VOLUME 5 (2019) ISSUE 2

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

Interview with Andrus Ansip

The weaponisation of social media. The use and abuse of human dispositions

Two reasons not to miss the quantum race

ANALYSES • POLICY REVIEWS • OPINIONS

The Kosciuszko Institute

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

The European Cybersecurity Journal (ECJ) is a specialised publication devoted to cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem--solving instruments.

ISSN: 2450-21113

Citations: This journal should be cited as follows:
"European Cybersecurity Journal"
Volume 5 (2019) Issue 2, page reference

The Kosciuszko Institute

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków

Phone: 00 48 12 632 97 24
E-mail: editor@cybersecforum.eu

Printed in Poland

Contents

Editorial

Barbara Sztokfisz

Chief Editor of the European Cybersecuirty Journal

Dear Reader,

It is my greatest honour to hand over to you this special issue of the European Cybersecurity Journal that coincides with the fifth, anniversary edition of the European Cybersecurity Forum – CYBERSEC 2019 under a unique leitmotif, which is "Securing the world's digital DNA".

Until recently, the history of humankind has largely consisted of step-by-step mastering and taming the world that people happened to live and grow in. Yet as of now, one of the major priorities for us as the human race is to learn how to attain mastery over the world we have created ourselves – the cyberworld. As Yuval Noah Harari, a great thinker of modern times, has put it, people were always far better at inventing tools than using them wisely. After all, it is much easier to engineer a river by just damming it instead of trying to foresee all ramifications this may cause in the surrounding environment. Cyberworld works the same way.

It is this mindset of caring for cyberworld that spurred us on to set up CYBERSEC five years ago and to have a hand, through our actions, in shaping a secure digital ecosystem. We believe cybersecurity ought to be embedded in the process of creating digital tools, products, and services whose basic aim is to serve the prosperity and welfare of every human being. We need to learn to predict what consequences our actions have, as very often their outcomes are irreversible. And cyberworld, much like the world that surrounds us, is a critical element of the current reality.

I am convinced that taking a read of this very issue will enrich your knowledge of cyber complexity and eventually contribute to spreading the approach that it is our common, undeniable responsibility to protect the world we are creating.

May we live in peaceful and tranquil digital times.

Enjoy the read!

Barbara Sztokfisz

THE BIGGEST CYBERSECURITY EVENT IN CEE

SECURING THE WORLD'S DIGITAL DNA

KATOWICE, 29-30.10.2019

Cybersecurity of the Digital Single Market*

Interview with Andrus Ansip, Member of the European Parliament and Former Vice-President of the European Commission

** This article is based on an onstage interview that took place on 20 February 2019 at the 2nd CYBERSEC Brussels Leaders' Foresight 2019 in Brussels. It has been edited for clarity.*

John Frank: Thank you Mr. Ansip for accepting our invite to this interview. To begin with, the controversies around Huawei and Chinese technology for 5G are broadly discussed in the news and yet, there is not much information we can really evaluate. What is your take on how we should be thinking about the Huawei situation?

Andrus Ansip: Chinese technologies were a topic of discussion at a press conference in December 2018, during which the following question was raised: do we have to be worried about Huawei? At the time I said, 'of course we have to be worried. – A better question is – why?'

We have to be worried because of China's intelligence law of 2017. According to this law, all software and hardware producers have to collaborate with Chinese intelligence services. However, this is problematic because those intelligence services are secret services. We have to be worried now because we need to make a decision about what kind of equipment we will use when building 5G networks in the European Union.

To put those two things together, we have to deal with a risk assessment. Some argue that we do not have solid evidence against [Huawei/China].

However, the question of what evidence we do or do not have, or even what evidence we can use publicly, is irrelevant. Due to the 2017 intelligence law, we have to deal with risk. By the time we have enough solid evidence which we can use publicly, it will already be too late.

John Frank: In regard to this topic, Ciaran Martin talked about doing a broad risk assessment[1]. He mentioned we should try to consider these issues on a more principled basis, and certainly this would be one of those principles. It seems we are moving towards a world where perhaps geopolitics and technology sourcing become even more entangled.

Andrus Ansip: Yes, but it is a huge simplification of the situation when some people claim that this is about a global trade war between the United States and China. In Europe, we have our own concerns and our own interests, and we have to think about those issues. Some Chinese companies say that they will never collaborate with their secret services despite the 2017 law. I am sorry, but I think I prefer to cooperate with those companies which respect their national laws, not with those which are ready to violate them. At the same time, we also have to consider reciprocity, which is a very popular topic right now. On my desk, there is a new Chinese laptop. In the European Commission, we organised an open tender for laptops and a Chinese company provided the best price. The quality was also adequate, so we decided to buy them. By contrast, in Beijing, the use of equipment or software produced outside of China is not allowed. When we look at 3G and 4G networks in Europe, the market share of Huawei is 40%. Meanwhile, the market share of Ericsson and Nokia in China is only 15%. Where can we see the reciprocity here? In a nutshell, we do have to be worried and we have to deal with the risk assessment. However, I have never said that we have to ban some companies – it must be a knowledge-based decision.

