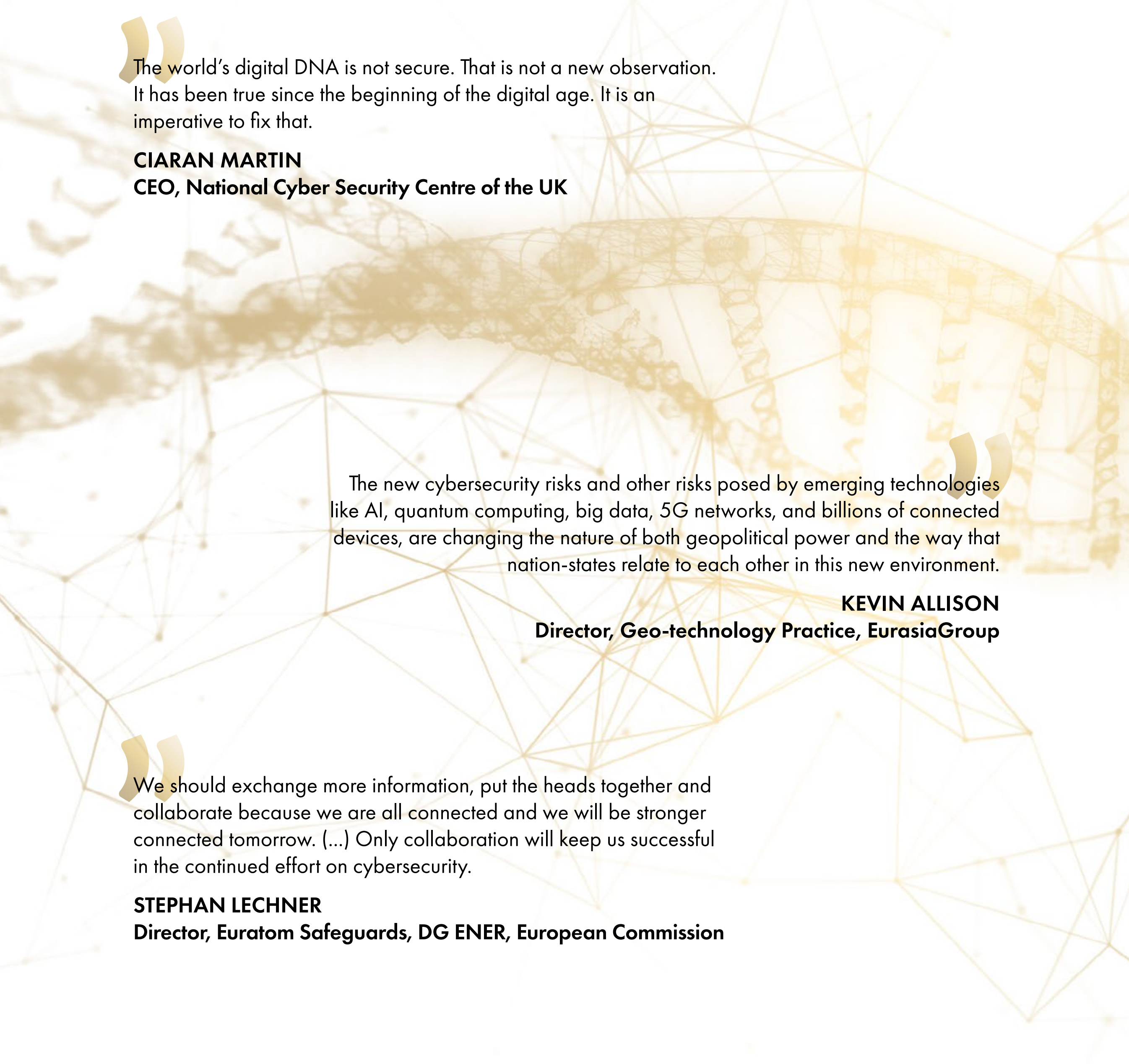
CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

CYBERSEC 2019
RECOMMENDATIONS & KEY TAKEAWAYS

5TH EUROPEAN CYBERSECURITY FORUM – CYBERSEC, KATOWICE 29-30.10.2019

#CSEU19 #SecureDigitalDNA cybersecforum.eu

SECURING THE WORLD'S DIGITAL DNA



> The world's digital DNA is not secure. That is not a new observation. It has been true since the beginning of the digital age. It is an imperative to fix that.
>
> **CIARAN MARTIN**
> **CEO, National Cyber Security Centre of the UK**

> The new cybersecurity risks and other risks posed by emerging technologies like AI, quantum computing, big data, 5G networks, and billions of connected devices, are changing the nature of both geopolitical power and the way that nation-states relate to each other in this new environment.
>
> **KEVIN ALLISON**
> **Director, Geo-technology Practice, EurasiaGroup**

> We should exchange more information, put the heads together and collaborate because we are all connected and we will be stronger connected tomorrow. (...) Only collaboration will keep us successful in the continued effort on cybersecurity.
>
> **STEPHAN LECHNER**
> **Director, Euratom Safeguards, DG ENER, European Commission**

DISCLAIMER:

During two days of the European Cybersecurity Forum – CYBERSEC 2019, around 100 speakers discussed how to secure the world's digital DNA. The CYBERSEC team has prepared the recommendations by following closely the statements made by CYBERSEC 2019 participants. This document does not credit any particular person with any particular remark as topics explored in different debates have not infrequently been merged here. Please bear in mind that the experts on a panel were not always in agreement, thus not every assertion or recommendation reflects each participant's point of view.

The takeaways are based on original speeches delivered during CYBERSEC Forum 2019. They have been reformulated and edited for clarity. Only the parts accompanied by quotation marks are quotes and reflect the wording used.

CONTENTS

STATE STREAM

DEFENCE STREAM

BUSINESS STREAM

FUTURE STREAM

PREFACE

Ladies and Gentlemen,

When we held the CYBERSEC CEE 2019, the world was indeed different.

Unfortunately, the COVID-19 pandemic has recently changed the way we live, work, interact and engage. In times of the pandemic lockdown and with most of social and business activities moving rapidly to the Internet, cybersecurity becomes more essential than ever. The CYBERSEC Community is deeply worried about the possible trajectory of expected cyberthreats. We are all acutely aware that they can be the next wave of the pandemic consequences, hitting our economies and well-being.

For that reason, we believe that presented recommendations need special attention of decision-makers all around the globe to help them secure the world's digital DNA. Unfortunately, years of alarming reports published not only by the Kosciuszko Institute but also by tech companies, consultancy firms and expert organisations didn't receive enough attention. Most of the countries in the transatlantic sphere still don't have resilient cybersecurity infrastructure, efficient and agile institutions and emergency plans prepared, not to mention digitally educated leaders able to tackle the most critical and essential threats to digital transformation, now literally the digitisation of everything.

It is time to make a change in our approach to confronting the emerging global challenges among which cyber ones are now a priority.

Since during CYBERSEC CEE 2019 no one expected the pandemic to happen in 2020, the presented recommendations are covering all the most important cyber-risks but not the current dynamic of cyberspace expansion day after day in front of our eyes. However, the dynamic of the implementation of these recommendations should significantly increase as we now more than ever need secure digital solutions along with launching a geopolitical response to emerging threats related to the disruption in the global digital supply chain which was additionally accelerated by the COVID-19 outbreak.

With lots of challenges ahead of us, we deeply hope that this set of recommendations will be an important source of inspiration and will spur cybersecurity stakeholders and decision-makers on to take bold measures aimed at ensuring safe cyberspace in a time when we all need them.

Please, enjoy the read!

Izabela Albrycht

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

The European Cybersecurity Forum – CYBERSEC is the biggest cybersecurity event in Central and Eastern Europe and gathers a community of people for whom **securing the world's digital DNA** is not just a job but a passion.

During CYBERSEC 2019 the Kosciuszko Institute proudly presented the Securing the World's Digital DNA Declaration. We shall never forget that cyberspace is human-made, and we should keep proactively shaping its DNA structure and characteristics.

THE SECURING THE WORLD'S DIGITAL DNA DECLARATION

1. The human is the weakest link in cybersecurity, but it is also the most important one in the digital world's DNA and therefore cyberspace should serve people. **#HumanCentricApproach**

2. We need to stop the uncontrolled processing of personal data and regain the control of the use of private information. **#PrivacyByDesign #DigitalFootprint**

3. New digital technologies, infrastructure, products and services should be designed, developed and used in a secure way in the whole life cycle and throughout entire value chain. **#SecurityByDesign**

4. It is our duty to protect our democracy and freedom against cyber disruption and disinformation, which might compromise, respectively, the voting infrastructure and the integrity of our decision-making process. **#CyberResilienceOfDemocracy #InformationSecurity**

5. Responsible and normative international collaboration, advanced public-private partnerships and cross-industry cooperation is needed more than ever to address global digital challenges. **#Multi-stakeholderApproach #CybersecurityCSR**

6. Diversity in cybersecurity contributes to the efficacy of cybersecurity teams and sustainability of solutions. Inclusiveness is a key factor in security issues and significant gender imbalance has prevented cybersecurity from developing full scale. We need to have inclusive and diverse teams in order to tackle current digital threats. **#CyberInclusiveness**

7. Strengthening forward posture in deterrence and defence, building and sharing cyber capabilities of like-minded countries, and improve attribution through better, more powerful technological potential might help to counter malign actions in cyberspace taken by state and non-state actors. **#ActiveCyberDefence #DefendingForward**

8. In the face of exponential development of deep technologies such as AI, quantum computing, IoT or blockchain together with their intersections, to identify future risks and address them up front is required. **#One-Step-Ahead-Cybersecurity-Policy #DeepCybersecurity**

9. Technological development must be ethical, sustainable and underpinned with values. We need to advance innovation against emerging threats. **#TechnologyForGood**

10. We need to make sure that humanity will be forever kept in the loop and that digital technology will never overpower us – that is cybersecurity per se in the new digital world. **#TechnologicalSingularity**

