spending obligations comes first,** as NATO relies on cyber capabilities provided by the member states.

- The Three Seas countries should be more active in the European Union's efforts to develop cyber tools and laws as they can provide valuable input due to the **region's constant exposure to malicious cyber and hybrid conducts.**

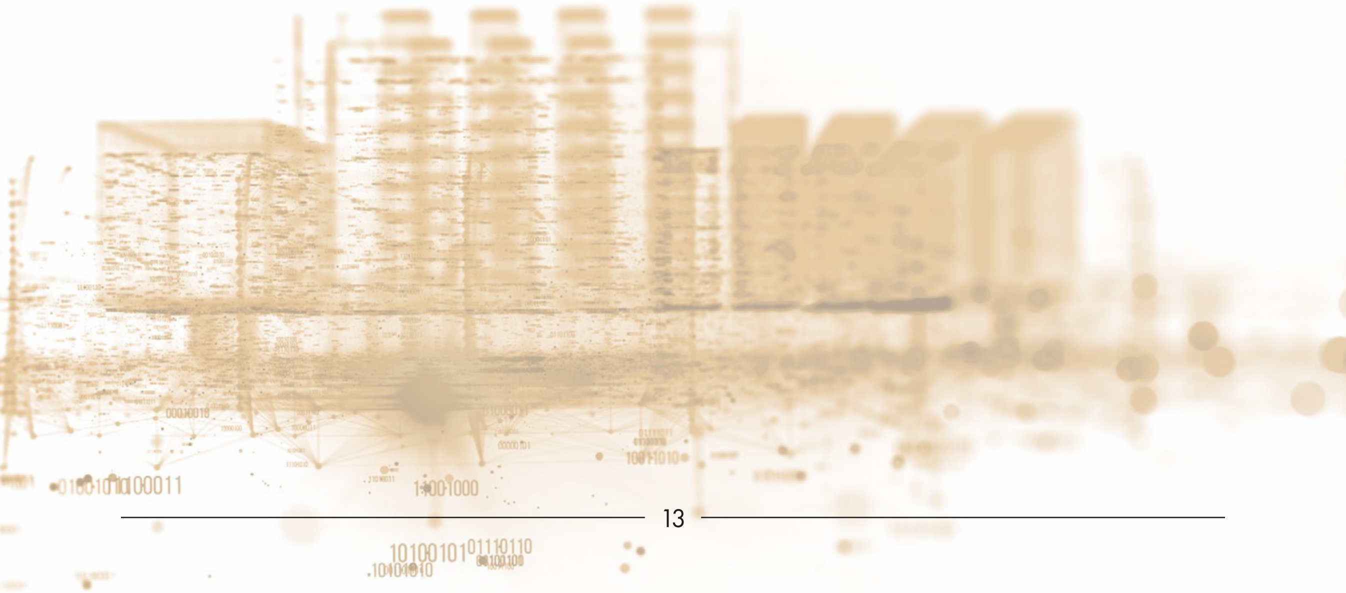
- The biggest obstacle to the efficient cooperation of CERTs from different countries in the region comes from **different legal frameworks.** The adoption of **common regulations** will lay ground for the regional exchange of data or people and the sharing of infrastructure. Existing **frameworks for co-operation within NATO and PESCO** can also be utilized as a way to overcome the challenges originating from different legal landscapes.

- Countries in the Three Seas Region should **adopt and make use of important international initiatives** such as the US effort on the Cyber Deterrence Initiative, NATO's playbook on imposing costs and the EU's diplomatic toolbox.

- It is key to build multi-stakeholder ties and frameworks **across different sectors.** Businesses should share information with each other and with the government as each sector faces specific types of threats and in its own specific way counteracts **the overall vulnerability of a community.**

- **The public sector should establish fellowships with the private sector** in order to build trust, familiarity and understanding of the full spectrum of resiliency a community needs.

- Rather than to think about critical infrastructures as entities, governments should start to **think about the critical functions of these infrastructures that the citizens depend upon.** The role of the government in the **protection of those functions** and services should be redefined.



> We have to look at this framework of cooperation within Three Seas as a chance to deal with obstacles.

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

Photo Credit: CEPA

> US National Cyber Strategy has a very important section where it says: in cyberspace, if we are going to actually deter conduct, we are better acting together than we are alone. The United States is better if it is acting collectively with its allies and partners than when it is acting alone.