John Frank: What is the timeframe for building out 5G?

Andrus Ansip: We are in a terrible hurry already. We are setting new connectivity objectives for the European Union, and according to them, operators have to provide 5G services on a commercial basis in all urban areas by 2025. All major transport routes must likewise be covered by 5G networks.

There is also an important sub-aim which stipulates that by 2020 5G services must be available on a commercial basis in at least one major city in all member states. This sub-aim is especially important because it is easy to think that people can produce cars or create apps based purely on a theoretical knowledge of 5G. However, the best solutions come when people are able to encounter challenges in real life. Given these aims, as I mentioned before, the next step is to decide what kind of equipment will be used. We must also remember that national security falls under the competence of member states and not the European Commission. When the member states ask to create a coordinated approach towards cybersecurity, we will of course say 'yes' to that.

We are setting new connectivity objectives for the European Union, and according to them, operators have to provide 5G services on a commercial basis in all urban areas by 2025. All major transport routes must likewise be covered by 5G networks.

John Frank: Six years to have a functioning 5G network in a major city in every country and the major transport arteries – this is the aspiration and goal. I do not think there is any major city in the United States that is going to have 5G in six years.

1 Presentation delivered by Ciaran Martin, CEO of the National Cyber Security Centre of the UK during CYBERSEC Brussels Leaders' Foresight 2019 is available at the CYBERSEC YouTube Channel.

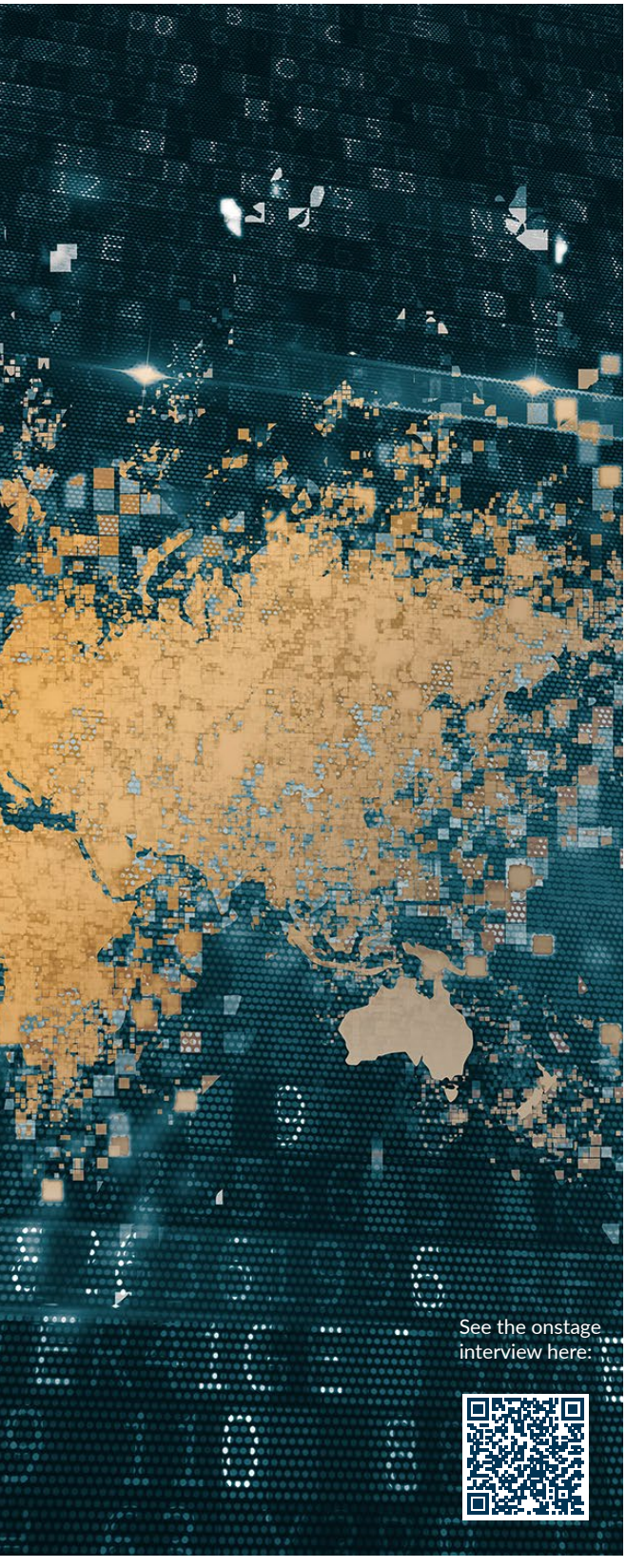
Andrus Ansip: Optimism is our moral duty. I really believe that we will have 5G networks by 2025. Maybe the United States will have those 5G networks even earlier than we will have them here in Europe. It seems that those developments are very rapid ones, especially in the United States and in China.