STATE STREAM

THE ROLE OF STATE ACTORS IN SECURING THE WORLD'S DIGITAL DNA

- The first step towards securing the world's digital DNA is to fix "endemic and chronic weaknesses" of the digital systems. State actors are a crucial element in this process and there are a few steps on how governments and public authorities might help:
  1. Stepping in and **taking the lead in areas where companies fail to ensure a greater security.**
  2. There is a need for concrete remedies and not only the problem diagnosis. Instead of repeating the narrative saying that "people are the weakest link of the chain" there should be guidance regarding **simple things to make them safer online.**
  3. **Developing standards and labels** which indicate the security level of IT products (as is happening at the EU level with the Cybersecurity Act entering into force in June 2019).
  4. **Disclosing the information on vulnerabilities** in order to allow IT services and products providers to find solutions and fix them.
- One permanent duty of the state authorities is **to protect national critical infrastructure.** Nowadays, this encompasses especially two major issues:
  - **The development of the 5G infrastructure** → the totality of systems should be resilient and a decision on vendors is only a part of a wider approach to 5G security risk.
  - **The protection of election infrastructure** which is crucial for our democratic societies → fixing the digital DNA is also ensuring the security of national digital DNAs, which includes **defending democracy against malicious actors.**

TWO MAJOR ASPECTS IN PROTECTING NATIONAL CRITICAL INFRASTRUCTURE:

✓ Development of resilient 5G networks

✓ Protection of election infrastructure and values

> There can be no more precious commodity than our democracy, so when I go home one of our major challenges will be to defend the forthcoming election from interference. We've learned a lot from partners, we've learned a lot from the hugely impressive US operation in the midterms in 2018, and if we do nothing else for the rest of this year, then our passionate commitment to defending democracy will be our highest priority because in fixing our digital DNA we have to make sure we protect our wider national fabric, our national DNA as well.
>
> **CIARAN MARTIN**
> **CEO, UK National Cyber Security Centre**

SECURE 5G INFRASTRUCTURE AS A BACKBONE OF DIGITAL TRANSFORMATION

10 RULES TO BE APPLIED TO SECURE THE DIGITAL DNA OF 5G:

1. A **common, unified and homogenous approach in the EU** is a crucial step in the further development of the Digital Single Market.

2. Security is a **joint responsibility** of vendors, operators and regulators.

3. 5G will inevitably enable massive development and implementation of the Internet of Things and artificial intelligence solutions. It is of the utmost importance to demand that the producers create and deliver products which are **secure by design** and **by default.** Security for the 5G supply chain is a must.

4. Taking into consideration the importance of digital infrastructure security, public authorities should have at their disposal **tools to evaluate and accept the decisions made by telecom operators** regarding the security of next-generation wireless networks. This approach should be applied and harmonised at international level.

5. We should look beyond 5G and take advantage of the political will that developed around the subject. As 5G will also have wider implications for the whole digital ecosystem, including new use cases and applications, it will be a key link in the global ICT supply chain. Therefore, it is a political and strategical opportunity to look into the overall issue of increasing **security of the digital supply chain.**

6. Decisions regarding the roll-out of the digital infrastructure must be based on **thorough risk analysis processes** and **risk mitigation plans** which will take into consideration a wide spectrum of factors (technical and non-technical) and provide the scope to see the problem both from the national security perspective and that of geopolitical reality.

7. Digital networks can't be dependent on one vendor. Dependency on any single supplier and lack of diversity increases the exposure to a potential supply interruption. **Diversification** is therefore much needed and there is room for setting specific rules in this area. In this context interoperability will serve as an important factor that may help to avoid the vendor lock-in problem.

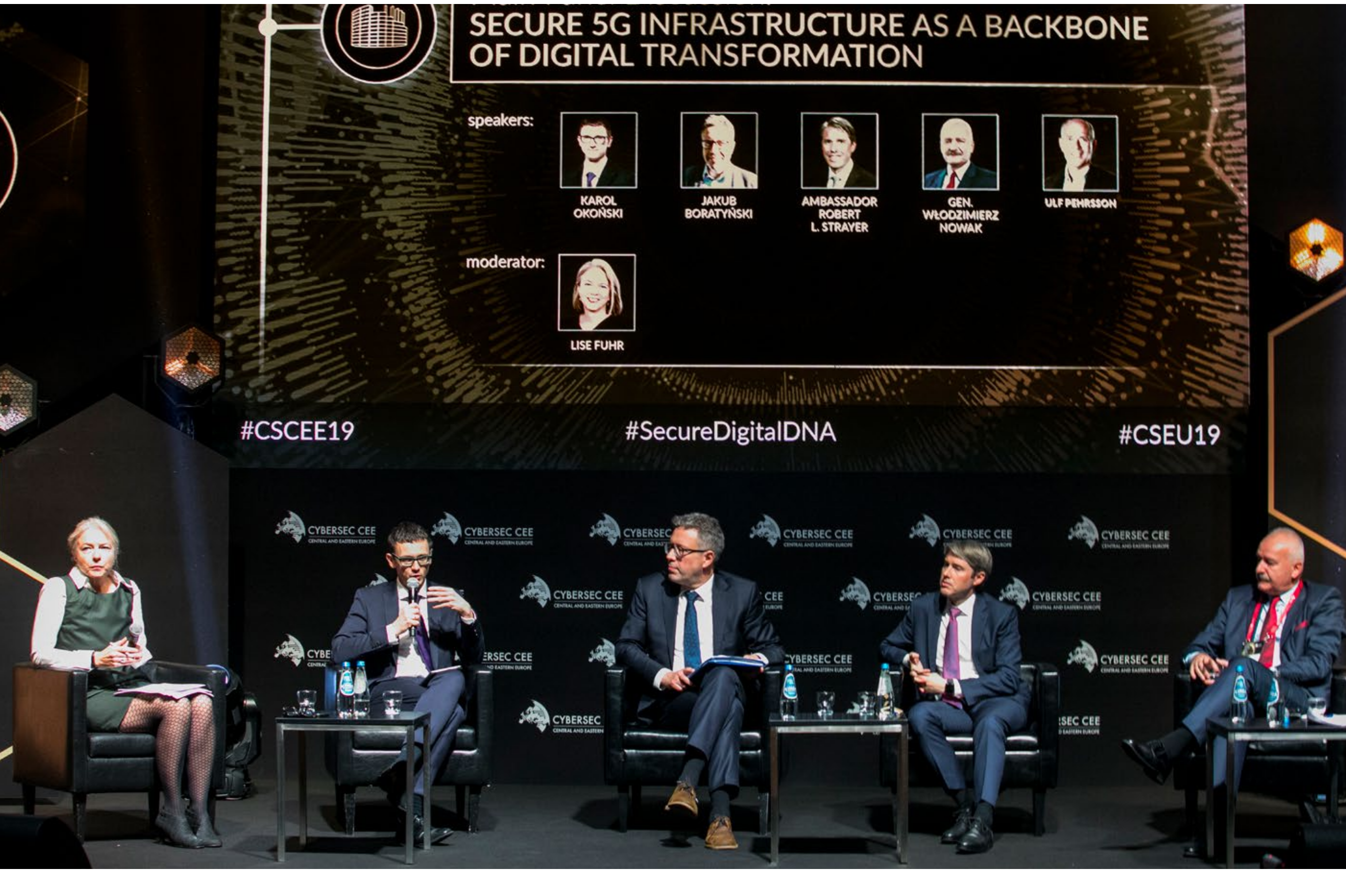
8. Choosing **trustworthy partners** plays a central role in assuring the security of new-generation networks; trust in technology suppliers has become one of the major concerns for some countries and the direct reason for unwillingness to implement technology components from some of them. Smaller countries, in particular, do not have capabilities for and cannot afford to pay sufficient attention to testing both software and hardware. Therefore, the overall security is based on trust in the supplier.

9. Some measures, to have their intended security effects, have to be implemented much more widely. **Cooperation with other regions** outside of the EU is therefore essential.

10. While architecting 5G networks, the whole lifecycle of network maintenance and operation must be taken into account. When it comes to maintenance, it must be ensured that updates are not directly implemented in the network, but **audited in advance. End-to-end encryption** in order to prevent espionage is also crucial. Mechanisms that would help to test security of the updates used for next-generation wireless networks should be created.

> We cannot be in a position where the whole 5G network is dependent just on one vendor. (...) We have to keep the market as competitive and as open as possible to the extent that we will not be monopolised by any vendor.

KAROL OKOŃSKI
Secretary of State, Polish Ministry of Digital Affairs;
Government Plenipotentiary for Cybersecurity



> 5G is also a major opportunity for us to look into the overall issue of increasing security of digital supply chain.

JAKUB BORATYŃSKI
Head of Unit, Cybersecurity & Digital Privacy, DG CONNECT,
European Commission

> For those who care about citizen data, which we do in the US and I know folks do in Europe, it is important to recognise that any part of that 5G network where there is computing power is a place where someone can exfiltrate data and use it for purposes that have not been authorised.

ROBERT L. STRAYER
Deputy Assistant Secretary for Cyber and International Communications and
Information Policy, U.S. Department of State

HOW TO FIX (DIGITAL) DEMOCRACY?

- Analysing the phenomenon of election meddling only through the lens of disinformation is simplistic and counterproductive to providing effective answers. Election meddling campaigns must rather be seen as part of a **complex information confrontation, which has a holistic structure and combines various elements** such as electronic warfare, information operations and psychological operations.

- Big tech companies and digital platforms, which nowadays are among the major actors in delivering political campaign content, cannot win the battle against election meddling on their own. Despite increasing efforts currently undertaken, more is expected from them. Concurrently, cooperation with NGOs, academia and most importantly with public administration needs to be fostered.

- It must be at the core of social media platforms' principles to **fight against misinformation spread by fake accounts**. If they fail with self-regulation, legislators would have to take up the issue and put **binding regulations** in place.

- **Cyber-hygiene** is the lowest common denominator in fighting against election interference and should be fostered rather than overlooked.

- In the context of information overabundance – from trustworthy as well as untrustworthy sources – there is a critical need to invest in **media literacy** from the younger age and to involve all kind of institutions from schools to retirement homes in this matter.

