
CYBERSEC
EUROPEAN
CYBERSECURITY FORUM
TOGETHER AGAINST
ADVERSARIAL INTERNET
RECOMMENDATIONS & KEY TAKEAWAYS
6th EUROPEAN CYBERSECURITY FORUM – CYBERSEC GLOBAL, 28-30 SEPTEMBER 2020
&
4th CYBERSEC BRUSSELS LEADERS' FORESIGHT, 18 MARCH 2021
#CSGlobal20
www.cybersecforum.eu
#CSBXL21

> ***Together Against Adversarial Internet*** **means in fact: together against an adversarial world.**

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

CONTENTS

OPENING REMARKS 4

Includes keynote speeches on the role of NATO and the EU in securing cyberspace, the concept of quantum politics, the evolution of the threat landscape, a conversation on the US perspective on the transatlantic relationship, and other formats.

STATE STREAM 16

Includes a keynote speech on the effects of the pandemic on cybersecurity, a panel discussion on democratic and authoritarian practices of digital governance, a conversation on Europe's digital strategic autonomy, and other formats.

DEFENCE STREAM 36

Includes a keynote speech on Germany's defence mission, panel discussions on military use of 5G and information warfare, a conversation on the rejuvenation of the Transatlantic Alliance build on technology cooperation, and other formats.

BUSINESS STREAM 64

Includes a keynote speech on new geopolitics, panel discussions on challenges related to big data and on digital investments in the Three Seas region, conversations on the future of digital platforms and norms in cyberspace, and other formats.

FUTURE STREAM 90

Includes a keynote speech on the future of the Internet, a panel discussion on threats to digital identity, an oxford debate on Splinternet, conversations on the future of transatlantic data flows, and other formats.

SIDE SESSIONS AND SPECIAL FORMATS 110

Includes keynote speeches on EU Cyber Package and ENISA's role in the new cybersecurity ecosystem, sessions on securing 5G networks through international cooperation and geopolitics of emerging technologies, and other formats.

Dear Friends of the CYBERSEC Community,

the past year has not only brought us a prolonging global shock in the form of the pandemic, but also, consequently, an unprecedented acceleration of the digital transformation. We have experienced how the network connectivity and reliability are crucial for the continuity of operation in almost all sectors of our economies. It is fair to state that the Internet made it possible for us to live on. However, as our reliance on a plethora of digital tools and services has increased, so has our vulnerability to numerous new ways of digital misconduct. The imposition of national lockdowns and the collective struggle against the coronavirus crisis was accompanied by the rise of cyberthreats, targeted against individuals, businesses, and state and international institutions, including the health sector. We have observed an expansion of specific types of cyberattacks, including those taking advantage of social uncertainty and pitfalls of the healthcare systems, and those exploring vulnerabilities in the supply chains.

We cannot forget the importance of effective cooperation in overcoming the crisis and rebuilding the economy. Guided by shared values and shared goals, we can join efforts for ambitious future political and economic agendas. The ascent of the Joe Biden Administration has revived hopes on both sides of the Atlantic for a rejuvenation of the transatlantic relationship. We firmly believe that cooperation in technology governance and cybersecurity should be at the centre of the efforts to rebuild global transatlantic leadership. In this respect, the democratic countries' cooperation and stable partnership in a wide range of challenges such as global economic recovery, investments, cybersecurity, or data management, to name just a few, are a necessary step forward to secure digital future.

In an era when everything goes digital, our mission to foster the building of safe cybersecurity frameworks has never seemed so important and meaningful to us. We proudly present to you this set of actionable recommendations from two CYBERSEC conferences that gathered a group of the brightest cybersecurity visionaries, experts, decision-makers, and business leaders from across the globe. We trust that it will serve as a valuable compass for institutions, businesses, and individuals alike, especially at a time when the digital world has reached unprecedented scope.

Michał Rekowski
CYBERSEC Programme Director, Research Director, the Kosciuszko Institute

&

Barbara Wilk
Research Fellow, former CYBERSEC Programme Director (2019-2020)


TOGETHER
AGAINST ADVERSARIAL INTERNET


CYBERSEC DREAM TEAM
BEHIND THE SCENES
#CSGlobal20


CYBERSEC
EUROPEAN CYBERSECURITY FORUM


TOGETHER
AGAINST ADVERSARIAL INTERNET


TOG
AGAINST AD

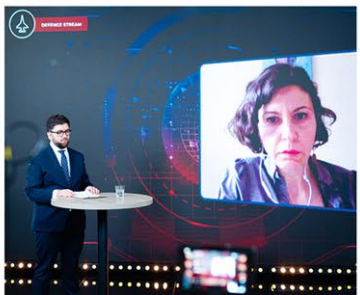

TOGET

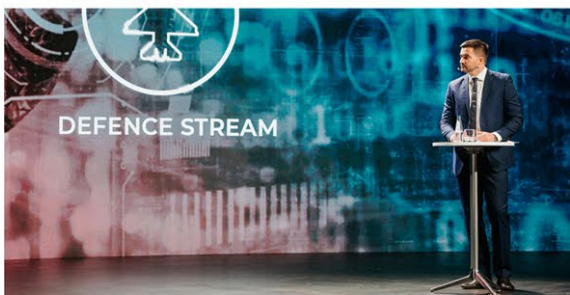

TOGETHER
TOGETHER


TOGETHER
AGAINST ADVERSARIAL INTERNET


Keynote speech
KEYNOTE SPEECH BY POLISH MINISTER OF DIGITAL AFFAIRS
speaker:
Marek Zagórski
Let's advance
STATE-of-the-art cybersecurity
TOGETHER
#CSGlobal


TOGETHER


DEFENCE STREAM


DEFENCE STREAM

OPENING REMARKS

6th EUROPEAN CYBERSECURITY FORUM – CYBERSEC GLOBAL 2020

INTRODUCTION TO THE THEME OF THE CONFERENCE – TOGETHER AGAINST ADVERSARIAL INTERNET

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

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

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The Internet is powerful – it connects us, supports information and experience exchange, and allows our lives, businesses, and democracies to keep going, even more so during the ongoing health crisis. In times of social distancing one can hardly imagine being entirely offline. Technology, however, oftentimes comes at the price of our security and privacy. As the exploitation of our rights and freedoms online is accelerating with each passing year, the global community should join forces in protecting the Internet as an open, free, and accessible tool for everyone. Technological and digital transformation of societies, economies, and defences has become a key topic on the political and strategic agendas of states and international organisations. The new digital reality that is emerging right before our eyes should be created in the spirit of responsibility that will drive a more inclusive, innovative, and progressive world, not only in the next few years but also for the decades to come.

MAIN THREATS & CHALLENGES:

- Internet as a tool can both empower and overpower us. Through activities such as surveillance, fraud, identity theft, and interference in democratic processes, cyber criminals are abusing rights and freedoms all over the globe.
- Over the past few years, we have observed a significant spike in cybercrime, in particular attacks and campaigns threatening democracy, distorting the truth, promoting nationalism and autocratic practices. Simply, the Internet and new technologies have become an attractive venue for power projection. This trend is raising geopolitical tensions all over the world.

THE WAY FORWARD:

- The global community should join forces in protecting the Internet that is open, free, secure, and accessible for everyone.
- Our plans and projects supporting, regulating, and protecting both the Internet and other technologies should go beyond addressing exclusively the current challenges. We should make sure we are prepared for what may come in the future as the digital transformation is accelerating.

- Like-minded countries and other stakeholders should lead by example, promoting the democratic approach and respect for human rights. Our strategies for the society, economy, and defence systems should be based on commonly shared values.

"Over the years we have observed that the Internet has become a mirror, which reflects many of the trends that impact the real world. Since there is a such strong convergence, a fusion of digital technologies and physical realm, 'Together Against Adversarial Internet' means in fact: together against an adversarial world."

IZABELA ALBRYCHT

MESSAGE FROM NATO DEPUTY SECRETARY GENERAL

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Mircea Geoană – Deputy Secretary General, NATO

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

As the most powerful alliance in history, NATO has to constantly adapt to the challenges that might threaten our security and undermine cooperation among like-minded countries. As a result of accelerating technological developments, today's battlefields are located not only on land, sea, and air, but also in space and cyberspace. Moreover, current threats come from multiple dimensions at once, from both humans and machines powered by technologies such as AI and robotics. Undoubtedly, technology has great potential for progress that all of us could benefit from, but as many other things – it comes at a price. Unregulated and uncontrolled use of certain technologies puts our lives, rights, and safety at stake. In this regard, international cooperation between like-minded countries and stakeholders from across all sectors is absolutely key.

In 2014 the allies have agreed that a cyberattack can trigger Article 5 of the Washington Treaty, allowing member countries to take collective defence measures. Since then, NATO has officially recognised cyberspace as a military domain, a decision which was followed by the establishment of the Cyberspace Operations Center. The Alliance has also announced plans to integrate national cyber strategies into its missions and agreed on a cyber defence pledge enhancing the collective resilience, and even issued a joint statement condemning destabilisation and malicious cyber activities exploiting the pandemic. NATO has to keep up this momentum to make sure cyberspace is as secure as possible.

MAIN THREATS & CHALLENGES:

- The Alliance has to adapt to the ongoing digital transformation, digital arms race, and technological developments fuelling geopolitical tensions across the globe.
- Cyberthreats are becoming more prominent, complex and destructive, especially now during COVID-19 pandemic. Threat actors are exploiting our vulnerabilities and disrupting our lives by targeting research institutes, hospitals, and critical infrastructure, leading in extreme cases even to fatal casualties.
- Emerging and disruptive technologies (EDTs) are developing at full speed. NATO has to remain competitive in the field while ensuring safety in the face of new threats.
- Countries rejecting our fundamental values are using technology to increase the control over their own citizens and influence other parts of the world.

THE WAY FORWARD:

- Making sure international law and norms of responsible state behaviour in cyberspace are respected is of key importance for the Alliance. This will not only protect the member countries but also bolster our collective capabilities and resilience.

- National cyber networks and infrastructure should be stronger and more resilient. The cyber defence pledge agreed in Warsaw in 2016 calls on allies to engage in innovative projects supporting the necessary upgrades.
- While competing with countries that abuse technologies to not only harm their citizens but also to destabilise the political West, NATO has to focus on protecting our fundamental values, freedom, democracy, and the rule of law.
- To maintain the technological edge, NATO member countries have to build effective partnerships both between governments and with the private sector, industry, academia, etc.

"We, the political West, are on the verge of a new Sputnik moment, where a non-western power might actually overtake us. We are now competing with authoritarian regimes that misuse and abuse new technologies to destabilise us and to manipulate and disrupt our free and democratic way of life."

MIRCEA GEOANĂ

AN ERA OF QUANTUM POLITICS FOR A HYPER CONNECTED WORLD

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Armen Sarkissian – President of the Republic of Armenia

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The world is currently filled with a lot of uncertainty. Technology, networks, and systems are now visibly ingrained in our lives and the pandemic is only accelerating that process by making nearly every aspect of our existence device-dependent. Connectivity matters more than ever and new solutions affect our society, economy, and politics – because of that, the dynamics have changed. As our new reality is taking a new shape through our actions, we need to be prepared for and anticipate what is to come in the next decades.
In a sense, the new world is quantum – interconnected and interdependent as never before. We might need quantum politics to face modern challenges and that involves changing our thinking and rules of the engagement. Only then will we be allowed to fully enjoy the benefits of the digital transformation and evade the havoc.

MAIN THREATS & CHALLENGES:

- Our societies, economy and politics are hugely dependent on technology and connectivity. Data and the Internet are singlehandedly powering the innovation and progress, but at the same time posing serious threats to the stability of our world.
- Digital transformation and new technologies mean power. We have reached the point where even a single individual is capable of organising a revolution using connectivity and networks. Such a prospect brings a lot of uncertainty in many spheres of our lives.
- Many issues the world is facing right now, such as climate change, are a result of technological advances.

THE WAY FORWARD:

- Classical ways of thinking and engagement do not apply anymore. The world is changing rapidly, and the international community should adapt to the new rules of the game.
- Cooperation among like-minded countries should not be limited to superpowers, but engage a plethora of stakeholders. This process should result in resilient systems, agreements, common understanding, and recognised limitations.
- When developing and deploying new technologies, stakeholders should take under consideration not only the benefits and direct risks of the tools, but also their impact on other parts of our systems, including environment, human rights, and cybersecurity in a broad sense.

"The way forward is to realise that there are new rules that are running this new world, the quantum world. Quantum in this case means that this world is run not by classical rules, it also means that we are so interconnected and interrelated that the ordinary systems and ordinary values have to be adapted."

ARMEN SARKISSIAN

4th CYBERSEC BRUSSELS LEADERS' FORESIGHT 2021

INTRODUCTION TO THE THEME OF THE CONFERENCE – TOGETHER AGAINST ADVERSARIAL INTERNET

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

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The development of technologies drags the transatlantic allies into the global competition with both their rivals and their adversaries. We are currently witnessing geoeconomics and geopolitics being impacted by various digital technologies facilitating economic growth and enhancing a build-up of high-tech military capabilities and thus political power of states. And therefore we can also see a fully-fledged competitive race between the countries to become the data and technology powerhouses able to fuel the economy of the future and upgrade their defence postures. That is why we are observing for instance the growing importance of data-sharing frameworks between like-minded countries to let business prosper and take advantage of free and secure flow of digital data.

The EU member states and NATO nations' leaders need to focus on dealing with the challenges of global technological disruption NOW and TOGETHER. European institutions are having dozens of files open with regulatory and policy proposals aiming at developing and deploying the key technologies safely and sustainably to boost Europe's digital autonomy as well as adapting cybersecurity standards into the fast-developing digital realm with the expected "Brussels effect" in other parts of the world. With the new Digital Compass presented by the European Commission and EU-US Trade and Technology Council, new opportunities for technology cooperation are arriving too. Taking that approach, we can see an opportunity for Europe and NATO to strengthen comprehensive transatlantic cooperation, with technology playing a central role. NATO for its part continues to boost its cyberdefence posture as well as starts putting forward an emerging and disruptive technology implementation strategy, and setting up new business models to foster innovation. Both organisations now agree that getting TOGETHER in addressing the security challenges of the cyber-physical convergence and geopolitical shifts closely related to the global technological rivalry is a must.

MAIN THREATS & CHALLENGES:

- We are continuing to deploy at unprecedented speed new emerging and disruptive technologies into our economies, societies, and all military domains – air, land, sea, cyber, and space. As a consequence, our vulnerability landscape broadens exponentially.
- Cybercriminals often supported by state actors have been gaining access to more and more powerful tools. The SolarWinds hacks have not only compromised US government agencies but also institutions all around the interconnected world.

- We can already see cyber armies being established and growing, as well as more sophisticated cyber weapons being developed and proliferating. The threats that we face include Cyber Pearl Harbor scenarios with numerous cyberattacks on critical infrastructure, such as power plants or water facilities.

THE WAY FORWARD:

- There are at least four important dimensions which transatlantic partners should address to avoid heading to the adversarial Internet world:

    1. reinforce cybersecurity agendas to address the increasing number and sophistication of cyberattacks,
    2. cooperate on advances and technological breakthroughs in AI, 6G, quantum technologies as well as on the reorganisation of digital supply chains in a way that will strategically contribute to resilience,
    3. develop the technologies in a way which positively impacts our geopolitical and geoeconomic position, and
    4. will be in line with our democratic values.

- The increasing scope of vulnerabilities stemming from the development of emerging and disruptive technologies requires implementing cybersecurity upfront into the process of designing and deploying such technologies as AI and human enhancement as well as solutions based on them to make sure they will be resilient. It can be done within NATO and EU, for instance by setting common security standards and baseline security requirements and by gaining bigger influence on this process in the international standard-setting bodies.

"The only thing that can save us from all-out cyberwarfare with escalation of adversarial activities and countless cyberattacks of geopolitical impact equal to or even greater than Pearl Harbor is concerted effort and cooperation. Like-minded countries and the private sector should build a full-spectrum approach to cyber resilience, deterrence, and defence systems TOGETHER and right from the beginning of this decade."

IZABELA ALBRYCHT

OPENING ADDRESS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Josep Borrell Fontelles – High Representative of the Union for Foreign Affairs and Security Policy; Vice-President of the European Commission

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The digital revolution is affecting every single aspect of our lives. From the way we work or socialise to how we buy. Our world is more digitalised and interconnected than ever, a trend that has further accelerated with the COVID-19 pandemic. In this unprecedented period, the European Union needs to be fit for the digital age. In a world where malicious cyber activities know no borders, we will need effective partnerships to tackle the increasing challenges that we face. Sharing expertise and building capacity together with our partners maximises our gains from the technological revolution and increases our common resilience in cyberspace. From this point of view, the transatlantic partnership is particularly relevant. For Europe, the United States is a natural partner and an ally with whom it shares both values and challenges.

MAIN THREATS & CHALLENGES:

- Cyberattacks, online theft, and disinformation are all on the rise, undermining also international security and stability and exemplifying the increasing interconnection between internal and external security.

THE WAY FORWARD:

- With the 2020 Cybersecurity Strategy, the EU is using its regulatory policy and investment instruments to strengthen the EU's resilience and our security, our digital sovereignty and prosperity.
- According to the strategy, the EU:
    1. needs to defend its vision of an open, stable, and secure cyberspace worldwide,
    2. use our political clout to reaffirm the primacy of international law in cyberspace,
    3. to ensure that everyone adheres to norms of responsible behaviour,
    4. deter and respond to the increasing number of cyberattacks.
- The EU should also aim to shape the standards of new technology and ensure individual security, safety, and privacy. It shall promote digital inclusion and a responsible digital transformation in emerging markets, allowing more people to reap the benefits of digital technologies in a more sustainable and secure way.
- The EU should work together with the United States to shape technologies, their use, and their regulatory environment. Both should also continue to work together with our key partners and stakeholders, including in the private sector.

"The United States are a natural partner with the European Union in cyberspace. We share the same values and challenges, notably on infrastructure, technologies and data."

JOSEP BORRELL FONTELLES

OPENING FIRESIDE CHAT

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

- **Michele G. Markoff** – Acting Coordinator for Cyber Issues, Office of the Secretary of State, United States Department of State
- **Izabela Albrycht** – Chair, The Kosciuszko Institute; President, Organising Committee of the European Cybersecurity Forum – CYBERSEC

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

One of the prevailing priorities for both the EU and the new US administration is the rejuvenation of the transatlantic relationship. This revival has been gaining momentum in the last few months, particularly due to increased dialogue between both sides of the Atlantic. Cyberspace and new technologies are surely an area where those debates can and should turn into tangible actions, especially as the digital world keeps on playing a huge role in our lives. Our decisions today will shape our tomorrow, which is why intensifying international cooperation is of critical importance for all of us.

The cooperation between the United States and the European Union covers a broad range of areas, with defence and diplomacy being at the forefront. In this regard, NATO's strategies for cyberdefence capacity building, and the recent UN GGE consensus report with the framework for responsible state behaviour in cyberspace are firm foundations for a forward-looking action roadmap, ensuring national and international security, wellbeing of societies, and limitless possibilities for innovation that serves all.

MAIN THREATS & CHALLENGES:

- The ongoing COVID-19 crisis has shown some correlation between the state of public health and cyberspace – with the spread of the virus, cyber incidents have become not only more frequent, but also more severe, affecting our response to the coronavirus and posing serious threats to national security of states. Both the health and cyber pandemics are global and difficult to control, as no state was prepared to prevent or react to either of them.
- Cooperation on promoting stability in cyberspace should be international and cross-sectoral, which oftentimes hinders the dialogue and elongates the process due to the number of stakeholders involved.
- Lack of common understanding and clarity of terms among partners is hindering the dialogue on extending and protecting our values in cyberspace. That results in difficulties when it comes to investigating and meting out justice for malicious behaviour.
- There is a strong need to upgrade network defences of allies and build awareness and cyber capacity round the world, because even a strong framework based on norms and international law cannot enforce itself.
- Political commitments alone are not enough to deter and prevent cyberattacks. Ensuring that states face consequences for engaging in irresponsible behaviour in cyberspace is difficult when the actions are based on a voluntary pledge, not a legally binding agreement.

THE WAY FORWARD:

- Promoting stability and security in cyberspace is necessary to guarantee safe and innovative future for all. That is why cyberdiplomacy efforts continue playing a critical role, and results such as the framework for responsible state behaviour are firm foundations to build on, reducing the overall risk of conflict in cyberspace and strengthening political commitments.
- Constructing clear, transparent, and meaningful consequences for malicious behaviour in cyberspace will result in better enforcement of norms, reduce the risk of conflicts, and create more understanding among partners. The new EU cybersecurity strategy and the cyberdiplomacy toolbox, as well as the US cyberdeterrence playbook are prime examples of that, while also building foundations for transatlantic cooperation.
- Cyber incidents should be addressed through international and cross-sectoral cooperation, involving bilateral and multilateral forums, and regional organisations. There is strength in unity and together with both the public and private sector, as well as technical standard-setting bodies, trade organisations, and the civil society it is possible to come up with actionable strategies that will be beneficial to all.
- The US-EU relationship on cyber issues is particularly critical to defending an open, interoperable, reliable, and secure Internet for all. This cooperation should be fostered and extended to other like-minded countries, for example through cyberdiplomacy and capacity building measures.
- Cooperation among allies should be held at multiple institutional levels at once, engaging entities such as EEAS, diplomatic services of states, technical security agencies, law enforcement, and militaries, under the auspices of NATO.
- Investments in innovation, regulation, and deployment of key technologies should result in enhanced defence capabilities of states. Pursuing a proactive approach in this area through a comprehensive strategy addressing a full range of cyber issues – such as supply chain security, Internet standards, use of emerging and disruptive technologies, and protection of privacy and human rights online – will increase the collective strength of all partners.

"We need to upgrade our network defences and build our awareness and cyber capacity around the world, but even a strong framework based on norms and international law cannot enforce itself. Besides our work in this area, we must create clear, transparent, and meaningful consequences for malicious actors in cyberspace."

MICHELE G. MARKOFF

HOW ORGANISATIONS SHOULD ADDRESS CYBERTHREATS IN THE ADVERSARIAL ONLINE WORLD

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

Joshua Burch – Senior Managing Director, Head of Cybersecurity for the Europe, Middle East, India, and Africa Region, FTI Consulting

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The security landscape has changed, even more so during the pandemic as most of us were forced to carry on with our lives and businesses online. Technological advancements not only transformed our economy and society, but also made us dependent on data and connectivity. Businesses are not an exception, as they learned to embrace data and benefit from it. Cyber criminals, however, stand ready to exploit our vulnerabilities, oftentimes being one step ahead of us. Both the public and private sector are targeted by threat actors, as the Hafnium attack or the SolarWinds hack have shown.
Cyberattacks are spreading like wildfire and all of us need to have the tools to protect our data, devices, networks. Especially entities handling sensitive data or being a part of critical networks and systems should pay attention to the cybersecurity of their assets, increase their resilience, and ensure the highest possible level of security.

MAIN THREATS & CHALLENGES:

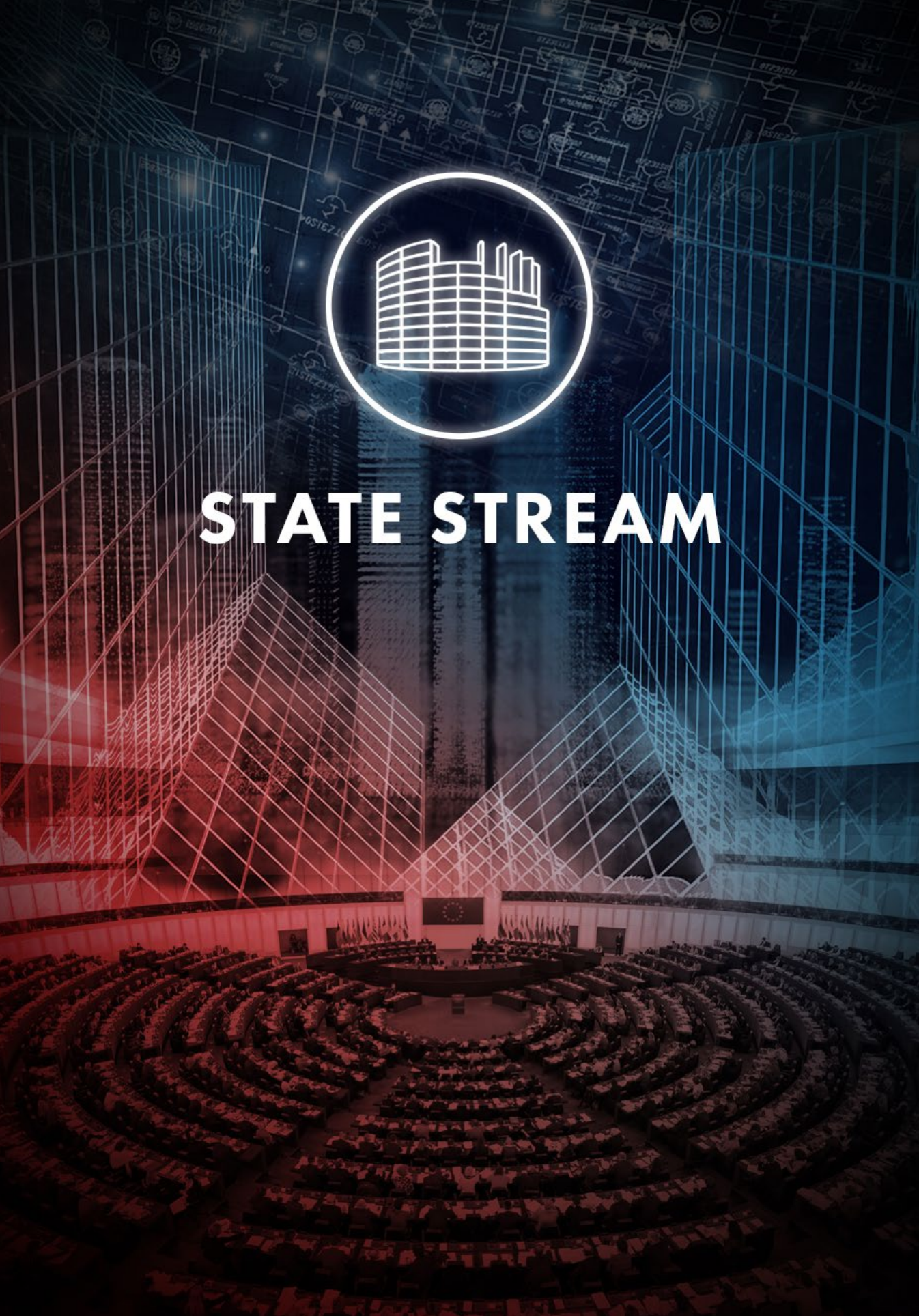
- Businesses' dependence on data and technology poses serious threats to confidentiality, integrity, and protection of data and networks.
- Cyberattacks are used as means to achieve geopolitical objectives. Moreover, the lines between hostile nation-states and organised crime groups are blurring as governments continue hiring criminals in order to easily deny being responsible. Their targets range from government agencies and financial institutions to hospitals and private companies.
- Cybercriminals have adapted to the new reality, oftentimes using the pandemic-related rhetoric to harvest credentials and infect systems. Phishing attacks and ransomware are becoming even more common, exploiting remote working environment.

THE WAY FORWARD:

- Companies all over the world need to re-examine their cybersecurity systems and cyber risk profiles. Understanding the risk environment, current trends, and threat actors, and then determining how those may affect the business continuity is absolutely crucial.
- Resilience is both practical and attitudinal – cybersecurity practices and defence upgrades should go hand in hand with a mindset acknowledging the fact that cyberattacks are not a matter of if, but when.

"A cyberattack is a matter of when and not if, so the most important thing an organisation can do is to strive to become a cyber resilient organisation, one which focuses on identifying and protecting its Crown Jewels, the assets, data, and systems that make the business what it is."