John Frank: Looking towards the future, 2019 is the end of the mandate for your Commission. What would you say was your Commission's most important accomplishment on cyber?

Andrus Ansip: Before discussing cyber, I would like to return to 5G networks. Recently, we have agreed on a new telecommunication code. This change was necessary because according to our analysis, had we continued on the basis of the existing code, we would have faced a huge investment gap. To reach our current connectivity aims, about 500 billion euros will be required per year. If we had kept the existing code, the lack of funds would be around 155 billion euros. I hope that thanks to this new telecommunication code, we will be able to cover the gap.

Let's talk about cybersecurity now. In 2016, we agreed on the Network Information Security (NIS) Directive. As we all know, the NIS Directive is mainly about cooperation and transparency. Transparency not in the meaning of the modern media, but in regard to the fact that people working on relevant issues have to get information about cyberattacks. This is necessary because it often happens that methods are used against somebody in one country, then modified a little bit and used again in a different country. According to the NIS Directive, all member states also have their institutions dealing with cybersecurity issues. We now have CSIRTs and CERTs in all member states. In some member states, CERTs are able to protect their networks and in others, not so much. But, at the very least, all member states have those institutions in place.

In 2018, we launched a new cybersecurity strategy in Europe which followed the previous strategy from 2013. Some people thought that introducing a new strategy after just five years was much too quickly.



However, in 2013, the cybersecurity dimension of the Internet of Things practically did not exist. We all remember how some people in the United States were able to create botnets based on connected devices and take down huge global service providers, such as Amazon. So, when this existing strategy from 2013 was no longer able to cover all the new aspects of cybersecurity, we had to intervene. We also introduced a new Cybersecurity Act in December 2018 pertaining to cybersecurity certification schemes. Once again, some member states have their own schemes, whereas others do not and would rather use those created by the first group of countries. However, there is also a third group of countries which do not have their own schemes, which are also not using others'.

John Frank: I remember when we started talking about certification schemes at Microsoft three years ago. From the engineering point of view, they were first viewed as regulatory burden. Then, throughout the course of the conversation, people came to realise that this is actually an advantage for the industry. Because there are so many devices, we need to do a better job of not just providing point of sale certification, but also throughout their life-cycle and retirement.

Andrus Ansip: Fragmentation is a real headache not only for Microsoft, but also for all of the companies acting here in the European market and for our citizens. I think that Microsoft and other global service providers are able to manage 28 different sets of rules, as you have enough funds to hire lawyers to understand those differences. But what about small and medium-sized enterprises? What about start-ups? If we continue on the path of this fragmented Europe, we will send a very bad message to our start-ups: stay home or go to the United States where there is already a huge single market. When we consider cybersecurity products, we have a similar issue. It happens quite often that you launch a product in one country and then in another EU member state, you have to start again with the certification processes, which can last for years. It is unbelievable.

When we discuss the concept of the Digital Single Market, it also supports the broader concept of a secure Europe.

John Frank: When you consider where we are today and think about the Commission that will arrive later this year, what do you think they should give consideration to for their agenda on cyber?

Andrus Ansip: Unfortunately, real life is not so easy. But, if I have to name just one possible topic then I think that much more attention has to be paid to the security of the supply chain. It seems that we have returned once again to Huawei and Chinese producers. However, in reality, this is a much broader issue. Even in Europe, when we began with a track and trace system for food, critics said that this would be an impossible task. They were wrong and today this system works. The same is true for pharmaceutical supply chains. However, electronic devices are yet another topic. It is currently very difficult to say where all the parts and chips in an electronic device have originated, or even what their purposes are. Of course, it is possible to check an individual device, but then each new device must be checked separately. Given these facts, the first step for the coming years is to pay much more attention to supply chain security. Then, we must also begin to work on great cybersecurity projects here in Europe, such as our network of cybersecurity excellence centres.

I think that much more attention has to be paid to the security of the supply chain. (...) It is currently very difficult to say where all the parts and chips in an electronic device have originated, or even what their purposes are.