- Technical and automated indicators are essential to detect and identify influence campaigns targeting democracies, but they should always be **backed by human intelligence**. Also, in addition to the "real-name policy", AI and machine learning are powerful tools to counter threats coming from troll farms and take down fake accounts. **Technology and policies** have to be combined to fight hostile influence and fabricated opinions.

- **Blockchain** could be envisioned as an effective technical solution to fight against deep-fakes as it can help to create a credible trail verifying the source and going back to the original file.

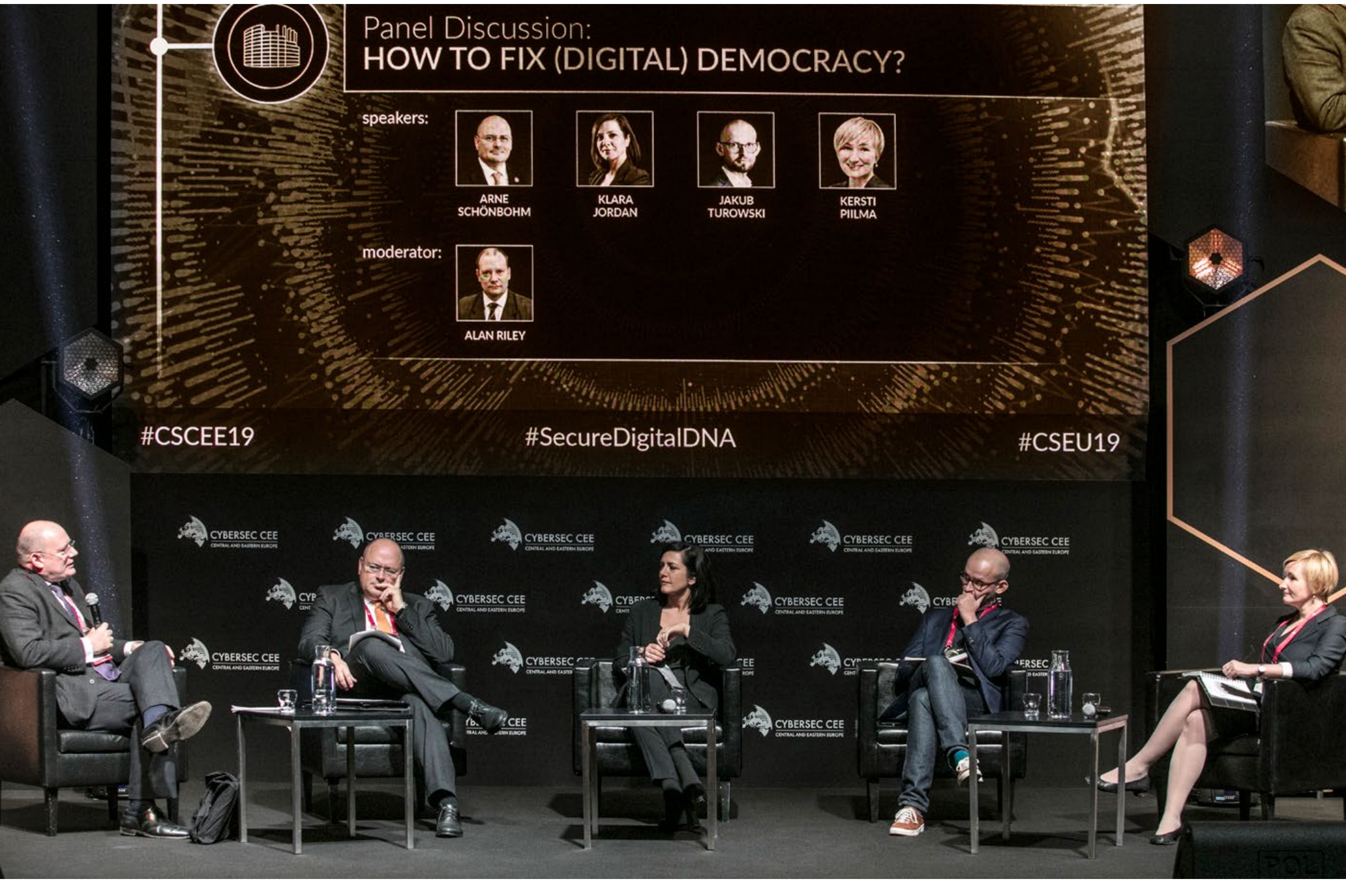
- Tailored and selective news feeds online often trap people in their beliefs (the so-called information bubble) and undermine the **value of dialogue and confrontation of ideas**. It is a duty of governments to support social media companies in opening their platforms to the exchange of ideas as an early defence mechanism against hate speech.

- Two essential aspects in securing the election processes:

  1. **Harden the system →** secure the voting machines and the transmission systems of the results.
  2. **Protect the people →** accompany the candidates in protecting their emails and social media accounts and teach the public to verify the sources of information.

We have done a lot around disinformation, we have done a lot around election infrastructure, there is a lot to think about cyber-hygiene.

KLARA JORDAN
Executive Director EU and Africa, Global Cyber Alliance



I think it is very important for us to understand that looking at technical indicators alone is not sufficient to identify if someone is trying to influence a democratic process or not.

ARNE SCHÖNBOHM
President, German Federal Office for Information Security

I don’t think that democracy needs to be fixed. I think we should simply use the strengths of democracy like freedom of speech in the context of the times.

KERSTI PIILMA
Counsellor, Cyber Diplomacy Department,
Ministry of Foreign Affairs of Estonia

CYBERSEC FOR DEVELOPMENT: BRIDGING GLOBAL GAPS IN CYBERSECURITY

- Public authorities from developing countries should make a constant effort in keeping up with the development of new technologies and provide the proper **legislative framework** needed for their smooth implementation, at the same time not hampering the innovation processes.
- All countries, especially developing ones, should encourage the development of their own **national cybersecurity talents** by designing high-level university programmes and building strong links between the universities and the industry sector. Furthermore, governments should foster the development of **national cybersecurity solutions and brands** and rely on them as much as possible to reduce dependency on foreign players.
- Public authorities should engage in providing **continuous and lifelong cyber-education** and improving **cyber-hygiene** standards for a wide range of sectors. The content and the method must be adapted to the audience.
- Governments should take the lead in developing practical solutions and most importantly **standards of care for sectors (sets of recommendations and good practices)** that must be especially cyber protected but at the same time do not have the financial or human resources to do so in a proper way. Standards of care for hospitals or local government units would be a much needed first step.
- Actors involved in capacity building programmes should work towards **coordinating the efforts on the ground** in order to create synergies and achieve effective and sustainable results.
- Cybersecurity efforts and dialogues between governments must include representatives from as many departments as possible. A **whole-of-government approach** produces a richer environment and allows for the development of unified and coordinated actions.
- Developing countries should **draw lessons and inspiration** from the experiences and mistakes of other, more digitally advanced countries. In the field of cybersecurity they might tailor the tools and solutions already available to their own context and situation. In cybersecurity **there is no 'one-fits-all' solution** and all measures should be carefully studied.
- The security of certain critical **government communications tools** often relies on the services of regular private telecom operators and therefore on their choice of equipment vendors. A dialogue should be rapidly established between governments and operators to address this critical issue.
- The massive involvement of one single player – China – in building the digital infrastructure in developing countries, especially on the African continent, should not stop Western countries from engaging in the same region. It is vital for developing countries to be able to **benefit from alternative options** to the often restrictive systems – restricting not only malicious activity but also online content – proposed by China.

> Cybersecurity is an important technical issue but as long as ministers or leaders of government think of it as just a technical issue, that's not going to really get the traction it needs. It needs to be thought of as a key issue of national security, key issue of economic policy and ultimately a key issue of foreign policy and really national policy.
>
> **CHRISTOPHER PAINTER**
> **Commissioner, Global Commission on the Stability of Cyberspace;**
> **Former Coordinator for Cyber Issues, U.S. State Department**

We are about to define our critical infrastructure and the cooperation with the private sector is especially crucial here, because most of the critical infrastructure is actually in the private sector and we need to set jointly the rules, the legislation and the cyber-resilience towards this.

DAMJAN MANCHEVSKI
Minister of Information Society and Administration, Republic of North Macedonia

Cyber-risk and cyberthreats are global and the moment they become successful and have material impact whether on us directly or at the dependency that we have, we all suffer, and we all lose. That's why I think it's important to understand that we're all in this together, it's absolutely fundamental to invest an effort (...) in capacity-building wherever it's possible and it's absolutely important to establish trust-based relationships.

MICHAEL BEM
Executive Director, CISO, UBS

SMART GRID CYBERSECURITY – ITS STATUS AND NEXT STEPS AT THE EU LEVEL

- In the future grids, the smart IT will be included in every component – communicating to each other, balancing each other and connected to the grid outside. The potential attack surface will significantly increase. Thus, the **overview of different cybersecurity risks** must become a priority.
- The energy sector is unique in cybersecurity implementation:
  - It has **real-time requirements** and cannot be addressed by standard cybersecurity solutions (like authentication or encryption which both entail some time delay).
  - It might cause **cascading effects** and can trigger blackouts in other sectors and countries.
  - There is a **technology mix** in the grids that creates risks from legacy components designed when cybersecurity was not a priority, and from new IoT devices not made with the *security by design* approach. The split is getting bigger and is creating additional risks.