JOSHUA BURCH


STATE STREAM

6th EUROPEAN CYBERSECURITY FORUM – CYBERSEC GLOBAL 2020

HOW HAS THE CYBERSECURITY THREAT LANDSCAPE CHANGED DUE TO ACCELERATED DIGITAL SHIFTS CAUSED BY THE COVID-19 PANDEMIC?

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Abigail Bradshaw** – Head, Australian Cyber Security Centre

BIG PICTURE – WHY THE TOPIC MATTERS?

Most of the innovations that have changed the global economy over the last few decades rely on network connectivity in commerce, communication, education, and training supply chains. The COVID-19 pandemic has only accelerated this process, making a huge impact on nearly all areas of our lives. The digital environment is not an exception as states have learned how crucial a safe, secure, and strong infrastructure is to the national and international stability. Internet, as one of the key elements of the digital ecosystem we are living in, has been an enabler of learning, earning, prosperity, and communication, and it will play an even bigger role in the post-COVID recovery. Because of increased technology use we are also more vulnerable, and threat actors are quick to find ways to exploit that, causing damage to individuals, businesses, governments, and critical infrastructure that ensures proper functioning of societies. Such a situation requires an adequate and thorough response from all entities involved in creating the digital ecosystem, representing both public and private sectors.

MAIN THREATS AND CHALLENGES

- During the pandemic the number and frequency of cyberattacks such as phishing, message scams, and ransomware has risen exponentially. The proliferation of low-cost malware tools through dark web is helping the spread of online crime.
- In addition to already known forms of attacks, cyber criminals are also seeking new ways to profit from the ongoing health crisis using loopholes found in new policies and safety measures, which are oftentimes introduced ad hoc.
- Threat actors are capitalising on uncertainty and new vulnerabilities uncovered in part due to the rapid switch to remote work. Online scammers and hackers are more frequently targeting vulnerable home infrastructures and businesses for profit.
- State-based threat actors also remain actively targeting governments, industry, healthcare, banking, education, and critical infrastructure. Their sophisticated and well-resourced methods, if not countered, are likely to succeed in breaching national security and economic prosperity of states, causing shortages of medical supplies, food, and water, disrupting telecommunications and functioning of businesses and governments, and in most extreme cases – resulting in loss of life.

- Internet of Things solutions offer a vast range of new opportunities for businesses, governments, and people, but the connectivity and data sharing between devices also invites threat actors to exploit them. As the number of IoT devices is expected to rise exponentially (reaching 21 billion globally by 2030, according to forecasts), the risk of information being compromised is even bigger, which puts pressure on both users and developers of those solutions.

THE WAY FORWARD

- Prevention, mitigation, and elimination of threats requires collective action from entities across all sectors and backgrounds, especially government, industry, and academia. The response cannot be limited to national efforts, but should be developed on a global scale in collaboration with like-minded countries. An example of that is Europol's public-private collaboration "No more ransomware", which helps victims retrieve their data without engaging with criminals.
- Effective cyber defence requires a global shift towards an approach with cybersecurity at the forefront of all entities, processes, and systems. This way the global society can improve its overall resilience and responses to threats.
- As the use of the Internet is omnipresent in nearly all spheres of our activity, there is a need to make it safe for everyone involved. In cooperation with the global industry and governments all over the world, we should work towards enhancing our capabilities so that we are able to remove and mitigate harms before they actually happen.
- Response to cyberattacks and threats should be adequate, active, and in certain cases automated to ensure that we can counter threats at scale and in a timely manner. Governments should support business in developing and implementing automated threat prevention solutions, such as name filtering and SMS phishing blocking.
- IoT devices can be protected through collaboration between governments and businesses. An example of that is the Australian voluntary Code of Practice for consumers, which equips users with knowledge on cybersecurity solutions and shares practical guidance on safe use of IoT.
- No cyber vulnerability should be left unanswered and untreated. There is a strong need for a cross-sectoral cooperation in threat assessment, risk management, and regulating the use of technologies – that requires effective systems of information sharing, preparatory activities for operators, mutual assistance, and exchange of best practices. The cost of passive attitudes towards cybersecurity and resilience is too high for the global community.

"Internationally, we're at the cusp of a global trend, towards companies and countries working together to ensure the next wave of technologies that will reshape our societies, will do so in a positive way."

ABIGAIL BRADSHAW

TOWARDS A GLOBAL SURVEILLANCE SOCIETY? THE RACE BETWEEN AUTHORITARIAN AND DEMOCRATIC PRACTICES OF DIGITAL GOVERNANCE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

VIP PANEL DISCUSSION with the particiaption of:

- **Margrethe Vestager** – Executive Vice-President, European Commission
- **H.E. Kersti Kaljulaid** – President of the Republic of Estonia

Chaired by **Joanna Świątkowska** – Assistant Professor, AGH University of Science and Technology; Initiator & Cybersec Programme Director (2014–2019)

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The omnipresence of technological tools – from basic smartphones to advanced IoT devices – is transforming societies to their very core, changing interaction between people, and remodelling the way states carry out their duties. Leading by example, the world's digital frontrunners like Estonia demonstrate how digital solutions can efficiently administer and protect citizens in both ordinary and extraordinary times. Like-minded countries are seeking ways to use technology for the common good, and one of these examples is the EU toolbox for the use of mobile applications for contact tracing and warning in response to the coronavirus pandemic published in April 2020. While preparing new legal frameworks, member states and the EU entities should work with hardware providers, software providers, and telecoms to make sure that deployment of new technologies such as 5G is done in a safe way. Moreover, the regulations should be as precise as possible and oftentimes accompanied by practical toolboxes.

However, as disconcerting and unfortunate as it is, the digital transformation is not always aligned with respect for democratic values and principles. The use of ICT to monitor, repress, and manipulate domestic and foreign populations – also called digital authoritarianism – is on the rise and spreading quickly along with worldwide technology deployment. It is therefore crucial to strengthen and support a model of democratic digital governance in order to protect citizens' fundamental rights and freedoms – if not globally, then in as many countries as possible.

The utopian idea that the flow of new information and ideas from the outside world would pull authoritarian states towards economic openness and political liberalisation has failed to come true. In reality, the Internet, just like most technologies, is neutral, but it can bring out what's best in humanity but also reveal its darkest. We need to come up with solutions for democratic states to make sure that the common values will govern cyberspace whilst simultaneously looking at ways to counter an adversarial vision of the Web's future.

MAIN THREATS & CHALLENGES:

- During the COVID-19 pandemic we can observe omnipresent espionage and a surge in cyberattacks on critical infrastructure, particularly the health sector, proving that the threat actors and adversaries are more active than ever.
- Internet is used by authoritarian regimes as a tool to oppress their people, rather than being the reason why the oppression occurs.

- Further fragmentation of the Internet between authoritarian and democratic spheres of influence is only enabling more oppression and exploitation.
- The Internet is a lightly regulated space which, due to the relative free rein, can threaten the security of the individuals using it. It is fairly easy to pretend to be someone else and using another person's identity online is just as unacceptable as using falsified documents in analogue world.
- People increasingly work independently as well as are hired by many companies in many jurisdictions simultaneously – all because their jobs are in their pockets. Without proper updates, for example in the tax systems, such a situation becomes counterproductive as individuals' needs for social services, security, education are also evolving but remain separated from specific systems.

THE WAY FORWARD:

- The Internet should not be separated into two parts consisting of one for democratic nations and the other for the others. We need to insist on the democratic rights of all people globally, as well as make sure we understand and regulate the risks.
- All international laws created for an analogue world should apply in Internet. Protecting and respecting human rights should be our goal in both an analogue and digital world.
- The Internet being a tool which should be accessible to everyone, a system such as eIDAS 2.0 would be able to give Europeans the possibility to act and transact with those they know through an internationally operating digital ID mechanism. This should result in more secure, trusted, and accountable digital realm.
- Data handled by the government still belongs to the citizen, who should be given power over that data. Each look into that data should be reported to the citizen, and unjustified access should be punishable as a crime.
- We should equip every citizen with digital skills, so everyone is able to freely navigate new technologies used on daily basis. This way we can globalise their potential and capabilities, thus increasing their independence in economy and society, and unleashing the full potential of society.

"Only if we fundamentally trust that technology will serve us well, will we be able to unleash the full potential of technology in our society – of better health, better education, fighting climate change, enabling convenient transportation. All of that potential can only be unleashed if we trust technology."

MARGRETHE VESTAGER

"All international law created for analogue world should apply on the Internet (...) Instead of fighting specifically totalitarian regimes on the Internet, we should understand what we could do to help citizens who live under these conditions where they are not free to express their views and deal with that. There is no difference between analogue space and digital space in this."

KERSTI KALJULAID

HOW TO CYBERSECURE DIGITAL INFRASTRUCTURE OF THE FUTURE – THE VIEW FROM POLAND ON THE ADOPTION OF THE EU REGULATORY FRAMEWORK

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Marek Zagórski –** Minister of Digital Affairs of the Republic of Poland

In 2018, the Act on the National Cyber Security System established a new framework for the cybersecurity system in Poland. Since then, there was a clear shift at the EU level, with cybersecurity becoming one of the top priorities for the European Commission through the adoption of the European Electronic Communications Code that unifies national procedures for reporting security incidents and the publication of the 5G Toolbox. Poland has long appealed to the EU for a decisive approach to the security of telecommunications networks. Based on vast public consultations, the Polish government has submitted an amendment to the Act on the National Cyber Security System. It proposed for the Advisory Committee to be given the power to assess whether the hardware and software provided by a given supplier poses a risk to the national system of cybersecurity – a measure compliant with the EU 5G toolbox. All digital technologies should meet the highest security standards, therefore, not only next generation networks, but also cloud computing services should be supplied by verified and trusted vendors. With the amendment the government is also opening the door for the creation of sectoral CERTs in all sectors essential for the social and economic security of the country. Furthermore, it is introducing security operations centres (SOCs) into the national cybersecurity framework. Apart from a robust infrastructure built with verified equipment and software, citizens need to trust the technology, and for that they need to have access to reliable information.

Poland and many other European countries have been submerged by a wave of disinformation campaigns concerning mobile networks, particularly 5G technology which in some cases led to attacks on the telecommunications infrastructure. In order to combat these false claims, the Ministry of Digital Affairs (recently incorporated into the Chancellery of the Prime Minister) launched a broad educational campaign concerning both telecommunications networks and the possible impact on health. The Ministry of Digital Affairs organised a series of workshops, reached the public through the social media, and most importantly published the so-called White Book, explaining how a telecommunications network works, what an electromagnetic field is, and how it can affect the human body. The Ministry believes it is crucial to offer people proven, credible, and reliable sources from experts in the field, instead of anonymous people online. However, national efforts might not be enough. This is a transnational issue and as such should be addressed at EU level. Consequently, in cooperation with other member states, Poland will be calling on the European Commission to implement measures counteracting disinformation regarding telecommunications networks and 5G in particular, such as an awareness-raising campaign across the continent. With a common coordinated action plan, we should be able to provide EU citizens and local authorities with clear facts, which will allow them to extract the truth from this information.

"The COVID-19 pandemic has put even more pressure on governments worldwide to deliver a safe environment for digital services to accommodate the needs of our citizens. We'll do our best to overcome the challenges that lay ahead and work towards creating a cybersecurity digital future."

MAREK ZAGÓRSKI

COMMON CODE: AN ALLIANCE FRAMEWORK FOR DEMOCRATIC TECHNOLOGY POLICY: INTRODUCTION TO THE TECHNOLOGY ALLIANCE PROJECT BY CNAS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

INTRODUCTORY PRESENTATION by:

- **Martijn Rasser** – Senior Fellow, Technology and National Security Program, Center for a New American Security (CNAS)
- **Shin Oya** – Senior Consulting Fellow, Asia-Pacific Initiative
- **Rebecca Arcesati** – Analyst, Mercator Institute for China Studies
- **Ainikki Riikonen** – Research Assistant, Technology and National Security Program, Center for a New American Security (CNAS)

THE BIG PICTURE & THE MAIN CHALLENGE:

We're entering a new era of global rivalry with the growing competition between democracies and authoritarians' visions for technology. Those opposing visions have implications for economic and political power. Authoritarian regimes are abusing new surveillance technologies, powered by algorithms and AI tools, to repress their citizens. Leading democracies should spearhead the creation of a new multilateral architecture for technology policy, but currently they lack a coherent vision for ensuring technology leadership. However, democracies have yet to form a united front to propose responsible norms for these tools. They face barriers to cross-border innovation and they also risk getting overrun by standard-setting bodies influenced by authoritarian actors. Liberal democracies have not reached consensus on how to deploy emerging technologies according to their values. We are seeing this play out in the AI facial recognition and surveillance technologies, in data privacy, in the debates around 5G, and in the US engagements. The current approach to the technology policy coordination is ad hoc and disjointed. This approach blunts the efficacy of each nation's policy decisions and seems a missed opportunity to leverage democracies' combined momentum.

Therefore, the Center for a New American Security together with partners from the Mercator Institute for China Studies and the Asia-Pacific Initiative have proposed the Technology Alliance. The Technology Alliance is aimed at strengthening cooperation between like-minded countries, to regain the initiative in global technology competition. The objective is to boost competitiveness and promote a democratic vision of technology for the future. This initiative is spearheaded by vast consultations with international stakeholders, government officials, researchers, and industry experts from the United States, Europe, and Asia-Pacific.

THE WAY FORWARD:

- The Technology Alliance Project proposes an informal multilateral mechanism to enable flexible and issue-based partnerships. Core members should be countries with large economies and leading technology capabilities; this group should be small, to ensure effective decision-making, but at the same time be nimble and flexible.

- These countries must have long-standing interest in international collaboration, shared ties with each other, and a shared commitment to liberal democratic values, such as the rule of law and respect for human rights. Voting should be consensus-based but remain flexible. Annual head of state or ministerial meetings should be held, with a focus on regular meetings between working-level officials.
- It should focus on key policy areas: the supply chain resilience, protection of critical technology, coordination on development of digital infrastructure and on norms and standards.
- The long-term agenda of the Technology Alliance might include areas that take more planning or more time to cultivate consensus on. These areas are: measures to promote joint R&D, technology forecasting, data flows, a common data governance regime, and technology interoperability.

"Together democracies can seize the advantage and ensure a responsible vision for the technology future. This is why, we propose a Technology Alliance – a multilateral architecture for tech policy coordination."

MARTIJN RASSER

"Technology interoperability, common standards, and protocols would create more scale across the allied innovation ecosystem and also counter potentially harmful standards from authoritarian states."

REBECCA ARCESATI

"Countries have tools to protect advanced technology they deem critical. But they are stronger in concert."

SHIN OYA

DECOUPLING OR DELUSION? RETHINKING DEPENDENCIES IN TECHNOLOGICAL SUPPLY CHAINS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Sir Julian King** – European Commissioner for Security Union (2016–2019)
- **Izabela Albrycht** – Chair, The Kosciuszko Institute; President, Organising Committee of the European Cybersecurity Forum – CYBERSEC
- **Martijn Rasser** – Senior Fellow, Technology and National Security Program, Center for a New American Security (CNAS)
- **Ulf Pehrsson** – Vice President; Head of Government and Industry Relations, Ericsson
- **Richard Spearman** – Group Corporate Security Director, Vodafone
- Chaired by **Samir Saran** – President, Observer Research Foundation

RECOMMENDATIONS PREPARED BY SAMIR SARAN

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Although there was a growing political apprehension around technological supply chains pre-COVID-19, the pandemic has revealed and added to the anxieties on this front, and has also spurred conversations on 5G infrastructure and technology choices among private companies and government bodies. In this discussion, we focus on technological supply chain interdependencies, and the possibilities and implications of this new mood for "decoupling".

The pandemic has been a major disruptor of globalisation, highlighting the vulnerabilities and the chinks in the armour of this hyper-international network and globalisation itself. The increasing dependency on overseas manufacturing for many countries has proven to be a source of insecurity and strategic concern; and experts agree this is a good time to start thinking about decoupling, digital sovereignty and enhancing resilience. In the digital realm, there is an ever-growing threat of powerful governments offering efficient technologies packaged with regressive values and norms around data control and privacy. Given that data is a core building block of these times, it is crucial to think about how these interdependencies are going to affect economies, governments, and private citizens, particularly in light of the pandemic-induced mass migration onto the digital sphere. Global data flows could easily be compromised by injecting vulnerabilities into technological supply chains, allowing malicious suppliers to turn them into powerful surveillance apparatuses and cyber weapons that threaten national and individual security.

Thus, it is imperative during this period to discuss and decide upon the process of remapping the system, which now would be defined not only by the security of physical supply chains, like in the past, but also by the security of digital infrastructure and its autonomy, whilst also keeping in mind the series of challenges that it might pose.

MAIN THREATS & CHALLENGES:

- The discontinuation of the previously established supply links needs to be assessed thoroughly. As the world's manufacturing hub, China exerts tremendous control over global supply chains and aims to become a dominant player in all aspects of technology manufacturing. It poses a strategic dilemma for most countries – over the easy and affordable access to China's technological thought and its products versus the increase in Beijing's influence and its policy impact.
- The rise of surveillance capitalism and the spread of authoritarian surveillance technologies and values present a formidable challenge to the global state of freedom and civil society, especially in new emerging economies. Exports of invasive authoritarian tech could enhance the germination of surveillance societies and corrode fledgling democratic institutions. These political and security implications stemming from growing dependencies on such technologies have also propelled democratic countries to adopt more inward-looking state policies, with many preferring to close off open avenues of interaction, trade, and commerce. The specific exclusion of Chinese suppliers for 5G equipment in several countries is a case in point.
- While responding to these challenges, states should be weary of the trap of protectionism. The closure of national and regional economies should not be an answer as it will cause greater division and fragmentation of the global system, thus bringing us closer to the Splinternet.
- If states want to make changes to global supply chains, they need to assign adequate time for the decoupling process. They need to tread lightly as any sudden shift in the existing supply alignment could pose the risk of destabilising the entire system.

THE WAY FORWARD:

- Any attempts to decouple should ensure data security, including in the contexts of processing, gathering, transferring, and generating data. It is not enough to simply move away from previous suppliers. Baseline standards should also be envisaged and implemented to build trusted technological supply chains and robust data security frameworks, including through multi-lateral and multi-stakeholder cooperation. In attempts to build robust global value chains, the "value" should denote more than just the economic measure.
- No single government or company can handle the complexities that accompany this endeavour. Given that the old supply chain was rooted in global interconnectedness, a multilateral approach seems to be not only advisable but also necessary.
- Liberal democracies need to define the appropriate use of technology and provide emerging economies with affordable but secure alternatives to offerings of the authoritarian regimes that seem to increasingly develop and apply digital tools to suppress dissent and ensure regime continuity.
- While each country needs to keep its national obligations and values in mind while developing its policy agenda, it also needs to work hand-in-hand with the relevant industries involved. Though the technology sector has been dynamic and quite adept in dealing with the changing times and delivering on the evolving needs of society, it still requires the state to step in and assist with subsidies, investments in key areas, regulations, and restrictions on unfair competition.

- Governments might advocate for a tightening in security and a transfer of control over data from private companies, but such obligations are accompanied by additional costs and can change the prevailing economic model. The call for strict data localisation we are increasingly witnessing, which involves limits on cross-border data transfers, is an example of a policy measure that may benefit from further research and more careful consideration.
- A certain degree of decoupling in the next decade is probable. We might be heading towards a form of "gated globalisation" where cooperation between like-minded nations – rooted in shared values, common interests, and sometimes proximity – will define decisive criteria. As we create these new funnels and frameworks that will enable sustainable and safer trade and engagement, we have to be careful not to erect barriers lest we start resembling those we keep outside our gates.

"As countries become more inward looking (...), the Chinese offering of being able to control data, of being able to control the citizens, of being able to indulge in surveillance governance is very appealing. How do you counter that?"

SAMIR SARAN

"Decoupling is not only about the security of the supply chains, it is also about the security of digital infrastructure which includes processing, gathering, transferring, and – soon to be – generating massive amounts of data. And another vulnerability comes with the fact that all parts of digital infrastructure are dealing with data."

IZABELA ALBRYCHT

"There are some real risks to rapid decoupling and there is real risk to not thinking through the second order consequences in sufficient detail (...). The root cause for it is the fundamental shrinkage of the range of options available in the supply chain over the last 10 years. And that means that any change in the existing supply chain arrangements risk really destabilising supply chains overall."

RICHARD SPEARMAN

"Regional supply chains make all of the sense in the world (...), so yes, some decoupling but it's driven by business objectives."

ULF PEHRSSON

"I very much see that a multilateral approach to dealing with this issue is necessary. Not even the European Union on its own would be able to remap key supply chains."

MARTIJN RASSER

"That work that the Europeans are doing to build resilience, to push back against some of the negative features, involves a degree of decoupling but it doesn't necessarily mean embracing confrontation or bifurcation or absolute clean break."

SIR JULIAN KING

THEMATIC BLOCK: ELECTION SECURITY

SECURING THE INTEGRITY AND RESILIENCE OF ELECTION INFRASTRUCTURE #PROTECT2020

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PRESENTATION by **Bob Kolasky** – Assistant Director, National Risk Management Center, US Cybersecurity and Infrastructure Security Agency (CISA)

ONE STEP CLOSER TO A SECURE DIGITAL DEMOCRACY – DEFENDING ELECTIONS AGAINST HOSTILE INTERFERENCE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSIONwith the particiaption of:

- **David Carroll** – Associate Professor, Media Design, Parsons School for Design
- **Marietje Schaake** – International Policy Director, Cyber Policy Center, Stanford University; President, CyberPeace Institute
- **Jakub Turowski** – Head of Public Policy for Poland, Baltics, Romania, Bulgaria, Facebook

Chaired by **Michał Rekowski** – Director, Strategic Partnerships and Projects, The Kosciuszko Institute

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Elections are the backbone of democracy. In recent years, however, they have also become a prime target for adversaries trying to destabilise a number of them. Starting from 2016, we could have observed how electoral processes in democratic countries are subjected to adversarial actions carried out by malign foreign powers. With that process we could see how the very digital tools that we use on a daily basis in our lives, businesses, and social interactions are being weaponised to destabilise the electoral processes around the world. 2020 was not an exception and with key strategic votes taking place around the globe, election systems were put under an unprecedented level of pressure. Over the course of the US presidential elections, the Cybersecurity and Infrastructure Security Agency has been working tirelessly to ensure the democratic processes in the country are as resilient as possible. Bob Kolasky, Assistant Director at CISA explained the Agency's #PROTECT2020 plan created to prevent attacks against integrity and safety of the 2020 vote. Nevertheless, as the COVID-19 crisis prolongs, an increasing number of societies will be faced with a growing need to hold their elections via digital infrastructure. There is a global urgency to share best practices and refine existing solutions that stem from present experiences. Due to ever increasing and more sophisticated disinformation campaigns as well as growing concerns over the security of voting equipment and integrity of e-voting election systems, all stakeholders – state and private actors – should be able to effectively prevent such misconduct and protect their systems against it.

MAIN THREATS & CHALLENGES:

- Foreign interference is getting more frequent. In the past few years we have seen an increased interest in undermining democratic processes and elections all over the globe, also through cyber and hybrid means.
- The ongoing health crisis forced societies to adapt the election procedures by introducing precautions to mitigate the spread of the virus. This oftentimes meant moving parts of the process online, which created new vulnerabilities as a side effect.
- Rights of the people represented by democratically elected officials are under pressure by those who seek to manipulate, hack, or otherwise change the outcomes of the elections, oftentimes abusing vulnerabilities of the systems and infrastructure. Disinformation campaigns are a huge part of that strategy.
- In more complex electoral systems, infrastructure can be decentralised, thus showing significant differences between certain states, regions, and areas and making it hard to come up with universal security guidelines and schemes. Moreover, many local authorities are working with volunteers and on a low budget, which is also a big challenge to security and trust in elections.
- Disinformation surrounding electoral processes keeps growing and influencing voters and the media. Campaigns undermining legitimacy and trust in democratically elected officials are gaining more significance.
- Social media platforms which are used as tools to spread disinformation and misinformation have differing strategies on handling such content. Despite their efforts, monitoring suspicious activity and coordinated inauthentic behaviour along with quickly identifying and removing content that violates companies' policies is not a flawless system and requires many improvements.
- As a result of voter suppression and voter deterrent campaigns, machines and algorithms have the power to decide which votes matter and which will be supressed. Lack of accountability regarding targeted ads and political content poses a serious threat to democracy.

THE WAY FORWARD:

- Building public-private partnerships will allow to support election officials. Sharing tools and good practices with the ideas of trust, understanding, and common purpose in mind will make the elections more secure.
- Information sharing and incident reporting are key in responding to potential or ongoing attacks, incidents, and breaches. This should involve the entire community, as one vulnerability in one jurisdiction could easily spread across other places, causing a much greater damage to the system. Establishing networks such as the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) and collecting intelligence are essential in that.
- To mitigate the risks associated with voter registration databases and election management systems, particularly the Internet touching parts of the infrastructure, we need to invest in more secure systems, but also in training and knowledge. Making cybersecurity a central part of the procurement processes can have a significant effect on reducing cyber vulnerabilities.
- Defeating false narratives, particularly those spread on social media by bots and trolls is absolutely key in instilling trust and confidence in legitimacy of their elected representatives. Partnerships bringing together different levels of the public sector and the civil society will only strengthen the democracy as a whole.

- Partnerships and intelligence sharing should be extended to an international level, also through norms created by and respected in like-minded countries. Many governments all over the globe are dealing with similar threats, and standing together against the exploitation and foreign interference will bring better results for all.
- Creating a common set of cybersecurity criteria, one built on expert level knowledge, regularly stress-tested and updated, is essential to ensure that authorities can trust the system and rely on it.
- Independent oversight and scrutiny is a must. As we focus on foreign interference, we cannot forget about domestic threat actors who are also actively challenging election systems.
- Understanding how individual voters are targeted and how tech industry is interconnected with the advertising industry enabling one-to-one voter targeting is key to creating new regulations that are able to protect voters and citizens against targeted campaigns.
- Independent researchers need to have much more access to information to understand better, in the public interest, what happens under the hood of big technology platforms, especially in the context of how much power private companies are holding over the democratic process without any accountability and without much transparency into what is happening.

"Ultimately the point of election is not just for the voters to give their preference through the democratic processes, it's also for the electorate and the citizenry as a whole to have confidence that our leaders are legitimate and our leaders represent the will of the people."

BOB KOLASKY

"In the previous years, starting from 2016, we could have observed how electoral processes in democratic countries are subjected to adversarial actions carried out by malign foreign powers. (...) We could see how the very digital tools that we use on a daily basis in our lives, businesses and social interactions are being weaponised by malicious foreign actors to destabilise the electoral processes around the world."

MICHAŁ REKOWSKI

"Machines and algorithms are increasingly deciding which voters matter and which voters don't, and which voters will decide the election, and which will be suppressed and deterred from participating. Until we can create accountability to these technologies and tools it does threaten our basic confidence that every vote is counted, every vote is equal and every voter has been enabled to participate"

DAVID CARROLL

"It's been many years that we call (...) for more regulations. Is it the best case scenario that a private company has to choose on its own what is for instance a social ad, what is to be called a social issue? Of course not, and we would be more than happy to have more guidelines in the different countries where we operate."

JAKUB TUROWSKI

"It is very popular for Europeans to market-sell and celebrate the General Data Protection Regulation and I agree that it was a step in the right direction – but it did not in any way curb the outsized power of big tech companies."

MARIETJE SCHAAKE

4th CYBERSEC BRUSSELS LEADERS' FORESIGHT 2021

THE QUEST FOR EUROPE'S DIGITAL STRATEGIC AUTONOMY – WHERE AND HOW SHOULD IT LEAD?