John Frank: Earlier we had the opportunity to discuss regulatory models and the use of voluntary codes versus hard regulation. If I can just make an observation: at Microsoft, we used to ship a new version of Windows every three or four years and a new version of Office every two or three years. Now, we essentially ship these products once a month. There is more experimentation and more learning on an ongoing basis. At the same time, when we talk about regulatory systems, we sometimes say that we want to future-proof legislation for 20 years. This is a big challenge. Now let's talk about the advantages of self-regulatory models, of which you are a proponent.

Andrus Ansip: My dear president Toomas Hendrik Ilves also touched on those issues earlier during the conference but in the context of disinformation campaigns. Other panellists said that maybe it is time to regulate. Yes, regulation is possible, but I believe much more in self-regulatory measures. This is because when we impose regulatory measures, platforms can meet the given requirements and claim to be fully respecting all regulations. However, these platforms are rapidly evolving, and this process will actually make them less responsible. In contrast, self-regulatory measures are much more flexible. When we consider social media platforms, I am convinced that it is in their business interest to regain people's trust when it is lost. It doesn't matter that some platforms today are really big because, as the past 15 years have shown us, people can switch quite easily to other sources of information.

Self-regulatory measures are much more flexible. When we consider social media platforms, I am convinced that it is in their business interest to regain people's trust when it is lost.

Then, when speaking about disinformation campaigns, of course we also have to deal with those really serious issues. *Russia Today* and *Sputnik* are quite well-financed. Their budget is 1,1 billion euros per year, and in the St. Petersburg troll factory they have 1,000 full-time workers. In response, we have doubled the StratCom budget to 5 million euros. Despite this, all of the StratComs together remain at just 15 workers. However, I am not complaining because information warfare will never be part of our military doctrine as it is in Russia.

John Frank: The asymmetry of information and pure cyber offense have, at the moment, a significant advantage over defence. In the private sector,

we have certainly recognised that we need to get better. Not just at making our products and services more secure, but at working as a collective industry towards making the entire system more secure. However, we have talked today about the roles of Russia, China, North Korea, and Iran as actors in cyberspace and, in some cases, their engagement in disinformation. Given this asymmetry and the nature of these actors, it seems that at some point governments, and not the private sector, need to address these issues.

Andrus Ansip: Yes, I agree. However, it is sometimes quite difficult for governments to understand the importance of cyber defence, or how to deal with disinformation campaigns. Even in European countries, high-ranking politicians are not paying attention to digital issues. Many are still counting on traditional strength and believe that planes, trains and ships are all about steel. In reality, this is no longer the case. For example, when talking about Rolls Royce, many think only about fancy cars, even though today Rolls Royce can be considered one of the biggest data companies in Europe. The same is true for Siemens producing trains, which are used today in Spain, or Microsoft connecting engines on airplanes. Another example is Wärtsilä, a really good Finnish company which many people are not even aware of. They produce engines and transmissions for huge ships. It is not just about steel anymore, it is all about data. When I am talking about the free flow of data principle, I am not talking only about Google, Facebook, Amazon, or Microsoft, but also about Wärtsilä, Siemens, and all of the other traditional industries.

It is not just about steel anymore, it is all about data. When I am talking about the free flow of data principle, I am not talking only about Google, Facebook, Amazon, or Microsoft, but also about Wärtsilä, Siemens, and all of the other traditional industries.

John Frank: I know that you also have a passion for the capabilities of technology to transform agriculture. There is an aspect here where rural areas need broadband connectivity. At the same time, in many countries, rural areas do not yet have a good 4G system, let alone a plan to advance to a high-speed system. It seems that we need to find solutions that can bring affordable broadband to cover wide rural areas for the purpose of agriculture.

Andrus Ansip: I fully agree. The entire continent has to be covered with 5G networks in the future, not only urban areas and those main transport routes. We have to demystify artificial intelligence and the Internet of Things. Too often people think these concepts are so highly sophisticated that they do not apply to them. This is why I like to use examples of the agricultural sector and cows. If you have not yet heard, 20 years ago the average milk production in Estonia was 3,5 tonnes per cow per year. Now it is already 9,4 tonnes. Only the cows in Denmark and Sweden can compete with Estonian cows. This change was possible because Microsoft created sensors that were put on cows which allowed their feed to be balanced in correlation with their production. There were no changes to the cows themselves. The same was true on chicken farms. We prefer to buy one-kilogram chickens, so today they are using sensors on chicken farms and they were able to increase the percentage of one-kilogram chickens from 35% to 85%. If our farmers are not able to provide high-quality one-kilogram chickens at an affordable price, then somebody else will. I do not want to waste all of your time talking about connected cows for too long, but I do think it is very important to bring these issues to a grassroots level. When we speak about cybersecurity, it is not somewhere at a very high level. Average people have to deal with these issues.