The European Green Deal will be the overarching goal of the new term of the European Commission and will also have some implications for power grids. It will tackle such **digital challenges** as: renewable energy, decentralised power generation, decentralised storage and prosumerism. The digitalisation of all these processes and the increasing number of smart devices connected to the grid would be an important part of attaining climate neutrality and in the overall **future energy landscape.**

REAL-TIME REQUIREMENTS	• Use international standards • Apply complementary physical measures • Classify/manage your assets • Consider privately owned communication networks, or consider specific measures • Split system into logical zones • Choose secure communication and authentication
CASCADING EFFECTS	• Evaluate interdependencies • Figure out the impact of the failure of an asset • Ensure communication framework for early warnings and to cooperate in crisis • Ensure level of security for new devices • Consider cyber-physical spill overs • Establish design criteria for a resilient grid
TECHNOLOGY MIX	• Follow a cybersecurity-oriented approach when connecting devices • Establish monitoring and analysis capabilities • Conduct specific cybersecurity risk analysis for legacy installations • Collaborate with technology providers • Update hardware and software

The details of the above mentioned recommendations can be found in the European Commission document C(2019)2400, available here:
https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf. More on the policy context, energy specificities, international standards, or research services can be found in the European Commission Staff Working Document C(2019) 1240 available here:
https://ec.europa.eu/energy/sites/ener/files/swd2019_1240_final.pdf

- **The continued effort** on the follow up on the recommendations with Member States should be pursued. The specifics of the energy sector should also be included into **national risks assessment and national cybersecurity plans**.
- The Cybersecurity Act prepared the ground for the **certification frameworks** which might be considered by the energy sector. As the answer regarding the specific impact of certification on this sector is not yet known, the stakeholder community and industry associations should work together and look on how beneficial certification of processes and products might be in creating more stable, safer and cyber-resilient energy sector.

> The future grid will not be able to be completely different because the infrastructure is already laid out. We'll have to add to the infrastructure the information technology. (...) At this point not only the connected information technology will be omnipresent but also the cybersecurity risks, because we are increasing the area that can be attacked.

STEPHAN LECHNER
Director, Euratom Safeguards, DG ENER, European Commission

SECURING DIGITAL DNA BY BUILDING CYBER PEACE AND STABILITY

- It is in the common interest of like-minded countries and the international community to ensure the cyber peace and stability; all **multilateral approaches** that we are currently witnessing are the proof of that. Private companies and civil society, which are key players in the cybersecurity ecosystem, are increasingly contributing to the debate underlining the need to reach the international consensus.
- **Bottom-up initiatives** should be embraced and included in the process of creating norms of responsible behaviour in cyberspace. **The voice of civil society and industry** should also be taken into account while creating more formal and binding outcomes.
- **Two parallel UN processes** (Open Ended Working Group (OEWG) and Group of Governmental Experts (GGE)) should be perceived as complementary rather than competing. They can support each other through the constant dialogues between their Chairs. In this way, both processes can be successful.

OEWG

Because of the possibility of wider participation, the OEWG could serve as a **platform of capacity building** that needs to occur to allow UN countries to fully implement the norms of responsible behaviour in cyberspace. What is more, the **OEWG supports the multi-stakeholder approach** which in the interconnected cyberspace seems crucial. Civil society and industry can inspire and complement discussions with their own contributions.

GGE

A more **exclusive approach** might facilitate reaching a consensus about the relevance of particular norms of responsible behaviour in cyberspace.

- There should be a common understanding and actual **implementation of norms of responsible behaviour** that should guide the activities of states in cyberspace.
- In the process of developing norms of responsible behaviour in cyberspace, the questions of **capacity building and digital maturity** of countries arise. Countries are at different levels of development, face various challenges and have different levels of understanding of the cyber issues (struggling sometimes with very basic administrative and institutional problems). Therefore, the discussion on awareness raising, education and creation of institutional framework is still valid and should be carried on. If like-minded countries want to promote the model of cyberspace which is open, free, secure and accessible, support and assistance in building local as well as national capacities should be provided.
- Advancing stability in cyberspace requires higher clarity with regard to incident **attribution**. The EU Cyber Diplomacy Toolbox is a good step in this direction as it lists escalatory measures that could be taken once misbehaviour or cyberattack is detected. The reaction to cyberattack should reflect different levels of certainty and more robust measures should be taken only in cases of very high degree of certainty. Countermeasures must stay within the framework of international law and keep the moral high ground. Also, the industry and civil society can contribute to the discussion on accountability and attribution while at the same time recognising that as a government's duty.

If like-minded countries want to really promote this model of cyberspace – open, free, secure, and accessible – we must also provide some support and assistance in building local and national capacity, because otherwise there might be a kind of alternative model that will be available for many countries that are struggling with very basic administrative or institutional and technical capabilities.

MAREK SZCZYGIEŁ
International Cybersecurity Policy Coordinator, Polish Ministry of Foreign Affairs

Resilience is one thing but if it comes to taking countermeasures, I think it is important that we ourselves look to it that our countermeasures stay within the framework of international law so that we always keep the moral high ground.

RÜDIGER BOHN
Deputy Federal Government Commissioner for Disarmament, Arms Control and Cyber Policy, German Foreign Ministry

One thing that we have learned over the years is that it is very hard to deal with the cyberincident when it has already occurred. It is much better not to let the genie out of the bottle than put it back later. So that's why we have paid so much attention to how to prevent the cyberincidents from happening (...) because it's better to implement and use the trusted technology and the trusted systems than to deal with all these issues later.

RAUL RIKK
National Cyber Security Policy Director, Estonian Ministry of Economic Affairs and Communication

DEFENCE STREAM*

SECURITY AMONG THE ALLIANCE – JOINT EFFORTS IN ENHANCING DIGITAL CAPABILITIES

- **Absolute deterrence** is unconceivable and impossible to achieve in cyberspace, but like-minded allies must come together to contain and mitigate the risks related to cyber in the military field. In order to achieve a reasonable level of global deterrence, **cyberspace should be treated together with other domains of military operation.**
- Time is of the essence. Putting the emphasis on crucial topics raised by allied countries or organisations, such as developing cyberdefence capabilities, increasing situational awareness, cooperating with partners and industry, as well as envisioning possible operational consequences of certain choices in the digital domain is important for NATO. From a convergence of concerns, we should achieve a **convergence of efforts**, creating synergies and ensuring a sustained pace of actions to protect the defence sector and place the Alliance ahead in the race against time.
- The **cooperation between NATO and the defence industry** is essential, mutually beneficial and should therefore be further deepened. On the one hand, it allows companies to learn more about the functioning of the Alliance, most importantly its actual needs, but also to group up with companies from other countries to learn new ways of thinking or exchange views on technical, management or financial issues. On the other hand, it allows NATO to be equipped with the latest technologies.
- Building **common structures** within NATO is a way to move forward against cyberthreats, as it will ensure joint surveillance and protection. **The Cyber Operations Centre (CyOC)**, established in 2018, should evolve into ultimately becoming the NATO Cyber Command.
- Having a **whole-of-organisation approach** in NATO is the first step in order to be better able to face up to the challenges the Alliance is confronted with.

KEY ASPECTS TO SECURE THE SUPPLY CHAIN IN THE DEFENCE INDUSTRY:

✓ Limiting the dependence on foreign suppliers

✓ Buying only proven products and services

✓ Working with reliable intermediaries

*THE DEFENCE STREAM WAS CO-ORGANISED BY CYBERSEC MAIN INSTITUTIONAL PARTNER – NATO COUNTER INTELLIGENCE CENTRE OF EXCELLENCE.

- It is crucial to ensure the **security of the whole supply chain** in the defence industry. Dependencies on foreign manufacturers are a major concern and it is a matter of policies and strategy to tackle this threat. Three simple recommendations to keep in mind and implement:

1. use products of national origin or coming from allied countries;
2. buy proven products directly from reputable manufacturers from allied countries;
3. buy through reliable intermediaries to limit the possibility of interference between the buyer and the seller.

> Digital capability is the capability to protect our assets; it is the capability to hunt for threats in the system, in the cyberspace. But this is also the capability to offensively respond to adversaries' hostile action and the capability to engage our adversaries according to our operational needs.
>
> **ROBERT BALA**
> **Chairman, Steering Committee, NATO Counter Intelligence Centre of Excellence;**
> **Former Director, NATO Counter Intelligence Centre of Excellence**

> You have to be clear that in the event of a major cyberattack, a cyber response is not the only conceivable one. According to NATO doctrine you may even respond to a large-scale cyberattack with the full spectrum of NATO capability.
>
> **ANTONIO MISSIROLI**
> **Assistant Secretary General for Emerging Security Challenges, NATO**

> I personally strongly believe in building structures, that's why the cyber.mil.pl program is based on four pillars and the first of them is building structures within the Ministry of National Defence in Poland and within the Polish armed forces.
>
> **TOMASZ ZDZIKOT**
> **Secretary of State, Polish Ministry of National Defence**

BEYOND CONVENTIONAL WARFARE – HEDGING AGAINST HYBRID THREATS

- The attention of national cyberdefence authorities has to be focused on how to define, how to monitor and how to shorten the time needed to detect a cyberattack. This should be based on **state-of-the-art technology** and teams of **skilled personnel** in various areas.
- Governments and industry have to build a **common picture for cyberspace**, create roles, define responsibilities and set norms for operating in this new realm, especially:
  - Governments need to build **customary international law** defining criteria of acceptable and non-acceptable behaviour. Only this will help prevent the use of cyber-weapons against civilians and interference in domestic affairs.
  - **Accountability** is a key point in the fight against fake news and hybrid threats. Governments have to clearly define mechanisms to hold people accountable for hostile cyber-campaigns and to come up with a process to sanction the authors.
- Governments and industry have to work together to provide the tools to citizens and users of social media that will enable them to make their own evaluation of the content they see online. **Digitally proficient citizens** are the first line of defence against disinformation campaigns.

A RELIABLE PARTNER IN CYBERDEFENCE IS A PARTNER THAT:

✓ is able to build and maintain the resilience of its network infrastructure

✓ takes part in the collective defence effort

> What governments need to do is to say what's an act of war, what's acceptable behaviour or not and how do we hold people accountable.
>
> **KEITH ALEXANDER**
> **Former Director, NSA; Co-CEO, IronNet Cybersecurity**

> Armies of different countries do their best to show the deterrence so there is a lot of military parades (...). However, thinking about the cyberspace we don't have cyber parades. I believe the best we can do is to invest in intelligence and building the intelligence capabilities – intelligence, surveillance, reconnaissance – to be aware what our adversary could use against us.
>
> **KAROL MOLENDA**
> **Director, National Cyber Security Centre of Poland**

REVEALING THE POWER OF OSINT IN THE DIGITAL ENVIRONMENT

- The **use of digital tools by liberal democracies** has to be careful, targeted, ethical and well governed.
- OSINT should constitute **the core of the analysis** and provide situational awareness landscape due to more and more information available.
- Advanced technological tools are good means to help intelligence work, however, there should always be **a team of human beings** monitoring the process and able to understand and detect when the machines are veering off.

