CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

SUMMARY

ROAD TO CYBERSEC 2020

SERIES OF VIRTUAL **TASK FORCE MEETINGS**

Dear CYBERSEC Friends,

"Digital" has become the new normal, increasing its role in the functioning of states, business continuity, and the societies' wellbeing. As the ongoing health crisis greatly accelerated the digital transformation, the need to discuss some of the key technological developments is even more valid. With this in mind, we decided to enrich the preparations for CYBERSEC Global 2020 through a series of consultations with Members of the CYBERSEC Programme Committee.

Within the span of four months we have organized nine webinars focusing on selected topics, some of which have later become part of the CYBERSEC Global 2020 agenda. The first digital-only edition of the Forum has already come to an end and we can proudly admit that the preparatory conversations we had certainly helped to shape it into a truly enjoyable and inspiring event.

This year's leitmotif – Together Against Adversarial Internet, perfectly illustrated what we should focus on: fostering multistakeholder discussions among like-minded countries and institutions, as it is key to understand and successfully undertake the challenges on the horizon. We are convinced that the Road to CYBERSEC meetings have not only contributed to the Forum's agenda, but also allowed us to exchange perspectives on some of the most crucial parts of the digital ecosystem. None of this could have been possible without you – our Experts, Partners, Friends.

With this publication we share with you the summary of all Road to CYBERSEC meetings. We have had many inspiring conversations on topics such as adversarial use of big data, military applications of 5G and human-level artificial intelligence. There are still plenty of other subjects that require our attention and we are looking forward to discussing them with you soon.

Thank you for your engagement in the meetings. We truly appreciate your support and hope to continue our fruitful discussions in the future.

Yours sincerely,

CYBERSEC Team

TABLE OF CONTENTS

4 **Meeting #1**
TOWARDS A GLOBAL SURVEILLANCE SOCIETY? THE RACE BETWEEN AUTHORITARIAN AND DEMOCRATIC PRACTICES OF DIGITAL GOVERNANCE

9 **Meeting #2**
BIG DATA = BIG CHALLENGES? COUNTERING ADVERSITY IN THE DATA-DRIVEN ECONOMY

13 **Meeting #3**
CYBERSECURITY IN THE ERA OF DECOUPLING IN THE DIGITAL SUPPLY CHAIN

17 **Meeting #4**
HOW COVID-19 REDEFINED THE CRITICAL SECTORS OF ECONOMIES

21 **Meeting #5**
SECURITY OF 5G AND INTERNATIONAL COLLABORATION

26 **Meeting #6**
MISINFORMATION IN TIMES OF #COVID19

30 **Meeting #7**
TACKLING CYBERSECURITY CHALLENGES DURING THE PANDEMIC IN THE FIELDS OF HEALTHCARE AND FINANCIAL SECTORS

34 **Meeting #8**
HACKING HUMANS – THREATS TO DIGITAL IDENTITY

38 **Meeting #9**
HUMAN-LEVEL AI – PROBABILITY, RISKS, OPPORTUNITIES

Meeting #1

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

14 May 2020

INTRODUCTION

For the better part of the last few decades, the Internet was idealised as a global open network which is free, interoperable, secure and resilient. Although these might have been the intentions once it was designed, all current emerging technologies, with the new opportunities they provide, also bring an array of challenges for human rights, democratic processes and privacy. Biometrics, artificial intelligence, smart cities, IoT or fifth-generation networks are only examples of technologies that might be used to advance digital transformation but also may be applied in an adversarial way, for example to enhance and enable so-called digital authoritarianism. The collection and misuse of citizens' data is breaking down traditional notions of privacy. There are countries which impose censorship and perform surveillance by using technology to achieve their political goals. Digital tools are facilitating the control over citizens. Governments are deploying sophisticated tools and microtargeting to carry on propaganda, often augmented by the AI in order to foster political divisions and spread fake news.

Therefore, like-minded countries have to stand together for the respect of democratic values, privacy and freedom of expression, and ensure that the Internet does not become a Trojan horse used for increased control, oppression and influence on societies' behaviour. Technology and online platforms must serve the public good and empower citizens to make their own social, political and economic choices without manipulation, surveillance, spyware and censorship. If democracy as we know it (and as we want it to be) is to get through the digital age, the real solutions to the problem of adversarial and abusive use of technologies must be found.

Nowadays, the discussion on the surveillance practices is very much narrowed to the topic of contact-tracing apps related to the current COVID-19 pandemic. The number of such apps around the world has sharply increased over the past month and the rush to digitise contact tracing is on. The apps are designed to help slow the spread of the virus by tracking the network of contacts between individuals and notifying individuals once they were in close proximity to an infected person.

But with all the good intentions that developers might have, these tools can also have some limitations from the privacy point of view. Based on statistics,[1] it appears that almost one fourth of the apps have no privacy policy. More than half of them do not disclose how long they will

store users' data for and have no publicly stated anonymity measures. Even when apps have these measures in place, they are exposed to hacking and could also tempt some governments to abuse the data and monitor people beyond the pandemic period.

The aim of the first webinar in the series of Road to CYBERSEC Task Force Meetings was to discuss with participants the following questions: how to deploy new disruptive technologies without crossing the invisible line of privacy intrusion; how to make sure that like-minded countries will set up tech policies in the right way; how important is the trust in technology itself or the trust in government while we are deploying intrusive solutions; what does it take to make technology for good and to get public acceptance for it in our democratic societies.

The following aspects were highlighted: the changing nature of surveillance; contact tracing in the times of COVID-19 and the importance of the narrative; political leadership and accountability; cooperation, multi-stakeholder dialogue and interdisciplinary approach, authoritarian practices in developing countries.

Each of the topics is elaborated below. As one of the main goals of the meeting was to clarify challenges and important points in the discussion on the subject of surveillance, very often more questions than answers appeared. We believe that this approach stimulates and serves public debate by boosting the need for a multi-stakeholder approach and by demonstrating the key aspects for further discussion.

THE CHANGING NATURE OF SURVEILLANCE

Human and machine interactions, increasing amount of digital data and the resulting information are changing the face of humanity. The lack of understanding of how these interactions are driving the surveillance activities, bringing an enormous intrusion into our lives, is becoming the cause of great concern. The societies are aware of the dual-use nature of emerging technologies. In the times of a health crisis, such as the COVID-19 pandemic, digital tools are faced with the challenging task to effectively stop the spread of the virus without endangering citizens' rights and privacy. Within like-minded countries, there is a consensus on the importance of personal liberty in the sense of the capacity to live the lives according to the reasons and motives that are our own. Fundamental freedoms and resistance against attempts to diminish them are the core values our society is based on. However, the nature of cyberspace and our increased digital presence has taken away a substantial amount of our autonomy (whether we live in a democratic society or under an authoritarian regime) – the autonomy that allows us to tell right from wrong. With the emerging technologies, the meaning of surveillance has been fundamentally redefined. The tools are becoming more and more powerful by enabling information to be collected, stored, and then connected together on an unprecedented scale. It is high time for the discussion on what controls we need to put in place in order to ensure the privacy, security and fundamental right to autonomy, exploiting at the same time the potential of technology for common good and productivity growths.

CONTACT TRACING IN THE TIMES OF COVID-19 & THE IMPORTANCE OF THE NARRATIVE

The current pandemic situation demonstrated the need for states across the world to intervene in unprecedented ways, redefining the state power that might seem frightening. Many governments are nowadays using digital tracing tools in order to protect the well-being of the people and to limit the spread of the virus. Their main objectives are to help manage the risk for individuals and to provide useful information to decision-makers on what steps should be taken in regard to the pandemic. However, one can notice worrisome voices and conspiracy theories about nations trying to build a mass surveillance tool. As stated by one of our experts: the truth is rather more boring and contact-tracing apps are not a one-way highway to a surveillance state. They are rather a careful and transparent experiment, open for independent technical critiques from security experts and cryptographers. The majority of the contact-tracing apps that appeared in the democratic countries are voluntary and do not collect or use any participants' location data, which is seldom adequately underlined in the public discourse. The question of the proper narrative remains therefore one of the most crucial ones – how the use of the seemingly same technology differs in democratic nations and in non-democratic countries.

COOPERATION, MULTI-STAKEHOLDER DIALOGUE & INTERDISCIPLINARY APPROACH

Contact-tracing apps are an interesting example and case study of not only the challenges that technology brings but also the uses of technology to deal with emergency situations. One of them is the question of national responsibilities versus international approach. Health domain is an area that national authorities tend to guard within their own framework of activities. The cooperation, in order to be successful, must be then bottom-up (one example of such a cooperation that gathered together national authorities is the common EU toolbox to support contact tracing in the EU's fight against COVID-19). The second issue is the need for an interdisciplinary approach and wider debate that is crucial in the governance of cutting-edge technologies, which is becoming less and less a matter of technology itself, and much more a social and economic matter in general. In the case of contact-tracing applications these are, among others, public health authorities, technology specialists, privacy experts, ethicists, sociologists. We must always think about a whole array of aspects and impacts a given technology might have.

There is also a need to formulate principles that are more practical, reasonable and feasible, and that hinder or even prevent the surveillance practices. While developing a proper model of governance for technological tools, it is worth to make use of both social and technological constructs at the same time. An example of this approach is the Estonian health records system. Estonia has a centralised, state-run health system accessible to authorised individuals, and citizens are notified once someone has accessed their health records (technology construct). This kind of notifications prevents unnecessary access, exerting social pressure and promoting widely accepted rules (social construct).

POLITICAL LEADERSHIP AND ACCOUNTABILITY

Another challenge is that we find ourselves in a situation where, besides activities carried out by the international bodies (EU toolbox created by the EC), technology providers (e.g. currently Google and Apple) are putting themselves as the gatekeepers on how this technology is going to work most effectively, how it is going to be deployed in an interoperable way, and how it can be shared. The challenge regarding the division of responsibilities in digital transformation between public and private sector arises. Therefore, the debate on the cooperation between technology providers and national authorities is ongoing and will probably crop up again for other emerging technologies in the future. Who do we want to take the leadership over the technological tools that are more and more present in our daily lives and to which we are giving more and more of our data – the European Union, the technology providers, or maybe the new coalition that we will create?

Another consideration in this regard is accountability and the question: who will be responsible if something goes wrong? Against whom citizens could seek redress? The more the technology providers set themselves up as rule-makers and gatekeepers on how we are going to use technology in the sensitive areas (like for example contact tracing), the more issues it raises on how to regulate them and how to hold them accountable. And although there are existing frameworks on how to hold national authorities accountable, we still do not have the clarity on how to hold big tech accountable. It is also a leadership challenge that will have to be addressed in the near future.

AUTHORITARIAN PRACTICES IN DEVELOPING COUNTRIES

Recent reports indicate that the export of digital technology from authoritarian countries often goes hand in hand with the export of anti-democratic practices. In 2019, for instance, Chinese technicians were found to work directly with government security forces in Uganda and Serbia to install advanced facial recognition cameras for surveillance purposes. The struggle between digital autocracy model and digital democracy model is set to intensify in the years to come. The questions arise: how to counter this risk of irreversible divide and how to protect developing countries – often looking for cheaper equipment in order to digitise quickly – from importing damaging governance practices as well? The narrative that prioritises security and its importance must be adopted. There is a need to embed in technology itself the measures of privacy by design and cybersecurity by default that strongly influence the whole ecosystem. Developing countries should be approached with attractive counter-offers and the ongoing development of the certification schemes in the European Union might be a good opportunity to widely promote the solutions and tools that offer security and privacy from the start.