When discussing our new cybersecurity strategy, we must mention the concept of cyber hygiene as well. Before people eat, they wash their hands without thinking. When we deal with digital devices, we must do the same and follow these very simple cyber hygiene rules.

We have to demystify artificial intelligence and the Internet of Things. Too often people think these concepts are so highly sophisticated that they do not apply to them.

John Frank: To finish, I have one final question. Given the shifting of the Commission's priorities over time, can you imagine changes for how the next Commission might organise to better address digital and cyber issues?

Andrus Ansip: Going forward, I think that digital must be the centre of attention. We have launched the Digital Single Market strategy. We have launched 30 different legislative proposals and already reached an agreement on 28 of them. However, these efforts are not enough. When I think of where we were just five years ago: for instance, 50% of European telecom operators blocked Skype. Now we have net neutrality rules, we have the NIS Directive, we have abolished roaming surcharges, we allow the portability of digital content, abolishing of geo-blocking, and have new telecom rules. It is still not enough. We have achieved quite a lot already, but we cannot claim that we are done and begin to set some other priorities. These issues have to stay our priority because our lives are already fully digital. ■

Andrus Ansip was elected Member of European Parliament in 2019. Before that, he served as Vice-President of the European Commission with responsibility for the Digital Single Market. Before moving to Brussels, he was a member of both the Estonian and European Parliaments. This followed almost nine years in Tallinn spent as Estonia's longest-serving Prime Minister, when Ansip worked with both centre-right and centre-left parties to lead three different coalition governments. During his time as Prime Minister, he also acted as chairman of Estonia's liberal Reform Party. Ansip first entered national politics in September 2004 when he became Minister of the Economy. Up to this point, his career was spent in Estonia's second largest city of Tartu where he was born in 1956.

John Frank is Microsoft's Vice President, EU Government Affairs. In this role, John leads Microsoft's government affairs teams in Brussels and European national capitals on EU issues. John was previously Vice President, Deputy General Counsel and Chief of Staff for Microsoft President and Chief Legal Officer Brad Smith based at Microsoft's corporate headquarters in Redmond Washington. In this role, he managed several teams including the Law Enforcement and National Security team, the Industry Affairs group, Corporate, Competition Law and Privacy Compliance teams and the department's technology and business operations team. For his first eight years at Microsoft, John was based at Microsoft's European headquarters in Paris. Initially he was responsible for the legal and regulatory issues involved in the launch of the Microsoft Network (now MSN).From 1996 to 2002, Mr. Frank led Microsoft's Legal and Corporate Affairs group for Europe, Middle East and Africa focusing on issues including privacy, security, consumer protection and antitrust. Mr. Frank began the company's European Government Affairs program, which focused on advocacy on software and online policy issues. Prior to joining Microsoft, John Frank practiced law in San Francisco with Skadden, Arps, Slate, Meagher & Flom. Mr. Frank received his A.B. degree from the Woodrow Wilson School of Public and International Affairs at Princeton University and his J.D. from Columbia Law School.

European Defence Agency's role in enhancing European cyber defences

Interview with Wolfgang Röhrig, Head of Unit Information Superiority, Capability, Armament & Planning Directorate at the European Defence Agency (EDA)

The European Defence Agency's stated mission includes developing defence capabilities and military cooperation among EU member states, as well as stimulating R&D among the European defence industry. What role would you say cybersecurity currently plays in these endeavours? Has the significance of cybersecurity increased in the EDA's projects in recent years? Does cyber differ from other domains of cooperation in terms of EDA's projects?

In 2011, EDA participating Member States (pMS) for the 1st time identified Cyber Defence as a priority area for capability development and added it to the Agency's work programme. This priority was reconfirmed in the 2014 Capability Development Plan and more recently in its 2018 revision. Since 2011 many activities have taken place and still are ongoing. They include cyber defence capability related projects as well as Research and Technology (R&T) activities. Several of these activities, like e.g. the 1st structured Cyber Defence Training Needs Analysis from 2014, which developed a comprehensive cyber competencies and skills framework, strongly influenced today's cyber defence capability landscape in Europe and, to a certain extent, also that of NATO given that we have 21 common Member States. This includes pMS' capabilities and capabilities at EU level. EDA also contributed, and still contributes, to cyber defence policy development: initially through its substantial contributions to the defence aspects of the 1st EU Cyber Security Strategy from 2013 and to the development of the 2014 EU Cyber Defence Policy Framework (EU CDPF) in its initial version, as well as to its latest review in November 2018. And for sure, EDA also substantially contributes to the implementation of the agreed actions within the EU CDPF.