Christopher Painter
Commissioner, Global Commission on Stability of Cyberspace;
Former Coordinator for Cyber Issues, US State Department

> It is important for countries in the region that they create like-mindedness and they relate to these playbooks and processes, they develop this kind of common trust so they can really support each other.

Sorin Ducaru
Senior Fellow, Hudson Institute; Former Assistant Secretary General for Emerging Security Challenges, NATO

Photo Credit: CEPA

> Every citizen needs to have a stake in understanding what the threats posed to them are, but also the opportunities these technologies provide. At the end of the day, security in the conversation with values, the funcationality that the technologies can add.

Trey Herr
Senior Security Strategist, Digital Diplomacy, Microsoft

> We need to continue to affirm that international law applies in cyberspace, which means you should not interfere in another nation's activities.

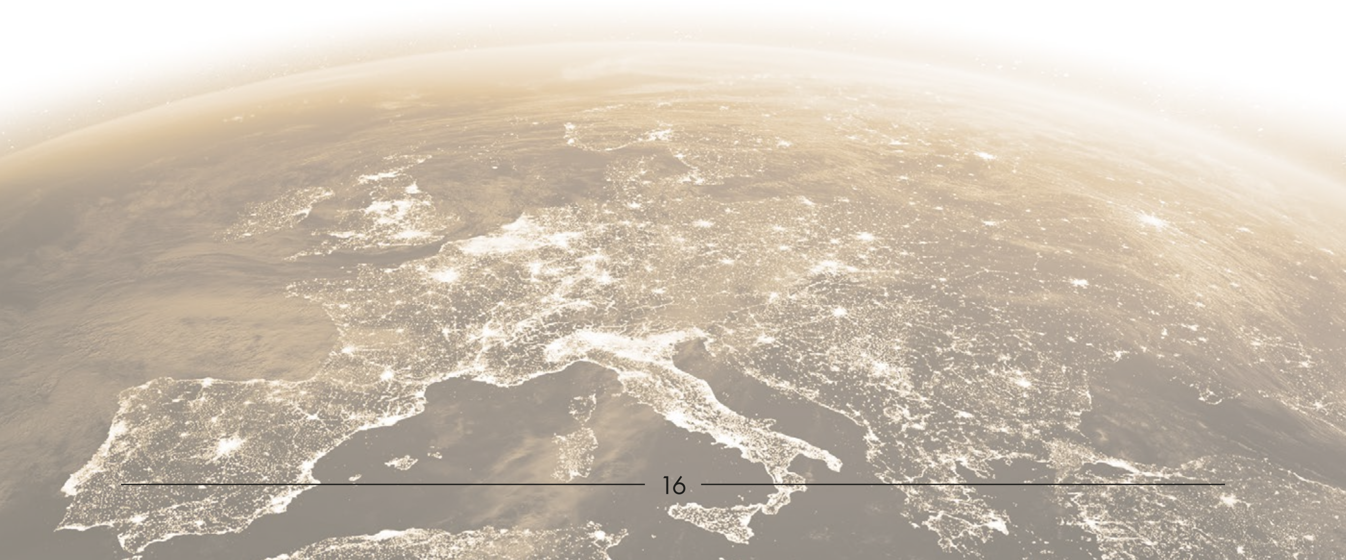
Robert Strayer
Deputy Assistant Secretary for Cyber and International Communications and Information Policy, US Department of State

> From the perspective of deterrence we are together because we can fight for each other when something is wrong.

Michał Kuczmierowski
Member of the Management Board, Polish Armaments Group

> The first threshold in cybersecurity that we faced was to go beyond this kind of segmented approach in which public units and private entities were not really willing to cooperate. We have gone beyond that threshold. The next one is how we actually establish this effective level of cooperation among the capitals and among the countries.

Réka Szemerkényi
Executive Vice President, Center for European Policy Analysis (CEPA)



> The more we can understand how others are positioning themselves, what other capabilities there are or what other things they are seeing with common adversaries, the better we can both protect our homelands. By working together we can collectively make it harder for the adversary.

Jeanette Manfra
Assistant Director, Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security

Photo Credit: The Kosciuszko Institute

When we are thinking about building resilience and deterrence we need to think about cooperation and solidarity. Sometimes I like to say that whatever happens to us today might happen to you tomorrow. And this sentence is true no matter from which side of the Atlantic it comes from, and I think this is the strongest and the most powerful message and the reason why we need to act together.