WEBINAR'S PARTICIPANTS:

Martin Achimović – Director, NATO Counter Intelligence Centre of Excellence

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

Julian King – European Commissioner for Security Union (2016-2019)

Ciaran Martin – Professor of Practice in Public Management, Blavatnik School of Government, Oxford University; CEO, National Cyber Security Centre of the UK (2016-2020)

Christopher Painter – President, The Global Forum on Cyber Expertise; Commissioner, Global Commission on Stability of Cyberspace; Former Coordinator for Cyber Issues, U.S. State Department

Jayshree Pandya – Founder and CEO, Risk Group LLC

Luigi Rebuffi – Secretary General, European Cyber Security Organisation

Andrea G. Rodriguez – 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)

Joanna Świątkowska – Assistant Professor, AGH University of Science and Technology; Initiator & Former CYBERSEC Programme Director (2014-2019)

Paul Timmers – Research Associate, Oxford University; Former Director, Sustainable & Secure Society Directorate, DG CONNECT, European Commission

Omree Wechsler – CYBERSEC 2019 Young Leader, Senior Researcher, Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University

Katarzyna Szymielewicz – President, Panoptykon Foundation

[1] COVID-19 Digital Rights Tracker (data as of 12 May 2020)

Meeting #2

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

28 May 2020

INTRODUCTION

The tensions and trade-offs related to data, the most valuable resource in the digital economy, are huge. The exponential growth of data is driving the interest in using it in marketing strategies and as amplifiers to spread the political and ideological messages. The exploitation of big data causes concerns about privacy, compliance, liability, information security and confidentiality. Because of its high value it is often worthwhile for other parties to chase after it, even by illegal means like data theft and economic espionage. At the same time, there is currently no broader legal or practical consensus on non-personal data governance, thus national authorities are taking the matters in their own hands by coming up with national frameworks. Also, data sovereignty and security are at the top of the EU agenda, as shown in the European Strategy for Data that includes the creation of common European data spaces aiming to boost EU data-driven economy.

The topic of data governance is very broad and complex. During the webinar the following aspects were highlighted: the complexity of data ecosystem, data ownership, European approach to data and data for common good.

Each of the topics is elaborated below. As one of the main goals of the meeting was to clarify challenges and important points in the discussion on the subject of data governance, very often more questions than answers appeared. We believe that this approach stimulates and serves public debate by boosting the need for a multi-stakeholder approach and by demonstrating the key aspects for further discussion.

THE COMPLEXITY OF DATA ECOSYSTEM

The connectivity is going to be the driver of digital economy. 5G, when widely rolled out, will fuel the growth of the Internet of Things. In Europe, the number of mobile IoT connections is set to grow from 140 million devices in 2018 to nearly 740 million by 2026. All those connections will generate data that will eventually become resource for data analytics and for the AI-based solutions. 5G fuelling IoT and IoT fuelling AI will become a powerful circle creating new opportunities for the global competitiveness of the European industries. It is important to underline that the relations between those technologies strongly depend on high level of cybersecurity. In this regard, with more data and more access point to the omnipresent devices, infrastructure

vulnerabilities must be absolutely minimised. Data, as powerful as it might be, is not an end in itself and must be treated as an enabler for the future business models and must be supported by complementary initiatives.

DATA OWNERSHIP

In the data-driven economy, big data gives possibilities to expand businesses and enhance market influence. It is also creating new sources of revenue as data itself becomes the subject of transactions. Companies collecting and managing data oftentimes require users to hand over some rights in exchange for the use of their services. This brings up questions on the ownership of data and whether it is possible to empower users to also benefit from the data they provide in addition to the regular use of the platform's services. In the traditional approach, users are giving up their data and their digital traces in exchange for the convenience of "free" services while platforms are earning money on the aggregated data, mostly through the advertising. In the last couple of years, however, it has become clear how valuable the data can be and what are the inherent security concerns. The problem is amplified by the fact that a handful of existing services are very dominant and it is hard to find competitive solutions that would offer the same services but with a different approach to data governance. On the other hand, while it might be easy to set the value of the aggregated data, there is no simple way to price the data per unit, thus, the compensation to users seems extremely challenging. Even considering that there is a market-created tool that might appraise the individual pieces of data that users are creating, the question arises on who and how should arbitrate this process.

EUROPEAN APPROACH TO DATA

In the Recovery Plan for Europe the European Commission underlined the need to invest more in connectivity and in the European industrial and technological performance, which overall are having spill-over effects on the EU's strategic autonomy. Digital economy, especially technologies such as AI, cloud and quantum computing, but also the development of digital infrastructure and next generation networks are all drivers for data production and flow, as well as engines of innovation and job creation. Thus, in the coming months the legislative actions will be taken as part of, among others, European Strategy for Data, Digital Services Act, EU industrial strategy or White Paper on AI. Data was put by the EC at the heart of the recovery for Europe in order to rebuild the single market and also to make it more green and digital. Boosting the data economy is the cornerstone of having Europe's digital leadership ambition fulfilled. The ambitious goals of the Commission to use measures to remove existing barriers to data sharing, to data pooling, and also to scale up in a coordinated way including the building of the European cloud system must be translated into concrete actions in order to stay globally competitive. It is crucial to support European industry in the sectoral common data spaces. The data exchange solution will be in this regard a great boost to businesses and to the SMEs to scale up without additional huge costs. An important component is also the promotion of business to government and business to business data frameworks (also in the light of the current European Recovery Plan). The advantage of European digital strategies also lies in the values

which are always given priority. One of the greatest strengths of the EU – the regulatory power – not only influences the ecosystem in the Member States but also resonates externally. Users' trust in this regard is very important and might become a driver of the competitive data industry which might not be the case in other places of the world where the data handling is not subject to transparent rules. Thus, creating secure and trust-based solutions at the heart of the data governance rules might influence other players on a global scale.

Digital infrastructure and cloud services, which are crucial for data processing and storage, are becoming part of strategic autonomy and also determinant of sovereignty. Cloud market is currently very much concentrated in the hands of non-European companies, thus EU has started to push forward the initiatives (such as Gaia-X) aiming at boosting competitiveness in the market and also set the rules regarding data governance. There are, however, the questions on how to build right and effective coalitions which take bold actions both at the level of private-public partnerships and between the countries. While it might seem easy to call for an alliance of like-minded countries, the practical dimension of the cooperation that requires aligning industrial policies and balancing policy interests is very difficult.

DATA FOR COMMON GOOD

With its characteristics of a public good, data should be used in ways that maximise sustainable wealth creation within society. One of the emerging trends in this area is data democratisation and open data movements – the process of ensuring universal barrier-free access to data, resulting in potential efficiency and productivity increases. It eventually leads to the perception of data rather like water, oxygen or sunlight (instead of oil, as a widely repeated metaphor goes). In the light of the COVID-19 crisis, the power of data was broadly understood and brought light to the importance of how data can guide public policy decisions. Anonymised and aggregated data from the networks is being used to help the health authorities to understand if the lockdown measures are effective and what territories are more at risk. Apart from emergency situations, the aggregated and anonymised data might be used for example for city transportation and mobility plans. Encouraging companies to share technology and data for the benefit of societies is a very important task for governments, which should influence this process by creating the legal conditions and incentivising industry. Data rewards collaboration rather than protective policies. Good data governance structure will enable Europe to set up norms, standards and value-based solutions that could enhance the region's global impact and shape a security ecosystem.

WEBINAR'S PARTICIPANTS:

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

Tadeusz Chomicki – Ambassador for Cyber & Tech Affairs, Security Policy Department, Polish Ministry of Foreign Affairs

Paul Cornish – Visiting Professor, LSE IDEAS, London School of Economics

Lise Fuhr – Director General, ETNO

Paolo Grassia – Director of Public Policy, ETNO

Andrew Hodgkins – Chief of Staff, NATO CI CoE

Ciaran Martin – Professor of Practice in Public Management, Blavatnik School of Government, Oxford University; CEO, National Cyber Security Centre of the UK (2016-2020)

Mimi Nguyen – Data Policy Officer, NATO HQ

Mariusz Nogaj – Deputy Director, NATO CI CoE

Christopher Painter – President, The Global Forum on Cyber Expertise; Commissioner, Global Commission on Stability of Cyberspace; Former Coordinator for Cyber Issues, US State Department

Luigi Rebuffi – Secretary General, European Cyber Security Organisation

Barbara Sztokfisz – CYBERSEC Programme Director

Joanna Świątkowska – Assistant Professor, AGH University of Science and Technology; Initiator & Former CYBERSEC Programme Director (2014–2019)

Paul Timmers – Research Associate, Oxford University; Former Director, Sustainable & Secure Society Directorate, DG CONNECT, European Commission

Jean-Christophe Le Toquin – President, Cybersecurity and Cybercrime Advisors Network; Coordinator, Encryption Europe

Jakub Turowski – Head of Public Policy for Poland, Baltics, Romania and Bulgaria, Facebook

Meeting #3

CYBERSECURITY IN THE ERA OF DECOUPLING IN THE DIGITAL SUPPLY CHAIN

18 June 2020

INTRODUCTION

International affairs are affected by the technological change to the extent which is hard to grasp and fully understand. Emerging digital technologies such as 5G or artificial intelligence have exacerbated the global struggle for power and domination. The complexities in the digital supply chain and the challenges regarding the decoupling might be called modern technological Gordian knots. Cutting them requires bold moves and decisions bringing at the same time unpredictable consequences. The recent social and economic crisis caused by the outbreak of the COVID-19 pandemic highlighted a major obstacle to digital autonomy stemming from the dependencies within global supply chains. The pandemic underlines the dangers of an over-reliance on overseas manufacturing capacities and raw material imports that are critical to the functioning of the modern digital economy.

During the webinar the following aspects related to the supply chains were highlighted: Europe and its position in the global technological supply chains; the need for the strong alliance of like-minded countries; decoupling – EU approach and willingness to follow this path; COVID-19 – supply–chain implications.

As one of the main goals of the meeting was to clarify challenges and important points in the discussion on the subject of supply chains, very often more questions than answers appeared. We believe that this would be food-for-thought material to stimulate and serve public debate and multi-stakeholder approach.

EUROPE AND ITS POSITION IN THE GLOBAL TECHNOLOGICAL SUPPLY CHAINS

In the last years we have seen the EU extending or broadening its concept of strategic autonomy to comprise various policy sectors such as cybersecurity, telecommunication, AI, cloud computing, space, medical assets, and for each one of them the question of supply chain plays a major role. To many, the European Union is a regulatory power, able to influence other actors through the promotion and export of its regulatory and standardisation frameworks. European countries, in their approach to foreign suppliers, tend to increase their requirements as regards reliability and cybersecurity. An example of that is the ongoing debate around the 5G networks and the existing EU toolbox for 5G security where the EU underlines the need to look at a variety

of aspects (also non-technical) and risks related to foreign suppliers (that are being for instance subject to interference from their governments, as exemplified by the National Intelligence Law of the PRC).

Also, the EU can enhance its role in the global digital race through the investments and funding programmes in the post-COVID-19 period, like the Connecting Europe Facility or Next Generation EU. Another opportunity lies in the bolstering of the European Digital Single Market.

THE NEED FOR THE STRONG ALLIANCE OF LIKE-MINDED COUNTRIES

The geopolitical debate is constantly evolving and various initiatives and wide coalitions of like-minded countries that are trying to deal with these challenges are emerging. One of them is the D-10 (G–7 countries plus Australia, South Korea, and India), initiative originated already a few years ago by the Atlantic Council, which is now regaining its attention because of the UK government support towards forging the alliance of democratic countries that would address the issues of both 5G networks and supply chain vulnerabilities.

One of the things that experts agree upon while framing a common approach to cybersecurity among like-minded countries is that it is crucial to build alternatives to the existing products and services in order to have a sustainable approach to the security issues. The debate should focus on how we can have more suppliers in the market, as in the globalised world there are still going to be inter-dependencies between countries and having the alternatives is an imperative must. Also, there is a need to start thinking how risks are going to be mitigated. 5G is not the finishing line. There will also be 6G and 7G networks and other breakthrough technologies. Even with the alternatives in the market, risks will always be there and we need to learn how to manage them. First of all, the reactive and episodic approach should be complemented by long-term strategies.