Today, cyber space is fully recognized as a domain of military operations and it is, *per se*, cross-cutting and of a pervasive nature. Cyber therefore strongly influences any kind of capability development. The digitalisation of the military battlefield is progressing and, today, almost all military capabilities include a multitude of integrated Information Technology (IT) and processing

capacities – from individual soldier systems and Main Battle Tanks to aircraft carriers. Not to forget all kinds of command & control systems and reach back capabilities back home that have to be reachable for service provision 24/7 over long distances. This multitude of IT brings a lot of advantages but at the same time it creates many new vulnerabilities along the military value chains. Hence the need to include cyber security and cyber defence considerations in any new capability development project.

Today, cyber space is fully recognized as a domain of military operations and it is, per se, cross-cutting and of a pervasive nature.

EDA differs from many other EU agencies in that it works from an intergovernmental approach, meaning it depends on the cooperation of national defence ministries of its participating Member States (pMS). Given the *a la carte* model you use for the projects, are member states usually eager to participate in projects related to cyber defence? Is there an increased interest for cooperation in the cyber domain? Which countries are the most active?

I wouldn't like to highlight specific pMS. In the cyber domain, EDA has established two standing working formats with representatives from pMS: firstly, the 'Project Team Cyber Defence' established in 2011 which deals with capability development related activities; and secondly, the 'Cyber Defence R&T Working Group' set up in 2015 which identifies and pursues the cyber R&T related work strands. Both formats usually meet three times a year for several days and pMS and other EU partners, like the EU Military Staff (EUMS), are well represented at high levels in both formats. If required, these formats are extended to include subject and/or project specific ad hoc groups.

A good indicator for Member States' eagerness to cooperate is the number of collaborative projects. EDA today has three ad hoc projects underway (Cyber Ranges Federation, Cyber Situation Awareness for HQs, Improved APT detection) with different constellations of contributing members in the implementation phase. At the same time there are also two cyber related projects progressing under the Permanent Structured Cooperation (PESCO) initiative. Additional cyber projects can be expected as a result of the 2019 call for new PESCO projects for which the deadline is end of July 2019. Furthermore, the European Defence Industrial Development Programme (EDIDP) and the consecutive European Defence Fund (EDF) are expected to incentivize cooperation in this field. The current EDIDP work programme includes topics on cyber defence and we expect new cyber project proposals to be launched by mixed consortia of pMS' and industrial partners as part of the currently open 2019 call for EDIDP project proposals.

What would you say is the biggest barrier to creating a strong European cyber defences? How is the EDA trying to overcome this barrier?

Trust among like-minded partners is probably the biggest enabler for cooperation, and the main obstacle to it is a lack of trust. Therefore, it is crucial to build the trust which then enhances the willingness for cross-border cooperation. The two afore-mentioned EDA working formats can also be understood as trust building and enhancement tools. When I look back at how the Project Team Cyber Defence started about eight years ago, it is obvious that it has developed from an initial forum where pMS' representatives were primarily in a listening mode to an active forum where we have today a lively exchange of new ideas and best practices. The reasons for this development is that everybody understood that this format is built on the common interests of like-minded partners.

How do the EDA's cyber activities support EU-led operations within the CSDP?

Let me make a distinction between direct support and indirect support to EU-led military operations.

First: indirect support. I already mentioned that EDA activities have strongly influenced today's cyber defence capability landscape in Europe.

This also includes influencing the development of concepts for cyber defence in EU-led operations and missions. Since 2012 the Cyber Defence Concept for EU-led operations has been revised twice by the EU Military Committee (EUMC) with support from EUMS, last time in 2016. Through the continuous and trustful dialogue between EDA and the EUMS, all the results of EDA's cyber activities and projects were seamlessly integrated in the update and improvement of the concept and most recently the related Cyber Defence Standard Operating Procedure (SOP) for HQs. More specifically, the Pilot Exercise for Cyber Operations Planning (CYBER PHALANX), which was developed, organised and conducted by EDA in Salzburg in June 2018 in close cooperation with Austria as the Host Nation, has helped the EUMS to test and validate the draft SOP. This is just one of many possible examples for indirect support to operations.

Let me now come to direct support to operations. In 2014, EDA launched an initiative to provide regular Cyber Awareness Trainings to HQ staff involved in commanding EU-led military operations. Why to start such an initiative? One has to understand that Operations Headquarters (OHQ) are not usual HQs with fully manned staff but, instead, are activated for a specific operation and include many frequently rotating augmentees from several Member States who change at least every six months. Therefore, in such a specific environment, traditional cyber awareness standards cannot be taken for granted. The Cyber Awareness Trainings initiative was initially applied at the OHQ in Larissa in Greece which, at that time, was in charge of operation EUFOR RCA, and it was later on pursued at the OHQ of EUNAVFORMED/SOPHIA in Rome. After several of such trainings for OHQ Larissa and OHQ Rome provided by mobile training teams organised by EDA, with the support of the Cooperative Cyber Defence Centre (CCD COE) in Tallinn, they are nowadays taking place regularly with any staff rotation under the auspices of the OHQ hosting Member State. We expect that our prototype for a Deployable Cyber Forensics Capacity, which currently undergoes testing, will be ready for operational deployment by end of this year.