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Bart Groothuis** – Member of the European Parliament
- **Tadeusz Chomicki** – Ambassador for Cyber & Tech Affairs, Security Policy Department, Polish Ministry of Foreign Affairs
- **Lorena Boix Alonso** – Director, Digital Society, Trust & Cybersecurity, DG CONNECT, European Commission
- **Luigi Rebuffi** – Secretary General and Founder, European Cyber Security Organisation
- **Līga Rozentāle** – Senior Director, European Cybersecurity Policy, Microsoft

Chaired by **Paul Timmers** – Research Associate, Oxford University; Professor, European University Cyprus

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Strategic Autonomy may be described as means to pursue and safeguard sovereignty; nevertheless, its concrete operationalisation remains elusive. In Europe, it is debated where the quest for European Strategic Autonomy should lead us and how it should be implemented. We are yet to define what is "strategic" in the European context. It is also a topic that is hotly debated in Brussels, the capitals of the EU Member States, Washington, and Beijing alike. Strategic Autonomy also has a digital and cybersecurity aspect to it. In the context of digital technologies, it indicates a capability to develop and master strategic technology systems, products, and services. How should strategic autonomy be implemented when looking at supply chains and digital procurement? Europe has plenty of resources that can be used in the quest for Digital Strategic Autonomy – in academia, start-ups, innovative companies, research centres. Recently, the EU has created its European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) that has the potential to significantly contribute to Europe's strategic autonomy in cyberspace. Usually, it is assumed that in most areas regarding cybersecurity less discussion and more action is recommended. However, in the case of the Digital Strategic Autonomy concept, thorough discussion is necessary, not only to understand what it stands for, but also to define how to operationalise it. Strategic Autonomy should be about building on our strengths and reducing weakness, rather than about excluding others from our endeavours.

MAIN THREATS & CHALLENGES:

- Europe's resources that could be used to build its Digital Strategic Autonomy. But these resources are fragmented and lack alignment and common mission. There is insufficient level of strategic and sustainable coordination and cooperation between industries, security research centres, and governments.

- Europe cannot manufacture and provide everything on its own – it has to work with external partners and buy from external vendors.

THE WAY FORWARD:

- Europe needs to decide what it perceives as "strategic", to be able to define what capabilities it has and understand what is missing in order to develop it.
- To build Digital Strategic Autonomy along with its cybersecurity component, Europe should look to three areas of action. First, build its own robust capacities, services, and infrastructures. It means investing in its cybersecurity operations centres and networking them but also creating a joint cyber unit that will be responding to threats. Second, create a strong regulatory framework in accordance with European values. It is important to have rules on products and knowledge regarding vendors and producers. Third, in the international dimension, it is key to apply the rules-based approach, including attribution and sanctions, but also to cooperate with like-minded partners who adhere to the same values. Europe should partner with actors that have a long-term interest in safeguarding values they share with the EU. The United States is the most fitting partner for Europe to jointly strengthen the industrial and technological leadership.
- Reinforcement of supply chains and working with companies that respect, implement, and protect European values is extremely important. In that respect, the technical requirements for equipment can be regulated by European law but are thus harder to operationalise. Cooperation with companies should be regularly verified in terms of whether they respect the principal values.
- External procurement should be analysed from a point of view of strategic autonomy that, whenever considering what and from whom to buy, acknowledges both what the European private sector is investing in and what the public administration perceives as trusted in the context of strategic interests of a given country or its alliances.
- In the context of cybersecurity, as it is a heavily private-sector oriented market, the pursuit of strategic autonomy should be done through public-private partnerships. Public decisions on new investments to build strategic autonomy should be taken in close cooperation with the private sector.
- The ECCC should contribute to the development of European capabilities in cyberspace through joint projects from various Member States and through engagement of a diverse group of stakeholders from both central and local administrations, industrial research centres, academia, NGOs, and the private sector. The ECCC should act as a platform that is both vertical and horizontal, to bring together and combine resources that we already have but that are fragmented.
- Europe has a potentially huge competitive advantage in industry-generated data. It should use the free flow of industrial data and consider ways to monetise the data that is being currently available inside the industries.

"There is a new situation in the transatlantic dimension – the change towards the Biden administration – and some people would say of course the United States is our natural ally (...). I want to ask you: what do you think about the transatlantic cooperation – in particular of course in strategic autonomy, but in particular in the view that perhaps in four years' time we will have another administration."

PAUL TIMMERS

"Whatever the administration plays, the race for technological supremacy is here to stay, it's a global race. And we would need to work together to mutually reinforce common priorities and common interests and values, and certainly a common interest is to have a secure cyberspace."

LORENA BOIX ALONSO

"We have values and these values are somehow dividing us or making us closer to some and less close to the others. In a long perspective, I personally believe that the values of the American administration and the values running Europe will be more or less aligned and similar."

TADEUSZ CHOMICKI

"The US and Europe together are in a minority globally when these issues are addressed at the UN level. So maintaining that partnership and respecting each other's sovereignty in that partnership is essential for looking at these issues from the aspect of promoting and protecting democracy."

LĪGA ROZENTĀLE

"We have the right to collectively defend ourselves and we have the right to collectively say we want collective countermeasures in Europe. We should be one block addressing hybrid threats, like a sovereign block addressing these hybrid threats with countermeasures, and that is something that should start in Europe but it doesn't have to end there."

BART GROOTHUIS

"I think the effort made by the European Commission and also by an organisation like ECSO, like the one I'm running, it could be very important in getting together the different stakeholders in defining what is strategic and reduce this kind of fragmentation, which could also lead to a dispersion of the limited resources we have."

LUIGI REBUFFI

DEFENCE STREAM

6th EUROPEAN CYBERSECURITY FORUM – CYBERSEC GLOBAL 2020

MISSION TO DEFEND GERMANY AND ITS ALLIES

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Annegret Kramp-Karrenbauer** – Federal Minister of Defence of Germany

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Today, and even more so in the future, all parts of society depend increasingly on our digital infrastructure, our militaries included. Digitalisation will have tremendous effects on the development of both our societies and tomorrow's battlefields. Cyberspace as an operational domain is becoming more and more important. As our security environment is highly dynamic and cyberattacks are getting more and more complex and dangerous, to build up resilience is becoming indispensable as a task for all civilian and military security providers. We understand resilience and digital sovereignty not in purely national terms, but rather in the context of NATO and the EU, as these institutions are the bedrock of Germany's security identity. Digital sovereignty, as we see it, includes five lines of action: using trustworthy IT, building up key technologies, maintaining core command and control capabilities, increasing innovation capabilities, and promoting digital competences in all of our citizens.

One important component of expanding digital sovereignty and of targeted technological development is to increase investment in research and innovation. The German Ministry of Defence has taken extensive steps towards this goal through the Cyber Innovation Hub of the Bundeswehr and the CODE Research Institute at the Bundeswehr University Munich, which are some of the assets we use to speed up innovation and to enhance the agility of defence. The Bundeswehr recognised the importance of digitalisation and cyber defence at an early stage. As early as in 2016, we established the directorate general for cyber IT at the Ministry of Defence. One year later, we set up the cyber and information domain service as a separate military service branch. This new branch, the CIDS, specialises in providing IT services in conducting reconnaissance in the cyber and information domain. It is responsible for the protection of our military networks, closely cooperates with other federal authorities, and contributes to the whole-of-government efforts to provide security in cyberspace. The CIDS also bundles our capabilities across the spectrum of operations in the cyber and information domain. We also aim to build digital resilience by strengthening the digital competences and the cyber defence capabilities of the armed forces of all EU member states. The Bundeswehr stands ready to fulfil its mission to defend Germany and our allies in all domains: land, air, sea, space, and cyber.

MAIN THREATS & CHALLENGES:

- The digital technologies of today have not been designed with security in mind. Cyberattacks on governments, state institutions, private businesses, hospitals, financial institutions, and citizens multiply and manifest in a plethora of forms. Only a small fraction of these attacks become public.

- We see a strong increase of aggressive cyber activity which is clearly driven by foreign state interests and despite the difficulties of tracing back and attributing specific attacks to individual governments, we know that Russia, China, and North Korea are major players in that field.
- Dependency on a limited number of individual manufacturers of ICT products and relying on monopolies can create serious limitations to our ability to act, in particular in relation to the military. Attacks targeted at the military could be conducted by hacking commercial service providers that the armed forces use. Such attacks may be carried out to gain access to military areas of operations, while criminally motivated attacks against shipping companies could impact the logistics – the supply lines of the armed forces.

THE WAY FORWARD:

- To prepare our military for the cyber threat environment, it is not enough to provide state-of-the-art IT security for our armed forces. We have to understand cyber as a new domain of military operations. A domain in which we need to protect ourselves, but which we also need to harness to further our own interests. For the military this is just as important as the rise of aircraft and the establishment of air forces as a military branch in the 20th century.
- Today, the mission of the armed forces to defend our societies reaches far beyond the traditional land, air, sea, and space domains and requires us to include the cyber domain. We need to understand the full context of cybersecurity incidents on a nationwide scale and to be able to see whether a specific incident is a technical problem, a criminal activity, or part of a concerted political or military attack scheme.
- If we want to protect our military information networks effectively, making a clean distinction between civilian and military information infrastructures is hardly possible. Not least because the military often uses civilian contractors in logistics and communications. Thus, to protect the military we also need to take into account the security of civilian information infrastructure.
- A new, whole-of-government approach is needed, established through close cooperation between the relevant ministries and institutions. This perspective has to include major private sector service providers, which are essential to developing the proper understanding of cyber challenges we need to address effectively.
- Expanding digital competences is crucial for building cyber resilience and strengthening digital sovereignty, nationally but also on the European level. Digital resilience and digital sovereignty should be pursued cooperatively within NATO and the European Union. We need to maintain and expand the EU's ability to act and jointly meet the opportunities and challenges of digitalisation and new technologies.

"As our security environment is highly dynamic and cyberattacks are getting more and more complex and dangerous, to build up resilience is becoming indispensable as a task for all civilian and military security providers. The Bundeswehr stands ready to fulfil its mission to defend Germany and our allies in all domains: land, air, sea, space, and cyber. Just as the motto of this conference demands: together against adversarial internet."

ANNEGRET KRAMP-KARRENBAUER

MILITARY USE OF 5G

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Riho Terras** – Member, European Parliament; Commander of the Estonian Defence Forces (2011–2018)
- **Joseph Evans** – Technical Director for 5G, United States Department of Defense
- **Nikodem Bończa-Tomaszewski** – CEO, Exatel

Chaired by **Teri Schultz** – Freelance Reporter, Deutsche Welle, NPR

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The critical geopolitical significance of the 5G deployment paved the way for complex discussions on its security and impact on the economy and society. However, the development of 5G has been dominated by the perspectives of essentially civilian businesses and industries. Often overlooked, the military sector should also hold a prominent place in the debates on strategic considerations related to 5G. Apart from the national security implications correlated to the security of the networks, 5G technology also has the potential to enable numerous military applications, particularly those that benefit from low latency and increased speed of data transfers. From command & control and IST (intelligence, surveillance, and acquisition) to autonomous and network vehicles to anti-hypersonic defence, 5G promises a potential to boost the efficiency of these systems. Nevertheless, 5G has been framed as an essentially commercial (civilian) technology and although it does have a dual-use nature, it was not designed as a military standard. Therefore, the military needs solutions that harness the potential of 5G and stay consistent with the security and operational requirements. The military once led innovation in digital technologies, but it lost track after the Internet was founded. Now it must look for ways to restore its technological primacy under a new formula of collaboration with the private sector. The US Department of Defence runs a programme aimed to accelerate both the technology and the security aspects of 5G and to hasten the technology application for the DoD purposes. On the other hand, in Poland a state-owned network company Exatel proposes a vision of a nation-wide 5G network that will be secured for, operated by, and available to both military and commercial entities. While those visions vary, it remains clear that 5G technology requires huge investments and therefore the military has to align with the industry in further development of R&D in key aspects of 5G.

MAIN THREATS & CHALLENGES:

- Due to an incremental rise in the number of connected devices and services, the 5G roll-out increases the scope of digital vulnerabilities. As a plethora of solutions in 5G will be software-defined, it will introduce more opportunities for cyber mischief.
- The threat associated with the inclusion of high-risk vendors is real and should not be downplayed. None should use communications equipment provided by manufacturers or operators that are not trustworthy. In some countries commercial entities are legally obliged to cooperate with the state's security services, also in terms of gathering of external data and intelligence. It is reasonable to assume that they do comply with these provisions.

- In Europe, many commercial networks were constructed with the use of equipment from vendors considered to be untrustworthy.
- Due to the reliance on physical infrastructure, 5G is prone to signal disruption, interception, and manipulation. There is a need to introduce back-up systems in critical environments. This is crucial especially in battlefield management.

THE WAY FORWARD:

- It is fundamental to overcome the silos and separation between civilian and military domains in investments, development, cooperation, and application of the 5G technology.
- 5G is promising in regard to protection of military infrastructure, military training, and anti-hypersonic defence systems.
- Ideally, unmanned vehicles should not require receiving large amounts of data as they perform operational tasks. Depending on their level of autonomy, they should operate on the basis on short, concise communications. For that, deployment of 5G is not critical.
- The military has to consider how to deploy in environments where telecom equipment from untrustworthy or adversarial vendors is installed in the communications networks. Armed forces have to ensure that they remain operational and such conditions won't limit the scope of their actions.
- There are already reliable commercial solutions that can be used by the military. In relatively low-risk types of applications, the military can rely on the private vendors and should work hand-in-hand with them to identify and address the gaps between what is offered on the market and what are the needs of specific defence entities.
- With the introduction of the 5G, there emerges a need for a new cybersecurity approach that will not be based on security perimeters but will be looking at security throughout the network and throughout the protocol stack. It should combine encryption and key management techniques and network slicing for better separation within the network.
- Promotion and adoption of open standards is crucial for understanding of what is in the network. It is indispensable for the ability to conduct security evaluations and risk mitigation.

"When you look at the fact that military adversaries will be definitely exploiting it to its fullest potential don't you need to keep up? I mean, isn't that some of the problem here that Europe has definitely acknowledged – that it didn't put enough funding (...) into European systems?"

TERI SCHULTZ

"Military needs to use it, military must use it, we must find ways how to use it, otherwise we will lose again. But on the other hand, this technology is not meant to be military and the handicap of it is the security of the network."

RIHO TERRAS

"What we're doing is working with folks in industry to identify where the gaps are between what they're offering in terms of commercial offerings and what we need for different DoD use cases. And then investing in projects and programs to try to close that gap in order to provide the security we need."

JOSEPH EVANS

"We are looking at the cyberspace as a whole that you have to protect and where the future war will be touching everybody. So creating a separate military or internal security network, 5G network for example, only for the military use, would be not a good solution in this matter."

NIKODEM BOŃCZA-TOMASZEWSKI

INFORMATION WARFARE: EXPLOITATION OF HISTORY, RELIGION, AND ECONOMICS IN CYBERSPACE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Artis Pabriks** – Deputy Prime Minister, Minister of Defence of the Republic of Latvia
- **Jaroslav Nad'** – Minister of Defence of the Slovak Republic

Chaired by **Col. Martin Achimovič** – Director of the NATO Counter Intelligence Centre of Excellence

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Modern technologies and the Internet have made it possible to disseminate information in near real-time, resulting in the public being inundated with information, and it is challenging to separate false information from facts. Modern technologies have made it possible to easily spread "fake news" propaganda, which various actors use to influence populations and generate conflict. The Internet and social media have become not only platforms for gaining knowledge about the world around us and fora for exchanging views, but are also battlefields for ideas and opinions. The enemies are not tanks, planes, or armed soldiers but human minds and agendas. Information warfare has become an integral part of conflict.

Information warfare is an instrument that fundamentally changes the art and science of conflict; it employs information as the bombs and bullets used in today's battles for hearts and minds. Data, communications technology, and infrastructure in the global information network are used as effective offensive weapons. Access to these weapons is universal, making them available to individuals, professional groups, nation states, and national, ethnic, and religious organisations. Specialised state and private sector entities, armed forces, criminal organisations, terrorists, mercenaries, etc., have incorporated aspects of information warfare in their activities.

Information warfare is a complex set of measures that are not limited to one nation or another. Use of such tactics extends beyond physical territories and boundaries with consequences regardless of geographic location. Nations respond to growing cyber threats by building national cyber centres and specialised units to protect their national interests, developing information-gathering tools to identify and counteract disinformation. Some countries go much further and restrict internet access to "secure" their citizens. At the beginning of the new decade we can expect that the information warfare will continue to change its character and that of the overall security environment.

MAIN THREATS & CHALLENGES:

- Even though modern social media outlets are used in the information operations, in the minds of many people they do not fall under the same restrictions or are not perceived as tools having the ability to cause real harm. We have many new technologies and many countries that are increasingly using these modern technologies and fighting for users, but we still rely on the old understanding of war based on examples from the past.
- Thanks to social media, many matters of daily life have become much easier and more accessible. However, their dark side allows disinformation to spread like wildfire, which can be used to promote

damaging and illicit agendas. At the same time many countries do not react quickly enough to disinformation due to inexperience and lack of preparation.

- Democratic countries tend to adopt a more open attitude towards social media, where media can freely criticise their government. In regimes with strong state's control, the media is strictly and deeply integrated into the information warfare in its modern understanding.
- Thanks to algorithms underpinning internet platforms, people looking for news and information remain in their "bubble" of preferred ideas, thus threatening to create radicalised and divided society. The difference between disseminating disinformation and presenting alternative views is often indistinguishable.

THE WAY FORWARD:

- It is essential to raise public awareness on disinformation and counter its effects as well as to build social resilience by reacting in real-time through provision of the verified information and evidence indicating the false or misleading character of the communication in questions.
- NATO member states should not employ disinformation as a weapon. The aim of disinformation is to raise doubts that will eventually make intersubjective facts unbelievable. The way forward for the democratic societies is to fight disinformation, not to spread it.
- There are two approaches to counteract disinformation: proactive (preventive) and reactive. Both approaches should be developed and widely used. The reactive way involves fighting false information (myth busting) that has already been introduced and may have taken hold in the community. It requires a combined approach of many institutions and coordination between state organisations, NGOs, and media. The preventive approach is strategic communication. It is about informing society in advance about critical decisions and activities through digital and traditional media, in order to leave little or no space for disinformation agents to operate or be effective.
- Social media providers have their own social responsibility, and they must be transparent with their system algorithms to ensure that we can effectively respond to false information; otherwise, they may be viewed as biased platforms pursuing their own agendas.
- We need to work on new regulations and raise the awareness among social media companies. They need to fully understand the vulnerability of modern societies and modern states, and focus on how they can objectively help people receive useful information to avoid a fragmented society.
- NATO countries should deepen their cooperation and contribute to joint projects aimed to develop tools to combat the effects of information warfare. One result of this cooperation is a network of the Centres of Excellence, are NATO think-thanks increasing the allies' defence capabilities, working on new standards and preparing personnel for emerging and future challenges, including those related to information warfare.

"Distraction, misinformation, deception, being a pretender... These always have been a part of warfare, not only modern warfare because these people who control minds, those people who can make an impression, they also have a large chance to win or at least not to lose. Examples of Sun Tzu, Clausewitz, or even Japanese martial arts expert Miyamoto Musashi are always of great help. The difference between those days and today obviously is not the changes in use of misinformation but rather an appearance of a number of new weaponry. It's just like the invention of nuclear bomb at the end of the Second World War changed the pattern of how people were thinking about possible Third World War or next tensions. The modern social media are those new weapons which are at this moment still in the minds of many people not falling under the restrictions of old regulations, and that's the difference."

ARTIS PABRIKS

"One of the goals of information warfare is to plant a seed of doubt, and we should not use that because if these doubts exist and grow, then at the end of the day, we can doubt everything. Our goal now, our adequate role, is to fight against disinformation, not to spread disinformation. It is a very short game. At the end of the day the truth comes out and we need to focus on the next step, not to see only a few things in front of us. We're talking about democracy, we're talking about human rights, we're talking about values, and even if we try to change regime or to change the politics somewhere we shouldn't use this tool because it's something that will not work in a longer period of time."

JAROSLAV NAĎ

"The internet has enabled a capacity to distribute information in near real time, compared to the past when information was spread by leaders with little or no independent verification. From information warfare perspective, the society is now inundated with information and it has become very hard to separate fake information from real facts."

COL. MARTIN ACHIMOVIČ

FORWARD DEFENCE POSTURES IN DEVELOPING CYBERSECURITY CAPABILITIES

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Anna Fotyga** – Member, European Parliament; Member, NATO Reflection Group
- **BG Karol Molenda** – Director, National Cyber Security Centre of Poland
- **Rob Joyce** – Special US Liaison Officer, London
- **MG (Ret.) Brett Williams** – Director of Operations, United States Cyber Command (2012–2014); Co-Founder, COO, IronNet Cybersecurity

Chaired by **Amir Rapaport** – Founder & Editor-in-Chief of Cybertech and Israel Defense

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The cyber realm and the physical realm are merging together to the point where it is not feasible any longer to consider threats in one realm without considering the ramifications in another. We have yet to fully conceive how it affects and transforms certain characteristics of war and conflict. Much like when airspace was operationalised as a warfighting domain, the changed aspects of warfare in cyberspace can be recognised in terms of compressed time, space, and distance.

The challenges of the cyberspace require the armed forces to present the range of capabilities and forces both defensive and offensive to conduct the full spectrum of cyber operations, all of which must be executed within a strong legal framework and under significant political oversight. The thin line distinguishing "offensive operations" from "attacks" is also raising sensitive questions: can an attack be seen as a defensive measure? And what if is required for efficient cyber defence? To reflect on the consequences of these considerations is critical in order to be able to protect our societies and institutions against increasingly persistent adversarial operations. While responding to cyberattacks should states resort to means and instruments beyond the cyber (diplomatic, economic, military) to retain a full spectrum of options? And how to scale up the defences through allied cooperation? Collective defence in cybersecurity is recognised by NATO and the EU as a priority and a primary area of cooperation, but in both cases the capabilities themselves remain with the nation states – how can they contribute to a collective resilience?

MAIN THREATS & CHALLENGES:

- Rapid evolution of cyber capabilities has opened new doors for malicious state and non-state actors to influence and abuse cyberspace in order to weaken democratic institutions or gain economical, diplomatic, or military advantages. Not only are such attacks becoming more complex but also more common. What is more, they are being continuously fine-tuned so that they do not reach the threshold of an armed attack, leaving the target state perplexed.
- Our adversaries are continually resorting to cyber and cyber combined with physical operations to threaten and degrade the security of our societies and institutions. They are not only doing it in times of war, but also initiate conflicts below the threshold of war and constantly probe our systems, trying to get positioned, trying to understand how to generate harmful or threatening effects against us that create a tactical difference in cyberspace.

- The rise of cyberwarfare forces the defence community in the United States to reflect on its entire strategic outlook and vulnerabilities. Contrary to the experiences in air, sea, and land warfare, where the US has mainly projected its power to the far corners of the world, a strategic conflict with a near-peer adversary in cyberspace brings a very high possibility of the initial attacks been carried out against the American civilian population.
- Cyberspace favours the offender, as contrary to the defender – which is constrained by the rules of conduct, limited capabilities, and the pressure on the rate of efficiency. The attackers have a wide range of tools at their disposal and in theory they only have to succeed once while trying to break through the defences.

THE WAY FORWARD:

- When we think about offensive cyber operations, we relate to activities in cyberspace that project power to create effects which achieve military objectives. But it is critical to remember that the vulnerability that we intend to explore to mount a successful attack will become known to others and that the cyberweapon we develop can be stolen, copied, or reused, even against its initial creators. For this reason it is essential to strive to develop precision within our operational capabilities in cyberspace. It is absolutely crucial to escalation dominance and proper strategic signalling to the adversary. A failure to deliver on precisely targeted operations might jeopardise not only the success of an operation but also the credibility of the entire endeavour.
- As strategy of persistent engagements is an integral part of efficient cyber defence strategy. It is critical to be able to defend forward – to go out towards the adversaries and deny them their tools, their infrastructure, their trade craft. They need to be forced not only to stop their malicious operations, but also to retool. This is a work towards a goal where the adversaries no longer consider cyber to be their preferred method. As their attacks are being rendered ineffective we are able to efficiently contest the space of conflict.
- Once disclosed or discovered, it is important to share understanding of specific capabilities of the adversaries with our allies, capable cyber sector, and the public.
- The idea of collective defence underpinning NATO has to be extended to cyberspace further. NATO is still preparing to use the SCEPVA – Sovereign Cyber Effects Provided Voluntarily by Allies – process, which seems like an elegant solution given that NATO does not have its own cyber capabilities. More unanimity, synchronisation, and decisive steps in that direction are needed.
- Cyber is a domain of collaboration between the EU and NATO and there is a necessity to enrich this collaboration and strengthen resilience together. More discussion is needed on the clear division of work between the two but also on more use of tools at the EU disposal and tools predominantly in the civilian areas, like academia, business, or the NGOs, including the cybersecurity of civilian infrastructure, which in time of war would have to be used by military.
- Governments, commercial industry, and like-minded countries need to all come together to bring the power that they all each wield uniquely to figure out where to go from here. The partnership between the public sector and the private sector is critical as we can't look at cyberspace in isolation – there's much more of a civilian than military dimension to it.

"We understand that it's really important to defend your networks and it's very important to do the basics, right – the hygiene, the patching, the configuration, the maintenance. But that's not enough. It's not enough to have a good boundary. You've got to have the ability to frustrate your adversaries."

ROB JOYCE

"From malware attacks to meddling in domestic affairs and democratic processes – the cyber battlefield actually doesn't look, in any way, like the traditional warfare"

AMIR RAPPAPORT

"The alliance will benefit from cyber effects provided by nations in accordance with the legal and political principles agreed by the North Atlantic Council. They thought that there is the reason why they introduced the sovereign cyber effects provided voluntarily by allies – this process, which provides the required cyber support, is translated into cyber effects."

KAROL MOLENDA

"As much as the US government has a significant role in defending the nation in cyberspace, it really is the private sector, it's the civilians that are on the front lines. They're the ones that run all of the critical infrastructure."

BRETT WILLIAMS

"With new technologies, big data, artificial intelligence, quantum computing, all these issues, we probably have a better chance to attribute attacks. It was and still is the problem of EU member states, of NATO and organisations to (...) precisely quickly attribute attacks and therefore, I think, that keeping technological edge is extremely important also from this point of view."

ANNA FOTYGA

AT THE FOREFRONT OF INNOVATION – NATO'S APPROACH TOWARDS SCIENCE & TECHNOLOGY

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

FIRESIDE CHAT with **Bryan Wells** – Chief Scientist, NATO
Chaired by: **Edward Christie** – Deputy Head, Innovation Unit, Emerging Security Challenges Division, NATO

BIG PICTURE – WHY THIS TOPIC MATTERS

Emerging and disruptive technologies constitute the major game changers in the international struggle for power, particularly between the US and China. But technology of the future which is impacting the warfare potential, presents the most considerable challenges to the security and defence not only of nation states but also the Transatlantic Alliance. These challenges are hard to tackle by governments themselves, because majority of innovation has its origins in the private sector, exactly where the majority of technological capabilities and digital infrastructure is also rooted. Additional difficulty lies in the fact that modern technologies are driven by the civil sector, rather than the defence sector. It results in a significant separation of science and technology from national security agendas and problematic dependencies of the market for a number of cutting-edge technologies which are invaluable for the security, military excellence and effectiveness of states. NATO as a defence Alliance is recognising those changes and the need of adaptation to maintain its technological edge. At the same time the cyberspace and lately the outer space have become new operational domains which were recognised as such by NATO in 2016 and 2019 respectively and give a multitude of possibilities to project power. Certainly, due to the technology advancements, NATO had to add domains faster than ever in its history which is creating an inter-domain battlefield challenges to deal with. It is also facing the challenges of interconnections between new technologies forcing a more dynamic pace of innovation. On the other end of this value chain, Alliance's interoperability is at stake. Mitigation of risks that are inherent to different levels of technological achievements overall and different capability levels between Allies is incredibly important.