One of the worrying trends that might cause some challenges in the area of EU common approach towards the supply chains is that we can observe two parallel processes. In western European countries, there is a strong push for autonomy and gaining the control over national infrastructure and assets. In the eastern European countries, however, the focus is more on the investments (even from companies coming from outside Europe). From the perspective of the CEE region, there are many opportunities and chances arising from decoupling and the need to reshore some US and global companies particularly to CEE. There is also a need to attract more FDI and allocate tech investments on the high level of value chains, such as R&D centres or SOCs.

DECOUPLING – EU APPROACH AND WILLINGNESS TO FOLLOW THIS PATH

One of the most important aspects while analysing benefits and challenges of the decoupling is the question whether we can afford to foster this process. The intertwining of interconnections in the global economy that is brought upon by the global supply chains is not perceived only as a profit maximisation process. To many, interdependencies are also a tool of influence that helps to render both governments and companies accountable, thus creating a more stable global

playing field. Global supply chains mean the export and import of norms, values, and standards as well. Thus, the question arises to what extent we can afford to retain this level of influence in a world that is accelerating in decoupling.

There is a risk associated with pursuing too radical splits. It might result in unintended consequences or failures both on the supply and on the demand side. Following the logic of complete bifurcation, we can end up with a divided world in which on the one hand there is a set of for instance Chinese suppliers and on the other a large block of like-minded Western countries following their own rules regarding supply chains. The question arises – what about the rest of the world? Are countries from Africa, Latin America, or Asia going to buy "Western-based" tech? Is price going to be a determinant or rather security and quality of the products and services? The problem is very complex and decision-makers must find ways and work together to answer those questions.

From the global perspective, the challenge of the debate related to the dependencies in the supply chain and strategic autonomy is the need for a mind shift across countries, governments, and the private sector. It will entail huge changes for the policy–making landscape as strategic autonomy and the moves towards decoupling will involve market interventions, common industrial policies long-term decisions, which might reinterpret interests and perspectives of the private sector.

Next to the threats , there are of course also opportunities and chances deriving from decoupling that need to be considered. In the context of the CEE region for instance, which is a market with huge innovation and human resources potential, allocating the tech investments (on the high level of value chains, such as R&D centres, SOCs, data centres, e-commerce centres) and developing regional digital infrastructure can boost the economic growth considerably.

COVID-19 – SUPPLY–CHAIN IMPLICATIONS

The current social and economic crisis that was caused by the outbreak of COVID-19 pandemic has brought us to a very peculiar moment in terms of decoupling. The so–called world's factory – China – has been stopped for a brief period which has sent shocks throughout the supply chains which could be felt in different parts of the world. Thus, the COVID-19 crisis in general has brought us to a point where we could actually witness for a moment what a closed world with globalisation put to a halt looks like. Some experts consider it to be a good starting point in trying to devise decoupling. Unprecedently, it has put the economies in a position where we could observe what the consequences are and where to look for opportunities to overcome the negative shocks that are associated with this process. Under typical circumstances, such "experiments" are not possible in the economy.

From the EU perspective, a discussion about recovery plan is ongoing (the so–called Next Generation EU) and not all Member States have the same approach towards funding it and more specifically, towards the areas that should be financed. Europe is still very much fragmented and we need to work on a common vision of the future. Without it, it is difficult today to see where to invest and also what technologies and companies Europe should support.

WEBINAR'S PARTICIPANTS:

Martin Achimovič – Director, NATO Counter Intelligence Centre of Excellence

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

Bonnie Butlin – Co-founder & Executive Director, Security Partners' Forum

Tadeusz Chomicki – Ambassador for Cyber & Tech Affairs, Security Policy Department, Polish Ministry of Foreign Affairs

Paolo Grassia – Director of Public Policy, ETNO

Levente Juhasz – Public Policy and Government Relations Manager, Google

Julian King – European Commissioner for the Security Union (2016–2019)

Robert Krawiec – British Embassy in Poland representative

Ciaran Martin – Professor of Practice in Public Management, Blavatnik School of Government, Oxford University; CEO, National Cyber Security Centre of the UK (2016-2020)

Robert Muggah – Principal, SecDev Group

Christopher Painter – President, The Global Forum on Cyber Expertise; Commissioner, Global Commission on Stability of Cyberspace; Former Coordinator for Cyber Issues, US State Department

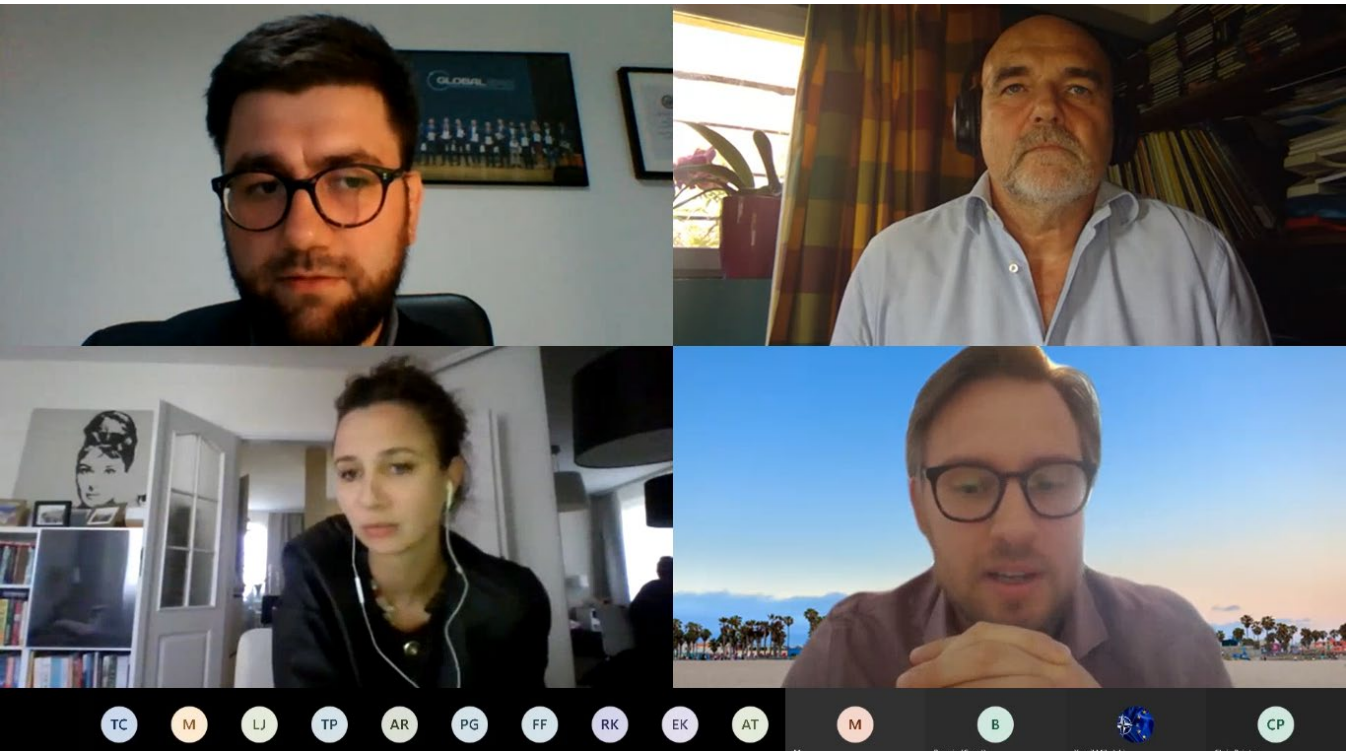
Florian Pennings – Cybersecurity Policy Manager, EU Government Affairs, Microsoft

Magdalena Petryniak – Communication Advisor, The Kosciuszko Institute

Luigi Rebuffi – Secretary General, European Cyber Security Organisation

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

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)



Meeting #4

HOW COVID-19 REDEFINED THE CRITICAL SECTORS OF ECONOMIES

29 June 2020
organized together with the British Embassy in Warsaw

British Embassy Warsaw

INTRODUCTION

The COVID-19 pandemic has changed societies' functioning in an unprecedented way. Nearly all industries were forced to adjust to the new reality in order to meet imposed safety measures and match customers' needs. Businesses and governments have seen their reliance on technology grow in every aspect of their activities. The crisis is particularly challenging for critical sectors, including health, energy, or telecommunications, which have now become even more indispensable. COVID-19 turned out to be a trigger accelerating (and forcing) digitalisation processes across all the sectors of our economies – something that had been in the making for a long time but not achieved yet. At the same time, digital transformation exposed new vulnerabilities that we were not prepared for. This steadily evolving threat environment demands from us strategic, political, and operational responses.

We are still at a stage where it's too early to capture the ultimate impact of this accelerated digitalisation. Preliminary conclusions are being drawn, but only with the perspective of time will we be able to assess to what extent the "new" normal will resemble the time before the pandemic. The ICT sector is particularly challenged. It has to ensure that everything is not only up and running but also as secure as possible. As we are reliant on technology in an unprecedented way, we are witnessing a perfect demonstration of why cybersecurity matters.

COVID-19 IMPLICATIONS FOR THE CRITICAL SECTORS

In our digital times, there is a need to define – and maybe rethink – what a critical infrastructure is. In the first decade of the 21st century, the focus was more on physical infrastructure like power plants or water facilities. It must be underlined that the scope of what is considered mission-critical has grown significantly, while the priority areas have evolved. Individuals and organisations have now made an accelerated move towards digital solutions and people are feeling more and more comfortable with digital tools. Even with the return to offices possible after the peak of the pandemic passes, the majority of employees often choose to keep working from home. Accordingly, there is a greater reliance on online services, specifically on video conferencing and cloud storage. To give an example, in the first weeks of lockdown, the use of collaboration tools (such as Microsoft Teams, Zoom, or Webex) has increased by more than 12,000%.

COVID-19 has highlighted cybersecurity threats and coincided with the increase of cyberattacks against critical sectors and data extractions through breaches. However, another effect of the crisis is also that companies have significantly less money and have shifted their priorities to keep the wheels turning. At the same time, funding is absolutely crucial to increase cybersecurity. Therefore, policy-makers need to be able to balance the need for more security and the risk that some companies might disappear (simply because their business models have been devastated by the crisis). Governments and industries will face growing financial problems, which needs to be taken into account in future policy strategies and recovery plans.

NEW APPROACH TOWARDS CRITICAL SECTORS

With critical sectors and services changing dynamically, we can observe how digital transition has speeded up over the last months and how ICT tools are, most likely irreversibly, converging with our physical realm. COVID-19 implications added new services to the list of the ones that we now see as critical, for instance: cloud services, telemedicine, online learning, or mobile networks. The telecommunications sector has experienced a tremendous strain in the recent months and turned out to be absolutely crucial as people started working from home and began to put new demands on the networks.

An increasing amount of hostile activities against the telecommunications infrastructure has also been observed. As an example, on 15 June, there was a major outage in the US for T-Mobile (overall, the infrastructure was offline for 7 hours). At the end of June, there was a five-hour telecommunication services outage in London. These case studies are a cause to sound the alarms. We have finally started to understand that telecommunication infrastructure is in fact critical to nearly all activities. Therefore, with the growing dependency of other critical services and sectors on the telecoms, the deployment of next-generation networks must unquestionably take into account the reliability, resilience, and security of their equipment. For sure there will be winners and losers of the current crisis, but the choice which infrastructures have to survive must be made according to dependency on them. Then, once the new critical services are determined, we must make sure that their whole supply chain is also secured, otherwise the risk of disruption is still too high. It is the entirety of the critical industry ecosystem that needs to be kept in mind.

THE REVIEW OF THE NIS DIRECTIVE

The NIS directive was conceived at a time of more “traditional” thinking about critical infrastructure, when the list of critical sectors was shorter and digital services were still relatively new.

It was mostly rooted in incident-based thinking with the underlying question of what might happen if there is a major incident and how severe can the damage get before an infrastructure is declared critical. Nowadays, other challenges are coming into the picture (whereas previously they were left out of the NIS directive). For instance, in the discussion on fake news and the role of social platforms one might say that these platforms are critical for our countries’ autonomy and for democratic values.