> At the end of the day, a good analysis should blend the 90% that comes from scanning what is openly and legally available with the other 5-10% that comes through specific sources, be they human intelligence or be they technical sensors from satellites to drones or other kinds of sensors.
>
> **SORIN DUCARU**
> **Director, European Union Satellite Centre; Former Assistant Secretary General for Emerging Security Challenges, NATO**

> Disinformation has replaced hack and leak as the principal worry of democracies.
>
> **CIARAN MARTIN**
> **CEO, UK National Cyber Security Centre**

> I think that one of the things you can do is first of all not to be intimidated by the deluge of data but swimming along the already most relevant ones and this is for the moment less of a science and more of an art.
>
> **ALESSANDRO POLITI**
> **Director, NATO Defense College Foundation**

TAPPING THE POTENTIAL OF NATO CENTRES OF EXCELLENCE

- **The strength and excellence of CoEs** lies in their experts. The 26 CoEs gather more than 900 experts, which is more than NATO Allied Command Structure and Allied Command Transformation together.
- **The uniqueness of CoEs** lies in their mission to support NATO and member countries as well as their capacity to work. Cooperation and willingness of member countries to pool their efforts together is a key to the success of CoEs and ultimately of the whole Alliance.
- **Cooperation, preparation** and **training** are the key aspects for the future of the fight against cyberthreats. These should take place not only among nations but also between different NATO CoEs and the EU.
- Existing successful **crises mechanisms** in different member countries should integrate cyber and hybrid threats in their missions and acquire tools to respond to cyber-crises in addition to more traditional ones.

NATO CI COE CASE:

NATO official policy clearly stipulates that counterintelligence is purely a national responsibility. However, eleven nations decided to join forces to act together within the NATO CICOE, to share information and experience, and to prepare their personnel to be able to cooperate during operations.

> We have to get out there with our narrative, we cannot always wait for the perfect 100% solution (...). If we do that in cyberspace, we get out ahead of malicious actors, we will be able to get in front of the terrorists and their demands and in front of their narrative.
>
> **DANIEL W. STONE**
> **Acting Director, NATO Centre of Excellence for the Defence against Terrorism**

> Where is our future? I think our future is quite clear, we need to foster cooperation, preparation and training. Cooperation not only among the nations but maybe – and I'm deeply convinced about that – among our NATO Centres of Excellence too.
>
> **MARTIN ACHIMOVIČ**
> **Director, NATO Counter Intelligence Centre of Excellence**

> Only jointly can we succeed. Sharing information, developing common practice, tactics, techniques and procedures – that's the only way to go.
>
> **ROMUALDAS PETKEVICIUS**
> **Director, NATO Energy Security Center of Excellence**

BUSINESS STREAM

INDUSTRY AND DIGITAL SPIES: A BATTLE ROYAL

Like all other aspects of modern life, espionage has been digitally transformed. In the present day, digital spying is rendered complex by a combination of three intertwined factors:

(1) cybercrime

(2) competition and the race for supremacy over the emerging technologies

(3) the ever-expanding attack surface

- With digital take-up and transformation of companies and governments comes a higher level of risk, requiring a new perspective on security. Fostering collaboration and breaking the silos between the work of the IT, security and risk-management teams is needed to get a **holistic view of the threats** and business-driven security approach that will in turn allow for the creation of an effective roadmap and digital management strategy.
- When it comes to the protection of the organisations, **the technology for the proper detection** of threats is very often available. However, the mindset of a lot of organisations and countries must change in order to increase the willingness **to share the information and collaborate.** If we are sharing information on the threat intelligence, then other organisations can prepare themselves and can start taking precautions.
- The knowledge of prosecutors and law enforcement officers on how to obtain evidence for criminal proceedings related to cyberespionage is insufficient and should be further strengthened. National justice institutions are still struggling with very basic issues related to the digitisation processes, not to mention more advanced techniques. Therefore, **raising awareness and knowledge** should remain a priority.
- **Insider threat** also remains a big challenge. Training procedures and initiatives are needed to educate people to detect behaviour anomalies that would indicate an insider threat in the organisation.
- In addition to frequently mentioned cybercrime response patterns, particularly in the niche of cyberespionage – namely **deter, defend and defeat** – two more should be added:
    - **develop** – training of employees, development of new techniques and tools that can detect anomalies (especially with regards to the insider threat), development of relationships between businesses, between the law enforcement officers and security professionals, development of procedures and protocols;
    - **disseminate** – sharing experiences of breaches that have happened, sharing information about new threats that have been detected.

5 Ds IN CYBERSECURITY:

✓ **D**ETER

✓ **D**EFEND

✓ **D**EFEAT

✓ **D**EVELOP

✓ **D**ISSEMINATE

Cyberattacks occur every 39 seconds. 44 personal information files are lost every second. In the US, the unfilled cyber jobs are up 75% on the last 5 years, with over 3.5 million jobs in cybersecurity remaining unfilled as a result of a lack of skilled professionals. More than 77% of organisations do not have a cyber-response plan. It takes 6 months in some cases to detect a data breach and interestingly enough for those who are interested in the opportunities of cryptocurrencies, 46% of all bitcoin transactions worldwide are linked to cybercrime.

RAFAL ROHOZINSKI
CEO, SecDev Group

There has to be training, there has to be vigilance and there has to be a way to educate people that are on the inside to detect and look for the types of anomalies and behaviour that would indicate an insider threat in your organisation.

MICHAEL MALSCH
Legal Attaché, Federal Bureau of Investigation (FBI)

You have to expect that you will be hacked or breached at some point. However, how you will respond to that and be able to mitigate that from a business perspective will give the company confidence that they can handle the breach when it does occur and that's the fundamental change in mindset that is needed.

NIGEL NG
President International Sales (APJ and EMEA), RSA

SECURE & RESILIENT INDUSTRIAL IOT (IIOT) – MISSION ACHIEVABLE

- The first step should consist of putting **basic design and security practices** in the operational technology network environment.
- Several approaches can be adopted to mitigate the risk of untrusted foreign equipment flooding the market:
    - **Multi-stakeholder dialogue:** gathering regulators, manufacturers, standardisation bodies and academia to identify areas of threats and to jointly address them.
    - **Diversification** of equipment providers.
    - Development of standards to define **"trusted vendors".**
    - Further development of **frameworks**: security standards, certification mechanisms, toolsets and regimes.
- Understanding the vulnerabilities and securing the **supply chain** all along is fundamental. **Responsibility** must not fall on the final component only but be distributed among all parts.
- Running legacy systems with new technologies is not a problem in itself as long as the right **architecture** and barriers both in terms of components and process are placed.
- The **edge computing paradigm** is a strong tool to help leverage the security of a legacy system. Edge devices put close to low computational power devices will be acting as a liaison between these legacy systems and current applications, thus helping to build a more connected architecture and to increase its robustness.

> I think what we're asking people to do is to conceive the inconceivable. Everything is vulnerable, and you can't protect everything. There simply aren't enough resources, there's no way to protect everything to the same level. And you don't know where the next attack is coming from, or why.
>
> **BONNIE BUTLIN**
> **Co-founder & Executive director, Security Partners' Forum**

> I think a very common theme which is coming up in security these days is that nearly everything we are running is based on a complex supply chain. And unfortunately, I believe, a lot of companies don't even really understand how complex their own supply chains are. So, securing the supply chain is absolutely fundamental.
>
> **STEVE PURSER**
> **Head of Core Operations, ENISA**

> I think that one of the things that scares me most about the conversation that people have been having about securing the Internet of Things is there's a lot of different interpretations of what infrastructure is, and I think that there's not enough understanding of the geopolitical dimensions of this.
>
> **PATRICK TUCKER**
> **Technology Editor, Defense One**

SECURING THE DIGITAL TRANSFORMATION OF FINANCIAL SERVICES

- One security incident will be enough to change the perception of a financial institution and this is why financial sector must be especially **mature** when it comes to cybersecurity preparedness.
- At the international level, while working on policies and regulations related to cyber-risk management, the **convergence on the requirements** is needed. Facing diverging national frameworks makes it difficult for institutions to comply. Along with the convergence on requirements, **convergence on taxonomy and definitions** should be emphasised as well.
- With regard to the FinTech products, which aim at simplifying the services for end users, **the security by design** approach is of the most relevance.
- While estimating the cyber-risk, it is important to focus not only on a specific product, tool or institution. Instead, the analysis of the **end-to-end financial process** and the whole supply chain along with third-party suppliers is essential.
- Regulations will always lag behind technological developments. A regulation should be designed in a way that is **technology neutral.** It should not be too prescriptive, but rather principle-based and risk-based in order to be able to properly apply to new technology developments.

Banks should first of all continue to invest or invest more in information sharing and collaboration and cybersecurity. I couldn't emphasise more how important it is and it will help them become better and more competitive eventually because they will be more secure.

RAHAV SHALOM-REVIVO
Fintech and Cyber Innovations Manager, Israel Ministry of Finance

I think that banks should be open to cooperation with innovators, whether it's internally or with external suppliers (...). It is very important because I think it brings benefits both ways.

SÉBASTIEN DE BROUWER
Chief Policy Officer, European Banking Federation

The policies and regulations are very important of course to manage cyber risk in the financial institutions but it is also very important that the banking supervision is active in this area and makes sure it does not block the possibility of doing business.