MAIN THREATS & CHALLENGES:

- Threats deriving from the new technology landscape are linked to the fact that the civil investment massively outspends defence investment and that many responsibilities traditionally linked with states are now dependent on the innovation created by the civil sector. An additional factor of change relates to the reality of many technologies getting cheaper, more easily obtainable by many countries and non-states actors, and easier to use. So, the readiness and easy availability of these technologies can be an opportunity but also a threat, in the sense they could be used against us.
- The unique character of EDTs derives from their combination of technologies that are the principal game changers in the modern technology and principal triggers of the changes in the security landscape. Used together: machine learning, big data, and autonomy – have the power to make the real breakthroughs for the Alliance, but equally so for our potential adversaries. This is why NATO needs to be able to know how it can defend itself against them.

- Some new technological developments or forthcoming potential developments may prove disruptive in cyberspace with respect to either cyberdefence in a traditional sense or cybersecurity more broadly. It's the only non-physical domain and that brings with it a number of unique characteristics. Cyber is also the probably single area where the concept of technology readiness levels really doesn't hold so we can expect disruptive and often unpredictable developments in this domain.

THE WAY FORWARD:

- NATO has a number of strengths to deal with EDTs challenges with implications for defence that it can use to its advantage. It includes a scientific base of 18 of the top 20 universities in the world, Science and Technology Organization, which networks over 6,500 scientists in allied nations and has 300 ongoing research projects, from which around 200 are directly related to emerging and disruptive technologies.
- In respect of science and innovative contribution, there should be a very good representation across all allies because each ally can bring its own particular added value and its strengths. NATO should also make sure to have some very good contribution from partner countries as well.
- NATO should build on its research strengths to provide capabilities but also, with horizon scanning, offer the strategic foresight into the future and emerging trends, and constantly look at the forward programme relevant to its allies and partners. NATO should also be able to provide the advice on some very complex EDTs issues, which are of the great value to nation states in putting forward their own ways to respond to them and mobilise their domestic resources to level up their technology readiness in a timely way.
- NATO should be able to perform the well-informed prioritisation of the challenges in the security areas and consequently the defence related research and innovation ambitions of the Alliance. In this respect, NATO is also looking at a higher pace of innovation and keeping interoperability especially in terms of different pieces of equipment underpinned by the emerging and disruptive technologies. Right from the outset, it is at the core of a number of the research projects that the NATO Science and Technology Organization pursue.
- NATO should keep abreast of civil developments, using its good rapport with the European Union and its associated bodies, which fund a huge amount of civil research. We need to keep the open and actionable NATO-EU political dialogue around technology trends which is mutually beneficial.
- Another important security dimension is cyberspace and cyber readiness posture, which should be upgraded on the part of NATO, with cyber diplomacy, and a use of cyber tools to combat misinformation and disinformation, and advanced tools making a good use of EDTs such as for instance deep machine learning for cyber defence or cyber monitoring as a means of event detection and building cyber physical resilience in the NATO operations.

"It is very noticeable how modern technologies are very much driven by the civil sector, rather than the defence sector. We've only got to think of autonomy of data science, etc. – these are areas where civil investment massively outspends defence investment."

BRYAN WELLS

CYBERSECURITY OF OUTER SPACE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Carine Claeys** – EU Special Envoy for Space; Head of the Space Task Force, EEAS
- **Kfir Damari** – Co-founder, SpaceIL
- **Brig Gen (Ret) Robert Spalding** – Senior Fellow, Hudson Institute; Senior Director for Strategy in President Trump Administration (2017–2018)
- **Sarah Brown** – Senior Scientist, Capability Development Branch, NATO Cyber Security Centre

Chaired by **Sorin Ducaru** – Director, European Union Satellite Centre (SatCen); Assistant Secretary General for Emerging Security Challenges, NATO (2013–2017)

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Last years have been pivotal to outer space. In 2015 we saw the consensual agreement on a set of norms and confidence building measures (CBMs) has been developed regionally and in the OSCE framework. During the London Summit of 2019, NATO has declared space to be the operational domain. Also in 2019, Guidelines for the Long-Term Sustainability of Outer Space Activities have been adopted. And 2020 brought the US Space Policy Directive 5, centred around cybersecurity of space assets.

There is a lot of intertwining between space and cyberspace. Both domains are key enablers for all others (land, air, sea) and also cyberspace is a central enabler for space as the outer space assets depend on ICTs and process high value data that powers many civilian and military activities. All of the six space-dependent capabilities used by NATO – from position, navigation, and timing (PNT) to missile defence – rely heavily on digital technologies and cybersecurity measures. Also, national space systems must be considered critical infrastructure, as both nations and NATO rely on them for their commercial and military endeavours across all other domains. However, many of the currently operational space assets were designed in the past, when space systems have been considered to be relatively safe from cyberthreats due to their sole connection to protected ground infrastructure that is air-gapped and isolated. For this reason historical concerns about the cybersecurity of space assets were focused on jamming, spoofing, and other elements of electronic warfare, until Stuxnet forced us to rethink our understanding of the cybersecurity of these systems. With the progressive commercialisation and democratisation of outer space that puts on the orbit devices that are increasingly software-defined, and with the growing militarisation of space that reinforces the role of state actors as potential threats to space-based systems, an urgent need arises not only to enhance and cybersecurity of space assets but also to re-think and re-design national and allied space policies in the new era of great powers' competition.

MAIN THREATS & CHALLENGES:

- Space is already a contested domain. Our reliance on space assets for key functionalities makes space-based systems a critical infrastructure. This fact, combined with the currently observed rise of geopolitical rivalry in space provides for a rapid growth of threats to our space systems. The concepts of how to attack satellites and satellite-based communication systems multiply, with some states performing demonstrations of Anti-Satellite Weapons on their own systems and other actively undertaking to jam satellite communications of their competitors.

- States may be motivated to conduct attacks on space systems for a variety of reasons and through multiple ways. In sabotage, the attackers might aim to disrupt or destroy the networks that serve as a critical infrastructure and a cost of such an attack can be enormous, both from a financial and military perspective. On the other hand, in espionage, attackers might be motivated to steal information either for industrial purposes or for political reasons, or to gain unauthorised access to sensitive diplomatic intelligence or military technology.
- The avenues for cyberattack at space systems have been found in ground station terminals that provide a direct link to a satellite but are not protected by strong authentication or are running software that's not regularly patched or upgraded. Avenues for attack also exist in newer satellites that often run on software-defined functionalities for reprogramming in orbit. Another avenue of attack lies in the supply chain for satellite components, which are integrated into complex systems.
- Another area of vulnerability arises from an increasing number of satellite data exchange interfaces that are used between the military and civil sectors. For applications such as GPS, the existence of dual-purpose technologies brings in a risk that they can be claimed by attackers to be legitimate military targets.

THE WAY FORWARD:

- In regard to the traditional IT networks, an in-depth defence strategy that touches on the supply chain security controls on each part of the system of the architecture – the space, the ground, the link, and the user – is a useful approach. There are many other useful frameworks that can serve as a point of reference in regard to cybersecurity of space.
- Space Policy Directive 5, released in the US in 2020, provides key principles that should be followed. Software development, intrusion detection, and staff awareness are all key areas where cybersecurity control must be applied and that are key for this critical infrastructure sector. Hardware and software should be developed and operated using risk-based cybersecurity informed engineering approach. Operators and automated control centres must be able to retain or recover positive control of space vehicles and verify the integrity, confidentiality, and availability of critical functions.
- Cybersecurity requirements and regulations should leverage widely adopted best practices of norms and behaviours. Space systems security requirements should manage the appropriate risk tolerances and manage and minimise undue burden to civil and commercial partners.
- The MITRE ATT&CK framework provides a detailed categorisation of the tactics, techniques, and procedures used by the most sophisticated attacker groups operating today. It allows pen-testers to emulate the behaviour of an engagement to represent real world scenarios and help their customers determine the effectiveness of defensive countermeasures.
- Also worth considering is the ISAC model, based on sector-specific information sharing and analysis. The Information Sharing and Analysis Centres (ISACs) collect, analyse, and disseminate threat information to their members and provide them with appropriate tools to mitigate risks and enhance resilience. A public-private partnership in the form of an ISAC space community would be a mechanism to foster sharing of threats as well as best practices and this would collectively bring mature cybersecurity practices to the space domain.

- It is important for space organisations and space providers to understand the risk of the insecure supply chains. They should take effort to invest in security of the components they use and work only with trusted partners and vendors. The alternative cost of designing insecure systems is much higher. They need to understand ramifications of the risk of not taking the time to prioritise security of the supply chain. It is a culture and mindset change that's needed. It is also key to think about designing space systems with cybersecurity as a chief concern.
- Each supplier of components along the space value chain must be validated as a trusted supplier for a national critical infrastructure program. Any components must be integrated in a way that a compromise on one component does not lead to a compromise of the entire system.
- NATO and member states should deepen their understanding of the technical threats to space systems from the denial of service to data loss and malicious data corruption and exfiltration in the traditional IT environment. A threat-informed approach is essential to proactively protecting and defending against cyber threats.
- NATO does not own space assets and relies in that respect on the services and systems of its member states. As such, it is in an ideal position to encourage and promote amongst them mature policy, best practices, norms and standards that ensure a minimum level of cybersecurity maturity across NATO in the space domain. NATO could also encourage nations to develop common guidelines and coordinate in critical areas of cybersecurity of space with leading US space organisations and standards bodies, such as NIST or CISA.
- For effective multilateralism and effective global governance, the international order is geared to be based on three main pillars: 1) application of the international law to cyber space; 2) development of norms of responsible state behaviour; 3) capacity building as a means to strengthen global resilience in an increasingly interconnected world.

"There is a number of issues where there is an increasing recognition that space is going to be a much more crowded place, data is going to feature heavily in space and the need to ensure that the systems and the data is all kept secure are part of the fabric of the 21st century."

GEN. ROBERT SPALDING

"What comes immediately to mind is whether the normal approach that we would take on cybersecurity (...) in other domains is enough or whether there should be some special approach, some special prioritisation related to the cybersecurity of the space assets."

SORIN DUCARU

"We have to keep pace with an increasing complex threat landscape which will not only consist of isolated cyber campaign but also hybrid scenarios below the threshold of a real crisis that might seek to exploit any internal weakness."

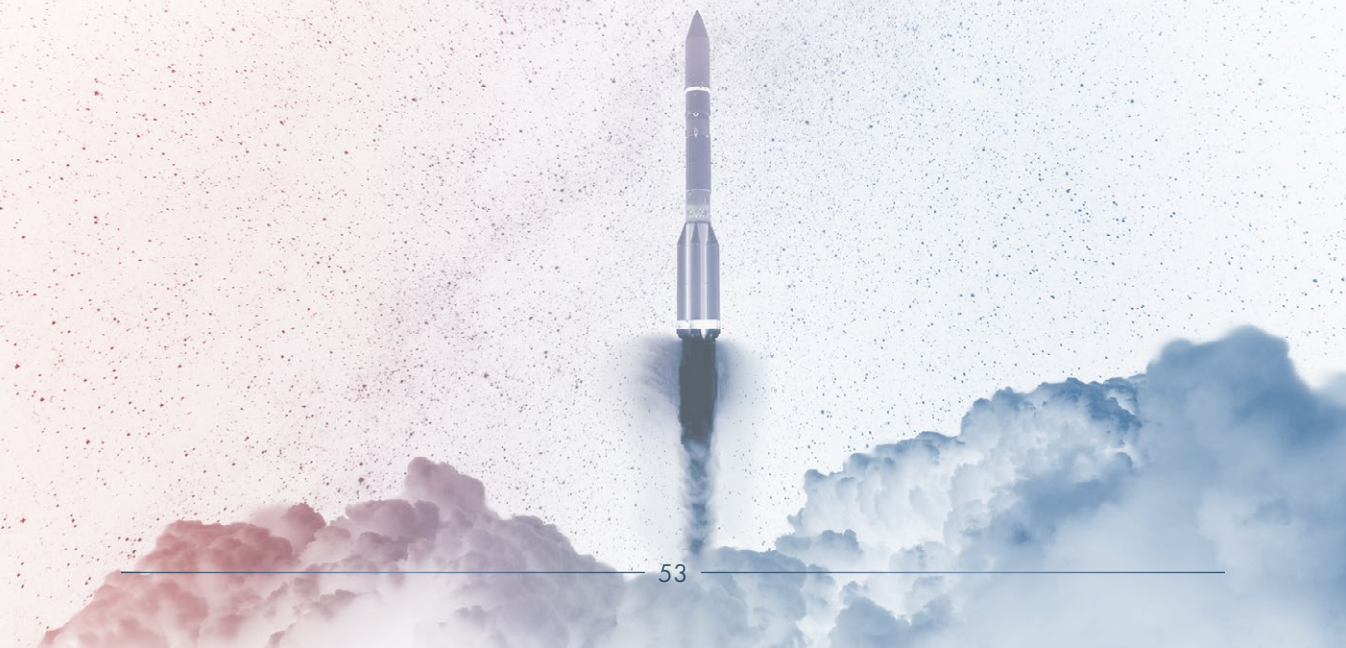
CARINE CLAEYS

"I think one of the crucial things is not just create awareness but educate this new space industry and make them realise from the moment they start that cybersecurity is something that they have to have in their minds all along."

KAFIR DAMARI

"Our dependence on space for communication and situational awareness activities combined with the increasing geopolitical tensions translate to an ever increasing threat to attack on the systems."

SARAH BROWN



4th CYBERSEC BRUSSELS LEADERS' FORESIGHT 2021

TRANSATLANTIC ALLIANCE: CLICK REFRESH. MAKING TECHNOLOGY COOPERATION CENTRAL TO OUR SHARED DEMOCRATIC FUTURE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Mircea Geoană** – Deputy Secretary General, NATO

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

New technologies are changing and reshaping not just our lives but also the art of warfare and global competition between countries and the very definition of security. Transatlantic community's dominance in technology and its competitive edge are aggressively challenged by nations that do not share the values of human rights and adherence to international law. Rapid developments in cyberspace and emergence of new technologies are important dimensions of the process of rebooting the transatlantic relationship. Putting technology and cybersecurity cooperation at the heart of the transatlantic community and cooperation among like-minded nations will be essential for our shared democratic future.

NATO needs to expand its ability to keep one billion citizens in NATO nations safe by maintaining its technological edge. Alliance has to also become future proof to make sure that it remains ready to tackle also tomorrow's threats.

MAIN THREATS & CHALLENGES:

- NATO is at risk of being outpaced or outgunned by Russia and China in the field of technological advances which are now happening at lightning speed. It requires NATO to move faster, at the speed of relevance, not at the speed of bureaucratic approval, in understanding, developing, and adopting new technologies.
- Keeping the interoperability of new technologies on both sides of the Atlantic is another challenge for NATO and key ingredient for the enduring success of Alliance.
- NATO needs to strengthen the framework of collaboration with the private sector because the game changing innovations are not driven by the governments anymore but mostly by the civilian private sector and innovative start-ups, and retain their dual-use potential.
- The lines between civil and military, conflict and non-conflict, peace and war, Article 5 and non-Article 5 are now more and more blurred and we need to have an accurate framework to react on security incidents with right attribution and adequate toolkit of responses.

THE WAY FORWARD:

- NATO has to narrow down technological effort and look to technologies which are the most impactful for NATO security and follow the coherent strategy for implementing the roadmap for EDTs.
- NATO has to foster development of new technologies hand in hand with protecting them from potential adversaries and competitors to mitigate the risks they pose.
- NATO Defence Innovation Initiative is a useful platform to catalyse the transatlantic cooperation and ensuring Allies' ability to operate together.
- NATO should enhance its role in Allied innovation ecosystems, adapting its operating procedures, working much more closely in the triple helix model engaging governments and public sector, industry and private sector, as well as academia and think tanks.
- Leveraging the comparative advantages and looking for synergies across 30 nations is crucial, as is utilising an abundance of world-class academic institutions, the finest scientific researchers and innovative start-ups from Silicon Valley to Central and Eastern Europe. Allies should consider new ways of cooperation with the civilian private sector, innovative and agile forms of financing EDTs, including venture capital.
- Concrete ways for cooperation with like-minded partners should be introduced, also outside of NATO, which may include UN specialised bodies and agencies as well as the OECD, and the EU to strengthen and protect the defence industrial base and foster the right regulatory environment for emerging technologies.
- Embedding democratic principles, values, standards shared across NATO into a system of global governance on new technologies from its very inception is essential.
- NATO's innovations should be protected from adversarial and illicit technology transfers, reducing vulnerabilities in our critical infrastructure and industries and increasing our resilience, including to cyberattacks.
- It is crucial to strengthen deterrence and defence in the new technological age, including a reaction on destabilising and malicious activities and efforts to uphold the international laws and norms of responsible behaviour in cyberspace. We should build NATO's capacity by integrating national cyber effects into Alliance operations and missions, fulfilling the cyber defence pledge, and ensuring all Allies continue to strengthen their national networks and infrastructures.
- NATO has to become a global driver of a values-based approach to defence innovation, to make sure that global rules and norms are shaped by our values: freedom, democracy, the rule of law.

"We must avoid the innovation gap and instead leverage the comparative advantage that NATO has as an Alliance. Together, our 30 nations have an abundance of world-class academic institutions; the finest scientific researchers and yes, including from Central and Eastern Europe, innovative start-ups. There is huge potential for synergies across the Euro-Atlantic area, from Silicon Valley to Central and Eastern Europe."

MIRCEA GEOANA

TRANSATLANTIC ALLIANCE: CLICK REFRESH. MAKING TECHNOLOGY COOPERATION CENTRAL TO OUR SHARED DEMOCRATIC FUTURE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Miapetra Kumpula-Natri** – Vice-Chair, Delegation for relations with the United States, European Parliament
- **Joanneke Balfoort** – Director, Security and Defence Policy, European External Action Service
- **Prof. Deeph Chana** – Chair of the EDT NATO's Advisory Group; Professor of Practice, Imperial College Business School; Co-Director, Institute for Security Science and Technology
- **Prof. Philip Lark** – Program Director, George C. Marshall European Center for Security Studies
- **Marta Pośład** – Head, CEE & Transatlantic Public Policy, Google

Chaired by **Beyza Unal** – Deputy Director, International Security Programme, Chatham House

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Since the online is the new frontline, the digital domain has become for Europe the key priority for engagement with its allies, particularly with the United States. We face common challenges related to critical infrastructure issues like 5G or cybersecurity, which are essential for our security, sovereignty, and prosperity. We can also see existing and growing threats when it comes to the competition and rivalry within emerging and disruptive technologies (EDTs) such as quantum computing, AI, and machine learning. There is a consequent need to develop rules and norms in transatlantic cooperation in this sphere, build systemic capabilities for innovation as well as address threats and security together. The EDTs are creating both opportunities and challenges and have a growing impact on our security and defence. The EU and US are at the point when they have to start working together not only to boost their cybersecurity posture and resilience but also to remain competitive and retain the technological leadership in the democracies based on shared values. In December of 2020, European Commission has published a new EU-US Agenda for Global Change, which called for the EU-US Trade and Technology Council – a platform for enhancing convergence of views on tech governance on both sides of the Atlantic. No other two regions in the world are as digitally integrated as Europe and the US. Europe is a top-ranked exporter to the US of digitally enabled services, and the US is the top exporter of digitally enabled services to Europe. There is a lot to build together and it's a critical time to make that happen by joining forces as allies to shape technologies of the future.

MAIN THREATS & CHALLENGES:

- Military innovations drove civilian ones in the past, but the situation with many technologies now is vice versa. Civilian innovative technologies with dual-use applications have gained an edge over the military in recent years, but they are also being increasingly weaponised and misused for political and ideological purposes. As a result they can jeopardise our democracy, economy, and national security and harm human rights and fundamental freedoms.
- The EDTs are becoming the battleground over the global technological leadership with profound economy and security implications. This connects with the fact that both the US and the EU are facing a big question on decoupling of global value chains which requires balancing economic, political, and security interests and rethinking the trade rules.

- China follows the path of civil-military fusion, steadily increasing its R&D spending in order to build its technological self-sufficiency and technological advantage over the US, the EU, and their allies.
- Disinformation, foreign interference activities, and malicious cyber activities continue to be used by state and non-state actors to undermine our democracies.
- In a matter of months, the transatlantic community needs to talk and agree on what are the shared values and with all stakeholders involved in this process. The EU and US, together with like-minded countries, need to strive for a more common understanding on many legislative issues, primarily the online privacy rules to be aligned to the way Europe protects them. This condition will let Europe remain an open data continent.
- Technological inequalities and existing digitally highly developed enclaves can result in future international and intranational tensions.

THE WAY FORWARD:

- There is a need for a more strategic focus in the transatlantic dialogue and more cooperation between the EU, NATO, and US on multilateral response to global cyber challenges and a strong collaboration between public and private as well as civilian and military actors.
- While further strengthening our civilian military cooperation we must aim at mainstreaming forward-looking geostrategic perspective into our policies, building strategic partnerships, promoting our approaches on 5G, AI, cyber security or the responsible use of technology in military applications, and safeguarding robust rules-based international order as a bedrock of our engagement.
- The EU and the US have to work together strategically on resolving difficult transatlantic issues (including the status of US digital giants, the digital tax, the Europeans' data protection in the USA) and set a common understanding of values and yet-to-be-defined concepts such as privacy.
- The Allies, including the United Kingdom, should seek agreement on the vision, standards, and rules related to different EDTs and show their global leadership based on values of democracy, human rights, and fundamental freedoms, and safeguarding the rules-based international order by being more active in multilateral discussions on the international structures. They should work towards establishing global norms to prohibit development of most extreme military applications of EDTs.
- Supporting the United Nations development goals with science and technology should minimise the risk of international conflicts. Following technology investments should be coherent with these goals and be directed in similar directions.
- The Transatlantic Allies need to step up research cooperation and considerably increase public R&D spending on vital novel technologies. They should strive to develop an innovative transatlantic market for EDTs with involvement from academia, industry, and governmental institutions, based on the concept of the triple helix model, with a cohesive picture formed for and agreement arrived at science and EDTs development and deployment between NATO nations and in cooperation with all these types of institutions.
- It is significant to further the complementarity between civilian and military aspects and dual use of technologies. Greater synergies between civil, defence, and space industries are needed, as well as the cross-fertilisation between defence and civilian spheres.

- The aforementioned institutions should consider ways to scale up support for critical technologies across civil, defence, and space applications such as drones, satellites imagery, secure communication, by creating combined effect of EU programmes and significant defence funding available.
- Americans and Europeans must work together to create clear and transparent meaningful consequences for malicious actors in cyberspace and build robust cooperation on tackling cybersecurity threats.
- EU should keep mobilising and expanding its wide toolbox to tackle different technological changes, and put in place new building blocks to boost resilience towards future technology challenges. It should work towards improving its situational awareness to assess and address security threats related to new technologies such as hybrid risk assessment surveys.
- The industry should play a role in re-energising the transatlantic relationships and meet its obligation to ensure that products they engineer respect the values, are safe, secure, and transparent for their users, customers, and partners on both sides of the Atlantic.
- Aligning the agreement upon definitions of political concepts, including digital sovereignty, open strategic autonomy, strategic interdependence within the EU, is a must.
- The EU should pursue an open strategic autonomy based on a coherent approach of all member states and at the same time avoid becoming protectionist.
- The whole-of-society approach should lead to individuals' involvement in identifying and detecting misinformation and disinformation and building their resilience in this respect.

"Emerging and disruptive technologies are becoming the battleground over the global technological leadership with profound economies and security implications (...). Whoever has the best know-how on AI and quantum computing, for example, will not only develop the consumer products and services of the future but will get a military edge."

MIAPETRA KUMPULA-NATRI

"We need to be at the forefront of technological progress, both foreign and military technologies, and given this increasing dual use nature of technology, which is especially true with with regard to technologies such as quantum computing, AI, and machine learning, a strong cooperation between public-private civilian and military actors is essential."

JOANNEKE BALFOORT

"We should develop and clarify shared approaches to holding states accountable when they do not act responsibly in cyberspace and to do that, we must be able to have sustained dialogue. The transatlantic partnership that exists and provides a foundation can lead the world in this effort, but we must work together to do it and that's going to happen through people."

PROF. PHILIP LARK

"Equity and opportunity is a central tenet of democratic aspirations and we are currently rapidly commoditising data and removing that access, which you might argue is really counter to this kind of tenet that we try to deliver in our democracies. This needs urgent attention."

PROF. DEEPH CHANA

"No other two regions in the world are as digitally integrated as Europe and the US. Europe is a top-ranked exporter to the US of digitally enabled services, and the US is the top exporter of digitally enabled services to Europe. There is a lot to build together and it's a critical time to make that happen."

MARTA POŚLAD

"Inclusivity means incorporating not only transatlantic alliance and EU, NATO but also being able to incorporate actors that are not the usual suspects in into the technology discussion, the neighbouring countries within Europe for instance. Because whenever we are going to build standards and norms and rules in this area, we will be we will be talking to these actors and states in the long run."

BEYZA UNAL

MAINTAINING TRANSATLANTIC SUPERIORITY: COOPERATION ON CRITICAL TECHNOLOGIES

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Melissa Hathaway** – President, Hathaway Global Strategies, LLC; Cybersecurity Advisor, George W. Bush and Barack Obama administrations (2007–2009); Expert of the Kosciuszko Institute

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Great powers have entered a race for building stable advantages in emerging and disruptive technologies (EDTs). China, in August of 2020, has amended its Catalogue of Technologies Prohibited or Restricted from Export, adding 23 categories of technologies that are barred from export and modified restrictions on some of the others. As a result, certain technologies like AI interactive interfaces or space technologies have been blocked from exports. A few months later, in December 2020 China has published its 14th Five-Year Plan that also identified key technologies crucial for China's self-reliance and development that included quantum computing and deep space exploration. The EDTs became a national priority for China's security, military, and defence. On the other hand, the United States, in October of 2020, has unveiled its National Strategy for Critical and Emerging Technologies that aims to promote the US technology advantage which also extends to its European allies. The document highlights 20 technologies, from advanced computing and artificial intelligence to biotechnologies to aero-engine technologies, that have been recognised as strategic and subject to further research and advancement through cooperation with like-minded partners. As global tensions continue to rise and the decoupling between China and the United States looms over the horizon, transatlantic cooperation will be of central importance to our shared interests and secure future.

MAIN THREATS & CHALLENGES:

- Emerging and disruptive technologies such as AI, quantum computing, or distributed ledgers will be used for national security purposes and warfare, and will be used in unexpected ways.
- China has not only imposed export restrictions on some of the key EDTs, which indicates that further limitations in this regard can be expected, but also stated that it aims to accelerate its defence modernisation with the use of these technologies, making the EDTs a priority for China's military and economic security.
- In the global race for innovation, China is outspending in AI and deep-learning patent filing the US, EU, and Canada with a ratio of 15:1.
- Artificial intelligence and machine learning can be weaponised through interference on various levels. One is data poisoning – data inputs can be skewed, leading to a misjudgement or reclassification of algorithmic decisions. Another is eliciting false algorithmic interfaces that can cause AI to make incorrect decisions. Biases and physical assumptions underpinning algorithms may also result in wrong classifications. The third one is model inversion, where a malicious actor can introduce modified data inputs or alterations which may lead to reverse engineering of the training models, causing the algorithms to misclassify or to uncover data that should be anonymous.