Considering today's realities, there is a need to look at whether the current NIS Directive is fit for purpose. The question of its scope is very much pertinent to the discussion and a part of the current open consultation by the European Commission is dedicated to seeking ways to adapt and expand the directive. In that sense, the COVID-19 crisis teaches us a very useful lesson. Indeed, we realised, to a greater extent than ever before, how profoundly important telecom networks and Internet access (including mobile one) are. We have also experienced the importance of the health sector, emergency services, food supply, and delivery services. The role of digital service providers must also be reassessed as their importance is bigger than four years ago.

Concerning the digital infrastructure, the review of the NIS Directive will also have to take into consideration what other elements of the surrounding ecosystem are critical for the effective and secure functioning of the Internet. So far, the NIS approach was to put the burden on the companies which are providing essential services, and which have a critical function in the society and economy. Today, an area to consider is the cybersecurity of products – the cybersecurity-by-design principle and supply chain issues.

THE ROLE OF THE PRIVATE SECTOR IN POLICY-MAKING

Public-private sector cooperation varies from country to country. In some of them, the engagement is very close, in others it is not seen as an immediate priority.

While sharing the information, there has to be an element of trust between the entities and sometimes information sharing is the most effective on the national level, as this is where a closer level of trust can be built. As an example, in the UK the National Cyber Security Centre is actively engaged with various sectors where a lot of information is shared; the systems that help examine threats come both from the NCSC and from individual sectors.

Given the international character of activities of big tech companies and digital services providers, public and private sectors should also cooperate more on the international level (for instance in reviewing the NIS Directive), especially considering that the private sector has a lot of valuable information to share. There is an underlying issue – the public administration views security (generally speaking) as a matter that only concerns the government. Though it might be true for security in the sense of border controls or the police, it is no longer the case for cybersecurity, which is, in reality, mainly a private market. The public administration can benefit from the knowledge that the private sector can provide concerning various threats. If we want an economic recovery from the current situation, we strongly need to spare no effort to bring the industries into that dialogue as well.

WEBINAR'S PARTICIPANTS:

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

Bonnie Butlin – Co-founder & Executive Director, Security Partners' Forum

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

Tadeusz Chomicki – Ambassador for Cyber & Tech Affairs, Security Policy Department, Polish Ministry of Foreign Affairs

Sorin Ducaru – Director, European Union Satellite Centre (SatCen); Former Assistant Secretary General for Emerging Security Challenges, NATO

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

Robert Krawiec – Project Manager, Defence & Security Unit, Department for International Trade, British Embassy Warsaw

Robert Muggah – Principal, SecDev Group

Florian Pennings – Cybersecurity Policy Manager, EU Government Affairs, Microsoft

Stuart Peters – Head, EU Cyber Security Team at Department for Digital, Culture, Media and Sport (DCMS), United Kingdom

Magdalena Petryniak – Communication Advisor, The Kosciuszko Institute

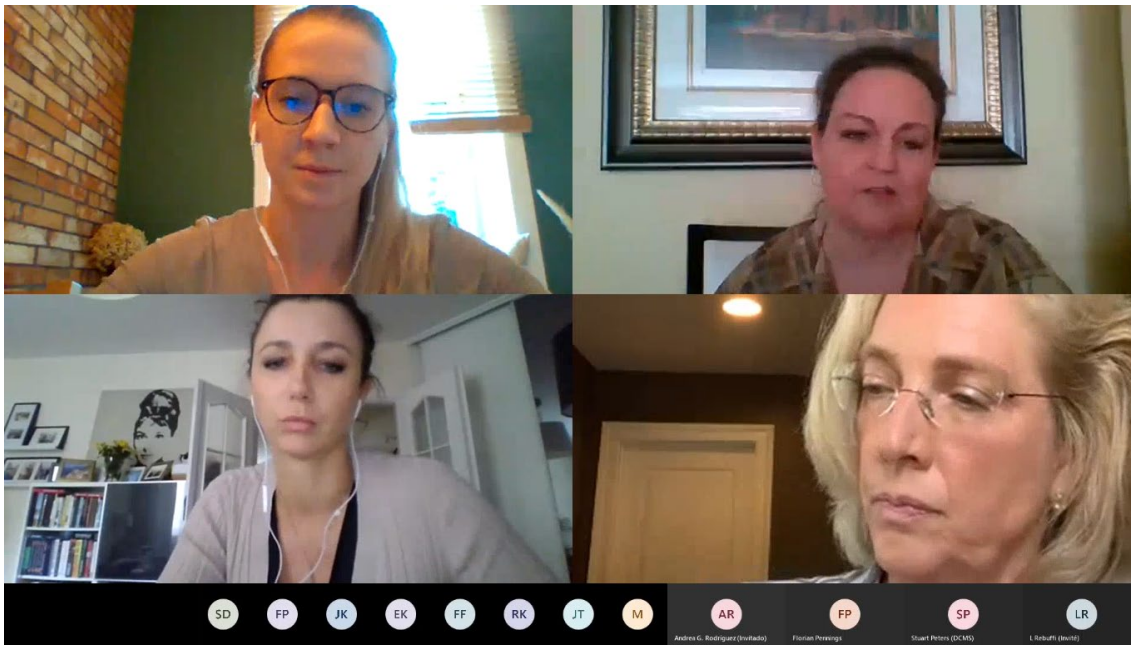
Luigi Rebuffi – Secretary General, European Cyber Security Organisation

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)

Barbara Sztokfisz – CYBERSEC Programme Director

Paul Timmers – Research Associate, Oxford University; Former Director, Sustainable & Secure Society Directorate, DG CONNECT, European Commission

Jean-Christophe Le Toquin – President, Cybersecurity and Cybercrime Advisors Network; Coordinator, Encryption Europe



Meeting #5

SECURITY OF 5G AND INTERNATIONAL COLLABORATION

16 July 2020

Informal 5G Summit with support from the Polish Ministry of Digital Affairs and NATO Counter Intelligence Centre of Excellence

INTRODUCTION

The 5G deployment requires enhanced cooperation and understanding of complicated economic and political circumstances, both for national security and economic development after the COVID-19 pandemic. Therefore, this Road to CYBERSEC webinar has been enlarged thanks to the participation of the representatives of Three Seas region countries (Austria, Bulgaria, Croatia, Czech Republic, Estonia, Latvia, Slovakia, Poland, Romania) which has allowed us to better understand the state of play regarding 5G deployment and cooperation possibilities. Given the dynamics of the decision-making process around 5G technology as well as its military dimension, a multi-stakeholder dialogue, the exchange of views regarding the interpretation of certain provisions of 5G EU toolbox (e.g. high-risk vendors or diversification strategy) as well as cooperation between like-minded democracies are absolutely crucial and form a necessary steps to build a secure and resilient 5G infrastructure.

The Road to CYBERSEC session turned out to be very timely as it took place two days after the United Kingdom's decision to ban Huawei from its 5G networks. Also, the wave of calls to toughen up telecom security in other parts of Europe has emerged with one of the most recent one made by Polish Prime Minister Mateusz Morawiecki in The Telegraph who underlined: "Protecting our technology is a crucial part of national security. We all must adopt robust measures to ensure our networks are secure. Disregarding the need to secure our critical technology would be a mistake for which Europeans would pay a considerable price. (...) For this technology to serve us well, its implementation must be based on trust and democratic control. Otherwise, we risk that today's crisis will be only a prelude to what awaits us if an unauthorised entity takes control of 5G networks and supply chains. (...) Countries must be able to control suppliers to ensure safety, which is why they must be from nations that respect our fundamental values: democracy, transparency, human rights and the rule of law."

During the webinar the following aspects related to 5G networks were highlighted: the position of the EU and the role of international cooperation in achieving secure 5G network, military dimension of 5G and Open RAN initiative.

THE POSITION OF THE EU AND THE ROLE OF INTERNATIONAL COOPERATION IN ACHIEVING SECURE 5G NETWORK

The international order has been changing dynamically for the last years. From the early stage of the 5G network development – and now even more with its effective deployment – we have witnessed shifts and splits between countries to the point where 5G is turning into the battle-ground of a global geopolitical technological competition. Some countries have been changing their legal and trade structures as well as interpretations of international law in ways that are frequently fundamentally incompatible with the approach of like-minded democracies. What we might observe now in terms of 5G technology is a resemblance to the cold war where countries are being forced to decide which side they are going to be taking.

5G is not only about a major shift in technology, it is also about countries' position in the global digital value chain. Therefore, it constitutes one of the key drivers to deliver Europe's top political priorities and the EU cannot afford to be late in its rollout. With the 5G network Europe can have an edge, be at the forefront and leverage 5G connectivity through rich and very diverse industrial fabric. The stakes are very high and security will be a defining issue.

Given the increasing role of suppliers and the complexity of the value chain, the degree of dependency on individual suppliers and cooperation with trustworthy partners have become one of the main security challenges and topics of the international debate on 5G. The EU, while remaining open for global competition set a very high standard for privacy and security for 5G deployment. There is a need to preserve the trust of citizens and investors in 5G. Hence, we need a coordinated response and the 5G toolbox is the first good step towards this. As Europe, we should cooperate with the international community and include all like-minded stakeholders in the debate to get a shared understanding of 5G security so we can all compete on equal footing. The EU needs to stay united in its approach and strive for the harmonised framework defined by the European Commission in 2019. As there is a significant convergence between EU economic plans and the 5G rollout, the connectivity (and smart connectivity) will be the link between EU's Digital Strategy and EU's Green Deal. It will also be instrumental to support Europe's recovery plans.

New technological challenges need strategic approach in the entire EU, Commissioner Thierry Breton said recently: "Of course, we already need to look beyond 5G. I am talking about starting to prepare for 6G of course, but not only. (...) The current fragmentation in Europe with suboptimised business models based on national markets and high costs for national spectrum licenses is holding back our collective potential compared to other continents. It is time to encourage consolidation (...) and to create a true internal market for telecommunications services."

5G – MILITARY DIMENSION

The introduction of 5G represents a critical change in the communications environment requiring significant effort to anticipate how its deployment will change the operating environment in NATO and in the military realm. 5G will provide increased support to secret services, special forces operations as it can give rise to control and espionage systems far more efficient than

those systems that are currently used. Major shifts in technology create a variety of opportunities but at the same time they create new threats that are enabled by the increased capabilities. National services can employ 5G across the spectrum of military operations to improve efficiency and effectiveness of weapon systems and involve whole new operational concepts based on machine to machine communication. Future military and security assets will use both fixed and mobile 5G networks to minimally process massive amounts of data that today's weapon systems rely on and future weapon systems will rely on even more by connecting distance sensors and weapons into a dense and resilient operational network. Widespread deployment of 5G networks can rapidly accelerate the integration of machine learning and artificial intelligence in decision-making processes with the potential to radically transform military operations. Lower latency communication will enable new generations of yet unmade and unknown weapons and systems within transportation and logistics areas.

Nonetheless, any compromise of the underlying 5G services could have catastrophic results. For this reason, defence and security assets must learn to use 5G capabilities and recognise transformative opportunities to operate with speed, precision and efficiency necessary to remain effective and survivable in the future. They must also be alert to the risks and unattended consequences that may accompany dependence on 5G technology. Sovereign nation states and their government authority are not the only actors evaluating technology and seeking to capitalise on these new threats and opportunities. Criminal enterprises and individuals are actively evaluating 5G technology looking for creative and innovative ways to leverage it to their advantage.

Historically the military was the engine to push towards tech development. Today, in many cases, the military adopts technologies that are developed by industries. There is a need for governments and military executives to understand that they should be more engaged in control and development of various pieces of technology as they are used as the backbone for future operations.

