



**CYBERSEC**

EUROPEAN  
CYBERSECURITY FORUM

---

# THE TRANSATLANTIC QUEST FOR CYBER TRUST

---

## **KEY TAKEAWAYS**

---

CYBERSEC WASHINGTON LEADERS' FORESIGHT, 19 MARCH 2019

**#CSDC19**

[www.cybersecforum.eu/washington](http://www.cybersecforum.eu/washington)

# CONTENTS

<b>PREFACE</b> .....	2
<b>MESSAGE FROM MINSITER MAREK ZAGÓRSKI</b> .....	3
<b>ADVANCING SECURE DIGITAL TRANSFORMATION IN THE THREE SEAS REGION</b> .....	5
PRINCIPLES: .....	5
IDENTIFYING KEY RISKS IN THE SUPPLY CHAIN:.....	5
DEEPENING THE SYNERGIES WITHIN TRANSATLANTIC COMMUNITY:.....	6
REGIONAL AUDIT OF ASSETS AND RECOMMENDATIONS:.....	6
MODELS TO APPLY – THE IMPORTANCE OF PUBLIC -PRIVATE PARTNERSHIPS:.....	7
3 SEAS DIGITAL HIGHWAY .....	8
<b>BUILDING CYBER DETERRENCE IN THE DIGITAL THREE SEAS REGION</b> .....	11
STRENGTHENING THE REGIONAL AND TRANSATLANTIC ALLIANCES: .....	11
COMMON RULES FOR DETERRENCE: .....	11
MODELS TO ADOPT, POLICIES TO IMPLEMENT: .....	12

---

## 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 the cooperation between The Kosciuszko Institute and CEPA.

CYBERSEC Washington Leaders Foresight featured government officials and brightest cybersecurity leaders 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. 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 could not have existed without its allies. It is obvious today that a new world order is taking shape, and so are alliances. **The Three Seas Region**, and more broadly speaking Central 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 to free and foster the Three Seas countries' digital potential which can contribute to the future shape of shared cyber realm.

The main takeaway point of the conference was that the **US and the Three Seas together have unique potential to protect the rule-based democratic liberal order** that is threatened by the rise of undemocratic regimes, often using powerful cyberweapons. To counter this threat, we need to merge transatlantic soft and hard powers together with our allies around the world and work hand in hand with corporate and non-governmental partners that think alike. We need to **build cyber resilience and deterrence together**. But there will be no cybersecurity without innovation, so we need to invest together 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 and for the Three Seas region's products and services. It can also help to enhance the digital and cybersecurity capabilities in the region by supporting Digital 3 Seas Initiative as well as by introducing a new Marshall Plan concerning technology.

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

---

**Izabela Albrycht**

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

# MESSAGE FROM MINSITER 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 – **it is people and our values.** Human-centricity has never been more needed than it is now. The Western civilisation focuses on human beings, who are at the centre of interest for science, politics and culture.

Today, however, political processes are increasingly dependent on technology. It has become a kind of resource – same as, for example, oil. **Access to tech solutions determines not only the strength of the economy, but also the political power.** Only a few decades ago, control over the military arsenal was one of the key attributes of the state. Can we say the same thing today? **In a time of the digital can we still say that the most dangerous and effective weapons are those that shoot bullets?**

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 the 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 exchange, joint projects, 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!





I would challenge everyone of us here in this room and 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 no better way in which we are poised to compete is in the dimension of the cyber.

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

The U.S. and the 3SI together have unique potential to protect the rule-based democratic liberal order that is threatened by the rise of undemocratic regimes, often using powerful cyber weapons.

**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 **common understanding** on how to use the 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.
- **A full transparency of the 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 THE SUPPLY CHAIN:

- **Supply chain requires 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 the 5G and connectivity it is fundamental to adopt a full risk-based approach that includes **focus on the technology provenance and the supply chain**. 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**. 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 the decision-makers. There is a missing understanding of where a **country might have critical dependencies that should be addressed** by the stakeholders. When the Non-Petya malware was released, it not only affected major companies reducing their market share, but also disrupted national economies those companies were part of. As a result, a rival company's market share increased, boosting a rival's national economy.