THE WAY FORWARD:

- AI needs a new security approach rooted in conventional information security. We must start to think about the fact that algorithms – the brains of the AI – were created by people with specific assumptions, that the mathematics applied might be fallible, and that the data sets might be small, allowing for easy data skewing.
- AI systems should be robust and secure throughout their entire lifecycle, including not only the conditions of its regular or foreseeable use but also the conditions of its misuse. It should be ensured that data inputs are robust, diversified, and drawn from large data sets.
- Certain principles on AI have to ensured, such as traceability, validation, and verification of data sets and algorithmic processes and decisions, as well as security by design embedded in both existing machine learning applications and its future use cases, for example optimisation in aerospace and defence. Multilateral fora and international accords are important to establish and spread such principles and compliance criteria.
- There are numerous opportunities enabled by the AI and machine learning. We already see some of them in smart buildings, personal digital assistants, finance, risk assessment.
- Like-minded allies should pool their financial resources together for joint research on the EDTs. They should also review the export controls, licensing restrictions and ensure market access.
- The EDTs require closer transatlantic cooperation, as well as alignment of interests with like-minded democratic countries.

"With innovations and tomorrow's technologies – whether it's quantum computing, artificial intelligence, the crypto currencies and distributed ledgers – we need to think that innovation will be in fact used for warfare and used in unexpected ways."

MELISSA HATHAWAY

THE CYBER PEARL HARBOR WARNING – 2021 AND BEYOND

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

INTERVIEW with **Leon Panetta** – Chairman, The Panetta Institute for Public Policy; Former Secretary of Defence
Chaired by **Robert Siudak** – Chairperson, Polish Cybersecurity Cluster #CyberMadeInPoland

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Cyber has become the biggest threat we are facing, with potential cyberattacks that could virtually paralyse a country. This threat has become much more real and much more likely, including Cyber Pearl Harbor scenarios that envision numerous cyberattacks on critical infrastructure, such as power plants or water facilities, possibly resulting in serious geopolitical impacts. The former US Secretary of Defence Leon Panetta has warned us about this threat almost a decade ago and even though some cybersecurity experts are critical of using this analogy, it is the scenario which cannot be forgotten, as is the scenario of outright cyber conflict. We cannot miss them out as imminent risks while we are fixing and building up cyberspace. Meanwhile we – individuals, states, businesses, and organisations – are in a constant state of "cyber-harassment", as Ciaran Martin has framed it. In fact, millions of individuals are impacted by consequences of cyberattacks taking place all around the digital world and undermining our security. The most important "weapon" to get us ahead of the cyber intruders is now cyber intelligence.

MAIN THREATS & CHALLENGES:

- Cyber has started to be exploited as a weapon and is seen as the battlefield of the future. It can be utilised to attack any country, national critical infrastructure, private sector at any moment, to undermine and paralyse even the institutions as sensitive for democracy as national election.
- We have seen that our adversaries and rivals develop greater cyber capabilities, whether it is Russia, China, Iran, or North Korea. While NATO countries have built greater awareness of the nature of the threat, we still have not developed the kind of defence that we really need.
- We need to improve safeguards and strategies to protect us from the threats which have been observed over the years of digital transformation, including risk assessment in terms of the full impact of cyberattacks and coordinated defence to be able to confront the potential cyberattacks that could really impact our security.
- We need to build an understanding of the nature of the cyber weapon, which is a multifaceted weapon that not only can be used for direct attacks but also for planting sophisticated viruses in our computer systems, sleeping them until a country decides to awaken these viruses and then proceeds to try to undermine the systems' operation.
- Critical infrastructure in big part is in private hands and so far the private sector has tried to develop its own ability to protect itself against those threats. We have to overcome the situation in which the private sector, targeted all the time by cyberattacks impacting national security, has been operating in its own sphere, and the public sector operates in its own sphere.

THE WAY FORWARD:

- We have to focus on introducing and gathering better intelligence that really focuses on cyberthreats to know what our adversaries are planning in terms of conducting operations against our country, when cyberattacks are going to take place, where these attacks may be coming from, when they may be coming, where viruses have been deployed in our systems – so that we know when we have been attacked and are able to take action to protect ourselves from the fallout.
- We need to strengthen the existing and build new alliances to be able to share critical information about potential cyberthreats, having regular meetings in the intelligence area, a kind of a cyber command bringing key people from different allied states to look together at ways and steps needed to be taken in order to better defend ourselves against intelligence threats.
- It is critical to develop strongly coordinated defence systems not only in government, but in the private sector too, capable to protect us from attacks. This requires enhancing a more trusting partnership between the leadership of the public sector and the private sector to share information on potential attacks and strengthening coordination of approach to dealing with the cyber threat. It takes not only particular governments but also international organisations such as NATO to be developing a stronger partnership with the private sector, and the private sector to be willing to reach out, to share information, to be able to develop common defences, so that we are fully protected from the potential of damaging cyberattacks.
- We should act upon creating the artificial intelligence with the ability to develop autonomous systems that can provide better security and improve offensive capabilities.

"We've got to wake up and realise that if we do not take action, better action, to defend ourselves and yes, to have offensive capabilities as well, that one day we will see a Cyber Pearl Harbor that can badly paralyse the security of not just the United States but of other countries as well."

LEON PANETTA


BUSINESS STREAM

6th EUROPEAN CYBERSECURITY FORUM – CYBERSEC GLOBAL 2020

BACK TO BUSINESS: THE DAWN OF NEW GEOPOLITICS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Samir Saran** – President, Observer Research Foundation (ORF)

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

We are already in a divided Internet. The technology domain is already split and the splinternet is already here. Fragmentation and exertion of sovereign control is visible at every level of the technology stack. We are observing a scramble for control over digital infrastructure in its various dimensions, from 5G networks to protocols and standards. We are also beginning to see a zero-sum competition in the business and political domains. The concept of cyber sovereignty is being increasingly used not only in China but also India and Europe; however, for each stakeholder it holds a different meaning and is very often wrongly deployed. Sometimes, it refers to exertion of sovereign control over certain businesses. There is a strong feedback loop between the politics and technology, between the policies of countries and economic actors. Private sector entities sometimes compete with and other times complement political forces – and this dynamic is shaping our world like never before. Economics will not remain the same as the work and workspace have changed forever. People are starting to mobilise and contest politics, change economics, and seek safety through different kinds of aggregations, many of which are virtual and technology-induced. Through this, a new global political system is being born. Globalisation is going to rapidly shift from being an open world framework to a gated system where countries will be given passes to enter and participate in each other's futures.

MAIN THREATS & CHALLENGES:

- We are experiencing a very contested and conflictual cyberspace. Discord and competition is increasingly reframing the digital domain.
- The US-China rivalry in technology will spread to other countries that may find themselves unable to continue to refrain from taking sides. They will need to make a decision and it is really a choice that has to be made now.
- A much different geopolitical reality is emerging in front of our eyes as we move from the age of iron, fuel, and oil to the age of lithium, nickel, and cobalt.

THE WAY FORWARD:

- We must engage with this new reality and that entails creating consensus amongst the open democratic societies if they are to be able to compete with others.
- The concept of trust will become contextual – several different systems of trust are likely to emerge: based on growth, based on values, and based on the market. This will also cause a global realignment on

technology that will be driven by the competing understandings of trust. Countries that trust each other will partner, creating a more fragmented system of locked networks of alliances.

- For example, for India the frontline of its future conflicts and security challenges will be defined by the digital Silk Road and the digital Indo-Pacific. As India emerges as a digital power, its most important partner in the upcoming future is likely to be Europe.

"What 9/11 did for surveillance, the COVID-19 is going to do for the technology's future."

SAMIR SARAN

BIG DATA = BIG CHALLENGES? COUNTERING ADVERSITY IN THE DATA-DRIVEN ECONOMY

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the participation of:

- **Dita Charanzová** – Vice-President, European Parliament
- **Matt Warman** – Parliamentary Under Secretary of State, Minister for Digital Infrastructure, Department for Digital, Culture, Media and Sport, United Kingdom
- **Cecilia Bonefeld-Dahl** – Director General, DIGITALEUROPE
- **Marta Pośląd** – Head, Public Policy & Government Relations, Central and Eastern Europe, Google

Chaired by **Paul Timmers** – Research Associate, Oxford University; Director, Sustainable & Secure Society Directorate, DG CONNECT, European Commission (2012–2016)

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Data has become the most valuable commodity. On the one hand, it is a driver for the digital economy, enabling new revolutionary business models and becoming the inherent element of building and maintaining market competitiveness. We begin to hear more about the potential of data to transform and enhance societies, raise the efficiency and innovativeness of public services and fuel growth. On the other hand, data is essentially what we protect with cybersecurity. It remains a subject of concern related to national industry ambitions, privacy, intelligence, and security, and as such is being increasingly linked to the notion of sovereignty, although opinions vary on whether this connection is justified.

The coronavirus pandemic has highlighted the key importance of establishing public trust and comprehension in regard to the role of data in our daily lives. Not only have our experiences from the responses to the COVID-19 crisis exposed the importance of timely, high-quality data, but also they underlined the urgency to build a foundation for public confidence in data-based solutions. As more and more private sector entities use public data for their business purposes, more and more users expect security and privacy of their data to be ensured. As a response, we can observe emerging strategies aimed to protect and harness data, both on national and regional levels, such as the EU's Data Governance Act. The European Commission has put data and digital agenda at the heart of the post-COVID recovery plan. Europe's digital development is closely linked not only to cybersecurity of data but also to the enhanced capability to use data across borders. The Digital Services Act and the Digital Markets Act proposed by the Commission in 2020 voice the call for the private sector to accept the great responsibility that accompanies its great power.

MAIN THREATS & CHALLENGES:

- Data is exposed to cyber threats and can be used for adversarial means like data poisoning, data theft, misinformation. Data can be compromised through numerous aspects of information security: data's confidentiality, integrity, availability, also compliance and liability that relate to it. An interruption to data-driven businesses, services, and activities can cause real disruption to our societies, businesses and public institutions.

- Public fears about safe, secure, and ethical use of data might result in barriers to how data is being used for the economic growth or innovation. We should tread carefully when trying to balance data protection and innovation as otherwise we may hamper European competitiveness and economic performance.
- Thinking about how to regulate data, we should not overlook its impact on SMEs. Very often we reflect on regulating big businesses but without consideration of the consequences for the smaller ones.

THE WAY FORWARD:

- When discussing all of the challenges related to Big Data, we should not forget the immense opportunities stemming from it. Data can and should be used for the public good.
- We need to establish foundations for data use. Data must be collected and stored in standardised ways which ensure sufficient quality of it. There is a need for a common agreement on making more data available through better coordination across public, private, and third sectors, as well as internationally. Data usage needs to be underpinned by trust resulting from collecting, storing, and deleting data in a way that is lawful, secure, fair, ethical, sustainable. The way forward should be based on a combination of common data standards, interoperable infrastructure, and rise in public's awareness and understanding of data.
- The government has the responsibility to ensure that data and its supporting infrastructure is secure and resilient. Data has to be protected both while it is stored and while it is in transit. The ability to share vital information quickly, securely, and ethically between the government and the businesses and organisations is crucial to ensuring the societal functioning in times of crisis.
- The government should transform the way it understands and uses its own data to improve public services and policy decision-making. It should establish a clear policy framework that defines what government intervention is needed, develop a data regime that is built on trust, and ensure that the benefits of data use are felt across every public sector.
- In terms of data security, a greater harmonisation of cybersecurity certifications, for example through a common framework, should be pursued to provide equal level of protection to both the consumers and citizens.
- The concept of sovereignty traditionally directs our thoughts towards a pursuit of a national solution. However, it is important to remember that cyberspace that does not care about national or regional boundaries. The concept of digital sovereignty should be carefully crafted so it does not turn into an "us first" approach that raises walls against others. Data presents us with global challenges that need to be discussed globally with like-minded partners. The world is hyper-connected and our ability to exchange data securely across borders is essential. To achieve real cyber resilience, governments should be aware of their strategic interdependence and seek to align their cybersecurity and data privacy rules.
- Private-public partnerships are key to developing data solutions. Data sharing between the public and private sector – working both ways – should be discussed in order to establish mutual understanding of goals. There is a competitive advantage that can be built on sharing and pooling of data, yet it is also important to protect IPRs.
- Greater data flows between like-minded countries should be encouraged and based on common understanding. Security and robust data protection standards should be the key element of agreements on cross-border data transfers. We should pursue an international solution on how we treat data security.

"Companies are using more and more public data for their own business purposes and I would like to see it reversed a little bit, so that we can also use some of their data, some of the private companies data for the public purpose."

DITA CHARANZOVÁ

"Data are very essential of course for each and every country and ever more so, data are very close to national security: the industry data for example is very close to national competitiveness. Governments have realised that and they are taking these large data initiatives."

PAUL TIMMERS

"I think the idea of the public data space, to pull the European data into a data space that gives the same data access for SMEs as for bigger companies with a lot of more resources to harvest that data across the different countries in Europe would be a major milestone."

CECILIA BONEFELD-DAHL

"To unlock the value of that data more broadly I think we've got to ensure that the physical and cyber infrastructure underpinning it is safe and secure and resilient, and that people trust that data."

MATT WARMAN

"It's incredibly important not to think about data as the only solution to further innovate. This is one thing that we cannot lose sight of. There is much more to innovation than just data and that applies to skills, the sentiment around the role of technology in society and societies, and we should be thinking about broader ecosystems."

MARTA POŚLAD

THE FUTURE OF DIGITAL PLATFORMS AND EUROPEAN REGULATIONS – WELCOMED OR CONTESTED

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

FIRESIDE CHAT with **Aura Salla** – Public Policy Director, Head of EU Affairs, Facebook
Chaired by **Michał Rekowski** – Director, Strategic Partnerships and Projects, The Kosciuszko Institute

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The year 2020 has brought a plethora of rapid developments that signal the upcoming change in how digital services providers will operate in Europe. First, the European Court of Justice has invalidated the Privacy Shield that used to regulate transatlantic transfers of data and access to data. Second, the European Union has stepped up its efforts to regulate digital platforms with a set of legislative proposals including the Digital Services Act or the European Democratic Action Plan that aim to raise accountability of social platforms and codify rules on how they should deal with election interference. European Union is moving to grasp the opportunity to connect and harmonise regulations across Europe and create a legislation that will set global standards. These steps have ramifications for some of the world's biggest digital companies operating in Europe, including Facebook, that have recently come under intense pressure.

MAIN THREATS & CHALLENGES:

- Despite the benefits brought by the variety of digital services and products, there has also been an erosion of trust towards online platforms.
- The proliferation of interferences in democratic processes through online platforms has raised the apprehension about misinformation, disinformation, influence operations, and foreign interference. There is much confusion between these phenomena in the debates that try to come up with measures to halt these practices. Such disorientation is further enhanced by blurred lines between illegal content and legal but harmful content (that is contextual and often legally ambiguous).
- There has been criticism that Facebook should do more to fight harmful content on its platforms.

THE WAY FORWARD:

- The definitions and concepts used in the regulations and debates on protecting the integrity of electoral processes should be clear and precise. As legal but harmful content should not be part of liability due to its legal ambivalence, it is important for society that platforms can address lawful but potentially harmful content in compliance with clear policies. It is crucial to ensure an appropriate balancing of safety and fundamental freedoms, like the freedom of expression.
- Rules governing political advertising should be straightforward and include greater transparency concerning financial contributions, expenditures and also an explicit definition of what constitutes a political ad.The efforts to combat misinformation should become holistic, equipping people with the skills they need to navigate through the digital world: critical thinking, media literacy, and responsible, respectful, and safe ways of participation in the digital society. Supporting journalism and helping news organisations to adapt to the digital world is also important and enhances this pillar of a democratic society.

- Facebook's strategy to protect election processes applies not only during critical times like elections periods, but throughout the entire year. It is centred around preventing interference, removing harmful content and reducing misinformation, and increasing transparency. In order to prevent interference, Facebook works with government authorities, law enforcement, security experts, civil society, and other tech companies, to stop emerging threats through the establishment of a direct line of communication, knowledge sharing, and identifying collaboration opportunities.
- One of the underlying principles of the EU's legislative proposals is also to build trust towards online platforms. It is important for Europe to come up with clear rules that have the users and the citizens at the centre and that provide a clear framework that makes platforms like Facebook accountable.

"We are a fundamentally different company than we were in 2016. We are able to anticipate threats and prevent election interference much better than before."

AURA SALLA

MOBILE ASSURANCE UNDER ADVERSARIAL ATMOSPHERE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PRESENTATION by **Daniel Ahn** – Senior Vice President, R&D Software Security, Samsung

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Mobile devices are exposed to adversarial situations, targeted by attacks coming through various channels such as websites and wi-fi access points. The goal of attackers is to steal some assets and information from our devices as well as attempt to compromise the frameworks of the devices. We need a discussion on available attack factors and then try to figure out how we can achieve mobile assurance against adversarial events and attacks. This will help reduce potential risks to our devices and networks.

MAIN THREATS & CHALLENGES:

- A compromised device attempts to disconnect from the cloud. Eventually, that device can be a tool to launch attacks against important assets and corporate information.
- Threats come from different sources, some even taken up from the physical layers. In sum, the tools utilised for the attacks can connect directly to our devices. On the other hand, through-the-network attacks will launch further attacks against other devices.
- Eventually, the goal of the threat actor is to make significant damage on devices and then consequently attempt to launch attacks at a higher corporate level.

THE WAY FORWARD:

- Customers must trust the devices they're using, and this trust should initially come from hardware and chips. From then on, it's a step-by-step process.
- Additionally, there must be some hardware-based maintenance trust, as well as one-time protection. Once this is done, there is a possibility to provide hardened versions of software layers which will leverage the security development life cycle.
- Before releasing a product, it is important to do various testing and assessments through the security development life cycle. This serves as an efficient threat detection analysis, which can be split into three main factors: understanding the up-to-date threat situation awareness, building situation awareness through partnerships, and finally staying aware and alert once the threat had been identified.
- Collaboration and partnerships involving customers, developers, security analysts, as well as the product managers is what the global community should strive for.

"We have to work closely with carriers and partners so that we can improve the security of our devices. Those quick responses and strong partnerships eventually will improve the trust relationship with customers. In other words, all of today's security protections are necessary once your product is released."

DANIEL AHN

GLOBAL CYBERTHREATS 2020

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PRESENTATION by **Tom Burt** – Corporate Vice President, Customer Security & Trust, Microsoft

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Cyberattacks are increasingly proliferating by taking the shape of various instrumental threats. Examples of such are deepfakes, which consist of video or audio files modified by the application of artificial intelligence to create situations that never happened. In response to such threats, the Microsoft Digital Defence Report was put in place. The report compiles all the threat information that can be assessed and discovered every day. This collection is then offered to customers, policy-makers, and others. The COVID-19 pandemic unveiled a new menace as cybercriminals quickly took advantage of public interest in order to lure people into clicking on malware links and files. Due to this new challenge, it is crucial to look at who the targeted audience is, as well as the factors involved with remote workforce.

MAIN THREATS & CHALLENGES:

- Disinformation is the main threat, and it requires solutions from a technology standpoint.
- Some previously established solutions have been deemed not strong enough to fight deepfakes, for instance because the AI used in deepfakes can be trained against detection technologies.
- Ransomware is one of the more sophisticated tools used by criminals, allowing them to search for the most vulnerable entry points. When the time is right, threat actors use those entry points to infect other devices and entire networks.
- State-backed attacks are mostly made by Russian groups that target non-governmental, governmental, and international organisations. Their tools look for vulnerabilities in the victims' unpatched systems.

THE WAY FORWARD:

- In order to prevent disruptions and intrusions, a service called "AccountGuard" could be used to detect forthcoming cyberattacks as well as make sure to notify the nation-state of the threat.
- Encryption-based solutions such as "ElectionGuard" could increase security of voting processes so that a vote can be recorded electronically whether it comes from a ballot marking device or a paper ballot.
- The "Video Authenticator" could offer a solution regarding deepfakes, as it can be used to detect artificially altered images or videos. However, it only works 80% of the time and what we learn from this is that we can't rely too much on deepfakes detection as a long-term solution.
- In order to counter unauthorised AI effort to try and alter the media, the Project Origin has attempted to offer a solution involving the watermarking of images or videos at the time they were captured. The technology then flags unauthorised attempts at altering the media.

- The most secure solutions in general involve multi-factor authentication for all accounts. Patching all applications and systems with security patches that come from vendors as well as segmenting the networks are some ways of slowing down attacks.

"Cybercrime and nation state attacks proliferate without conscience or deterrence. The COVID-19 pandemic and US elections have been seized upon as the basis for even more aggressive attacks. At no time has it been more important for the public sector and the private sector to find ways to work together better to face these challenges."

TOM BURT

EXPANDING RELIANCE ON DIGITAL TOOLS – BEST PRACTICES FROM DIGITAL LEADERS IN THE TIMES OF COVID-19

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the participation of:

- **Flavio Aggio** – Chief Information Security Officer, WHO
- **Ciaran Martin** – Professor of Practice in Public Management, Blavatnik School of Government, Oxford University; CEO, National Cyber Security Centre of the UK (2016–2020)
- **Andrzej Dopierała** – President, Asseco Data Systems Management Board; Vice President, Asseco Poland Management Board

Chaired by **Rafal Rohozinski** – CEO, SecDev Group

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The COVID pandemic presents an unprecedented challenge to the global system. It has accelerated the digital transformation of countries, corporations, and societies: with the imposition of lockdowns, restrictions in movement, and physical distancing, societies have been forced to work remotely, access essential services online, and communicate through digital means. Throughout that crisis, technology has kept us going both professionally and personally. The technology has proved that it is indeed useful and that it penetrates many aspects of our life. To many citizens, it was a transformative experience to discover how many things they can actually do online. Common trust in technology became an essential public good. However, the pandemic has further aggravated the conflict over data and privacy while the accelerated migration to cyberspace was accompanied by an exponential growth of COVID-related cyberthreats. The organisations that managed to implement cloud and cybersecurity strategies before the pandemic were able to go through it with fewer disruptions and maintain the integrity of their operations. Others – that failed to build their cybersecurity preparedness – have found themselves unable to develop necessary cyber resilience in short time when faced with urgency. Threats have multiplied, targeting both individuals and crucial infrastructures and services. We have even observed how criminally deployed ransomware actually impaired the provision of healthcare leading to fatal casualties.

MAIN THREATS & CHALLENGES:

- Recent growth of dependence on digital tools and services has been followed by a rise in cybercrime, including ransomware attacks against critical infrastructure, essential services, hospitals, companies, and governments. Ransomware became the most pressing plague accompanying the pandemic and one that has proved to be the hardest to defend against.
- Information warfare and disinformation became the centre of digital threats magnified by the pandemic, exacerbated by significant parts of the population switching to remote work and also moving to online content as their primary source of information. The decrease in real-life social interactions and the accompanying sense of isolation and emergency rendered users more prone to the spread of misinformation online.
- Malicious actors in cyberspace tend to adapt to changing social conditions but also to the advancements of technology. This has become particularly true in relation to both ransomware and disinformation.

Many of the proliferating threats were carefully accommodated to quickly mimic real-world situations like malware disguised as official communications from public institutions related to a government programme or a decision that was publicly announced by the authorities just few hours earlier.

- The human remains the weakest link in cybersecurity.. This fact should be particularly worrying under current conditions of remote working which might create a sense of decreased awareness while compared to working in the office.

THE WAY FORWARD:

- It is crucial that the citizens continue to trust the technologies they are using. The early stages of the COVID emergency required organisations and governments to impose solutions in regard to privacy and data when there was little time for thorough reflection and social consultations. Now, as we have seen some of these solutions work in practice, a time has come for a more open conversation about the various aspects of their application, especially regarding data and privacy protection. This dialogue should not shy away from discussing the trade-offs of pursuing and not pursuing specific strategies that affect privacy, for example in relation to contact tracing.
- The pandemic that forced people to change their risk calculations has thus proved that risk management is at the core of cybersecurity. There should be a greater implementation of risk-management processes, systems, and strategies across organisations.
- Zero Trust approach that comes from a premise that there is no 100% secure system might be useful in achieving more efficient protection in many organisations. It is a misconception that what is inside of the organisation's cyber perimeter is secure or that calling a specific application "secure" solves the problem. Zero Trust approach may give organisations the risk level that they can accept.
- Digital services providers and public institutions should step up and work together more on preventing cyberattacks but also on guidelines and managing services for organisations, especially those that did not reflect or invest in their cybersecurity structures before but now have been faced by an urgent necessity to build their cyber resilience. There is a need to assist the entities that are less advanced in their cybersecurity efforts, one which will include the transfer of best practices, creation of operation centres, rules on how and with whom to share reporting, etc.
- The governments should start to think about introducing cybersecurity as a part of compulsory curriculum at schools, implemented from the early stages of education. It should address the issue in a comprehensive manner, teaching first and foremost how to behave in the digital space, how to function, what can go wrong, and what to do when it actually does. If we invest so much in technology we should also invest more in human knowledge and human understanding of it.

"Embrace Zero Trust model, because only that will give us the risk level that we can accept (...). We need to make sure that we have multiple layers of security and this is what is based on the zero-trust model."

FLAVIO AGGIO

"It's a big role for both the government and the private sector to come up with such managed services and to help the organisations build their cyber resilience."

ANDRZEJ DOPIERAŁA

"Public trust and technology is now an absolutely essential public good (...). What I think is now absolutely critical for people like us is that we do everything we can to make sure that our public, our citizens have well justified trust in the technology they're using."

CIARAN MARTIN

"While it's tempting to think that better tools can get us through a crisis like COVID, the reality, I think (...), is that it's considerably nuanced. Informed and competent leadership, trust in science and facts, and intelligent governance are all key determinants of success."

RAFAŁ ROHOZIŃSKI

HOW COVID-19 REDEFINED THE CRITICAL SECTORS OF ECONOMIES

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the participation of:

- **Melissa Hathaway** – President, Hathaway Global Strategies, LLC; Cybersecurity Advisor, George W. Bush and Barack Obama administrations (2007–2009); Expert of the Kosciuszko Institute
- **Marco-Alexander Breit** – Head, Artificial Intelligence Task Force, German Federal Ministry for Economic Affairs and Energy
- **Evangelos Ouzounis** – Head, Secure Infrastructure and Services, ENISA
- **Tomasz Zdzikot** – President of the Management Board, Poczta Polska S.A.
- **Michael Bem** – Executive Director, CISO, UBS

Chaired by **Samuel Stolton** – Digital Editor, EURACTIV

RECOMMENDATIONS BY SAMUEL STOLTON

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

As Europe writhes from the aftershocks of the coronavirus pandemic and its continued impact on the economy, the talk across the continent has turned to ways in which businesses and governments can chart a resilient path out of the crisis. Critical sectors of the economy, ranging from healthcare to agriculture to energy, have been placed under challenging new conditions and governments are increasingly recognising the importance of digital tools in fostering a long-term recovery.

In the European Union, there has been a rapid uptake of digital goods and services in order to facilitate the increased transition to remote working as a means to ensure business continuity. The education sector has also been placed under even more pressure to find innovative methods that allow schools to continue operating. In this vein, shortfalls across digital capabilities have also been woefully exposed in Europe. This has been particularly pronounced across the connectivity landscape, where certain rural areas of the continent, without the access to key tools and services, have found themselves isolated. In this context, the President of the European Commission Ursula von der Leyen said in her State of the Union speech towards the end of September that 20% of the bloc's recovery fund should be allocated to "digital resources".

But the turn towards a more technologically advanced society also brings with it a plethora of new challenges and threats. Not least in the security domain, where during the early stages of the pandemic we saw a spate of cyberattacks directed at health institutions across Europe. As the coronavirus continues to impose physical restrictions on much of the world and as key sectors of the economy are becoming more digitalised, policy-makers and industry leaders are now considering the ways in which such challenges can be best met, in order to adapt to the new reality in a resilient and future-proof way.

MAIN THREATS & CHALLENGES:

- The extent to which critical infrastructure should be redefined, with the increased use of technological tools, such as cloud services, telemedicine, and mobile networks.
- The ways in which policy can support a more resilient cybersecurity landscape as part of the uptake of next-generation technologies. How can cybersecurity policy be revitalised to address the new threats that critical sectors will face as part of their digital transition?
- The effectiveness of policies such as the EU's NIS Directive in terms of cybersecurity.
- The employment of additional data sets that have been acquired through an increased use of connected tools across the economy. In terms of data, how business and government can extract the maximum value out of such streams, without placing personal data at risk.
- The role that cloud infrastructure can play in facilitating a better sharing of data in order to increase innovation for emerging technologies. Likewise, the extent to which Europe can build greater data sovereignty with the establishment of its "Gaia-X" project.
- How new channels of health data can be better mobilised in the increased digitalisation of the sector. The role health data plays in containing the future spread of the virus.