OPENRAN INITIATIVE – TOWARDS OPEN AND SECURE NETWORK

The entire telecommunications industry is undergoing dynamic changes and alternative technology options are being discussed and assessed. The Open RAN has been gaining coverage in the last months and can be presented as a way to decrease commercial dependencies and geopolitical tensions surrounding the deployment of 5G. Creating a partially virtual infrastructure that is interoperable and vendor-neutral might be an answer to governments for the challenges regarding the dependencies on certain vendors. With the open ecosystem, there are opportunities to leverage security features even more. It gives operators more flexibility to choose the best solutions of the networks and to shape and improve the infrastructure in a more specialised and tailored way. Open RAN is not, however, a quick solution to all challenges, it is rather a long-term project that demands cooperation between governments and industries. It has the potential to diversify the market of suppliers, especially in the domain of radio components. After opening the market and increasing diversification, there is still a need to oversee who will finance independent testing of the code. As history showed, open architecture is not always secure and the Heartbleed attack on OpenSSL (where everybody assumed that as it is open it is also secure) is a proof of that.

Earlier this year, an Open RAN Policy Coalition was created by 31 global technology companies with the aim to promote open interfaces that will help ensure interoperability and facilitate market entry for new innovative suppliers. Their aim is to also encourage policymakers to support open wireless technologies, fund research in this domain and build secure radio access infrastructure.

INFORMAL SUMMIT PARTICIPANTS:

CYBERSEC Programme Committee Members:

Martin Achimovič – Director, NATO Counter Intelligence Centre of Excellence

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

Bonnie Butlin – Co-founder & Executive Director, Security Partners' Forum

Tadeusz Chomicki – Ambassador for Cyber & Tech Affairs, Security Policy Department, Polish Ministry of Foreign Affairs

Lise Fuhr – Director General, ETNO

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

Julian King – Former European Commissioner for Security Union

Robert Muggah – Principal, SecDev Group

Christopher Painter – President, The Global Forum on Cyber Expertise; Commissioner, Global Commission on Stability of Cyberspace; Former Coordinator for Cyber Issues, U.S. State Department

Jayshree Pandya – Founder and CEO, Risk Group LLC

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)

Paul Timmers – Research Associate, Oxford University; Former Director, Sustainable & Secure Society Directorate, DG CONNECT, European Commission

Omree Wechsler – CYBERSEC 2019 Young Leader; Senior Researcher, Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University

NATO Counter Intelligence Centre of Excellence:

Martin Achimovič – Director, NATO Counter Intelligence Centre of Excellence

Mariusz Nogaj – Deputy Director, NATO Counter Intelligence Centre of Excellence

Andrew Hodgkins – Chief of Staff, NATO Counter Intelligence Centre of Excellence

Three Seas countries representatives:

Václav Borovička – Head of Cyber Security Policies Department, National Cyber and Information Security Agency of Czech Republic

Ulrike Butschek – Department for Security Policy, Austrian Federal Ministry European and International Affairs

Zhaklin Chalakova – Junior Expert, Communications Regulation Commission of Bulgaria

Dan Cîmpean – Director General, Romanian CERT-RO

Rastislav Janota – Director, National Cyber Security Centre of the Slovak Republic

Zdravko Jukić –Deputy Executive Director, HAKOM

Elisabeth Koegler – Deputy Head, Department for Security Policy, Austrian Federal Ministry European and International Affairs

Robert Kośla – Director, Department of Cybersecurity, Ministry of Digital Affairs, Poland

Danail Nikolov – State Expert, Communications Regulations Commission of Bulgaria

Matej Salmik – Director, Training, Awareness, Cooperation & Support Centre, National Cyber Security Centre SK-CERT

Raul Volter – Lead Cyber Security Expert, Estonian Information Systems Authority

Major Daniel Wurm – Cyber specialist, Ministry of Defense, Austria

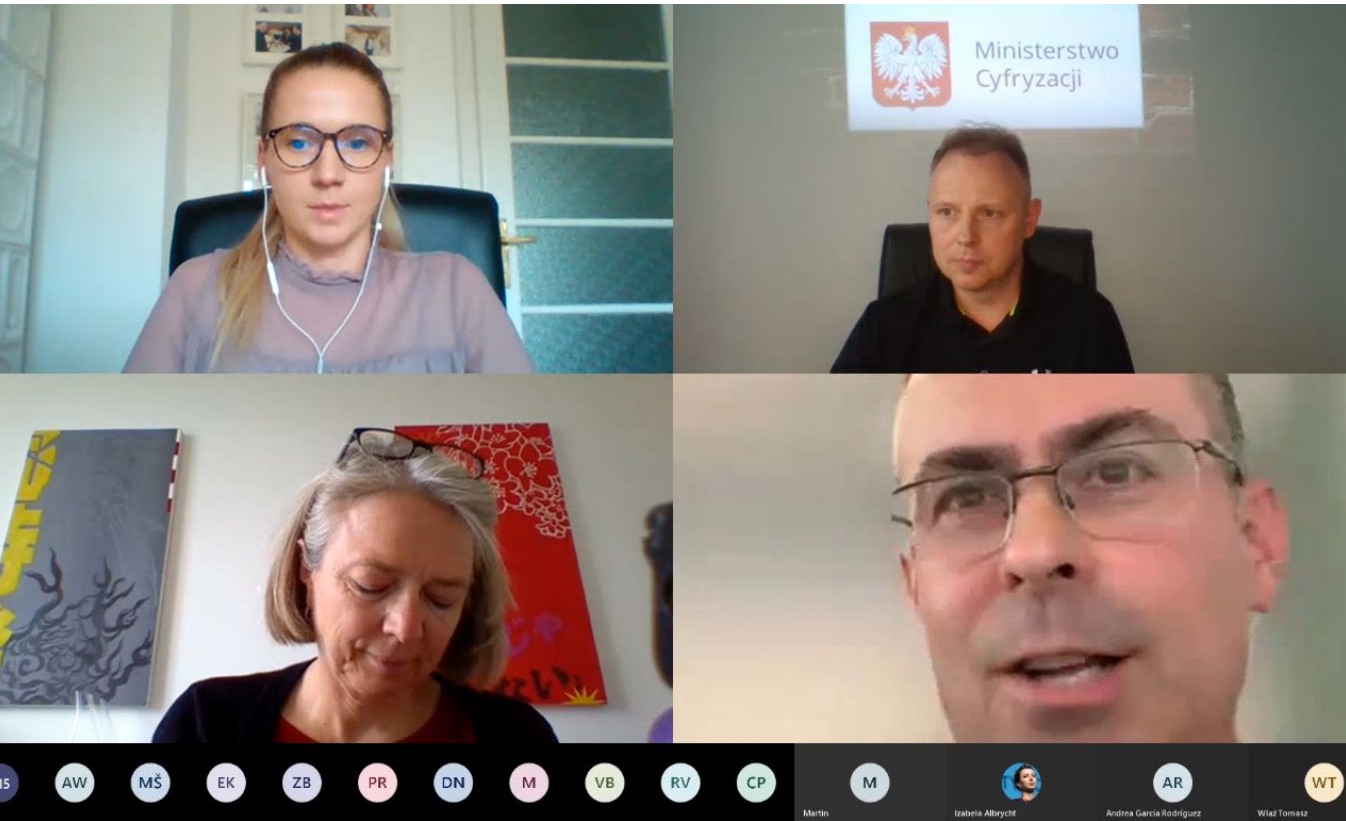
Sanita Žogota – Head of National Cybersecurity Policy Coordination Section, Ministry of Defence of Latvia

The Kosciuszko Institute:

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

Przemysław Roguski – Lecturer, Chair of Public International Law, Jagiellonian University; Expert of the Kosciuszko Institute

Barbara Sztokfisz – CYBERSEC Programme Director



Meeting #6

MISINFORMATION IN TIMES OF #COVID19

23 July 2020

open virtual meeting
organized together with the British Embassy in Warsaw

British Embassy Warsaw

INTRODUCTION

The surge of misinformation (frequently referred to simply as 'the pandemic') during the Times of Covid-19 is a source of concern to many. As opposed to its 'twins': mal- and disinformation, misinformation is frequently characterized as a factually fake, yet non-malicious (meaning non-intentional and non-manipulative) type of information distortion. Lack of malicious intent does not, in principle, limit its negative and dangerous impact on the general public, which in times of need looks for news and sources of information and can be tragically misled.

An efficient fighting of misinformation requires a number of preconditions to be taken – first, it is important to recognize misinformation as a phenomenon of its own (not all 'guardians' of information society distinguish it), second – acknowledge its range and multi-layered occurrence. Having these in mind it is easier to see the real nature and size of that threat, which leads to a better understanding of misinformation and indicates that the counter-misinformative actions ought to be taken on multiple levels and by all actors.

During the webinar we have asked our panellists about their perceptions of infodemics, their unique experiences and finally, their ideas on how to integrate different stakeholder to fight the misinformation. Owing to the fact that the experts come from and represent different areas and countries (the UK and Poland), we could shed some light on cross-sectoral and cross-border collaboration opportunities. As one of the main goals of the meeting was to clarify challenges and important points in the discussion on the subject of non-malicious information distortion, we have encountered a surprisingly concerted approach which clearly shows that there is a common perception of a problem and will to cooperate.

MISINFORMATION IN THE LENS OF ACADEMIA

Based on the findings of a special report published by S. Brennen, titled: "Types, Sources, and Claims of COVID-19 Misinformation", the misinformation environment demonstrates a complex picture summed up by a few observations: a) a lack of systematic approach to quantifiable research on misinformation which forces academia to rely on third-party fact-checkers report, b) 'Pareto' problem of misinformation sources (only around 20% of misinformation is top-down,

but this segment principally gets most of the traction, c) specific content, based on misinterpretations, misleading data and, sometimes, using a plethora of medical or technical terms, and d) claims that need to be verified. These elements build up a frame of Covid-19-specific misinformation in cyberspace.

It is noteworthy that attempts of curbing of misinformation have a potential to backfire. It has been observed that exposure of fake news to people sceptical towards legitimate news outlets and social media platforms make them spread fake news even more. This is a practical effect of a psychological confirmation bias which pushes for employment of psychology of misinformation in the process of its countering. The quality of work of various fact-checking organisations is usually seen as high by the academia which benefits from their studies. The academic research mainly focuses on big social media platforms which is both justified and calling for an expansion to other, less popular, means of electronic communication which gain more and more attention of misinformation actors. The recent changes of social media policies and progressive shift toward better content policing is needed and well-received.

MISINFORMATION FROM THE PERSPECTIVE OF FACT-CHECKERS

The surge of misinformation is a particular challenge to information societies as it undermines trust in legitimate and democratic institutions. Its size forced many fact-checkers to perform a full pivot from other research topics to Covid-19 which highlights the capacity issues and calls for building up capacity and resilience of myth-debunking organisations. The number of urgent issues and threats is overwhelming and fact-checkers are forced to prioritise and select which topic are they going to cover and which will have to be dropped. This organisational obstacle affects negatively other actors but could not be avoided without further development of this sector. This is visible especially in the light of the fact, that infodemics brought up a different, more organic, type of conversations which contrasts with usual disinformative content. Notwithstanding, it is still able to cause a genuine harm which calls for a serious and holistic approach to effectively tackle that threat. The holistic approach calls for a concerted, efficient and trust-based collaboration between fact-checkers and specialised institutions, especially when the misinformation pieces are highly specialised. Given to the fact that Covid-19-related fake news frequently stem from misunderstood or misinterpreted elements of actual research, fake-news-debunking may require a subject-specific knowledge that cannot come from the fact-checking organisation itself.

The synergy and capacity-building effects have to be achieved with a full awareness of the fact that even here regional specificity applies. False narratives such as ‘strong leaders handle crises better’ or ‘immigrants are responsible for spreading Covid-19’ are locally spotted and can be particularly harmful when these relate to a vulnerable group. The protection of people spills over to other fields as health-related misinformation has a tendency to associate itself with other topics, with notable examples being 5G and vaccines. In these cases, similarly to a situation where highly politicized events such as elections take place, fake news gain traction under circumstances where new technology or complex mechanisms play a role, allowing conspiracy theories to spread

and fuel misinformation. In parallel to academic perspective, practitioners stress the enormous traction of fake news spread by celebrities who receive disproportionately more attention than other misinformation actors.