Joanna Świątkowska
CYBERSEC Programme Director; Senior Research Fellow, The Kosciuszko Institute

Photo Credit: CEPA

STRATEGIC PARTNERS

Microsoft

PGZ
POLSKA GRUPA ZBROJENIOWA

MAIN PARTNER

PZU

PARTNER

EXATEL

LAUNCHED TOGETHER BY

CEPA
Center *for*
European Policy
Analysis

THE KOSCIUSZKO INSTITUTE

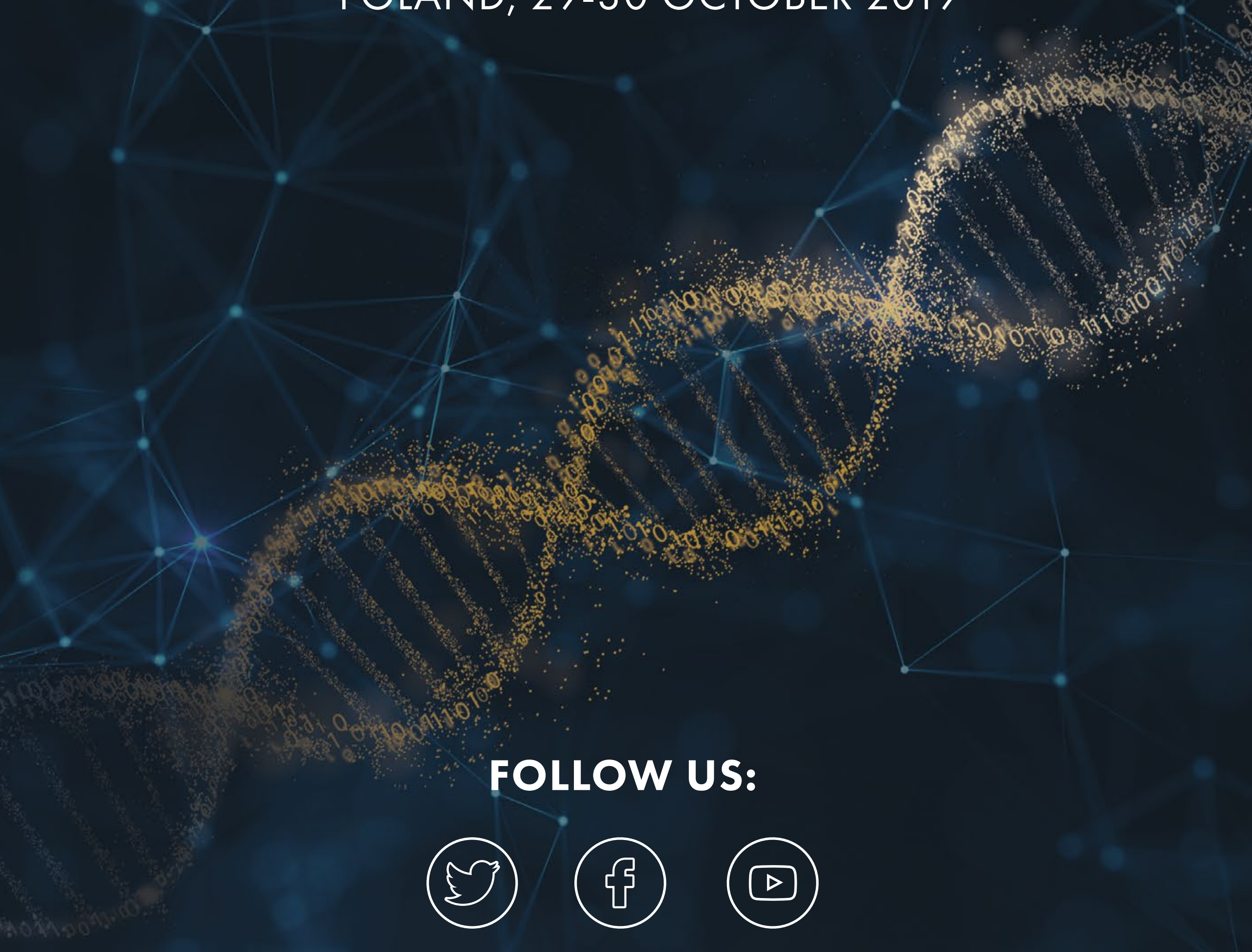
CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

SAVE THE DATE

SECURING THE WORLD'S DIGITAL DNA

POLAND, 29-30 OCTOBER 2019



FOLLOW US:

www.cybersecforum.eu