THE WAY FORWARD:

- The increased uptake of digital tools should be pursued swiftly, but governments must ensure that blind spots don't emerge in terms of the increased security protocols that need to be taken into account in this context.
- Our health infrastructures should have the most resilient cybersecurity protocols in place as a means of navigating the new threat landscape that has emerged amid the coronavirus pandemic. Policy-makers and industry leaders should be in close cooperation in order to make this objective a reality.
- While regulation plays an important part in fostering bolstered cybersecurity standards for key infrastructure, there should also be due consideration afforded to the value of providing incentives and additional investment for building up resilience in cybersecurity.
- In the European Union's data strategy, which aims to create more of a liberal environment for industrial data sharing, stakeholders should be aware of the necessary security pitfalls that could emerge in this respect.
- Sufficient attention should also be invested into supply chains and the origin of technological components used in key enabling technologies. Greater digitalisation of critical infrastructure should not lead to security loopholes. In this vein, Western governments should consider their geopolitical allies in the provision and subsequent deployment of upcoming technologies.

"And as we go forward, we'll need to better consider security at the inception of every single service that we'll devise and make available."

MICHAEL BEM

"It's essential as we accelerate our digital transformation as countries and companies, so that we design the architecture and embrace that enterprise with not just the privacy of the data, but the safety and security of those services and systems."

MELISSA HATHAWAY

"Cybersecurity is no longer simply nice to have. It's essential if you want to make your businesses run efficiently and your organisations to operate in a resilient manner."

MARCO-ALEXANDER BREIT

"We need to invest more in cybersecurity, and we need to understand supply chain matters. It's important to be aware of the geopolitical issues at play."

EVANGELOS OUZOUNIS

"Our role is to implement digital services in the most secure way that we are able to."

TOMASZ ZDZIKOT

THEMATIC BLOCK: NORMS AGAINST THE ADVERSARIAL INTERNET

FOSTERING TRUSTWORTHINESS AND RESPONSIBLE BEHAVIOUR IN CYBERSPACE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Michael Chertoff** – Co-Chair, Global Commission on the Stability of Cyberspace; US Secretary of Homeland Security (2005-2009)

THE ROLE OF TECHNOLOGY PROVIDERS, THE CIVIL SOCIETY, AND INTERNATIONAL INSTITUTIONS IN ENSURING THE PEACEFUL INTERNET

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the participation of:

- **Tobias Feakin** – Ambassador for Cyber Affairs and Critical Technology, Australia
- **Kerstin Vignard** – Head, support team to General Assembly processes pursuant to resolutions 73/27 and 73/266, UNIDIR
- **Eileen Donahoe** – Executive Director, Global Digital Policy Incubator, Cyber Policy Center, Stanford University
- **Līga Rozentāle** – Senior Director of EU Governmental Affairs for Cybersecurity Policy and Security of Emerging Technologies, Microsoft
- **Julia Jasińska** – Head of International Relations & Trade Policy, Nokia

Chaired by **Przemysław Roguski** – Lecturer, Chair of Public International Law, Jagiellonian University

THE FUTURE OF CYBER NORMS IN AN ADVERSARIAL CYBERSPACE

CLOSED SIDE SESSION

Moderated by **Przemysław Roguski** – Lecturer, Chair of Public International Law, Jagiellonian University

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The lack of global consensus on the international framework for responsible state behaviour in cyberspace made it easier for cyber mercenaries to take advantage of grey zones in the international law. In recent years one could have observed a significant rise of bottom-up multi-stakeholder initiatives gathering states, businesses, and civil society actors to promote stability of the Internet and cyberspace as a whole. The COVID-19 crisis has underlined the importance of cooperation even further, putting pressure on initiatives and organisations dedicated to cyberdiplomacy and norm-setting.

Initiatives such as the Paris Call for Trust and Security in Cyberspace and the Cybersecurity Tech Accord and their contribution to the global security of cyberspace are notable examples of what can be achieved

through collaboration. The global community is expected to take a step forward and come up with feasible and practical ways to enforce the frameworks and incentivise all stakeholders to join the fight for secure, open, and free Internet.

MAIN THREATS & CHALLENGES:

- As the pandemic forced a mass migration to cyberspace, the number of cyberattacks has been growing significantly, not just in frequency but severity as well, posing serious threat to citizens, businesses and states.
- The use of digital technologies for interference in international affairs and elections, misinformation and disinformation, spreading extremist views, and deteriorating the civil discourse is still escalating.
- The use of cyberspace for hybrid warfare by state actors is causing severe damage to their opponents, as they oftentimes target critical infrastructure, which can put entire cities, regions, and states in a blockage and power outage.
- International cooperation based on trust is a great challenge, due to lack of universally agreed views, for example on global commons, data management, privacy protection, security, and prospects of conflict. Such inconsistency and absence of consensus allows for greater exploitation of the grey zones.
- Countries that wilfully refuse to adhere to norms are often let go without facing any serious consequences for their actions due to low enforceability of rules.
- The increasing activity of non-state actors is raising both the degree and likelihood of damage for civilians. Allowing criminals and terrorists to engage in offensive cyber operations has a substantial effect on the functioning of the Internet and the society.

THE WAY FORWARD:

- The Internet is only valuable when all have the access to it, therefore further fragmentation could easily hinder innovation, prosperity, and exchange of information. A collective response ensuring stability and security of the global open Internet is what the community should strive for.
- States that are unable to implement norms should get support through capacity building, but those who simply refuse to adhere to certain rules should be incentivised in other ways, to be established through dialogue and concrete proposals. In case of the latter, the global community should also be prepared to react appropriately to malicious behaviour from their side.
- Frameworks with enforceable consequences for malicious behaviour should allow for greater trust, consistency, and predictability among partners. Dialogue and cooperation ensures that all stakeholders are on the same page and willing to sanction hostile actions.
- Making sure no adversary has the capacity or desire to disrupt or damage the functioning of societies should be the absolute priority for states all over the world. Framework for responsible state behaviour or the Paris Call are a firm foundation to start, but a more value-driven discussion should follow.
- Processes and discussions at the United Nations level are essential, but not the only way to address cyber issues, as states, companies, and the civil society also have the ability to raise the overall level of security. The private sector for example can do so through information sharing or adhering to high standards (such as those by 3GPP or ETSI) and ethical conduct in developing and deploying their products.

- Exchange of best practices among like-minded countries can raise the level of preparedness and incident response. A holistic and transparent partnership-based approach engaging the public administration, private sector, NGOs, and academia in the process that is already implemented in Australia could be found useful in other states as well.

"An internet that is merely a series of not well-linked national networks essentially eliminates much of the value of the Internet for the globe in general. In that way the Internet is a little bit like the sea – it's only really valuable if everybody can sail more or less unhindered."

MICHAEL CHERTOFF

"Values-driven discussion on technology development and what norms and law look like in the new technology space that we're in already – I think it's going to be pivotal in the months and years ahead."

TOBIAS FEAKIN

"As we see digital technologies being used maliciously by a variety of actors for interference in internal affairs of states, including in elections, for misinformation and disinformation, to fan and spread extremist views, content has come back to the table as not just a national security issue but an international security issue."

KERSTIN VIGNARD

"Job number one is for democratic governments to get together and rearticulate how we apply human rights values online and that liberty and security both must be protected. At the same time we must protect the integrity of elections. Those things must work together if we're going to have a democratic society."

EILEEN DONAHOE

"Building coalitions is very important, so that in the absence of consensus we can find those partners that truly are interested in contributing to different areas of responsibility in cyberspace, to make action or projects that actually underscore not only the awareness necessary, but the actions needed to find conclusive results so that there's a sustainable effort made to be able to build the foundations of a society that follows norms throughout."

LĪGA ROZENTĀLE

"As the 5G becomes more and more indispensable for our economy and for our society, so is the price for those with malicious intentions to interfere with it, be it hackers or hostile agents of domestic or foreign origins."

JULIA JASIŃSKA

"One of the crucial values is to protect how our democracies work, how citizens' rights are protected online, and with upcoming elections in the US, but not only in the US, across the world, it is increasingly important to protect election security."

PRZEMYSŁAW ROGUSKI

4th CYBERSEC BRUSSELS LEADERS' FORESIGHT 2021

THE THREE SEAS INITIATIVE AS AN INTEGRAL PART OF THE NEW TRANSATLANTIC TECHNOLOGY ALLIANCE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

FIRESIDE CHAT with **Marek Zagórski** – Secretary of State, Chancellery of the Prime Minister of Poland
Chaired by **Izabela Albrycht** – Chair, The Kosciuszko Institute; President, Organising Committee of the European Cybersecurity Forum – CYBERSEC

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The European Commission has unveiled the Digital Compass strategy, putting strong emphasis on issues related to the digital transformation and strengthening the EU's position in the digital sphere. In the global bipolar reality, where Europe is still catching up with the US and China in the tech race, there is a common understanding within the Union that we need a great deal of work, expenditure, and legislative activities to narrow the gap. Cybersecurity is a vital component of the digital transformation, which requires close cooperation between different state and non-state actors.

In this context, regional actions such as the Three Seas Initiative can play a key role in fostering the digital transformation and releasing the full potential of the Central and Eastern Europe. This requires a reflection on the form of cooperation within the Three Seas, one that could not only result in the successful development of the region but also provide for more support and better status from both the European Union and the US. Such development initiatives need to be also embedded in the transatlantic technology alliance to strengthen not only the strategic relations with the EU but also the US.

MAIN THREATS & CHALLENGES:

- The EU's position in the global tech race is behind the US and China, with the mounting pressure to overcome this gap. This relates to cybersecurity, technology, and digital sphere, where Europe should speed up to level up with its economic and political potential.
- In recent years it has become clear that technologies often serve as indicators of a state's geopolitical and geoeconomic position. The competence for building and applying digital tools is what really determines this position. Apart from the existing alliances and cooperation between the EU and the US, there is a strong need for new digital and technology coalitions.
- Recent developments concerning digital transformation force us to take a fresh look at work, investments, and economic growth, which are defined by significantly different properties than in the previous stages of industrial growth. In the context of the transatlantic cooperation, this requires a new approach to issues such as product accessibility or sharing the fruits of production and intellectual property.

THE WAY FORWARD:

- There is a common will within the EU to strengthen its digital and cybersecurity sovereignty. To achieve that goal, all member states should place more emphasis in the new financial framework on digital issues followed by reinforced cooperation with Europe's allies.
- While defining different areas of digital transatlantic cooperation, the primary focus should be put on initiatives which aim to increase the security level and enhance the economic potential. Reaching political goals has to be based on those two factors.
- To achieve the successful digital decade within the Three Seas region, the Initiative should focus on: building secure infrastructure between member states, using this infrastructure to closely cooperate, for instance through information exchange, and finally creating competence centres and solutions, by diverse state and non-state stakeholders, that would span the whole region.
- Regional activities have to be engaged in broader European actions, like the European Cloud Federation and deliver regional contribution to these programs.
- The recently signed V4 Digital Declaration is a good example of regional cooperation, especially as every initiative of this kind leads us closer to the goal of the digital decade. It is also important not to put barriers made out of too ambitious projects and take small but effective steps. On the regional level, especially within the V4 and the Three Seas countries, digital development needs effective coordination between the member states and more cross-border projects.
- It is crucial to coordinate the initiatives which the Three Seas states will pursue using their national means or their recovery plans within the digital and cybersecurity sphere. Creating common cybersecurity ecosystems, ensuring information flow, and building interfaces between new national systems have to be the first steps.

"There are no doubts the Commission, the EU, all Member States do notice the need to place a strong emphasis on digital transformation issues as such, and on the need to ensure that the EU enjoys a better position than the one it has now."

MAREK ZAGÓRSKI

GREEN AND DIGITAL THREE SEAS INVESTMENTS – ON THE WAY TO INNOVATIVE AND RESILIENT EUROPE'S EASTERN LUNG

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with participation of:

- **Jonatan Vseviov** – Secretary General, Ministry of Foreign Affairs of Estonia
- **Boris Koprivnikar** – CEO, Sincular Consulting; former Minister of Public Administration of Slovenia (2014–2018)
- **Piotr Karnkowski** – Head of Treasury, Polish State Development Bank; Chairman of the Management Board, Three Seas Initiative Investment Fund
- **Christopher Painter** – President, The Global Forum on Cyber Expertise; Commissioner, Global Commission on Stability of Cyberspace; Former Coordinator for Cyber Issues, US State Department
- **Karol Okoński** – Managing Director, Cybersecurity Lead for Public Sector (PL & CEE), PwC

Chaired by **Scott Malcomson** – Author of The Splinternet (2016); Director of Special Projects, Strategic Insight Group (SIG); former senior official at the United Nations and the US State Department

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The Three Seas Initiative welcomed its first digital investment, a large modern data centre outside Tallinn. Notwithstanding, the regional infrastructure, digitalisation, and energy gap between the 3SI region and its Western European counterpart amounts to 60–100 billion euro. In order to address this convergence challenge, the 3SI tries to increase infrastructural investments using EU, national, and private funds. The sole attraction of capital and investments is, however, not enough. The emerging infrastructure has to be both digital and green, which brings in a different sort of challenges. In the context of connectivity, overall security, and investment quality, it is crucial to answer the questions of who owns, who maintains, who runs infrastructure and energy facilities, which essentially adds a strategic dimension to the requirements mentioned afore. Tangible private sector investment commenced with the Estonian success story, where a green, secure, and scalable model data centre was established, with others to follow. Still, the regional transformation meets a broad set of challenges such as development of well-thought and proper regulatory frameworks, Internet legislation, building common solutions for the production and its control, and assuming applicability and compatibility out of the solutions that are built between the countries. Digital development of the Three Seas Region pushes for a development of adequate infrastructure. To meet these challenges and aim at building an innovative and resilient Eastern European ground, the 3SI became committed to coordinating these investments.

MAIN THREATS & CHALLENGES:

- Proper digital development requires good political coordination, synchronising the steps forward and ascertaining that the whole initiative is going in the same direction. Finding that common vision might be challenging.
- Besides cooperation among member states and entities from various sectors, trust should be also one of the requirements for third-party and external investments. Systems like Alipay or Aliexpress provide a way to create jobs in many cross-border sectors, such as e-commerce, yet they are still in a sense

linked to China, despite posing as private investments. Each investment from a foreign entity should meet adequate levels of security and trust which might be challenging with some partners.

- Bringing together the communities that are often rather separate – such as the technical, policy, economic, or security community – is another challenge for the region. There are also entities which, due to no history of cyberattacks and incidents, do not invest in cybersecurity and certainly do not treat it as one of their priorities.

THE WAY FORWARD:

- The public sector should reach out to their private sector partners to find innovative solutions to their problems. The authorities should communicate its role in coordination, decision-making, the vision, and data sharing. This partnership built on common goals and synchronised technologies can not only solve the pressing issues, but also boost the overall digital development of the region.
- Member states need to set certain principles and standards, enshrined either in laws or regulations, or as part of policies, that will be followed by investors. The governments are not directing the investments, but should expect investors to meet basic requirements concerning common values, such as democracy and free market principles.
- Rules of the game have to be clear and lasting, as this is of greatest interest for both the leaders and investors. This must, however, be based on trust, which should be achieved through monitoring, open and transparent discussions, and with respect to different legislations and norms present in the region.
- It is vital to ascertain that all of the partnering countries invest in the Three Seas Initiative Investment Fund and that expressed political commitments are more than just words. There is a strong support from the overwhelming majority of member states, and also from the United States of America. It is essential to make sure that each and every one of these commitments lead to an actual investment in the Three Seas Initiative and that it attracts private sector capital as well.
- The level of digitalisation of the service industry in the Three Seas is still relatively low. The first goal for the 3SI would be to develop the North-South axis through combining increased digital investments with already existing advantages of the region. Such modern, solid, and secure infrastructure will be an incentive for domestic and foreign investment projects, positively impacting the region and the companies operating on the internal market.

"If you manage only the physical part of the country then you basically manage only half of a country – and who is managing the other half? (...) You cannot divide physical or digital anymore, so you have to understand digital if you want to maintain the country or the region, if you want to maintain the economy or the defence system."

BORIS KOPRIVNIKAR

"We, as governments, are not directing the investments, but we expect investments to meet certain basic criteria concerning our democratic governance and free market principles that are as basic as they get."

JONATAN VSEVIOV

"The Three Seas Initative Investment Fund is purely commercial, independent from any politician's decisions. We have an independent investment advisor that is looking for projects and is looking for money for the projects. From that end we have independent investment committee and it is not the decision of the certain country, this is the decision of the professionals that are looking for the projects for us and supporting us in this."

PIOTR KARNKOWSKI

"You have to think when you're building things, even when private sector is building these various structures – like the digital highway that was suggested by The Kosciuszko Institute – what that means. And if you're not on a secure infrastructure how that could be down the road, how that could affect your businesses and societies down the road, as security and supply chain issues are going to be a critical part of it."

CHRISTOPHER PAINTER

"We definitely need more involvement of private sector. I would reinforce this, and not only in terms of the investors, but also in terms of the private sector being part of delivery of those infrastructure, applications, and the services."

KAROL OKOŃSKI

"The private tech sector has not always done very well on making its own products secure. Until relatively recently, the idea was to build them and see what the problems with them were later."

SCOTT MALCOMSON


FUTURE STREAM

6th EUROPEAN CYBERSECURITY FORUM – CYBERSEC GLOBAL 2020

PRESERVING OPEN INTERNET

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Vinton Cerf** – Vice President and Chief Internet Evangelist, Google

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The Internet has become an integral part of many lives and it is vital to keep it open. An open place where information can be generated, discovered and shared. It has shown a remarkable ability to adapt to and evolve with the changing situation of our world. We have seen that it managed to support online interaction in times of great stress. We have seen that it is capable of evolving. There are significant upsides to the way in which the Internet is being used. It is an enormous source of information, it provides tools, it is enabling the production of information and its discovery. Nevertheless, it also enables bad behaviour like misinformation and disinformation, the spread of malware, denial of service attacks, hacking, fraud, bullying, and social divisiveness. It is a powerful tool also for those who want to use it to do harm. There is a need to find a middle ground between strong protection of people's privacy and the effect it may have on the efficiency of law enforcement, especially operating across the borders.

MAIN THREATS & CHALLENGES:

- In some parts of the world, the openness of the Internet is under threat.
- There is a danger that in response to online harm or in trying to protect our citizens we will go to the extremes, for example by suppressing and censoring information, by inhibiting access to various websites – none of it can and should serve as a one-size-fits-all solution. There is a tension between protecting people's safety using surveillance and other techniques of this kind and between protecting their privacy.
- Currently we witness rather segregated cloud environments. This creates a danger for the consumer of being trapped into using only one brand of hardware and software.

THE WAY FORWARD:

- The Internet should be kept open and people should be allowed to access, explore, generate, and share information that they believe is important to others. To face global challenges like pandemic, global warming or social and economic inequalities, we need high-quality information and the Internet will be the key tool to tackle them in this respect.
- Applications, protocols, and standards should be developed to allow for improved communication between processes in different cloud environments, owned by different operators and providers. We need intercloud standards to enable more secure and sustainable inter-cloud transfers of data, also in regard to regional cloud systems.

- International and cross-border cooperation underpinned by norms and best practices is necessary to protect citizens from online harm. As proposed by the Global Commission on the Stability of Cyberspace, the public core of the Internet should not be attacked, both during peacetime and in times of conflict.
- Strong authentication, which often translates into two-factor authentication, is critical for individual protection and for enabling online commerce and online transactions. It should also be championed by international cooperation and become part of an international agenda.
- Consideration of a digital single market should be focused on commonality, on shared safety, security, and affordability standards. At the same time, it should not inhibit the ability of exchange across the boundaries with the rest of the world.

"We must preserve all the positive benefits of the Internet that we know and have been experiencing for some decades now while at the same time dealing with some of the harmful behaviours that we know are possible. Finding a balance between those two is a job that you and I should undertake because if we don't do that, the value of the Internet will diminish and that will be a great loss for humanity."

VINTON CERF

HACKING HUMANS – THREATS TO DIGITAL IDENTITY

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Theresa Payton** – White House Chief Information Officer (2006–2008); CEO and Chief Advisor, Fortalice
- **Carsten Maple** – Professor of Cyber Systems Engineering, WMG, Principal Investigator NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research, Deputy Pro-Vice-Chancellor (North America), University of Warwick; Fellow, Alan Turing Institute
- **Paco Garcia** – Chief Technology Officer, Yoti
- **Vikas Choudhary** – Head of Cybersecurity for Europe, Tata Consultancy Services
- Chaired by **Aaron Ostrovsky** – Expert of the Kosciuszko Institute

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Already before 2020, the rise of commercially available solutions based on biometric data processing, genetic testing and nanotechnology has raised the questions over personal data protection and big data ethics. And with the COVID-19 pandemic we have witnessed a rapid spread and implementation of technologies like contact-tracing that touch upon sensitive civil liberty issues and that might be viewed by some as surveillance. It inevitably opens the discussion on how much access is needed, how data should be used and secured in this context, and whether the citizens should be allowed to opt out. The effectiveness of surveillance is also often questioned and whether the trade-offs of invading citizens' privacy is actually producing tangible results in terms of security. We don't really understand our digital footprints and what they actually tell about us. Whereas the use of facial recognition is more and more regulated, the rules vary depending on the sector – while often the private sector is guided by rules that define what is allowed under the law, the use of facial recognition in the public sector is much less transparent. The debates become more and more circular– some argue for the need of having security prevail over privacy in times of social stress while others point to privacy as the overarching value. At the same time malicious threats of data misuse proliferate as the pandemic shows us that it is demanding to ensure data protection under extraordinary circumstances.

MAIN THREATS & CHALLENGES:

- During the pandemic direct attacks on remote access protocols – underpinning remote working – were observed. Home infrastructure has never been built to be particularly secure plus for many the home environment provides more distractions than the normal course of working. As a consequence ransomware, business email compromises, and human-targeted attacks multiply.
- There are conscious and unconscious biases that exist in many surveillance technologies, for instance the application of AI to facial recognition. Engineered with ingenious protocols and algorithms underpinning facial recognition, the resulting systems are often biased due to the bias in databases upon which they have been trained.
- With regard to digital identity and digital footprint there is a rarely acknowledged possibility of poisoning and manipulation of that data for malicious purposes, e.g. by injection of fake information.

- Personal data can not only be stolen but also compromised. Personal digital footprints manipulated in this way can then be presented to behaviour-based analytics to influence misguided judgment calls on innocent people.
- There is a huge potential for mistakes and errors in terms of applying automated facial recognition. The effects might be highly disruptive, especially when considered in areas like law enforcement.
- By the time regulation is passed and actually understood it is often already out of date. Often regulation is a barrier that can effectively hamper an idea before it can even get started due to very high costs of compliance.

THE WAY FORWARD:

- There are no permanent fixes to the rise of successful intrusions caused by the multiplication of cyber-threats accompanying the pandemic. However, companies should focus on remote access protocols as they really limit user access controls and lower user permissions to the least privileged.
- A strong digital identity will make it easier for both governments and citizens to deal with emergencies like the COVID-19 pandemic. It will allow them to leverage the existing infrastructure to provide the citizens with quick access to government help and crucial services.
- There is a need for an individual or consumer privacy bill of rights. It should provide for a popular understanding of what constitutes a digital footprint and what rights stem from it, for example in ways through which it can be corrected or cleaned.
- More transparency is needed in terms of facial recognition performance. It is critical to ensure that we do not exclude specific groups by designing a system that will deny access to a particular service because a given individual is from a group (racially-defined, gender-defined or age-defined) that the AI is just not good enough at identifying.
- Regulators should be careful to make sure that the laws they impose won't block application of technologies, as such blockade is always temporary and leads to implementation delays. A stable regulatory framework has to be established, for new technologies to be piloted and monitored along the way. These regulations should be harmonised across borders and they should be preceded by sharing of harmonised practices and codes of ethics.

> "We have seen all of these businesses being forced to work in a completely remote scenario, sometimes, that has not been anticipated. I think that created a massive gap when it comes to security controls and access management systems (...)."

PACO GARCIA

"How to make sure that our digital footprint is something that is not up for sale, it isn't something that is exploitable, that is hackable?"

AARON OSTROVSKY

"One of the things that I think is important and should always be remembered is proportionality. If we are infringing on an individual's rights to privacy, then what we have to think of is: is it in the greater good? What kind of incursion on our privacy is created and how much does it benefit society?"

CARSTEN MAPLE

"We really do need some type of an individual or consumer privacy bill of rights."

THERESA PAYTON

"When it comes to security by design or privacy by design, this has to be really a continuous journey. Because what is reliable, what is robust, what is resilient today may not be tomorrow."

VIKAS CHOUDHARY

INTERNATIONAL SECURITY IN THE ERA OF QUANTUM COMPUTING

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Deborah Frincke** – Associate Laboratory Director for National Security Sciences, Oak Ridge National Laboratory, Department of Energy; Director of Research, National Security Agency, USA (2014–2020)
- **Michele Mosca** – Co-Founder and Professor, Institute for Quantum Computing, University of Waterloo; Co-Founder and President, CEO, evolutionQ Inc.
- **Jaya Baloo** – Vice-Chair, Strategic Advisory Board, Quantum Flagship; CISO, Avast Software
- **Vikram Sharma** – Founder and CEO, QuintessenceLabs
- **Vladimir Soukharev** – Principal Cryptographic Technologist, Chief Post-Quantum Researcher, Infosec Global
- Chaired by **Amit Katwala** – Senior Editor, WIRED UK

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Quantum computers have a potential to revolutionise everything from material science to financial risk analysis. Quantum-sensing opportunities – like quantum metrology, an ability to use entangled qubits in order to get more precise measurements – are often overlooked in the discussions on the transformative character of this technology. It can improve everything from the safety, security, and precision of the GPS to other kinds of sensors resulting in an increased ability to pinpoint where activities are occurring for national security purposes. But quantum computers can also have big cybersecurity implications – they can break some of the most used algorithms, including in communications and cryptography, carrying potentially big geopolitical implications on an international scale. In 1994, Peter Shor identified an algorithm capable of breaking the RSA cryptosystem that is at the core of public-key encryption. This concern initiated the quest for quantum-proof algorithms and development of post-quantum cryptography. Some allege that the dawn of quantum computing will have a devastating impact on national security. Nevertheless, it remains uncertain when and how efficient, sustainable, and applicable quantum advantage – the ability of the quantum computer to outperform the classical one – will be achieved and deployed to crash security perimeters in cryptography and cybersecurity.

MAIN THREATS & CHALLENGES:

- Quantum computers can theoretically perform some complicated computations exponentially faster than binary computers, thus creating an immediate danger to our encryption keys and algorithms. This threat caused research on quantum-resistant algorithms, a quest to devise a new algorithm that is secure against both classical and quantum attacks on encryption.
- The dawn of full-scale high-performance quantum computing will force both the security sector and the tech community to adapt their entire security architectures. It will take a long time to transition cyber systems to quantum-level resiliency. There is a danger that it will not be done in time.

- There is a risk in the legacy of outdated infrastructure used to transfer and store data, particularly in regard to the public sector. Lots of publicly managed databases, including for critical systems, are using crypto algorithms that are decades old. If they will not be updated with potentially quantum-resistant algorithms that are already available, they might jeopardise not only data that has been hitherto placed there, but also the security of data to be created in the future.
- Hybrid networks of computing infrastructure using the quantum might have vulnerabilities to both physics-based and mathematics-based cyberattacks. Security of the supply chains might contribute to the overall security of these networks.
- As much as the adoption of agile crypto is needed, it will also bring the challenge of standards application, namely, how to make the standards agile to keep up with the change of algorithms.