Social media platforms play numerous roles in the information environment, among them providing space for participation in the news workflow, but also, increasingly, content policing. Practitioners highlight the complexity of clash of values between freedom of speech and media quality. It is of highest importance for social media giants to find a right balance between the two, especially that there is an observable change of what people start publishing across social medias. Fight over media quality sometimes symbolically takes form of an information warfare which must not be lost.

MISINFORMATION AND THE PUBLIC POLICY

Academia, social media platforms and fact-checking organisations witness increasingly growing engagement on the side of the public sector. The acknowledgement and integration of anti-disinformation and anti-misinformation measures into public policies is a positive sign. Capacity-development and readiness materialises itself in the collaboration with domestic and international partners, forming specialised disinformation units within public administration and other activities designed to promote resilience and raise awareness. Among notable actions it is worth mentioning that UK government has launched a few online campaigns such as “Stop the spread” and “Don’t feed the beast”, while Polish government launched its “Fake hunter” campaign where it engaged with volunteers online.

Other good practices and tailored activities encompass sharing messages, conducting training and engaging with social media platforms by governments. The framework of international cooperation divides itself to both bilateral and multilateral forms, where multilateral mean first and foremost collaboration within EU and NATO. From the perspective of public policy, the role played by the independent fact-checkers is crucial as it contributes to overall media literacy and allows to understand what is happening in the cyberspace. It must be stressed that general resilience is strictly connected to trust in the democratic institutions.

PANELISTS:

Nicola Aitken – Policy Manager, Full Fact

Scott Brennen – Communication scholar and a postdoctoral research fellow, Reuters Institute for the Study of Journalism and the Oxford Internet Institute

Tim Moody - Head of Foreign & Security Policy Team, the British Embassy

Olgierd Syczewski – Program Coordinator, Center for European Policy Analysis

Paweł Terpiłowski – Editor in Chief, Demagog

Host: **Kamil Mikulski** – Disinfo Analyst, the Kosciuszko Institute

You can watch the recording of the session

on our YouTube channel here

Meeting #7

TACKLING CYBERSECURITY CHALLENGES DURING THE PANDEMIC IN THE FIELDS OF HEALTHCARE AND FINANCIAL SECTORS

28 July 2020

open virtual meeting
organized together with the British Embassy in Warsaw

British Embassy Warsaw

INTRODUCTION

The ongoing global health crisis has changed our lives in an unprecedented way. All sectors of the economy are struggling to adjust to the new reality. Both healthcare and financial services are crucial to ensure the society's wellbeing and functioning as well as business continuity. The digital leap accelerated by the pandemic crisis is transforming the character of those sectors – from the use of contact tracing apps, telemedicine, and reshaped payment methods, to operational resilience and data security.

What is more, people moved their businesses and lives online, and lots of digital tools were introduced to monitor the spread of the virus. Most companies around the globe have experienced a significant increase in cyberattacks as a result of employees working remotely. ICT tools have, most likely irreversibly, converged with the physical realm. Due to increased reliance on new technologies, the society is also more exposed to various cyberthreats. Newly unveiled vulnerabilities are being exploited through sophisticated phishing campaigns, network data breaches, ransomware, and DDoS attacks. COVID-19 resulted in the highest jump in malware numbers in history with a 92% increase in such threats compared to numbers before the pandemic.

CHALLENGES OF THE ACCELERATED DIGITISATION LESSON

In many organisations, at the beginning of the pandemic, employees who shifted to remote work did not have the necessary equipment (like laptops or monitors). They were very often using their private computers (used by the whole family with a lot of unverified applications and programs installed) which additionally increased the attack surface for potential hostile actors. Also, from the psychological point of view, home environment is not conducive to the proper maintenance of necessary rules and policies, unlike the office space. Employees were moved from an environment where they felt comfortable into a very different way of working with no training and no awareness of adequate behaviour. As systems are as secure as their weakest link, it only takes one user who clicks something inadvertently to possibly lead to a breach within the whole environment. According to Global Workplace Analytics, by the end of 2021,

25–30% of the US workforce will be working from home multiple days a week. Organisations should therefore significantly shift their focus to secure remote work environment.

Despite the fact that during the pandemic large global scale cyberattacks, such as WannaCry or NotPetya, did not take place, there were a lot of COVID-19-related scams and frauds. For example, in the UK, as much as between 1.3 billion to 7.9 billion pounds might have been lost in attacks targeting the governmental financial rescue schemes. Also, hostile actors took advantage of people's emotional responses to the pandemic. There were scams that were allegedly supporting NHS (which actually redirected payments to another purpose) or selling the only right disinfectant that kills the virus. However, from a more positive perspective, a large part of the society has finally understood that cybersecurity is not only a subject for CISOs or CTOs in the big companies. They realised that it is also the challenge of their everyday lives, and CEOs of smaller and medium companies understood that they need to invest to boost their cybersecurity and resilience.

CYBERDIMENSION OF THE CRISIS IN THE HEALTHCARE SECTOR

During the pandemic we could observe that not all sectors were seemingly prepared for the cybersecurity challenges. Unfortunately, hospitals and health institutions were among organisations that were very often compromised in the first weeks of the crisis. Malicious actors have been targeting their databases and the systems that maintain the functioning of the hospitals, taking advantage of difficult times where health services focused their attention on the crisis in the physical world and took care of a large number of patients, often beyond their capacities.

There is a sort of paradox in the health sector – insufficient security can result in loss of human lives. However, one simple and easy argument that there are more important things to invest in than cybersecurity (medical devices, medicines, etc.) outweighs others. The fact is that the same medical devices bring cyber-risks to the hospitals and lack of preventive measures might have tragic consequences. There should be a change in the paradigm of and approach to cybersecurity in the areas of common public interest. One of the solutions are dedicated budgets at the state level which would be allocated only to cybersecurity and would not give hospitals a choice in what to invest. Another solution is to decrease inefficiencies (in procurements or in contracts) which are largely present in this sector.

Regulations concerning the health sector are relatively recent, with NIS Directive entering into force in 2016 (obliging EU Member States to take specific steps by August 2018). The two-year period was not enough for hospitals to put in place cybersecurity measures. Health institutions still have a long way ahead of them before they reach a sufficient level of security. What is more, the pharmaceutical sector has also come under attack during the pandemic. Taking into account what is at stake, it is worth assessing whether for example this sector should also be included in the NIS Directive (as the review of the NISD is currently ongoing). The interdependencies between sectors make a holistic approach that takes into account all linkages necessary.

There is a need for organisations to build adaptive and flexible architectures that could weather unforeseen and disruptive circumstances (not only pandemics but also major cyberattacks). There are some decisions that are being assessed at the moment. The current situation makes people reflect on what they have learned in recent months, what needs to be avoided in future, and what the digital infrastructure of organisations which facilitates remote work should look like.

HOW TO LEARN FROM THE BEST? PERSPECTIVE OF THE FINANCIAL SECTOR

The majority of financial organisations coped very well with the pandemic crisis. The existing challenges concerned mainly moving to the remote or hybrid mode of work (equipment, accesses, bandwidth requirements, etc.), as was the case with the majority of sectors based on office work. Also, financial services had to be adjusted as people significantly shifted to contactless payments (for example the UK has increased the spending limit for contactless payments from 30 pounds to 45 pounds). Payment intermediaries (such as PayPal) were also more exposed to frauds due to the increased interest in e-commerce. Despite that, the short-term solutions that industry applied worked very well, mainly because the sector was already heavily regulated for many years now, has built security and resilience measures and is investing a lot in security and in innovation. A lot of financial institutions were among early adopters of flexible infrastructure like cloud. Also, the mindset of staff in this sector differs as banks have always been a target for cybercriminals.

Overall, we should learn as much as possible from the financial sector in terms of building the operational capabilities. Financial sector outstands when it comes to cross-industry cooperation which can be observed at three levels – regulatory, incident response, and information sharing. It is something that could be embraced by other sectors, for example the health industry. It should be underlined, however, that sticking too much to sector-specific strategies and policies – one-size-fits-all approach – is not the best option as each sector has its own characteristics that should be taken into consideration.

PANELISTS:

Andrew Fitzmaurice – CEO, Templar

Mirosław Maj – Founder and President, Cybersecurity Foundation

Cezary Piekarski – Global Head of Cyber Defence & Threat Management, Standard Chartered Bank

Sean Sutton – Cyber Security Partner, PwC UK

Magdalena Wrzosek – Head of Strategic Analysis and Emerging Technologies Team, NASK

Host: **Aaron Ostrovsky** – Expert, the Kosciuszko Institute

You can watch the recording of the session

on our YouTube channel here

Meeting #8

HACKING HUMANS – THREATS TO DIGITAL IDENTITY

30 July 2020

British Embassy Warsaw

INTRODUCTION

The human race has been on the journey of self-exploration for a very long time now, whether through scientific research within disciplines like biology and medicine or by taking a cognitive approach and investigating the human nature from a psychological and philosophical point of view. The expedition to the core of humanity has evolved and what was previously built up in the minds of the greatest thinkers is now very often outsourced to big data algorithms. Biometric processing enables digital analysis of peoples' appearance, movements and emotions shown through facial expressions and behaviours. Physiological data hidden under our skin (visible for instance in body temperature or heartbeat) decodes real emotions and genetic testing helps discover less visible characteristics like ancestry or proneness to illnesses. The potential is remarkable, as solutions based on the abovementioned could introduce great improvements for example in medical research and prevent identity theft, due to the uniqueness of identifiers. At the same time, as our lives become more and more digital, the technology exposes us to greater manipulation, deception, surveillance, control and even gradual loss of autonomy in making decisions, all of which can lead to one thing – hacking a human being.

Over the past few months those risks have become even more evident as digital tools are deployed to fight against coronavirus. That includes contact tracing and tracking solutions which are most often using mobile and biometric applications issued by governments all over the world. Various entities such as OECD and the European Data Protection Board have been highlighting the importance of protecting data and fundamental rights and left recommendations for introducing new solutions in those challenging times. The digital transformation has only accelerated this year because of the ongoing health crisis and the ongoing health crisis has somehow forced us to become even more dependent on the digital world.

The plethora of risks associated with increased digital presence of human beings as well as enhancing brain power and physical capabilities of our bodies for example through microchips should be addressed through a public and political debate. Participants of this webinar tried to answer an existential question on how to ensure that by moving our lives more and more to the digital world and making our bodies more digital or digitally-integrated, we do not lose what constitutes the essence of our humanity – autonomy, freedom of will, and the right to a subjective perception of the world.

MINIMIZING THE RISK OF EXPLOITATION AND HACKING OUR IDENTITY

We live in a time where our privacy is very often traded for convenience and for higher productivity. The omnipresence of technological tools, that aim to make our lives easier, comes with a price that we pay every day, but which we may not be fully aware of. The increasing possibilities of tools empowered by data might result in the adversarial use of the technology leading to the hacking of our identity. The biometric identities, used currently for security purposes, once stolen might become a powerful weapon in the hands of hostile actors – identities might be duplicated, or authentication systems might be cheated (for example through generating a face that can pass as someone else) and used for criminal activities. However, we are not able to slow down the march of the technology. We can come up with regulations and laws, but the technology is evolving too quickly and there are going to be countries around the world that are going to use it to their advantage. There is a need to have a global and systemic conversation – how should the technologies (like for example facial recognition) be used, what are the dangers, and what are the chances they will be manipulated in the future with deep fakes.

A proactive approach and the development of new tools aiming at securing our digital presence are needed. Regulations and policies, though very helpful, are not the only solution. Innovation as a response to adversarial activities might become the most effective solution. Also, establishing trusted and secure digital identities (along with the control over our privacy) is critical for the further development of the digital world. At the same time, the education of the society and the awareness raising on how the emerging technologies work and what are their consequences should become a priority for policymakers and technology leaders. To solve the challenges, we need to first define and understand them.