ARTUR RUDZIŃSKI
Director of IT Risk and Continuity, Alior Bank

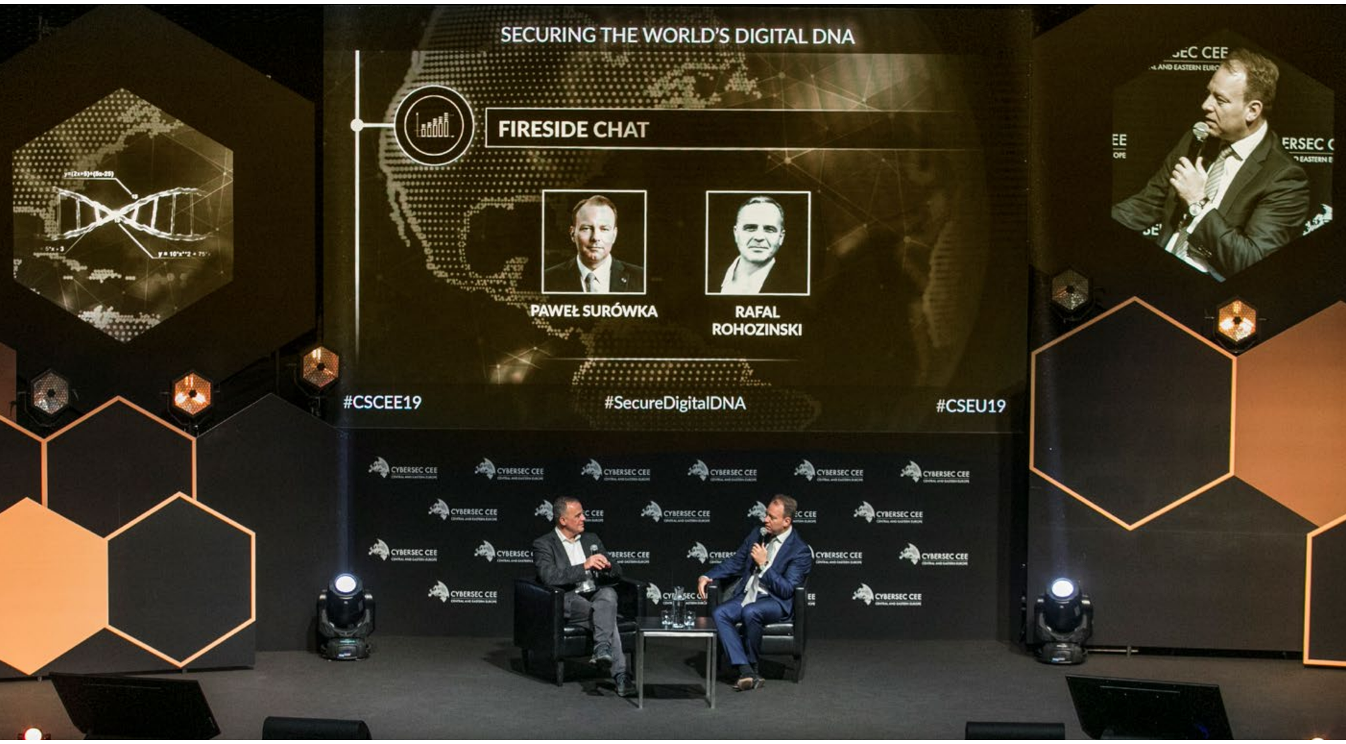
CYBERTHREATS AS A FACTOR CHANGING THE INSURANCE LANDSCAPE

- Insurance companies could take advantage of the changing threat landscape. They could serve as **"standard setters" for good cybersecurity practices for companies** which they provide their services to.
- Insurance companies need to take a **proactive approach** in teaming up with their clients in order to effectively mitigate the risk, including the aggregated risk. They need to become partners of the corporates, going far beyond being only a transfer of risk. This process will require **bespoke dialogue with the corporations.**
- The **awareness among companies** regarding understanding and assessing how data integrity and the maintenance of clients' data is fundamental to their reputation and to the business continuity should be constantly built.

An example of what large European insurers practice to meet the challenges of cyberthreats is acquiring cybersecurity companies. Then, clients for which they provide insurance are required to use these companies' cybersecurity products and services. This allows the insurer to continuously monitor the security status and personalised metrics of the threat level.

> Don't underestimate the threat, don't underestimate how interesting you are to some potential parties that don't wish you well, and don't try to solve everything yourself. Try to team up, try to work with companies that already have solutions and make sure to invest the right amount of money.

PAWEŁ SURÓWKA
President of the Management Board, PZU SA



CREATING AN EFFECTIVE DEFENSIBLE SYSTEM

- Nowadays, the approach adopted by most actors in defending their systems is flawed and leaves them responding to attacks rather than defending their system. A different approach is needed to create **an effective defensible system**. It is based on:
    - A **platform reflecting a real-time picture of the situation** in the systems. It should be based on behavioural analytics and designed to be shared among like-minded actors in order to allow them to work collectively for a common cyberdefence.
    - A strong anchor of the platform in **machine learning and artificial intelligence** in order for it to be able to adapt to AI-powered attacks or intrusions.

> The amount of unique information that's being created is doubling every year. It means we'll create more information this year than in the last 5,000 years combined. That is huge. (...) The legacy approach that we have for defending our networks will not keep up with the speed and change of the amount of data that's being created, the amount of equipment that we have and the amount of devices. We are not going to keep up with it.
>
> **KEITH ALEXANDER**
> **Former Director, NSA; Co-CEO, IronNet Cybersecurity**

FUTURE STREAM

PRINCIPLES OF RESILIENCE FOR OUR CITIES IN THE DIGITAL ERA:

FIVE STRATEGIES THAT NEED TO BE A BASELINE FOR THE SECURITY OF CITIES' DIGITAL DEVELOPMENT

1. The concept of "smart city" should go hand in hand with that of "**digitally secure city**". Therefore, cities need to adopt a **digital safety mindset** that includes:
   a. **plans, protocols and personnel** in place as well as **intelligence and data-driven tools** to detect and prevent strikes before they start;
   b. a thorough **understanding of traffic flows** to anticipate and neutralise anomalies;
   c. an effort to **reduce the attack surface** and increase network segmentation in order to ensure that a single point of entry doesn't collapse the entire city system.

DIGITALLY SECURE CITIES
must have in place:

✓ plans, protocols and personnel

✓ intelligence and data-driven tools

✓ good understanding of traffic flows

2. Mayors and city executives around the world have to take on the **leadership in digital safety and security** and not wait or rely solely on nation-states to ensure their cybersecurity or on businesses to save them. They urgently have to engage in a conversation about minimum global and national standards to improve their digital security and become advocates of these rules on a global level.
3. The adoption of a comprehensive **approach** to digital security aligned with smart city strategies should become a priority. The development of **municipal CERTs** could be instrumental in this regard.
4. City authorities need to recruit the **right workforce – including coders, engineers, white hat hackers** – to deal with upcoming digital challenges and provide routine training and education to city staff as well as providers and subcontractors.
5. Building **innovation ecosystems** will undoubtedly help advance the prevention of cyberattacks and disruption of cybercrime. This can take several forms such as establishing open data portals, organising hacking competitions or setting up bug bounties. By incubating solutions both locally and globally, cities will boost their own capacities and at the same time reduce their reliance on external vendors.

> Cities need to adopt a digital safety mindset. A smart city is a digitally secure city. City leaders need to recognise that the strategies that protected cities in past centuries may not be so appropriate for the current one. Gates, guards and guns are powerless against bits and bytes that traverse the world at light speed.
>
> **ROBERT MUGGAH**
> **Co-founder, Igarapé Institute;**
> **Executive Director, SecDev Group**

GEOPOLITICS OF CYBERSECURITY – FORTHCOMING IMPLICATIONS OF THE DIGITAL COLD WAR

- The revolution that has started a generation ago was mostly about empowering the individual and the Internet was seen as a mechanism to spread freedom and democracy around the world. In recent years, however, **we are observing a counter-narrative**. The revolution that is happening right now might be bolstering systems that use data in order to control people's behaviour. This shift should be taken into account by like-minded countries in order not to let foreign powers influence their systems.

The new cybersecurity risks and risks posed by emerging technologies like **AI, quantum computing, big data, 5G networks and billions of connected devices** are changing the nature of both geopolitical power and nation-states' relations with each other in this new environment.

- **The deployment of 5G networks** is critically important from the geopolitical point of view. Whoever gains control over that technology will become a geopolitical power. That is one reason why the vendors' diversity is strongly recommended.
- The question of **digital autonomy** is very important to address. The tools countries are using should be adjusted to the local needs and countries should always have the ability to take their own decisions. At the same time, in order to boost innovation and growth, the cooperation among countries needs to be fostered.

- We need to build **technological foundations that restore a power balance** between individuals, states and large tech companies. Individuals should control their own data and decide whether third parties can access that data in line with defined principles and a trust-based relationship.
- **Investments in research and development and in education** are crucial for further advances and for maintaining competitive advantage. Western countries should create new policies of promoting the national industrialisation strategies in order to keep pace with the rest of the world.

SECURING THE WORLD'S DIGITAL DNA
Panel Discussion:
GEOPOLITICS OF CYBERSECURITY
– FORTHCOMING IMPLICATIONS OF THE DIGITAL COLD WAR
speakers:
BRIG GEN (RET) ROBERT SPALDING
JACEK BARTOSIAK
JAYSHREE PANDYA
NIKODEM BOŃCZA TOMASZEWSKI
moderator:
KEVIN ALLISON
#CSCEE19
#SecureDigitalDNA
#CSEU19
CYBERSEC CEE

Right now, we are living in the digital age and it is much harder to answer what it means to be sovereign in cyberspace. And I think that basically, for the nation like Poland and other nations in Europe and all the governments in the free world, it's a notion of being able to tell our citizens that you are free in the internet or in the cyberspace, that we as a state assure you freedom and assure you security in the cyberspace.

NIKODEM BOŃCZA TOMASZEWSKI
CEO, Exatel

I think states need to have an infrastructure that allows for digital citizenship within their own borders, in other words, identity management access control encryption or applied across in system in a way that ensures that every citizen owns their data.