In the 2018 Capability Development Plan Revision, the EDA adopted particular focus on 5 key areas: cyber cooperation and synergies, cyber research and technology, systems engineering framework for cyber operations, cyber education and training and specific cyber defence challenges in domains of warfare. Which of these are currently undergoing particularly intense development?

The first four of the five topics you mentioned have been growing over time in EDA based on existing activities and expertise. When it comes to fifth topic, the specific cyber defence challenges of the traditional domains of operations - land, maritime, air as well as space as a vital enabler for operations – we are entering new territory.

We realised that over the past years, the focus has been on developing and implementing centralised, standard commercial-of-the-shelf (COTS) IT and network-centric cyber defence solutions. However, Armed Forces have their own weapon and sensor systems with very specific functions which require very specific and individual IT solutions, which means that they also have very specific vulnerabilities. Here we want to put a new focus as these assets are at the heart of any military operation. We currently cooperate with the European Space Agency (ESA) to further define and refine space-related cyber threats as well as cyber aspects in the aviation area, in the context of the Single European Skies (SES) project. We intend to expand these activities to the land and maritime domains later on.

How would you assess the cooperation with the European industry in terms of projects related to cybersecurity? How does the EDA engage the private sector?

We first have to acknowledge that the information and cyber domain is technology driven – which means that it is mostly driven by the private sector and their innovation cycles. Therefore, the starting point of this relationship is to consider how the military - as a technology demander, user and consumer – can join and influence industry driven innovation with their own specific defence requirements

at the earliest moment possible. To be able to do that, you have to have a forward looking understanding of where innovation is heading to. Therefore, EDA has established a Cyber Strategic Research Agenda which is continuously updated and which identifies, from a military perspective, the different Technology Building Blocks (TBB) required for achieving cutting-edge cyber technology able to cope with current and emerging threats. Roadmaps are then developed for these TBBs which further specify the research and development activities and projects that are necessary to bring these building blocks up to the required technical readiness level within a certain time frame. EDA has identified eight TBBs. For three of them the roadmaps are already established while the remaining five will be developed by mid-2020. This work is done by the Cyber R&T working group. Different instruments can be used for the implementation of the roadmap activities: EDA ad hoc projects, EDIDP/EDF projects, PESCO projects or other cooperation formats.

In order to have a constant dialogue with industry, the Cyber R&T working group also frequently meets with European industrial partners. Furthermore, specific industry days are organised, the last one on 'Cyber in the Aviation domain' in March 2019. With shouldn't also forget the relationship EDA has with the European Cyber Security Organisation (ECSO). This contractual Public-Private-Partnership (cPPP) of the EU Commission brings together the European key players in the private sector - be it industry or academia – on civil cyber security. Since there is no strict separation between the civil cyber security market and the military cyber defence market, this interaction with the private sector is of relevance for EDA cyber defence activities. Therefore, EDA has established a strong and dynamic dialogue with ECSO since its establishment and also actively contributes to the work of several ECSO working groups. As you can see, projects are only a small facet of the EDA-industry relationship.

EDA has established a Cyber Strategic Research Agenda which is continuously updated and which identifies, from a military perspective, the different Technology Building Blocks (TBB) required for achieving cutting-edge cyber technology.

In May of 2018, the EDA signed a Memorandum of Understanding (MoU) with the EC3, ENISA, and CERT-EU to establish cyber cooperation and synergies. What are the main challenges in coordinating between these institutions? What benefits do you envision will come from this cooperation?

The four signatories are quite different in terms of mandate, size and governance. EC3, for instance, focuses on the fight against crime and is specialised in areas such as forensics, malware analysis and international online crime organisations. ENISA has a research and policy support programme that focuses on the civilian/private sector. CERT-EU has a very specialised knowledge in network monitoring in this environment. EDA covers the military side and focuses on capability development, research and technology and policy support.

This diversity is both the main asset and the prime source of complexity for the MoU working group which needs to strike a delicate balance between operational and non-operational taskings, research versus adoption, technology versus policy making, military versus civilian areas.

We realised that it is extremely important to mutually inform each other of the respective work plans in the short term, to attend and participate in each other's events, to identify areas of common interest - for instance forensics, training and education - and to harmonise the respective work plans. All this may look obvious at a first glance, but had never really been done before.