CHALLENGES AND SOLUTIONS TO TRUSTWORTHINESS OF TECHNOLOGY – FACIAL RECOGNITION CASE STUDY

The progress in facial recognition technology which has been recently made allows us to currently observe a lot of different use cases, including live facial recognition, all around the world – ones already crossing the line of surveillance and others being tests on how society is willing to coexist with such technology on a daily basis. First of all, it raises data security concerns – how long the data is kept for, where it resides, who has access to it. Another challenge is false-negative and false-positive outcomes – based on the tests in London, 30% of the criminals will not be detected with the facial recognition systems even if their picture is in the database (false-negative). On the other hand, false-positive will be generated by one in a thousand. Opponents claim that facial recognition systems are biased and inaccurate for black and minority ethnic people pictures because of the non-sufficient training sets.

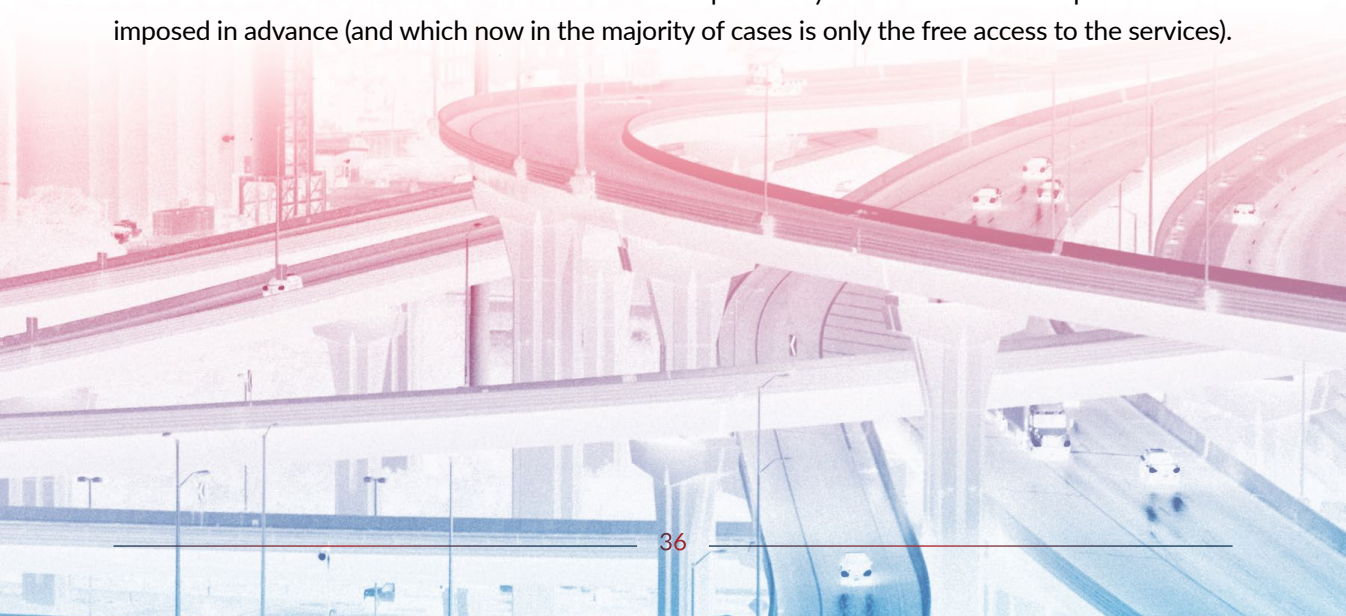
Also, the public perception of the facial recognition systems puts the large-scale use of this technology in question. More than 50% of the society do want the government to impose restrictions on its use by the police. Normally people would be very keen to support the police in matters of national security, for example to counter terrorism but here it is not the case. People feel

it is invading their privacy. Nearly half (46 %) wanted the right to opt out of facial recognition which brings a challenge in itself – how can we avoid cameras on the streets? And of course, if there is the option to opt out, then criminals would also take advantage of it and avoid cameras wherever possible. Within ethnic minorities, the percentage of people wanting the opt out was higher (56%) because of the fear of being unfairly targeted. The key question that arises here is: Is the technology really doing enough benefit to warrant the discomfort and distrust of many parts of society?

The trustworthiness should be a key priority in building the digital identity systems, especially those based on the biometric data. The systems which are trustworthy can be defined as secure, confidential, privacy preserving, ethical, transparent, fair (unbiased), resilient, robust, repeatable, accurate and explainable. Those attributes might seem easy to say but hard to bring to life. They demand advanced security techniques as well as consensus and international cooperation among various stakeholders.

DATA PROTECTION AND OWNERSHIP

The amount of data the society is currently generating is enormous and is growing every day. Over the past few years, we have observed a continuous surge in the deployment of new solutions based on biometric data processing (for authentication processes or border protection), neuro-measurements, genetic testing and nanotechnology. The number of entities ready to invest in those technologies is growing largely due to the unique character of the data powering them. It is fairly easy to single out a person from a crowd, which sparks debate over personal data protection, big data ethics and privacy. It is important to underline that not all the pieces of data are crucial to deliver or sell a product. There is a need to draw a clear line on how much data exactly is required in different use cases – it might be accomplished by both regulation and awareness raising (people simply will not be willing to share their data as they will be aware of all privacy and security concerns). Also, the important question arises – how can we prevent or stop potential abuse of the data from companies and from governments? One of the solutions that was theoretically discussed during the webinar was to balance away the control over privacy from those who monetize it to those who are actually producing it. It is worth considering creating systems that are gathering data on individuals (both in the online world and in physical space) which is subject to property rights. Individuals could then be able to sell or lease their data at the price they want and not at the price which is imposed in advance (and which now in the majority of cases is only the free access to the services).



WEBINAR'S PARTICIPANTS:

Bonnie Butlin – Co-founder & Executive Director, Security Partners' Forum

Michael Earle – Cyber Threat Intelligence Lead, CyberQ Group

Hervé Le Guyader – Deputy for strategy and international partnerships, Ecole Nationale Supérieure de Cognitique (ENSC); Vice-chair, Architecture and Intelligent Information Systems, NATO Information Systems Technology Panel; Member, NATO High-Level Group of Experts Allied Future Surveillance Control (AFSC)

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

Christopher Painter – President, The Global Forum on Cyber Expertise; Commissioner, Global Commission on Stability of Cyberspace; Former Coordinator for Cyber Issues, U.S. State Department

Jayshree Pandya – Founder and CEO, Risk Group LLC

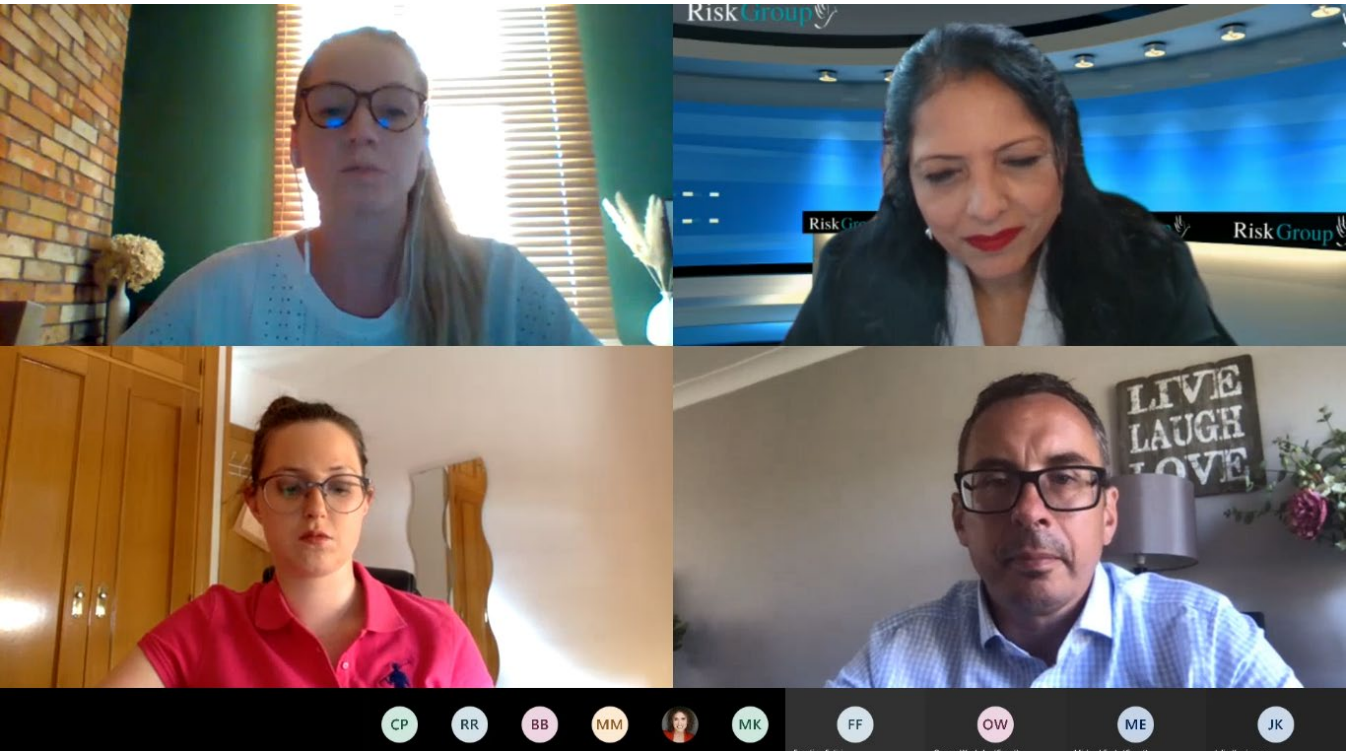
Andrea G. Rodriguez – CYBERSEC 2019 Young Leader; Researcher and Project Manager, Barcelona Centre for International Affairs (CIDOB); Associate Member, Observatory for the Social and Ethical Impact of Artificial Intelligence (OdiseIA)

Rafal Rohozinski – CEO, SecDev Group

Barbara Sztokfisz – CYBERSEC Programme Director

Paul Timmers – Research Associate, Oxford University; Former Director, Sustainable & Secure Society Directorate, DG CONNECT, European Commission

Omree Wechsler – CYBERSEC 2019 Young Leader, Senior Researcher, Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University



Meeting #9

HUMAN-LEVEL AI – PROBABILITY, RISKS, OPPORTUNITIES

17 August 2020

INTRODUCTION

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 behaviour. Arguably, some chatbots have already passed this test, but we cannot say that sentient machines are fully developed, at least not yet. The concept of machines surpassing human abilities is widely known as the "technological singularity", yet some scientists prefer to avoid the term itself as it is often associated with unsubstantiated claims and leads to even more confusion. The focus has therefore shifted to human-level Artificial Intelligence (AI), as it has made substantial progress in the recent years and might be the way to reach the human-machine convergence. Superintelligence could drastically change the future of humanity by immense advancements in the science and technology sectors, but it might come at a price of possible increase of control over the society.

Regardless of whether we are going to reach the point of human-level AI we are certainly seeing an advance in a more sophistication of the algorithms and how they are impacting our daily lives.

TOWARDS HUMAN-LEVEL AI – WHERE ARE WE?

Intelligent solutions are developing at an incredible speed and they are seemingly catching up with human intelligence. The technology-triggered revolution together with the scale, scope, and complexity of the impact of emerging digital tools is unlike anything the humankind has ever experienced before. Along with the significant advances in software development there also seems to be a parallel evolution in computer hardware to enhance machine intelligence capabilities (it is for example visible in the intensification of efforts towards developing more efficient, lower energy consuming, microprocessor chips). Since AI is becoming more and more part of our everyday lives the question arises whether we have decoded (or even whether we are able to decode) human intelligence that will allow us to create AI that is human-like. As a result, many complex challenges are emerging from our current approach to AI – i.a. what information looks like in the human brain and how it is integrated. It is essential to have advances that can address the interconnectedness gaps of event linking. It is said that what we do not understand we cannot create.