THE WAY FORWARD:

- As much as quantum computing can pose a threat to some of the techniques that we're using today to safeguard sensitive information, it offers an opportunity to strengthen it as well.
- The dawn of quantum and accompanying worries should be taken as an incentive to rebuild foundations of our security by redeploying new crypto and adding new defences like quantum key distribution or quantum random number generation.
- It is important to try to develop diversified algorithms for post-quantum cryptography and aim to have multiple standardised algorithms with different mathematical problems underpinning them.
- We should start to enhance the protection of critical infrastructure with hybrid cryptography combining classical and post-quantum crypto in order to ensure that it will be secured when the future quantum threat materialises.
- The adoption of hybrid cryptography should be followed by a transition to crypto agility. Agile algorithms and agile key management will be important to address future vulnerabilities and respond to future standardisation steps.
- Every large enterprise organisation needs to develop a serious risk-based quantum readiness plan and update it regularly. It should be remembered that different companies might have different timelines in this respect, depending of the character and lifecycle of their products or services. Companies that want to prepare for the dawn of quantum, in particular essential service providers or critical infrastructure operators, should run an inventory of their crypto assets, assess their implementation readiness for new crypto, and plan transition to agile crypto. They should also identify assets and innovative technologies that a company already has and build on that. Finally, they should also ensure that the supply chains they rely on are secured with adherence to certain standards.
- From a security point of view, the debate about how to transition to post-quantum cryptography should be prudent and restricted. While the threat should not be downplayed, it is easy to misjudge where the dangers are and rush to inadequate actions. In the nearest future, we should perhaps worry more about a poorly designed algorithm rushed to defend against a hypothetical quantum computer than about an actual one. Flawed implementations present a risk of potentially damaging loses, so it is important to remain pro-active but prudent at the same time.

"To dismiss this as hype is very dangerous, I think. Very serious people around the world sincerely believe and then the key milestones keep being achieved again and again and again. So I think the threat is real. The certainty is not there, yet by the time it's certain it's far too late to react and I think the temperature is already too high to keep in a wait and see mode."

MICHELE MOSCA

"There are so many creative ways people attack computing systems, it might be bio-inspired next (...). It means that the reality of our profession is we have to think ahead in terms of what adversarial action there might be. Agility, resilience, all of those things are important for designing security."

DEBORAH FRINCKE

"Beyond the whole idea of a digital divide simply by the haves and the have-nots, there're going to be very specific restrictions imposed, even if you could potentially afford this technology, it wouldn't be allowed to be used by anyone."

JAYA BALOO

"What we think is critical is for organisations to really understand the data holdings that they have and what is sensitive within those data holdings. What potential threat vectors those holdings are exposed to. And therefore coming up with an appropriate protection profile to protect that information."

VIKRAM SHARMA

"Cryptographic agility comes at various levels we are implementing step by step. Algorithms, of course, are the first thing to do but then the keys, and then – if we ever actually solve this problem somehow – to get secure yet agile certificates."

VLADIMIR SOUKHAREV

SPLINTERNET – POSSIBLE SCENARIO OR TECH-DYSTOPIA?

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

OXFORD DEBATE

FOR: Robert Knake – Whitney Shepardson Senior Fellow, Council on Foreign Relations; Director for Cybersecurity Policy, US National Security Council (2011–2015)
AGAINST: Milton Mueller – Founder, Internet Governance Project; Professor, Georgia Institute of Technology, School of Public Policy
Host: Neal Pollard – Chief Information Security Officer, UBS AG

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Robert Knake: At some point in this decade the Chinese government, with the support of Russia and other authoritarian regimes, will move forward with plans to establish a separate DNS root system for their share of the Internet. It will be a point that will indicate that we really have a fractured or fragmented Internet. For China having its own root server is a matter of international prestige and this can be observed in its actions in ICANN. The Chinese perceive it as a showcase of their technological capabilities and resources. They have also begun to establish their own root server for research purposes.

Milton Mueller: By providing a consistent global root for all domain names, we ensure that any domain name in the world can connect to any Internet service provider and thus any end user in the world. If a different root server was introduced, it would mean that a specific domain would be different in different places. We're debating whether the domain system is going to be the site of fragmentation and whether China is going to be the one that initiates that fragmentation. I think this is not going to happen. The power of global compatibility and interoperability of a common naming system is so strong that nobody has an incentive to break that up.

THE THREAT:

Robert Knake: We are heading towards the direction of splinternet and a lot of that has been caused by the Trump Administration's responses to China's Huawei and other companies. China will continue to manipulate the application layer and if the geopolitical situation will compel it to, China might change its copy of the root zone file. This may happen for instance in case of a conflict with Taiwan. China has also showed interest in messing with the fundamental compatibility in other areas. For instance, their new IP approach may lead to fundamentally altering the suite that has served us since the Internet's founding in order to provide an easier kill switch over the Internet traffic.

Milton Mueller: Yes, we can observe the fragmentation in the application layer, but that demand is coming from the United States, not China. It is the US that is initiating this fragmentation. It is true that China as an authoritarian state wants to control the Internet in their domestic territory. But what China does not want is to rupture the fundamental global compatibility that allows it to communicate when it wants to. The so-called New IP approach is not a move towards incompatibility or isolation of China but a purely commercial initiative. They are promoting a new IP and they want it to be globally compatible, to be standardised by the ITU and the EITF. The measures that the US is taking to block China are actually counterproductive. In a few years it will force China to create their own chip industry and exert more control over their manufacturers and suppliers.

THE WAY FORWARD:

Robert Knake: We need to come together as democratic and capitalist nations – a democratic Internet freedom league. United States should agree with Europe on shared standards regarding the free flow of data and against data localisation. The US and EU should aim to create an Internet maybe less global but more free than it is today. It should take the form of a system, perhaps a digital trade zone that will not be dependent on China and in which China will be able to participate if it accommodates to its rules and reforms.

Milton Mueller: Even if we see some sort of a technical division of work in the Internet stemming from the actions of the United States aimed against China, it will not come from the domain name system but rather supply chains, etc. If we maintain compatibility with China, the global Internet will head rather peacefully towards a more integrated global economy. A digital free trade zone is an idea, but it should be extended to include the authoritarian countries as much as possible. We should bargain with them to get them to open up. We should be expanding and globalising the Internet as it was intended to be, using freedom or the popular sovereignty in cyberspace as the constituency for this effort.

"China's interest in controlling the Internet extends well beyond just their national borders and outside their national firewall, they're also exporting these ideas to others."

ROBERT KNAKE

"The measures that the US is taking to cut off the Chinese are actually reinforcing all of the nationalistic and authoritarian elements."

MILTON MUELLER

"We see a patchwork of disparate privacy regimes going in some cases towards data localisation which also has interest in hampering the free flow of data across borders."

NEAL POLLARD

ARTIFICIAL INTELLIGENCE – HORIZONS OF THE NEAR FUTURE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Aleksandra Przegalińska-Skierkowska** – Associate Professor, Kozminski University; Associate Researcher, American Institute for Economic Research; MIT Research Fellow (2016–2020)

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Currently, we are in a phase where we no longer only talk about artificial intelligence, we no longer just speculate about how it is going to unfold in the future, what it is going to bring, what potential threats and opportunities it offers. We are already in a moment where we can say that artificial intelligence is here and is becoming productive in many different domains of life. From logistics to transportation, from the medical sector to the financial sector, from tech to education – wherever you look, you already have applications of artificial intelligence. Also, the artificial intelligence itself is developing very rapidly. We no longer have systems that solely reply to people, we have systems that build narratives and stories. We have major developments in image recognition and machine vision. In 2020, just before the pandemic, xenobots were created. These are systems designed by the artificial intelligence, carbon-based cell clusters thought up by silicon, the first display of something that can be called artificial life. All that adds up to a very robust picture of what artificial intelligence already can offer.

MAIN THREATS & CHALLENGES:

- In the upcoming future we will face many pressing challenges: how to teach artificial intelligence, how to raise awareness around it, and how to combine AI with sustainability.

THE WAY FORWARD:

- Explainability and transparency in artificial intelligence is the condition for future growth and scaling, particularly when you think about the issue of scaling deep learning to such domains as medicine, judiciary, or finance.
- The future we are heading towards might rather be a future where humans and machines work together than a future where machines will work fully on human's behalf thus rendering humans unnecessary. Such human–machine collaboration will result in a work that will be more efficient, and – for humans – perhaps more satisfying.
- Quantum computers may help in gathering and harvesting huge amounts of data, a problem that is emerging today.

"In the future we will have a discussion about for instance the big data paradigm (...). Thus, who have more data, definitely have a competitive advantage. In the short-term future we can expect a major discussion about infrastructure that can help in processing that data."

ALEKSANDRA PRZEGALIŃSKA-SKIERKOWSKA

HUMAN-LEVEL ARTIFICIAL INTELLIGENCE: PROBABILITY, RISKS, OPPORTUNITIES

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Allan Dafoe** – Director, Centre for the Governance of AI, Future of Humanity Institute; Associate Professor, International Politics of AI, University of Oxford
- **Stuart J. Russell** – Professor, Electrical Engineering and Computer Sciences, UC Berkeley
- **Przemysław Biecek** – Principal Data Scientist, Samsung R&D Institute Poland

Chaired by **Andrea G. Rodríguez** – CYBERSEC 2019 Young Leader; research fellow, Barcelona Centre for International Affairs (CIDOB); Associate Member, Observatory for the Social and Ethical Impact of Artificial Intelligence (OdiseIA)

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

70 years ago, Alan Turing initiated the quest to develop a computer smarter than a human brain by introducing a test examining the ability of a machine to imitate intelligent human behavior. Arguably, some chatbots have already passed this test, but we cannot say that sentient machines are fully developed, at least not yet. It seems to be a matter of time before we reach the monumental stage of the human–machine convergence by developing a perfect integration of human and machine, or a machine even more capable than a human being. Superintelligence could drastically change the future of humanity by immense advancements in the science and technology sectors, but it comes at a price: we would have the potential to cure diseases, fight climate change, eliminate poverty, and achieve higher levels of productivity, but run the risk of increased surveillance, possible unparalleled inequality and bias, and control of society. Technological singularity is a futuristic concept that might turn into reality once technology exceeds the computing power of a human brain and will be able to comprehend and master any cerebral task that humans can do. It was first presented to the world by Stanislaw Ulam, brilliant Polish mathematician who reported on his discussion on that matter with John von Neumann, and we feel obliged to warn the world against this existential challenge.

MAIN THREATS & CHALLENGES:

- Humanity needs to change the course of action to solve the problems of control and alignment. Without solving them, humanity may face the side-effects of advanced AI (such as polarisation in the algorithmic management of social media). Bias and transparency derive from the problems of control and alignment.
- Artificial superintelligence may replicate the biases of humanity and become an existential risk. It is "humanity's final test".
- AI competition jeopardises the development of advanced AI and threatens the development of aligned AI systems.

THE WAY FORWARD:

- We need to transcend the "standard model" of AI in which machines achieve pre-defined objectives to a model in which machines know that they don't know what the real objective is.

- We need to create new communication channels and means between humans and machines that will allow for more precision in communication.
- To solve bias, we – society as a whole – need to have a conversation to translate the result into metrics.
- Invest in cooperative AI to complement AI safety to increase humanity's wealth and well-being.
- There isn't a single set of universal values that can be embedded into machines: we need to learn how to aggregate preferences and establish trade-offs.

"We are having different ecosystems that are competing with each other in terms of technological development (...). Most of the other problems – we're more or less dealing with them: biases in transparency, in the algorithms... but the problem of alignment is a long-term problem."

ANDREA G. RODRÍGUEZ

"In the development of advanced AI, common interest vastly exceeds any conflict of interest."

ALLAN DAFOE

"Alignment is not a matter of guessing what the right objective is and putting it in. Alignment is designing systems that don't know what the objective is."

STUART J. RUSSELL

"The development in AI will be very close to the development of new interfaces in communication between these machines and humans. So I don't think of superintelligence as a separate being that will evolve despite of us, or against us, but I think that it will be very closely combined with our goals and tasks."

PRZEMYSŁAW BIECEK

4th CYBERSEC BRUSSELS LEADERS' FORESIGHT 2021

THE SUN AFTER THE RAIN? FREE AND SAFE DATA FLOWS ACROSS THE ATLANTIC AND BEYOND

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Didier Reynders** – Commissioner for Justice, European Commission

BIG PICTURE – WHY THIS TOPIC MATTERS?

The pandemic has underlined the importance of privacy and data flows. In fighting the virus or helping the recovery of our economies, innovative digital solutions can really make a difference. From the common standards for contact tracing apps to the legislative proposal we are preparing for a digital green pass – EU-COVID-card to enable Europeans to move. Privacy is part of the solution in response to the pandemic but also more generally as technology continues to transform our lives. We also experience in these challenging times how critical the transfers of personal data are, for so many aspects of our lives – to ensure the continuity of government and business operations or education activities, to develop cooperation in scientific research, or to enable social interactions.

Robust data protection safeguards are a key part of the trust towards institutions. This has been the case in many initiatives. It is on that basis that two years ago we created with Japan the world's largest area of free and safe data flows. We are concluding a similar deal with Korea as we speak and two weeks ago we launched the adoption process for two adequacy decisions concerning the United Kingdom as an important piece of our new relationship after Brexit, it is clearly also a priority on both sides of the Atlantic. The amount of changes and lessons learned from the past marks the significance of the subject and leads us to rethink safe data flows.

MAIN THREATS & CHALLENGES:

- Probably more than ever before it has become clear that protecting privacy and facilitating data flows have to go hand in hand.
- New opportunities facilitate trusted data flows and thus trade, as well as cooperation between public and regulatory authorities. Opportunities correspond with the growing number of privacy laws around the world.
- Facilitating free and trusted data flow also plays a central role in the new forward-looking EU-US Agenda for Global Change that the EU has proposed to the Biden administration.
- The issues that need to be solved between the EU and the US can strike the delicate but crucial balance between national security and privacy.

- Only an arrangement that is fully compliant with the ECJ judgments can deliver the stability and legal certainty businesses deserve and expect on both sides of the Atlantic. Finding a legally solid arrangement is in everyone's interest.

THE WAY FORWARD

- Cooperation with regional organisations ought to be intensified, such as ASEAN where the EU uses model contractual clauses. Developing a successor arrangement to the EU-US Privacy Shield is important.
- The Transatlantic Community should be able to develop appropriate solutions and to address principles that are cherished on both sides of the Atlantic: access to court, enforceable individual rights, and limitations against excessive interference with privacy.
- The EU and US have to make sure that technologies protect privacy and make democracies more resilient and need more cooperation with like-minded partners to shape behaviour of emerging technologies and establish guardrails against misuse.
- Together with like-minded partners the EU and the US should intensify their cooperation at bilateral and military level. The Transatlantic Community ought to ensure effective law enforcement cooperation adapted to the realities of today's digital world. It is also working on a bilateral agreement that will facilitate the gathering of electronic evidence including true direct cooperation with service providers while reducing possible conflicts of laws.

"Only an arrangement that is fully compliant with the Court judgment can deliver the stability and legal certainty businesses deserve and expect on both sides of the Atlantic. Finding a legally solid arrangement is in all mutual interest."

DIDIER REYNDERS

FROM DATA LAKES TO A DATA OCEAN? DEBATING THE FUTURE OF TRANSATLANTIC DATA FLOWS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Mark Montgomery** – Executive Director, the US Cyberspace Solarium Commission
- **Patrick Breyer** – Member of the European Parliament
- **Cecilia Bonefeld-Dahl** – Director-General, DIGITALEUROPE
- **Lise Fuhr** – Director General, ETNO
- **Alisa Vekeman** – Policy Officer, International Data Flows and Protection, DG JUST, European Commission
- Chaired by **Ana Jankov** – Director, Strategic Communications, FTI Consulting

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

The exponential growth of data proves how rapidly we are digitally transforming all domains of our social and personal lives. However, it can also be subjected to misconduct regarding privacy, citizens' rights, democratic processes and even to human rights abuses. As despite its air-like features, data still has to be stored physically (and therefore be geographically located) in many parts of the world, we can hear calls for greater data localisation and protection. Data transfers between the EU and entities outside of Europe are one of the bigger bones of contention, also for the transatlantic relationship. In 2020, we saw the European Court of Justice invalidating the Privacy Shield, a base for the transatlantic data transfer between the EU and the US. It was accompanied by new regulations, like the Data Governance Act proposed by the European Commission that has put an obligation on data sharing intermediaries to appoint a legal representative in an EU member state that will be accountable to laws and authorities of that state. Europeans have also sped up their efforts to establish a European federated cloud under the name GAIA-X, in order to achieve greater sovereignty.

Navigating this evolving landscape is a great challenge for politicians, entrepreneurs, and privacy activists on both sides of the Atlantic, who should not lose sight of the common direction that is the revival of transatlantic relationship. Establishing a data ocean, built upon the Atlantic Ocean, where pooling and sharing of data will be done while respecting the rules and values acceptable to all involved is one of the ideas for solving this challenge. Regardless, a debate on the future of data management is now needed more than ever, not only to make more of the digital assets, but also to enhance and structure the EU's relationships with its main partners.

MAIN THREATS & CHALLENGES:

- The so-called Schrems II judgement by the European Court of Justice which invalidated the Privacy Shield has brought a lot of confusion and uncertainty, in particular to businesses operating on data. Many companies on the international market are unsure how to function without breaking any laws and some are even unaware that they might be operating illegally.
- Standard Contractual Clauses are the most used tool for data transfers in Europe. The challenge for the European Commission is to update the SCCs so that they reflect the needs of the companies and are in compliance with current laws, such as the GDPR.

- Many disagree that in the economy there is no non-sensitive data, but undoubtedly there are certain types of data which are more or less sensitive, and therefore require adequate levels of protection, in some cases not as rigorous and strict as in others. Finding the balance and writing it into law so that people are safe but businesses are thriving will be challenging.
- A potential disruption of data flows will have a huge effect on everyone. Ultimately, data will be the main driver of the recovery, and going forward it will power our connectivity through the 5G, IoT, and AI. We cannot afford neither unregulated nor obstructed data flows.
- The negotiations between the EU and the US are complex because of different perspectives on data privacy and mass surveillance. Both sides need to reform their regulatory landscape to provide for more understanding, transparency, and finally a comprehensive agreement.
- The precedence of either privacy or national security in certain cases is pretty blurry. Mass surveillance poses a lot of questions and challenges in relation to human rights and stability of states, and data collection, management, and transfer are sadly in the middle of that.

THE WAY FORWARD:

- Ensuring that personal data of EU citizens is key for the European Commission and it is reflected in both its communication and EU-related activities, such as the update of standard contractual clauses, but also in the negotiations with the US. The transatlantic data flows should be regulated in a way that respects the rights of both Europeans and Americans and does so in a coherent approach.
- Modern businesses thrive on data. It should be our priority to protect the data powering those companies and check that the companies themselves have the tools to ensure that. Such action will empower businesses to play an even bigger role in the recovery process.
- Federal data privacy law in the United States could solve a lot of issues in the negotiations with the EU, by placing both sides of the Atlantic on the same adequate level, especially when it comes to common values and trust between partners.
- The transatlantic negotiations are not the only process in the field of ensuring data protection. Adequacy talks with other like-minded countries, for example in Asia or Latin America, are equally as important to allow the European market and international trade to grow while putting in place the highest standards of security for the citizens' data.
- Finding the balance between privacy and national security is key to make sure neither citizens nor states are on the losing side in the process of setting up data protection laws. International cooperation in this field is absolutely crucial to make sure no laws or human rights are breached.

"Data protection is about the right to informational self-determination – every citizen should have the right to decide themselves who knows what about our private life. This is needed for the exercise of many fundamental rights. If you don't know who's aware of your secrets, then you cannot behave freely."

PATRICK BREYER

"I do think the biggest obstacle in the European Union – US data talks is one of trusts and in some respects a fundamental mismatch in the reality and the perception of surveillance regimes in both jurisdictions."

MARK MONTGOMERY

"We see the rapid growth that the 5G will actually make. It will make IoT happen and IoT will feed a lot of data into AI, and all of this actually embraces the digital ambition and leadership we have in the EU. We need data flows and we need international data flows to feed all of this, so we need the connectivity."

LISE FUHR

"Right now we know that 85% of all growth will come outside Europe. Where does that leave European global companies if they can't transfer data? It would be devastating for our economy. We should put demands on our trading partners to find solutions with us – that's the road ahead that we should take."

CECILIA BONEFELD-DAHL

"More and more countries around the world are addressing similar challenges that come with the new digital globalised world in similar ways, for example by putting in place similar privacy laws. There is now a momentum for like-minded countries to work together on these issues."

ALISA VEKEMAN


TOGETHER
AGAINST ADVERSARIAL INTERNET


Keynote Speech
FUTURE STREAM KEYNOTE
speaker:
Let's step into the cybersecure FUTURE
Vinton Cerf
#CSGlobal


European Cybersecurity Journal

SIDE SESSIONS AND SPECIAL FORMATS

6th EUROPEAN CYBERSECURITY FORUM – CYBERSEC GLOBAL 2020

TOGETHER AGAINST DISINFORMATION – WHERE PUBLIC SECTOR MEETS PRIVATE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

SPECIAL LUNCHBREAK SESSION with the particiaption of:

- **Viktoras Daukšas** – Head of Debunk.eu initiative, Debunk EU
- **Jonáš Syrovátka** – Program Manager, Prague Security Studies Institute
- **Magdalena Wrzosek** – Head of Strategic Analysis and Emerging Technologies Team, NASK
- Chaired by **Nikos Sarris** – Project Coordinator, Social Observatory for Disinformation and Social Media Analysis (SOMA)

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

One of the most pressing issues surrounding the setup of a resilient European system against hybrid threats and disinformation is the fragmentation in the field. Local and national initiatives are becoming more and more widespread, which – while contributing to the sectional capacity – adds little to the build-up of regional resilience. For their part, the European Union institutions strive to streamline strategically justified resources in order to promote a more all-encompassing approach, e.g. by establishment of a pan-European SOMA Disinformation Observatory. Similar endeavours, such as the European Digital Media Observatory, are expected to work as collaborative platforms for even more collaborative communities, as well as to provide a solid base for operational activities.

The SOMA Disinformation Observatory serves the community of experts and gathers around 90 organisations, some of them outside the European soil, as a collaborative forum for joint investigations and information-sharing. Still, the setup of a resilient system require undertaking a whole-of-society approach with a clear objective of an integration of all sectors – public, private, and the so-called Civil Society Organisations (CSOs). The structural differences, diverging modi operandi and (sometimes) colliding objectives can make the successful and good-faith collaboration a serious strategic challenge. This calls both for an information-exchange space and, more importantly, for an increased mutual understanding and finding a common denominator.

For that reason, (self-)regulatory initiatives such the Commission's Code of Practice on Disinformation are valuable yet must be complimented with a good cooperation between the private and public sector, NGOs, and academia. All sectors have their resources and possess unique expertise they can contribute, and which is crucial for rolling out a successful and resilient system.

MAIN THREATS & CHALLENGES:

- Disinformation and InfoOps represent types of information disorders (hybrid threats) carried out to achieve strategic and overarching objectives of dividing societies, undermining public trust in democratic institutions, distorting decision-making process, etc. In the European Union disinformation and InfoOps are frequently attributed to the external actions of the Russian Federationz as they are present in their military strategy (the so-called Gerasimov's doctrine).
- Mass-scale attempts of a public opinion manipulation on social media platforms, proved by the material leaked in 2018 by a Cambridge Analytica ex-employee, has attracted a lot of attention from EU regulators. Some posted content qualifies as InfoOps, electoral interference, and coordinated influence operations.
- The year 2016 was an eye-opener due to the US presidential elections and Brexit, both of which were investigated under suspicion of foreign electoral and influence operations. Their eventual outcomes confirmed that foreign interferences had indeed taken place and were reported in the set of the US Senate Intelligence Committee's documents between 2019 and 2020 and by the UK Parliament in 2019.
- A significant threat is using democratic values against democracies themselves. Rule of law, complexity (and sometimes sluggishness) of decision-making processes, fundamental and human rights, and multi-stakeholder management in democracies can all be instrumentally exploited by third-party actors who can try e.g. to impede the processes themselves or abuse democratic freedoms, such as the freedom of speech.
- National laws regulating such issues as obligations of the social media platforms or ensuring protection of free speech lead to regional divergence of definitions, scopes of application making the efforts even more taxing.
- Unquestionably one of the rationales behind malicious and coordinated campaigns is to polarise and divide societies. This can result in scapegoating and spreading hatred against particular communities, such as minorities.

THE WAY FORWARD:

- A new regulation is indispensable, but from the very beginning must be based on cherishing freedom of expression and on protecting the EU citizens. It should bring in more clarity and understanding between member states.
- The community should strive to involve researchers, universities, civil society organisations, and think tanks in the fight against disinformation. It has to be treated as a cross-competence field, and be transparently and strategically funded.
- The community must not overlook the growing role of artificial intelligence and process automation, balanced with human work and expertise. These may both decrease the costs (especially per unit) and increase productivity over time.
- Enhanced cooperation and greater information exchange could positively affect general efficiency of the community.

- Critical thinking and media literacy competences and tools ought to be trained and available to all citizens. Our resilience should not shun an open conversation about what is working and what isn't. There is a need to push for a greater transparency and responsibility of the platforms.
- The more platforms open their data to researchers, analysts, and journalists, the better and safer society we will have. This involves also the right to privacy and its sufficient protection.

"This debate about the ratio between the computational method and the human touch is very much relevant, but this has to be even more nuanced and [we need to understand better] the sphere [in which] we are operating."

JONÁŠ SYROVÁTKA

"We need to look on what human tasks could be automated, so humans could focus on more creative work and become more productive than they are right now."

VIKTORAS DAUKŠAS

"It's all about the data and how in the modern world your own data could be weaponised against you. To really regulate this area, we really need cooperation between the sectors.""

MAGDALENA WRZOSEK

"Collaboration is not easy (...) where on the one side we have the official institutions and the governments, and the platforms that are trying from their side to minimise disinformation. On the other side, we have the private sector, who many times are sceptical against (...) some actors of the public sector."

NIKOS SARRIS

THE REVIEW OF THE NIS DIRECTIVE

INVITATION-ONLY VIRTUAL ROUNDTABLE

Moderated by **Jakub Boratyński** – Acting Director, Digital Society, Trust and Cybersecurity Directorate, DG CONNECT, European Commission

BIG PICTURE – WHY THIS TOPIC MATTERS?

The NIS Directive is the first EU-wide cybersecurity legislation addressing, among others, risks and the damage posed by cyberattacks. As part of the new work programme unveiled in January 2020, the European Commission has undertaken the review of the Directive – a routine procedure of assessing the effectiveness and practical impact of the legislation, which as a result will help address the gaps and inconsistencies by proposing new solutions. The main areas covered by the revision encompass identification of operators of essential services (OES), the role of digital service providers (DSPs), the scope, sectors and services, and lessons learned from COVID-19. The Commission has gathered transposition reports from member states, as well as feedback from businesses and organisations during the public consultations.

Currently, all the member states have transposed the Directive into national laws and have adopted national cybersecurity strategies. The significant outcome of NIS Directive is raising awareness regarding the cybersecurity, as well as boosting preparedness, cooperation, and information exchange among member states. The next step for the Commission is to further strengthen the European cybersecurity posture.