- 
- Currently most IoT devices are not protected against cyberthreats. This state of affairs cannot continue into the 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 TRANSATLANTIC COMMUNITY:

- Companies from the Central 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 synchronised 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 the great powers' competition.
- While adopting a new cybersecurity certification regime, the European Union should ensure that it will be **compliant with the international norms** in order to avoid regional blocks of standards that will obstruct international interoperability. European governments should ensure that they remain allied while adopting standards and regulations and that their decisions won'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 standardisation 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 up 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 is 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 the political or geographical 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**.
- **The 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 **localised 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 bring ease to existing communication bottlenecks or create new connections are vital as they **contribute to the 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 it 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.
- **The 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**. Fibre optics and the telecommunication antennas can be built along the 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.
- 3<sup>rd</sup> Generation Partnership Project (3GPP) showed that industry-led standards are crucial. **The industry should be in the driving 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 a long term.
- **Initiating multi-stakeholder processes** will strengthen the immune system of the 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. **Public sector should think on how to expand the threat assessment with the help of the private sector**, also to be more anticipating.

” 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 corporation 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



We should change our paradigm to not think about low-cost as a key value in creating cyberspace, but at strategic political, economic and other goals in a 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 will 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, U.S. Department of State



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 border 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 it comes with this list so that you can do maintenance, so you know what you are buying. We don't have it on the 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, U.S. 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 operationalise the assumptions and aims of this initiative.
- **As Central 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 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 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 short-falls 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 defences of the region. They have to understand that their soldiers there rely on an infrastructure that is under heavy pressure from cyberattacks their adversaries mount.
- The United States **enhanced cyber resilience posture** in the Central Eastern Europe will improve **American situational awareness**.

## COMMON RULES FOR DETERRENCE:

- **Cooperation and allied conduct in cyber defences** 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 the 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 measured by the extent to which a country is able to **ward off serious intrusions**.

## MODELS TO ADOPT, POLICIES TO IMPLEMENT:

- Deterrence can be built in two ways that should be developed simultaneously. **Deterrence by denial** should be achieved through 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 to achieve **deterrence is by retribution**.
- 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 defence efforts.
- It is a task for every member state to contribute to the Alliance; **meeting the NATO defence 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 exposition 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 utilised as a way to overcome the challenges originating from different legal landscapes.
- Countries in the Three Seas region should **adopt and make use of the important international initiatives** such as 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 a specific type 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, the 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.

”  
On this political-strategic level all of the activities of NATO and of the European Union very much influence the situational awareness of the decision-makers.  
I think it is crucial.

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



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, U.S. 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.

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



Every citizens needs to have a stake in understanding what are the threats posed to them, but also the opportunities these technologies provide. A the of day security is in conversation with the values, the functionality that the technologies can add.

**Trey Herr**  
**Senior Security Strategist, Digital Diplomacy, Microsoft**

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**





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 me today, might happen to you tomorrow. And this sentence is true no matter from which side of the Atlantic it comes, 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**





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

**Robert L. Strayer**  
**Deputy Assistant Secretary for Cyber and International Communications  
and Information Policy, U.S. 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, Polska Grupa Zbrojeniowa**



The first threshold in cybersecurity that we faced was to go beyond this kind of segmented approach in which public units and the 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)**

STRATEGIC PARTNERS

---



MAIN PARTNER

---



PARTNER

---



LAUNCHED TOGETHER BY

---





**CYBERSEC**

EUROPEAN  
CYBERSECURITY FORUM

# SAVE THE DATE

## SECURING THE WORLD'S DIGITAL DNA

POLAND, 29-30 OCTOBER 2019

**FOLLOW US:**



[www.cybersecforum.eu](http://www.cybersecforum.eu)