Also, it is important to consider that possibly the current methods of doing research and developing AI-based solutions will change in the future. The way AI is taught at the moment might not be the same in a couple of years. Therefore, assessing AI advancements from the perspective of today might be biased and might not take into account all circumstances that could potentially appear. Even though right now the neural networks models are the most advanced, we are already thinking of other ways of developing AI as reinforcement learning, rewards and many others. We should also consider other technologies breaking into the field such as quantum computers (or quantum neural networks) which is already under research and could significantly impact the AI development.

NON-LINEARITY OF THE WORLD AND DIFFICULTIES IN MAKING PREDICTIONS – CHALLENGES IN THE DEVELOPMENT OF AI SYSTEMS

Human intelligence consists of whole collection of mental processes (like problem solving, thinking abstractly, decision making, learning, understanding, reasoning and more) which are all interrelated and interconnected. For the last century we have heavily relied on the current information theory concepts which assume that irrespective of complexity every single event that has happened (or is happening or would happen) would be written as a sequence of simple "yes" or "no" answers to a series of questions. Whatever be the complexity of events it is believed that one could merge all of them, rewrite in a line and execute in a sequence. The underlying concept is that events cause predictable reactions, but in the real world they actually do not. All the systems we have built so far assume that if one event happens there will be linear consequences or reactions. For the further development of intelligent solutions, it is therefore essential to understand that we are not living in a linear world where actions cause predictable reactions and there are many interconnectedness and interdependencies in the entire human ecosystem and in the universe.

THREATS OF SUPER-INTELLIGENT SYSTEMS

There is a major challenge around super-intelligent systems which is the threat of manipulation and the adversarial attacks on machine learning be it in the training data sets or afterwards. Decision-making process manifest itself through a feedback loopy – a machine is told if something is a good outcome or a bad outcome and based on that it reacts accordingly. Manipulated data sets can have catastrophic effects given that the presence of AI-based technologies in everyday life is increasing, including in critical areas of our economy. It also entails an issue of systems being explainable (how was this decision made and why?) and the need for humans, who should always be in the loop, to understand when something is wrong with the decision-making process based on intelligent systems.

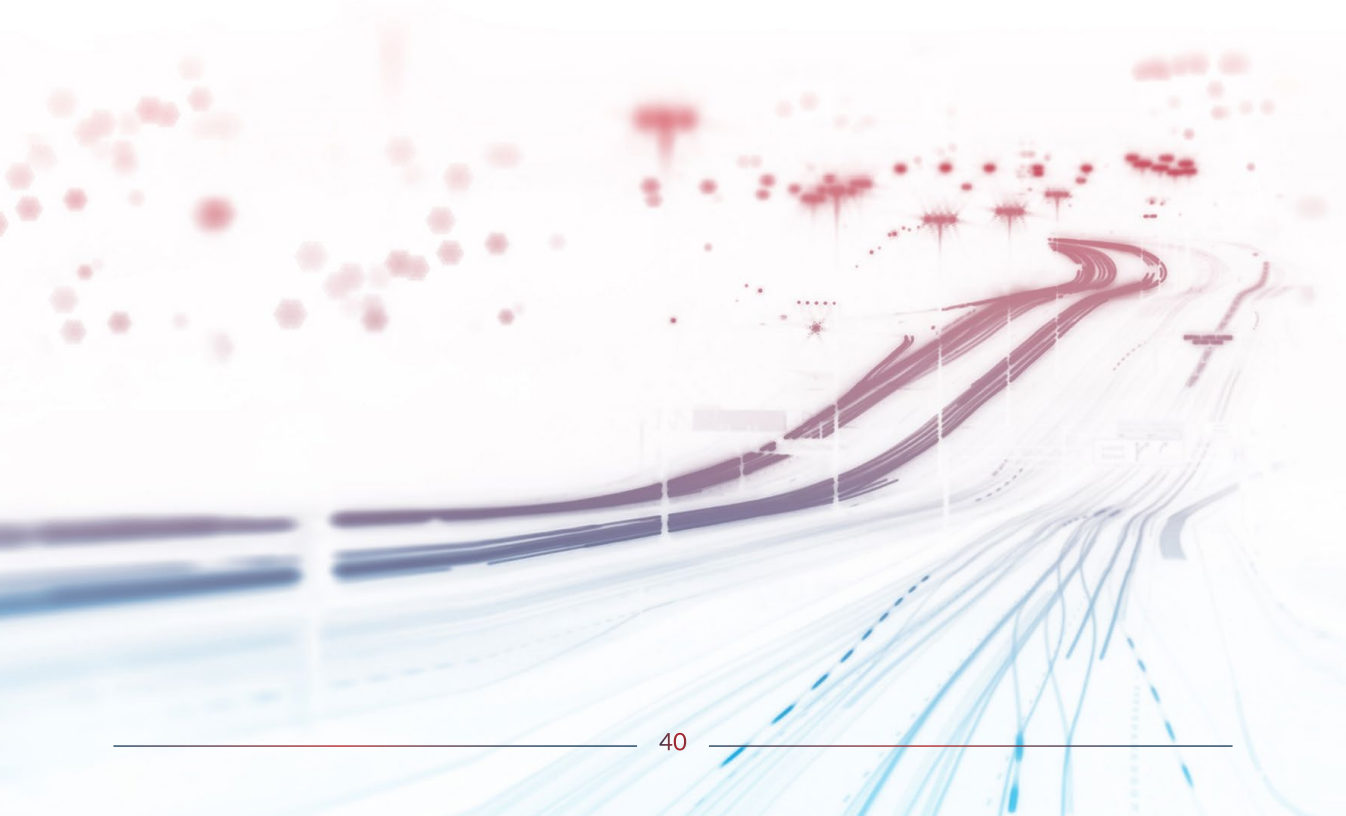
The application of artificial superintelligence in public, private and military spheres should be sustainable in order to minimize threats to humankind and to ICT networks and systems. As the AI is a purely dual-use technology, it is said to significantly change the warfare battlefield. We can already observe AI weaponization as a cybersecurity threat to the geopolitical order. AI-based weapons in cyberspace, geospace and space (CGS) might be used as a part of strategic competition

between global powers. Listing the AI-augmented cybersecurity risks should end with the ultimate threat – technological singularity which will allow AI systems to exceed human capabilities. It is in fact a cyber-world derived threat for the human race that needs to be considered while we are speeding up AI deployment.

Regardless of whether or not we will reach the point of human-level AI, we should carry on the discussion that in the event we reach it, how ready we will be in tackling and solving the already arising problems of AI, like biohacking, transhumanism or false data injections and manipulation.

PREPARING THE SOCIETY FOR AI ADVANCEMENTS

It is important to understand that once machines become better in a specific area, it entails the change of our role as humans in different processes and the way we engage with machines. If we look at machine vision as an example of the AI-based solution, for a long time the existing techniques were very poor. Nowadays, however, machine vision has significantly exceeded human capabilities what entailed the changes of human role in the processes where the machine vision is used. Society needs to adapt to the increasing presence of AI-based tools, take a proactive approach and consider different scenarios for the future. One of the methods that was discussed during the webinar was scenario planning which enables long-term strategies and at the same time keeps a high degree of flexibility (depending on the circumstances, the method is being adjusted). In order to achieve a specified and desired outcome there are some points on the path that need to be completed (for example improving digital skills or promoting life-long learning initiatives). The method combines already known facts and key driving forces at several levels such as social, economic or political. It is also very valuable for security experts who can analyse the potential impact of emerging threats.



WEBINAR'S PARTICIPANTS:

Martin Achimovič – Director, NATO Counter Intelligence Centre of Excellence

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

Bonnie Butlin – Co-founder & Executive Director, Security Partners' Forum

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

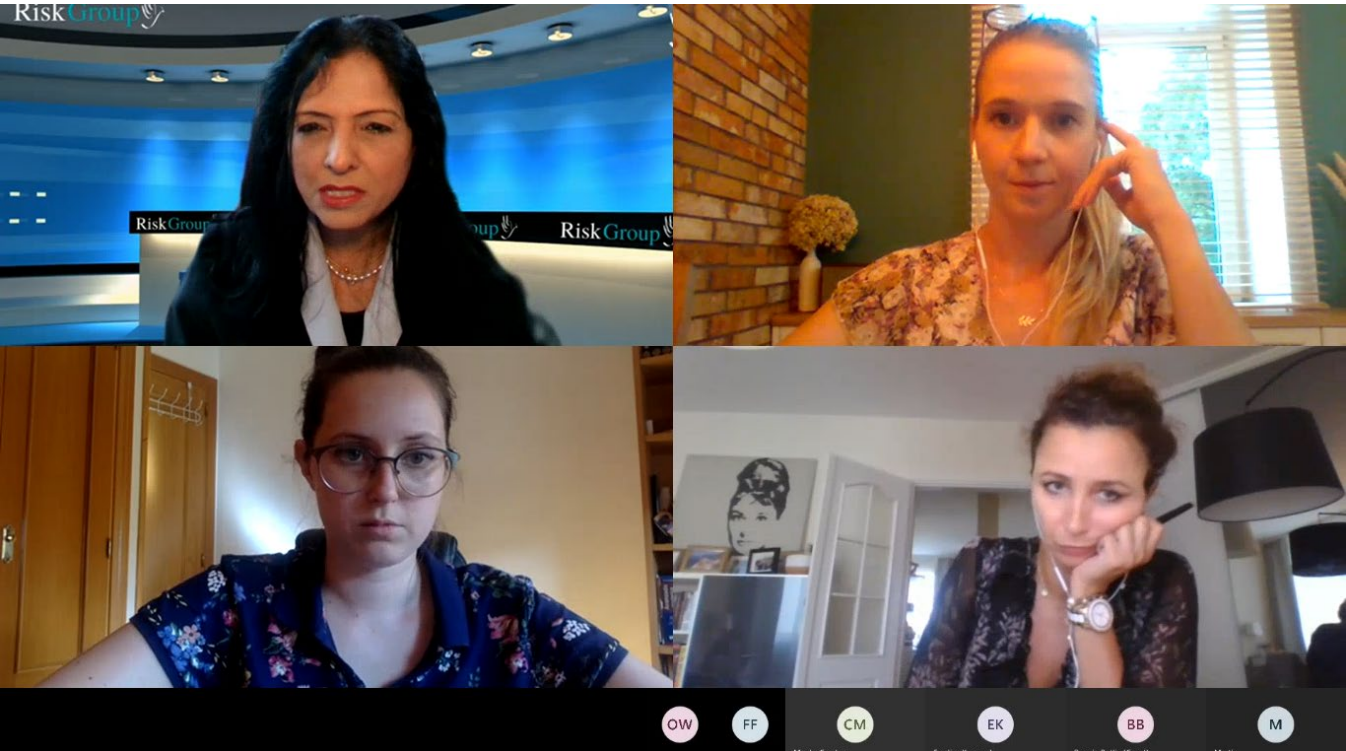
Jayshree Pandya – Founder and CEO, Risk Group LLC

Andrea G. Rodriguez – CYBERSEC 2019 Young Leader; Researcher and Project Manager, Barcelona Centre for International Affairs (CIDOB); Associate Member, Observatory for the Social and Ethical Impact of Artificial Intelligence (OdiseIA)

Rafal Rohozinski – CEO, SecDev Group

Barbara Sztokfisz – CYBERSEC Programme Director

Omree Wechsler – CYBERSEC 2019 Young Leader, Senior Researcher, Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University



ROAD TO CYBERSEC PARTNERS:

MAIN PARTNER

ORLEN

PARTNERS

NATO CI COE
Counter Intelligence Centre of Excellence

British Embassy Warsaw