MAIN THREATS & CHALLENGES:

- Inconsistencies in implementation and gaps in transposition are affecting the overall cybersecurity system of Europe. Due to lack of commonly shared standards in this regard certain actors might be treated differently and abide by different rules depending on the country.
- Different sectors show different maturity levels in cybersecurity, especially when it comes to their ability to handle incident response. Such fragmentation is visible not only between companies but countries as well.
- The Cybersecurity Act, whilst building on the NIS Directive, introduces new themes and challenges. It is important to recognise whether the potential overlaps bring added value or impose conflicting requirements.
- Incident reporting depends on where the legal representative of a company is located and to whom they answer. Europe-wide, the rules on reporting lack consistency and effectiveness, which only raises the stakes of potential attacks and hinders our collective response.
- The threat landscape is changing rapidly, as cyber criminals find new ways to exploit vulnerabilities of our systems, infrastructures, and devices. Ransomware, credential harvesting, malware, VPN exploits, and IoT attacks are on the rise, posing serious threats not only to businesses and institutions, but national and international security as well.

THE WAY FORWARD:

- Many member states decided to go beyond the Directive and cover additional sectors, such as food, public administration, and judiciary. The Commission should recognise the importance and criticality of some sectors and consider adding them to the revised version of the Directive. This will not only limit discrepancies and gaps, but also harmonise the system across the entire EU.
- Reporting thresholds should be improved through stronger legislative harmonisation. The rules should be reasonable, qualitative, risk-based, and threat-based, taking into consideration the amount and character of the information shared.
- Public-private partnerships should be improved, not only when it comes to incident reporting, but also deploying new systems, handling data, and operating on the market. All parts of the digital ecosystem should work together and have their respective responsibilities, especially when it comes to cooperation with external partners.
- Member states and the private sector need practical guidelines on risk management: how to identify risks, perform risk management processes, and mitigate threats.
- In the NIS Directive, only three types of digital service providers were covered. The catalogue of DSPs should be therefore revised and possibly extended. Responsibilities of DSPs, especially in the context of cloud service providers, also should be discussed.
- The EU should support coordination and finding solutions to the question of a common cloud approach, in particular when it comes to the practice of cloud service providers processing personal and non-personal data outside the EU territory.
- European Union regulatory requirements should be aligned with international standards and best practices. It is important when dealing with cross-border entities that deliver their services cross-border and operate on the European market.
- Supply chain value should be considered as an important building block for a high level of common security. The focus of the NIS is on the certification of products, while the Cybersecurity Act touches upon the certification of both products and processes, for example the elections. Those elements deserve the attention when building a stronger and more mature cybersecurity system.

FOSTERING INTERNATIONAL COOPERATION TO ACHIEVE A SECURE 5G NETWORK

INVITATION-ONLY VIRTUAL ROUNDTABLE

Moderated by **Ciaran Martin** – Professor of Practice in the Management of Public Organisations, Blavatnik School of Government, University of Oxford; CEO, UK National Cybersecurity Centre (2016-2020)

RECOMMENDATIONS PREPARED BY CIARAN MARTIN

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

5G security is now regarded as one of the most critical cybersecurity challenges of our time across a wide range of countries. The geopolitical aspect of it in the West, and the controversy over the role of untrusted vendors in the network from authoritarian countries, especially China, has dominated the discussion. But what lies beneath this?

The issues fall into two main categories. One is economic. The market for providers of telecommunications infrastructure has become dangerously consolidated in recent years. The second is technical. The telecommunications industry is behind where it needs to be already on infrastructure insecurity, and bringing it up to date with the demands of 5G is very challenging.

Furthermore, for a variety of reasons, telecommunications companies, particularly in Europe, have not been particularly commercially successful. Meanwhile, the commercial reality is that upgrading security and supplying safety costs.

Indeed, whilst the discussion followed the format of perspectives from governments, then vendors, and then operators, by the end participants agreed that an equally good starting point was the perspective of the operators. Solutions must work for them. Vendors agreed; open and interoperable frameworks had to work commercially. That was the challenge for governments as they sought to promote trustworthy infrastructure, built with adequate security.

MAIN THREATS & CHALLENGES:

- The starting point is precarious. Networks are not secure enough and the market contains few choices.
- Regulation, particularly in Europe, has not incentivised the correct commercial response to tackle the problem.
- The architecture of 5G is complex. Virtualisation offers some clear opportunities but needs to be carefully managed.
- The proposals for a more open, interoperable Radio Access Network (Open RAN) and other similar initiatives are very important, but have to take account of the reality that this is a scale business.
- International cooperation across different governments and global companies is difficult.

THE WAY FORWARD:

- Whilst difficult, international cooperation is essential to tackle this strategic challenge, so a number of suggestions were made about how to foster the required alliances.
- Open and interoperable systems are a critical and urgent part of the solution to the huge challenge of 5G security. Alternatives are badly needed for sustainable solutions.
- We need to be flexible to re-frame our way of thinking about this. In a market economy we have to be able to start with the citizen and the operator, not just the government. The solution has to work for them.
- Scale is required, and scale takes time, as well as money.
- Agreeing and enforcing appropriate, workable standards are also among the most critical areas. Building secure 5G networks is one thing; operating them over a period of several decades is another.

GEOPOLITICS OF EMERGING TECHNOLOGIES – NEW REPORT BY THE KOSCIUSZKO INSTITUTE

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

PANEL DISCUSSION with the particiaption of:

- **Teodor Buchner** – Information Technology Security Analyst, EXATEL; Scientist at Faculty of Physics, Warsaw University of Technology
- **Magdalena Wrzosek** – Head of Strategic Analysis and Emerging Technologies Team, NASK
- **Przemysław Roguski** – Lecturer, Chair of Public International Law, Jagiellonian University; Expert of the Kosciuszko Institute
- **Michał Jaworski** – Technology Director, Member of the Board, Microsoft
- **Izabela Albrycht** – Chair, The Kosciuszko Institute; President, Organising Committee of the European Cybersecurity Forum – CYBERSEC
- Chaired by **Michał Rekowski** – Director, Strategic Partnerships and Projects, The Kosciuszko Institute

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

Digital technologies are going to be a determining factor in the ongoing struggle for global leadership. Whoever masters the AI, cloud computing, big data, 5G, quantum computing will grant themselves a better and stronger position in the new multipolar international order that is in the making. The world's superpowers and biggest companies recognise that, which is why they are heavily investing in the development of the abovementioned technologies to secure their domination. This race, however, starts to resemble a digital Cold War resulting in the bifurcation of the digital world.

To be able to find our way in this ever-evolving landscape of threats and opportunities, like-minded countries across the globe need first and foremost to understand in depth the nature of challenges stemming from the consequences that technology advances have for politics, international security, and the economy. Those aspects remain largely unexplored and lack thorough understanding by the general public, hence the Kosciuszko Institute has published a detailed report examining and explaining the geopolitical significance of those developments. This timely subject was further explored during the Conference in a panel discussion with partners of the report.

MAIN THREATS & CHALLENGES:

- The technological rivalry between countries and companies is slowly turning into the digital Cold War, centred around the US and China, and their respective areas of influence. This race affects not only the geopolitical and economic relations, but also the military domain as emerging and disruptive technologies can bring tremendous advantages on the future battlefields.
- The value of data generated through digital technologies is growing exponentially, as a result having a significant geoeconomic and geopolitical impact. This process is likely to accelerate even more due to the digital transformation of economies and businesses, greater network throughput, growing number of connected devices, and finally the surge of industrial data that will surely fuel the international rivalry even more.

- Locations of data centres are dependent not only on the climate, accessible infrastructure, or the customer base – politics and legal regimes are equally as important. This raises two concerns: data stored in countries not abiding by the rule of law cannot be controlled nor protected from abuse of privacy; and countries hosting major data centres have great influence over cloud service providers under their jurisdiction, which can also hinder international cooperation and information exchange.
- European infrastructure and solutions are oftentimes built or provided by external partners from third countries, thus the Union does not have full control of the system. Lack of commonly shared regulatory rules for all member states and external parties raises many issues concerning ownership, protection, and privacy of data.
- The definition of digital sovereignty or autonomy in Europe is still in the making. The Union has to find a way to distance itself from China, notorious for lack of transparency, abuse of power, and violation of human rights.
- Over the past few years we have observed increased fragmentation of the global Internet into smaller nationally administered networks, as was the case in China, Russia, Iran, or North Korea. Other countries might follow suit in the future, which would hinder information exchange, isolate parts of the world and thus allow potential abuse of human rights.

THE WAY FORWARD:

- Big data and advanced analytics enable forecasting and support real-time decision-making, as a result granting critical advantage to those capable of using it. Accumulating data inside states and companies hinders free cross-border data flows, which is why like-minded countries should cooperate on ensuring more openness, transparency, and clear rules on data management.
- Trust should be embedded in both the development and deployment of technologies, which can be achieved only if all stakeholders work together to build partnerships based on shared values.
- Since many elements of the digital ecosystem in Europe come from external sources, the EU should focus on the protection of data and rights of its citizens. This can be done through standardisation and certification bodies which would enforce transparent and non-discriminatory rules on partners operating on the European market.
- Digital sovereignty in Europe should be built on clear rules, based on commonly shared democratic values. The new ecosystem needs legal mechanisms that would protect human rights and ensure both openness and transparency of the system.
- Fragmentation of the Internet along geographical borders of countries is only enabling more oppression and exploitation. The Internet as a tool should be accessible to everyone and not separated between authoritarian and democratic spheres of influence. Like-minded countries should cooperate on ensuring that international law is respected and working worldwide, thus protecting human rights and mitigating risks of abuse.

"I believe that data is and will be the engine of all sorts of value creation. Nowadays experts already consider data and the information it can generate to be the most significant and attractive geopolitical asset."

IZABELA ALBRYCHT

"The state where data centers are located or the state in which those big cloud service providers are registered has jurisdiction over them. This means that those states have big power of influence over both the actions of those companies as well as over the data that is located on them."

PRZEMYSŁAW ROGUSKI

"We can prepare the ecosystem here in Europe which will force companies to follow some kind of rules, and these rules would be certification and standardization."

MAGDALENA WRZOSEK

"Europe has completely overslept the technological race concerning data storage and encryption, and now they are trying to have the ground back. We will not start to develop our own products, but we will standardize them and in this way we will have the cards at hand again."

TEODOR BUCHNER

"For us at Microsoft and for other cloud vendors, the word trust is one of the keywords. We need to work together with the other stakeholders on how to build the trust in the IT environment, in the digital environment."

MICHAŁ JAWORSKI

"We might be heading towards not only the division of global universal internet, the so-called splinterment, but also towards bifurcation in the global technology management, one that may result in the establishment of two conflicting blocks of nations that produce and operate incompatible technologies."

MICHAŁ REKOWSKI

4th CYBERSEC BRUSSELS LEADERS' FORESIGHT 2021

EU DIGITAL POLICY FORESIGHT STREAM

EU CYBER PACKAGE – A SHIELD AGAINST ADVERSARIES

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

SPECIAL KEYNOTE by **Margaritis Schinas** – Vice-President for Promoting our European Way of Life, European Commission

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

In July 2020 the European Commission has presented its first-ever comprehensive Security Union Strategy that has taken cybersecurity out of its "technology" silo and put it firmly at the heart of the EU's security policy. It aimed to introduce an approach in which measures to tackle both physical and digital security threats run seamlessly. As physical and digital systems are nowadays interdependent, cybersecurity is the stream that will allow the EU to connect all the dots of the security ecosystem, and, under the single roof of the Security Union, develop the four strands of priority actions: ensuring a future-proof security environment; tackling modern threats; protecting Europeans from terrorism and organised crime; and building a strong industrial and societal security ecosystem. It will also contribute to the protection of citizens' privacy. The EU's Cybersecurity Strategy obviously concentrates on regulatory, investment, and policy strands in order to achieve greater resilience, technological sovereignty and leadership, build operational capacity, and advance a global and open cyberspace. However, the pursuit of digital sovereignty does not entail a protectionist move. It is about fostering the European values, defining Europe's own rules, and making autonomous technological choices. It also means putting on the market European solutions that are competitive and that enrich the palette globally.

MAIN THREATS & CHALLENGES:

- Malicious actors have continued their aggressive cyber operations during the pandemic, often taking advantage of the ongoing health crisis. Cyberattacks have targeted European health infrastructures, such as the European Medicines Agency, and state-sponsored cyberespionage actors have targeted pharmaceutical companies and COVID-19 vaccine researchers.
- The negative impact of cyberattacks on economy and society is rapidly increasing. According to the EU's Joint Research Centre, cybercrime is estimated to have cost the world EUR 5.5 trillion in 2020, and a ransomware attack is expected to target businesses every 11 seconds in 2021.
- Cyberattacks are becoming more and more sophisticated, thus becoming harder to detect. On average, it takes organisations six months to detect a breach in their network.
- We are facing a massive skills shortage in the EU in the field of cybersecurity. We estimate that we lack 291,000 posts for cybersecurity professionals in Europe.

- We are observing growing geopolitical tensions over the global and open Internet and over control of technologies across the whole supply chain.

THE WAY FORWARD:

- In the cybersecurity context, in the upcoming five years, the EU will have to respond to the deployment of key enabling technologies (like 5G or IoT) that will significantly increase the potential attack surface. Also, it will have to correct the difficulties unveiled by the pandemic that imply the digitalisation of most societal and economic activities.
- It is essential to strengthen EU's cyber capabilities, namely the tools to detect, mitigate, and deter cyber-security risks. To achieve it, a combined investment from the EU, its Member States and the industry is necessary, reaching up to €4.5 billion over the next seven years. It also requires long-term capabilities planning. Private sector must be a key part of this process.
- European Commission has announced the creation of a Joint Cyber Unit with the target of mobilising operational capabilities to enable response to significant cross-border cyber incidents. The JCU will serve as a platform bringing together the different cybersecurity communities in the EU, defence, civilian, law enforcement, and diplomacy and enhancing information sharing among relevant EU and national stakeholders, helping them to develop a common understanding of the threat landscape and coordinate their response.
- Law enforcement authorities should partner up with the private sector and research organisations to develop solutions that will allow European law enforcement to be at least at equal footing with cyber criminals.
- To address the skills shortage, European Commission has taken specific initiatives, like the European Education Area, Skills Agenda, and the Digital Education Action Plan, which all have a strong focus on investing in cybersecurity education and giving access to relevant learning opportunities in cybersecurity and IT. Educational activities should also strive to increase the inclusion of women in cybersecurity work-force in Europe.
- Culture of cooperation is essential for cybersecurity. European Union is open to working together with like-minded partners across the world towards a safe and open global cyberspace.

"We are changing the paradigm. And by doing this, we are protecting not only our critical digital systems, but also our businesses, our economy, our societies, our values, and ultimately our democracy. Cybersecurity is not just an objective. It is essential for protecting our European way of life. It is one of the fundamental pillars of what Europe represents in today's world."

MARGARITIS SCHINAS

ENISA'S ROLE IN THE NEW & UPGRADED CYBERSECURITY ECOSYSTEM

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Juhan Lepassaar** – Executive Director, ENISA

BIG PICTURE – WHY THIS TOPIC MATTERS?

For ages, communities all over the globe were studying the future – what is to come, when they can expect it, and how it is going to affect them. In the past, people have turned all of their burning questions to gods and higher beings seeking signs and advice, as was the case with ancient Greece. Once the Oracles shared their insight, the Greeks were able to make decisions that would help them avoid some perils and maybe even change the destiny in their favour.

Foresight is key to fully grasp the reality we are facing and prepare for the challenges that might come along. That task, however, is particularly difficult nowadays as we have found ourselves in a dynamically developing and interconnected world. The future is not fixed – it is constantly in flux, which is why we need international institutions and agencies to provide that much needed outlook and prepare us for what the future holds. In Europe that mission is fulfilled by the European Commission and ENISA, through guidelines found for example in the Cybersecurity Strategy, the Security Union Strategy, and the Framework of the Digital Decade for Europe, as well as threat landscape reports. Those documents help us understand the risks and opportunities, but also point towards the direction we should follow to maximise our security, resilience, and potential. Making sure our society, institutions, and infrastructure are well prepared for the future and trust each other is the priority for all of us.

MAIN THREATS & CHALLENGES:

- Resilient infrastructure is the fundament of the digital society, which is already emerging in front of our very eyes. As this new society will be dependent on technologies such as 5G, 6G, and quantum communication, the challenge for us is to prepare infrastructure that is strong enough to withstand any possible disruptions that could greatly affect all of us.
- Parts of new infrastructure are built on top of past elements, for example 5G operates on upgraded 3G and 4G systems. Using legacy systems is not inherently wrong, but oftentimes exposes new vulnerabilities that might be used by adversaries.
- Trust is the most important element of the digital ecosystem, enabling transactions, partnerships, collaborations, and information exchange. Especially now with the plethora of services and stakeholders involved, we need tools and frameworks that would allow citizens, institutions, and systems alike to trust each other to create a stronger digital society.

THE WAY FORWARD:

- Understanding risks and opportunities is absolutely key to prepare our infrastructures for the future, upgrade our defences, and fully benefit from the use of new technologies. Risk assessments and threat landscape reports should be the primary source of knowledge and basis for guidelines in this process.

- Risk assessments and incident reports help discover vulnerabilities of legacy technologies and provide guidelines for upgrading them in a way that raises the overall level of resilience, strength, and preparedness. This is particularly important when deploying new technologies or solutions that will operate on such infrastructure.
- Trust can be embedded into the digital society through authentication of actors, sources, and tools. This should extend to all parts of the society: the people, machines, and devices they are using. European Digital Identity project might allow for more robust authentication and as a result provide for a safer, stronger, and more trusted system.

"Public service and digitalisation of public service is an important challenge but if we look at the issues involved or if we look at the plethora of services that the public sector offers, the most important service is trust."

JUHAN LEPASSAAR

THE EVOLVING CYBERTHREAT & REGULATORY LANDSCAPE – HOW EUROPEAN REGULATIONS RESPOND TO GLOBAL THREATS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Raj Samani** – Chief Scientist, Fellow, McAfee

BIG PICTURE – WHY THIS TOPIC MATTERS?

The digital environment and cybersecurity are frequently seen as IT or digital issues, disregarding their impact on many other sectors and even society as a whole. The increasing number of cyberattacks and growing engagement of states and state-backed actors in illicit and malicious activities call for a better regulatory protection against cyber threats. Many sectors are exposed to cybercrimes and can fall prey to hackers and other malign actors, as was the case in the Operation Diànxùn and Hafnium attack earlier on this year. Public and private sector entities cooperate with the law enforcement, but making this process more effective requires a comprehensive regulatory framework and a better, closer, and more tech-savvy collaboration between different actors.

MAIN THREATS & CHALLENGES:

- Criminals care less and less about the damage they can cause, even when their actions are putting people's health and lives at stake. Moreover, their interest in the public sector and its services (including health) grows, spilling over to its democratic processes, such as elections.
- Cyberespionage campaigns, such as the Operation Diànxùn, can be targeted at 5G service providers and telecoms. Given the power and interconnectivity of (geo)politics and new technologies, the risks and potential consequences are tremendous.
- Misinformation campaigns, such as these connecting coronavirus to 5G networks are carried out with the use of botnets, which maximises their reach and raises the potential of constituting an alternative source of "information" undermining trust in institutions. Governments, while trying to fight the health crisis, face a surge of fake news on exaggerated risks of vaccines, which aim at slowing down or thwarting vaccination efforts.

THE WAY FORWARD:

- The cybersecurity discourse has to evolve from its IT/digital roots to a more inclusive, whole-of-society approach as its consequences impact us all. Only by understanding the interdependencies of cybersecurity and technologies, and embedding those in our frameworks, guidelines, and strategies, will we be able to create a more secure society.
- Our regulatory frameworks need to be redeveloped and backed with actionable intelligence and direct actions. Instead of retaliatory measures, these should include well-functioning response mechanisms.

- For a more secure digital society, we need to develop mechanisms that underline the importance of cybersecurity in our daily lives. This requires better communication and more active participation from the citizens themselves and companies. The public sector needs to be strengthened, enhanced, and more digitally capable to support that.

"Beyond the volume of attacks, I think the one thing that we often fail to do, because we're just so quick going from one major crisis to another major crisis, is [that] we're not really stopping to ask ourselves the question: what does this actually all mean?"

RAJ SAMANI

EUROPE FIT FOR THE DIGITAL AGE: WHY (DIGITAL) SOVEREIGNTY REQUIRES (CYBER) SECURITY

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

KEYNOTE by **Casper Klynge** – Vice President, European Government Affairs, Microsoft

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

One of the most pressing issues linked to the accelerating digital transformation is Europe's will to build its digital sovereignty. COVID-19 changed the way we function, highlighting growing dependency on digital solutions. The new reality underscored both the challenges and opportunities that derive from this shift to virtual and digital work and communication. It has also led European politicians to recognise the importance of digital sovereignty and its role as a response to the future and emerging challenges. Europe must base its actions on its strengths: research and academia. Bolstering digital cooperation comes with responsibility to build the Digital Age reality in harmony with Europe's core democratic values. In this context, the European Commission laid out the European Digital Strategy with ambitious plans of using digital solutions for the benefit of the society, creating new business opportunities, fostering technological development, ensuring security, privacy, and data protection. To be successful on the European level, digital transformation requires secure and sovereign digital infrastructure and bold legislation.

When debating whether Europe is fit for the digital age, one factor cannot be overlooked – cybersecurity, a necessary ingredient of digital sovereignty. Private businesses and governments are playing a crucial role in building the security architecture of the digital ecosystem. Cybersecurity is more and more vital for the secure and effective functioning of modern economies, especially during the current COVID-19 crisis which comes together with new cybercrime patterns and security challenges, shaking up the status quo.

MAIN THREATS & CHALLENGES:

- Past months have shown how modern societies are dependent on technology on every level, from education through economy to health systems. In this context one of the crucial challenges to tackle is the digital divide, these days visible more than ever before.
- Europe's answer to the digital transformation challenges, which is mostly focused on privacy issues, cybersecurity, economic opportunities, and mutual dependencies, needs to include guidelines on how to navigate between addressing these concerns and reaping the benefits.
- Lack of a commonly accepted definition and understanding of the digital sovereignty notion leaves a lot of room for different interests and stakeholders, as a result slowing the process down. Setting the trajectory of Europe's digital transformation should be based on the right balance between protection and openness.
- The COVID-19 crisis presented us with more evidence of expanding cybersecurity threat landscape. Many cybercriminals have turned their attention to healthcare systems, hospitals and vaccine distribution operations. These attacks and malign activities are characterised by its cross-border and global nature, which makes them impossible to combat only at the regional level.

THE WAY FORWARD:

- Promoting sovereignty by increasing cybersecurity requires more international collaboration. Cybersecurity is not bound by conventional borders – it is both cross-border and cross-sectoral, as underlined in the proposal of NIS 2 Directive. There is an urgent need to boost coalitions among responsible countries across the globe who share an interest in joint cybersecurity capacity building.
- Microsoft and other big-tech companies have a responsibility to contribute to the COVID-19 recovery process, also by addressing the concerns around technology and the role the industry plays in society. Technology should run on trust.
- Europe should use its unique opportunity to lead the way to the digital sovereignty. Defining the technological agenda based on European values and regulatory standards should be combined with setting necessary guardrails to protect democracy and the rule of law.
- Building a more secure, resilient, and forward-looking cyberspace should be based on multistakeholderism, partnerships, and information exchange. Enabling discussions on the norms in cyberspace, defending democracy and common values by boosting coalitions among like-minded countries, and expertise sharing are all vital to this process.
- Tech companies must develop technology that meets Europe's needs in terms of privacy, safety, security, one built on shared values, trust, and cooperation. At the same time, however, it should not matter where the products and services come from but whether their providers play by the rules of the game.

"There can be no digital sovereignty without cybersecurity. But what does this mean in practice? Today national security requires close collaboration due to mutual dependencies. Technology has in many ways changed the notion of what it takes to defend the nation and today's foreign cyber weapons pose a critical threat to the future of our societies and the stability of our government, our industries, and our infrastructure."

CASPER KLYNGE

PARADIGM SHIFT: TAKING A PROACTIVE STANCE IN RESPONDING TO CYBERTHREATS

WATCH THE VIDEO ON CYBERSEC YOUTUBE CHANNEL

FIRESIDE CHAT with **Dan Cimpean** – General Director, Romanian National Computer Security Incident Response Team (CERT-RO)
Chaired by **Michał Rekowski** – CYBERSEC Programme Director, Research Director, the Kosciuszko Institute

THE BIG PICTURE – WHY THIS TOPIC MATTERS?

In December of 2020, the Council of the European Union has selected Bucharest as the seat for the European Cybersecurity Competence Centre, the ECCC. It will massively contribute to the Europe's cyber posture by injecting new funds and launching new programs and research in cyber innovation. It will also foster direct industry support and cybersecurity awareness on an unprecedent scale. The ECCC will also provide Europe with more diversity of technological choices and better capabilities. It will be important, as some of the most notorious cyberattacks that we have witnessed at the beginning of 2021 – Hafnium and SolarWinds – have completely changed the way we think about cyberdefences. These attacks were executed with an unprecedent level of preparedness, as not only were the attackers very knowledgeable but also apparently well-funded and had a lot of time to brace up for the execution. With so much time passing since these attacks were apparently launched to the moment they were detected, to the moment the cybersecurity community started not to only to react but to coordinate the response with suppliers and the network of organisations looking into them, there is a need for a paradigm shift as the adversaries we face are much more sophisticated.

MAIN THREATS & CHALLENGES:

- The most recent cyberattacks have shown that malicious actors can be exceptionally prepared, highly professional, and well-resourced.
- Attacks that exploit supply chains significantly increase the attack surface, putting more pressure on the defenders.
- Capabilities of cybersecurity institutions in Central Eastern Europe are being continuously tested by the adversaries, some of which are the state actors.

THE WAY FORWARD:

- CERTs in Europe should be proactive. They should support other bodies in conducting an honest review of their own resilience capabilities, challenge them continuously, and test their stated level of security. CERTs should push those organisations to adopt the right frameworks and right type of assessment.
- As cyberthreats will likely not only stay with us forever but also increase in level of sophistication and complexity, decision-makers in Europe should accept risk. They should adopt the assumption that cyber crisis will happen at some point and learn to be flexible, evaluate the risks, and prepare proper responses.

- Cybersecurity assessment procedures in the EU should increase in frequency. Specific achievements should be presented and evaluated in a strict manner, and Europe should not rest on its laurels if it wants to keep pace with North America, Asia, and other geographies. It should raise its ambitions and goals, as it can still do much more in terms of its cybersecurity posture.

" We are kind of risk-adverse, we don't like risks. I think we should embrace those, we should know them, properly assess them, and evaluate them, work with the assumption that a cybersecurity crisis – which probably would be actually a hybrid crisis, so combined with other categories of crisis – will happen at the European level, at the member state level."

DAN CIMPEAN


Lunchbreak Session
TOGETHER AGAINST DISINFORMATION - WHERE PUBLIC SECTOR MEETS PRIVATE
speakers:
host:
TOGETHER
AGAINST ADVERSARIAL INTERNET
Viktoras Daukšas
Jonáš Syrovátka
Magdalena Wrzosek
Nikos Sarris
#CSGlobal
CYBERSEC
EUROPEAN CYBERSECURITY FORUM


Lunchbreak Session
TOGETHER AGAINST DISINFORMATION - WHERE PUBLIC SECTOR MEETS PRIVATE
speakers:
host:
Viktoras Daukšas
Jonáš Syrovátka
Magdalena Wrzosek
Nikos Sarris
#CSGlobal
CYBERSEC

CYBERSEC GLOBAL 2020 PARTNERS

Strategic Partners

Microsoft · SAMSUNG · PZU · FACEBOOK · ORLEN · Google

Main Institutional Partner

NATO CI COE

Main Partners

ERICSSON · vodafone · asseco · UBS · T · NOKIA

Partners

orange · inSilesia · aws · Kraków · EXATEL

CYBERSEC BRUSSELS 2021 PARTNERS

MAIN PARTNERS
CYBERSEC Brussels 2021

Microsoft · ORLEN · Google

PARTNERS
CYBERSEC Brussels 2021

pwc · PZU · McAfee · THREE SEAS INITIATIVE INVESTMENT FUND