ROBERT SPALDING
Senior Fellow, Hudson Institute; Former Senior Director for Strategy in President Trump Administration

MEETING WITH AUTHOR OF THE BOOK: *STEALTH WAR: HOW CHINA TOOK OVER WHILE AMERICA'S ELITE SLEPT*

- In the 21st century the power of states results mainly in their **financial and economical capabilities**. Gaining the influence does not require military resources anymore. This significant shift should be taken into account by both business and government strategies.
- One of the major challenges to 5G technology development is that it is not only a network that aims to amplify 4G but also a platform for the services, business models and the whole IoT world. Only considering 5G deployment as a **national strategic problem** can give an actual leverage to governments.
- Significant **social media presence** and **propaganda operations** from some major actors of the world's economy should not be underestimated and should be treated as a serious threat to the democratic values. For example, as many as half a million people in China might be involved (professionally, also known as "50 Cent Party") in the direct creation of propaganda both for domestic consumption within China and also for foreign consumption abroad.
- The development of the digital sphere entailed the **structural challenges** in our economies regarding appropriate responses from both governments and companies to the influence operations. The capability to **aggregate data** (now in the hands of totalitarian regimes and large tech companies) is a powerful competitive advantage tool and is equivalent to aggregating power.
- There is a necessity to foster the ability of the individuals **to own their data** and understand how their data is used. Not having an understanding of who is using personal data and for what purposes creates challenges to liberties.
- **Democratic principles** and **free-trade principles** go together. The creation of an open and inclusive world might be possible only with the combination of these two principles. For democracy to persist, it requires protection of all elements – finance, trade, investment, migration, media, politics, academia, and the internet among them.
- **Investments** in people, STEM education, research and development, infrastructure, manufacturing and industries is a necessary condition for countries to grow.

COUNTERING AI-POWERED THREATS

- Promoting an **active dialogue** between all parties – decision-makers, industry and business representatives and researchers – is key in maintaining a necessary level of understanding of AI's impact on national and international security and on the way our societies function.
- Any regulation on AI should be **technologically neutral** and **principle-based** and adopt a **sectoral** and **risk-based approach**.
- Clear delineations have to be drawn between fields where people are **in the loop or out of the loop**. At times of increasing dependence on critical information and infrastructure, it should be clear to what extent humans can allow machines to take decisions instead of them.

KEY ASPECTS OF REGULATIONS ON ARTIFICIAL INTELLIGENCE:

✓ TECHNOLOGY NEUTRAL

✓ PRINCIPLE-BASED

✓ SECTORAL

✓ RISK-BASED

The risk of overregulation should be avoided at all costs.

- Any attempt to develop a regulation on AI should be preceded by a thorough research about the actual state of play of the technology. Only a deep analysis will enable to draw up a regulation that protects the fundamental human rights and values and does not jeopardise progress and businesses which form the pillars of the European economy. The **risk of overregulation** should be avoided at all costs.
- When thinking about **AI insecurity**, it is necessary to not only consider the technical aspects of AI but also the non-technical and contextual aspects of the systems.

There is no bad or good technology. The technology and its usefulness depend on in whose hands it is. I think there is not enough finances and resources invested into the study of ethics of AI. At times of crisis, at times of dependence on critical information and infrastructure, to what extent can we allow machines to do decisions instead of us?

MERLE MAIGRE
Executive Vice President for Government Relations, CybExer Technologies

The more advanced we become, the more advanced are the tools we get, and we just have to keep up with this technology. Cybersecurity is not a kind of an answer to any statement, it is a process.

LUDMILA GEORGIEVA
Public Policy and Government Relations Manager, Google

When we speak about AI insecurity, we definitely cannot speak only about technical aspects. We need to speak about non-technical and contextual aspects of the systems that are actually being developed. We need to speak about ethics and if we speak about ethics we need to speak about our values. (...) I am very happy that here in Europe we can see a lot of effort to work on a set of values and ethical guidelines, especially ethical guidelines for AI. I think this is a great achievement, this is a good basis for further development of really ethical AI, and I hope we can export it from Europe.

PETR OČKO
Deputy Minister of Industry and Trade, Government of the Czech Republic

CYBERSEC
Women

The need to have inclusive and diverse teams to tackle current cybersecurity threats has significantly increased in recent years. The global demand for knowledgeable professionals is currently tremendously high. Beside the need for human capital in cybersecurity, it is important to make further research on the effects of not having a gender-balanced sector.

This is why the Kosciuszko Institute, originator and organiser of CYBERSEC, in admiration for all the great women who participated in the previous editions of CYBERSEC, has decided to launch a new format which accompanied the 5th European Cybersecurity Forum – CYBERSEC 2019.

CYBERSEC WOMEN, organised in partnership with the European Cyber Security Organisation's Women4Cyber initiative, aims to reduce the skills gap by increasing women's participation in the cyber field and also highlight the important role that women play when it comes to creating a balanced and effective cyber ecosystem.

How big is the current female scarcity in cybersecurity?

The low percentage of women working in ICT is further diminished by the "security" aspect of the cybersecurity field.[1] The Cybersecurity Workforce Study (2019) indicates that women working in cybersecurity currently account for about one third (30%) of the overall workforce.[2] This is a higher rate than in 2018 when the same study indicated women were 24% of the total workforce.

Despite still being a matter of debate, the proportion of women working in the cybersecurity field is slowly moving towards a balanced figure. The trend is on track, but the industry needs to continue pushing for more women in cybersecurity.

What are the causes of women's underrepresentation in cybersecurity and ICT? What are the obstacles for women to start their educational and professional career in cybersecurity and ICT?

[1] International, Journal of Gender, Science and Technology, Gender Inequalities in Cybersecurity, vol. 9, No. 1

[2] *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens*, (ISC)^2 CYBERSECURITY WORKFORCE STUDY, 2018, https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx

One of the causes of women's underrepresentation in cybersecurity and ICT has been identified as the limited knowledge of cybersecurity matters at an early age when young people must decide on their career path. The low level of awareness about the cybersecurity topic in schools negatively affects their interest in the field, making them more prone to choose other subjects of study outside of technology and security.

Until recently, it was impossible to enter and work in cyber without a STEM background. There is a strong need to change our understanding of what is demanded in cybersecurity. This may lead to the inclusion of more women in the sector, and more globally, of people with different backgrounds.

In 2017, over half of all EU-28 graduates were women (57.6%) but almost twice as many men as women graduated from STEM courses, according to Eurostat.[3]

According to the Women in Cybersecurity Report, women cybersecurity professionals still face an uphill climb, especially in compensation, with 17% claiming to be earning USD 50,000–99,999 – 12 percentage points less than men (29%).[4] Additionally, the Global Information Security Workforce Study claims that 51% of women report on various forms of conscious and unconscious discrimination in the cybersecurity workforce.[5] In some cases, women have struggled to prove themselves by their knowledge on the field much more than men do, and/or have been the targets of destructive criticism in diverse conferences or in their work environment.

To sum up, the reasons for women's underrepresentation in cybersecurity are complex:

- low number of STEM female graduates;
- lack of awareness of the complexity and breadth of cybersecurity;
- lack of awareness on cybersecurity opportunities in schools;
- image – women aren't traditionally perceived as security or IT professionals;
- mindsets – during various contests, 85% of female startuppers are scared of being judged because of their gender;
- not enough role models and not enough people aware of the problem.

A holistic approach to working in cybersecurity is needed, otherwise, like every field, it will suffer from a lack of diversity.

What are the effects of women's underrepresentation in cybersecurity in ICT?

Inclusiveness is one of the key factors in security issues. Diversity in cybersecurity contributes to the efficacy of teams and sustainability of solutions, making it both important for national security and imperative for business.

This imbalance has prevented cybersecurity from reaching its full potential. A growing number of companies and organisations are recognising the importance of having an inclusive and diverse team in order to tackle current digital threats. But there is still a limited amount of universities offering careers in cybersecurity or with substantial participation of women pursuing technical or engineering academic careers.

[3] Eurostat, *Tertiary education statistics*, https://ec.europa.eu/eurostat/statistics-explained/index.php/Tertiary_education_statistics#Participation_of_men_and_women_in_tertiary_education

[4] *Women in Cybersecurity, Young, Educated and ready to take charge*, An (ISC)2 Cybersecurity Workforce Report, https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx

[5] Frost & Sullivan, *Global Information Security Workforce Study: Women in Cybersecurity*, 2017, pp. 13-17

According to different sources the gender disproportion has impacted and broadened imbalances in the labour market with an estimation of approximately 1 million unfilled IT security vacancies worldwide. Therefore, the sector has not fully benefited from innovation because it lacks teams' diversity. Diverse workforces perform better in decision-making, financial, and competitive matters. These are skills that are highly required in cybersecurity[6]. Furthermore, it has been found that certain emotional intelligence skills and insightfulness, characteristics typically apparent in women, are important in understanding the complexity of current cyber problems. The result of not having theses abilities or having a reduced amount of them aligned with existing skills can worsen the effectiveness of threat detection and prevent a more holistic approach to the field.

What are the positions that women are reaching in cybersecurity?

According to the 2018 (ISC)^2 Women in Cybersecurity Report, compared to men, higher percentages of women cybersecurity professionals are reaching positions such as chief technology officer (7% of women vs 2% of men), vice president of IT (9% vs 5%), IT director (18% vs 14%) and C-level/ executive (28% vs 19%). [7]

This situation is a result of different skill sets. Women bring to their professional work emotional intelligence, the ability to create engagements, and the ability to overcome contradictions. The more people are able to collaborate, the more they can show their leadership skills and the more they are likely to get a leading position in cyber.

PROPOSED RECOMMENDATIONS:

- ✓ **Commitment in ensuring diversity.** Institutions and companies should endorse an engagement on having employees from different social and educational backgrounds, gender, and nationality.
- ✓ **Dedicated programmes (with a special focus on girls and women).** Launching dedicated activities might at the same time help fill the employment gap and get a more balanced cyber ecosystem. Offering opportunities of lifelong learning and professional re-training for women coming from different backgrounds could bring great added value to the sector.
- ✓ **Focus on role modelling and mentoring.** Inspire other girls and help them improve.

> There are so many women working in cybersecurity but they don't know about each other. With connectivity, helped also by the conferences like this, they could communicate, talk about the profession, assist and help each other.
>
> **BONNIE BUTLIN**
> **Co-founder & Executive director, Security Partners' Forum**

[6] McKinsey&Company, *Diversity Matters*, https://aialosangeles.businesscatalyst.com/pdf/RESOURCES_POWERFUL.pdf

[7] Women in Cybersecurity, Young, Educated and ready to take charge, An (ISC)^2 Cybersecurity Workforce Report, https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx.

> Above all it is needed to underline the fact that cyber cannot be degenerated into a technical issue but cybersecurity automatically is a strategic question. (...) As a person with humanistic education I can say that having that kind of background helps support analytical thinking in cybersecurity.

MERLE MAIGRE
Executive Vice President for Government Relations,
CybExer Technologies

CSEU19 TWITTER WALL

#CSEU19 EARNED +168K IMPRESSIONS

Martin Roger
@mroger1000

#CYBERSEC Award 2019 was bestowed today on my President @KerstiKaljulaid and Estonia for the efforts in the field of cybersecurity at European Cybersecurity Forum CYBERSEC in Katowice by Minister of Digitalisation @ZagorskiMarek! Humbled to receive it on her behalf. #CSEU19

NCSC UK
@NCSC

Our CEO Ciaran Martin was proud to represent both the UK and the NCSC on the international stage at today's European Cybersecurity Forum in Poland #CSEU19 #CSCEE19 #SecureDigitalDNA

Br.Halopeau
@BrHa11

#CybersecMonth day 29: Securing the world's digital DNA declaration. Delighted to see emphasis on collective responsibility to act now & more human centric approach to #Cybersecurity - Read set of actions ow.ly/yu7V30pNnAw #CSCEE19 #SecureDigitalDNA @CYBERSECEU @ialbrycht

Global Cyber Alliance EMEA
@EMEA_GCA

Just landed in #Katowice for @CYBERSECEU (#CSEU19), the biggest #CyberSecurity conference in the #CEE region. This year's agenda is simply impressive: cybersecforum.eu/en/poland/agenda Looking forward to it! #CyberSecMonth

ECSO
@ecso_eu

Proud of having a chance to contribute to the @CYBERSECEU with our @Women4Cyber initiative. Thanks to @LiseFuhr, @ialbrycht, @anettmadinator & our Sec Gen Luigi Rebuffi for addressing the gender gap in #cybersecurity at #CSCEE19 #SecureDigitalDNA

de Brouwer S
@deBrouwerEBF

#Cybersecurity isn't just abt compliance w/t laws & regulations. It's abt guarding businesses from increasing danger of persistent threats. Enhanced infosharing & cooperation in PPP is the only way. BTW Shouldn't we also do the same in AML/CFT ? @EBFeu @CYBERSECEU #CSEU19

Defence MNE
@defence_mne

General Director Ivanović: #CYBERSEC has a crucial role in the development of national defence policy. As an ally, Montenegro is devoted to enhancing it is national cyber capacities. #CSCEE19 #SecureDigitalDNA @CYBERSECEU

Petr Očko
@PetrOcko

Happy to be in great company of excellent panelists at #AI powered cyber threats session @CYBERSECEU #CSCEE19 in #Katowice! #CZ appreciated as country with advanced #CyberSecurity ekosystém! AI regulation discussed: it's needed but must be based on deep assessment! @mpo_tweetuje

### ENISA
@enisa_eu

#ENISA Head of Core Operations, Steve Purser has been speaking at the #CSCEE19 EXPO on the Economy of Cybersecurity and on Secure and Resilient #IIoT. Thank you for the invite @CYBERSECEU

Patrick Donahue
@prdonahue

Had a great time talking about securing industrial IoT with my fellow panelists and representing @Cloudflare at @CYBERSECEU in Katowice, Poland. Thanks to @DefTechPat for being an excellent moderator #CSEU19 #CSCEE19 #IioT

Izabela Albrycht
@ialbrycht

The theme of this years @CYBERSECEU: Securing the World's digital DNA... well obviously it is not the only DNA which needs to be secured in the new digital world...

NCI Agency
@NCIAgency

Collaboration in #cybersecurity is critical. Defending @NATO's networks is a collective effort on the part of all 29 Allies. COL François Pons, Deputy Chief of our NATO Cyber Security Centre, discussed how our work supports those efforts at the #CSEU19 conference in #Poland.

Patrick Tucker
@DefTechPat

Antonio Missiroli of NATO on the future of cyber offensive capabilities for the alliance, Allies' offense tools will be part of the policy response discussion but, "they will remain national assets", not NATO's #CSEU19 #CSCEE19

Līga Raita Rozentāle
@LRozentale

Transparency, multistakeholder input and capacity building are key to implementing cyber norms. #CSEU19 #pariscall @MicrosoftEU

Rasto (Rastislav) Janota
@RastoJanota

Today second day of great CYBERSEC 2019 conference at #Katowice, now with gen. Keith Alexander, former chief of NSA, and also with Ciaran Martin, CEO of NCSC UK. #CSCEE19 #CSEU19 with @sk_cert

Jayshree Pandya Ph.D.
@jayshreepandya

Honored to have been invited to speak in a panel with @robert_spalding, @BartosiakJacek, @NikodemBT, @KevinAllison at CYBERSEC 2019 in Poland. It was a privilege to discuss many of the pressing geopolitical cybersecurity problems facing nations. #CSEU19 #SecureDigitalDNA #CSCEE19

PATRONS AND HONORARY PATRONS

Ministry
of Digital Affairs

NATIONAL SECURITY BUREAU
OF THE REPUBLIC
OF POLAND

Republic of Poland
Minister
of Foreign Affairs

Mariusz Błaszczak
Minister of National Defence

WP
WOJSKO POLSKIE

MINISTRY
OF INVESTMENT
AND ECONOMIC DEVELOPMENT

Ministry of Science
and Higher Education
Republic of Poland

Ministry
of Finance

Minister
of the Interior
and Administration

MINISTRY
OF INFRASTRUCTURE

MINISTRY
OF ENERGY

RCB
Rządowe Centrum
Bezpieczeństwa

PROKURATURA
KRAJOWA

Polish Investment
& Trade Agency
PFR Group

The National Centre
for Research and Development

PKN
POLISH COMMITTEE
FOR STANDARDIZATION

UNIVERSITY OF SILESIA
IN KATOWICE

Silesian University
of Technology

UNIWERSYTET
JAGIELLOŃSKI
W KRAKOWIE

UKE
Office of Electronic
Communications

URZĄD DOZORU
TECHNICZNEGO

INSTITUTIONAL PATRONS

AKADEMIA FACT-CHECKINGU
NASK akademia
ANTALL JÓZSEF KNOWLEDGE CENTRE
CSA cloud security alliance®
CONFLICT STUDIES RESEARCH CENTRE

DIGITALEUROPE
ECS EUROPEAN CYBER SECURITY ORGANISATION
SIEĆ BADAWCZA ŁUKASIEWICZ emag INSTYTUT SIECI
EBF European Banking Federation
EUROPEAN VALUES Protecting Freedom

GLOBAL CYBER ALLIANCE.
The Hague Centre for Strategic Studies
itapa
NASK
CASIMIR PULASKI FOUNDATION

SMART CITY BLOG
DEMAGOG
Fundacja Edukacyjna Perspektywy
FUNDACJA bezpieczna cyberprzestrzeń
Stowarzyszenie Top 500 Innovators

UNIA METROPOLII POLSKICH 1990
PERSPEKTYWY WOMEN IN TECH SUMMIT
WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION
CYFROWA POLSKA
ZWIĄZEK MIAST POLSKICH

MEDIA PATRONS

ROMANIAN NATIONAL NEWS AGENCY AGERPRES Updating the world.
BIZNES ALERT
CIBERSEGURIDAD <LATAM>
COMPUTERWORLD FROM IDG
CYBER DEFENSE MAGAZINE
CYBER SEC

CyberDefence 24
Defence 24
DLP expert Data Leak Prevention
DO RZECZY
EURACTIV.pl
Fintek

FORSAL.PL
GAZETA PRAWNA.PL
GEO politi.org
Głos SENIORA
ICT PROFESSIONAL
INTELIGENTNE MIASTA i REGIONY.pl

Inn:Poland.pl
ISB NEWS
IT professional
ITReseller Polska
IT w administracji
iTWIZ

mambiznes TU ZACZYNA SIĘ BIZNES
MANAGER
KARTA SENIORA OGÓLNOPOLSKA
pap POLISH PRESS AGENCY
POLSKA ZBROJNA
Polskie Radio Katowice

PORTAL SAMORZĄDOWY.pl
radio silesia 96.2
SIECI
smartcity expert blog o miastach prawdziwie inteligentnych
SGP smart-grids.pl
sztuczna inteligencja www.sztucznainteligencja.org.pl

TVP3 KATOWICE
TVS
wGospodarce.pl
wnp.pl
WP
W POLSCE PL
wprost

STRATEGIC PARTNERS

Microsoft

CISCO

SAMSUNG

T · ·

Google

PZU

facebook

PGZ

MAIN PARTNERS

CLOUDFLARE

ERICSSON

UBS

asseco

ORLEN

RSA

TAURON

PARTNERS

EXATEL

ORACLE

Enea

ARROW

Hewlett Packard
Enterprise

ALIOR
BANK

QBiTT

orange™

REGIONS & CITIES PARTNER

NOKIA

CYBERSEC RANGE PARTNER

vectorsynergy

SUPPORTING PARTNER

TRUSTED®
COMPUTING
GROUP

LOGISTIC PARTNERS

KRAKÓW
AIRPORT
im. Jana Pawła II

Katowice
AIRPORT®

KATOWICE AIRPORT
GENERAL AVIATION

NATO
OTAN

This conference is supported by
NATO's Public Diplomacy Division

SAVE THE DATE FOR THE 6th EDITION OF CYBERSEC

CYBERSEC CEE
#CSCEE20
SPODEK, KATOWICE
3-5 NOVEMBER 2020

INTERNET GOVERNANCE FORUM
#IGF2020
MCK, KATOWICE
2-6 NOVEMBER 2020

@CYBERSECEU

www.cybersecforum.eu