In the near future, we will look at improving our cooperation on highly visible areas such EU cyber exercises, the implementation of the latest political guidance (Cyber Defence Policy Framework, Cybersecurity Act) and the joint organisation of cybersecurity and cyber defence events in order to optimize efforts and avoid duplication.

Cyber Ranges was the first EDA's cyber Pooling & Sharing project aimed to result in an effective European network of national cyber ranges. What are the lessons learned so far from its implementation? How successful was it in increasing the participating Member States' exercise and training abilities? What do they gain from participation?

The project will be completed by Q1 2020 and followed by an appropriate lessons-identified process. Remember what the situation was in 2013 when the project started: while a few pMS' were looking at creating a military Cyber Range, there was no clear indication of how such an asset would look like and what requirements it should fulfil. Also, networking technology was improving but it was far from being reliable and permeant enough to guarantee a good user experience for decentralized computation- and network- heavy applications. Finally, cyber defence was still relegated to a mostly technical area, where elements such as training and education were seen as accessories. Today, we can acknowledge that many pMS either already own or are in the process of developing Cyber Ranges for their military forces. Furthermore, while networking technologies have improved, it is very hard (if not impossible) to create a synthetic environment where all aspects of modern IT are reproduced properly. For example, we can mimic the behaviour of a malware for training purposes but if it uses social media as a command and control endpoint, this can hardly be reproduced with enough realism. Also, the importance of having a virtual environment where students can exercise and play with tools and techniques in a secure fashion is even higher than before. The level of technical sophistication used by malicious actors in Cyberspace has grown so much that it is impossible to expect that people have the resources to learn on their own. Hence the need for a more structured and coordinated approach to learning.

All these factors confirm the need for strong international cooperation in this area in order to build up a more skilled workforce.

The level of technical sophistication used by malicious actors in Cyberspace has grown so much that it is impossible to expect that people have the resources to learn on their own.

The project has gone through several development steps, focusing on technical architecture to support the federation and on integrating existing assets from pMS. It also produced a market analysis of the products and tools available on the market and how their respective roadmaps can serve the increasing training needs.

An important conclusion of the project is that there is no dominating technology for Cyber Ranges but the solutions adopted by pMS differ greatly, with huge gaps in terms of interoperability.

Recently, EDA held the kick-off meeting for the Cyber Defence Situation Awareness Package Rapid Research Prototype (Cy SAP-RRP). How will this project contribute to the overall cyber defence posture of the Member States?

Situation Awareness has been a long-lasting military discipline in which inner decision processes such as decision-making, options generation, dynamic risk assessment were integrated in military doctrine. With the advent of innovative solutions such as Cloud Computing and Big Data, the situation awareness process has become even more sophisticated and requires new techniques and advanced support tools. Applying this process to Cyber Defence is of foremost importance.

In this domain characterized by speed of action, absence of geographic references and a prime role of industry who is the real owner of the Cyberspace, situation awareness requires new processes and new tools, often with a level of sophistication that is unknown to other domains.

In this context, pMS cannot afford to research, create and operate tools on their own. Instead, they have to engage in international cooperation to achieve better efficiency and higher effectiveness.

Participating Member States cannot afford to research, create and operate tools on their own. Instead, they have to engage in international cooperation to achieve better efficiency and higher effectiveness.

The intent behind the project is to leverage skills and technical knowledge from market leaders to experiment with new techniques to gather, correlate, index and visualise the overwhelming amount of security information produced by modern IT systems, in a form and with a pace that can be easily consumed by a military decision-maker. When this project will be completed, pMS will have acquired an invaluable wealth of knowledge in dealing with these problems, and we expect this to dramatically improve their ability to build more effective decision-processes for Cyber Defence.

How many more projects dedicated to cybersecurity should we expect in the near future? Are there any new projects being discussed currently?

It is of course hard to predict if and how pMS will agree on upcoming project proposals. Nevertheless, we can easily assume that the Capability Development Plan and the related Strategic Context Case (SCC) on 'Enabling Capabilities for Responsive Cyber Operations' will drive this process. The SCC contains several Avenues of Approach which will be addressed in the next years with project/activity proposals for concrete action.

Today, we in EDA are looking specifically at the following areas:

First, Cyber Ranges Federation. The current project will complete in Q1 2020. There is growing consensus in looking at a second iteration in order to focus on areas that have matured and changed since the inception. In this second phase, the project will focus on creating more services to be consumed by participating Cyber Ranges, in order to create an even more sophisticated environment to run exercises and training sessions. There will be more attention paid to cybersecurity trends, including the use of Artificial Intelligence (AI) and the need to propose interoperability standards for higher level services.

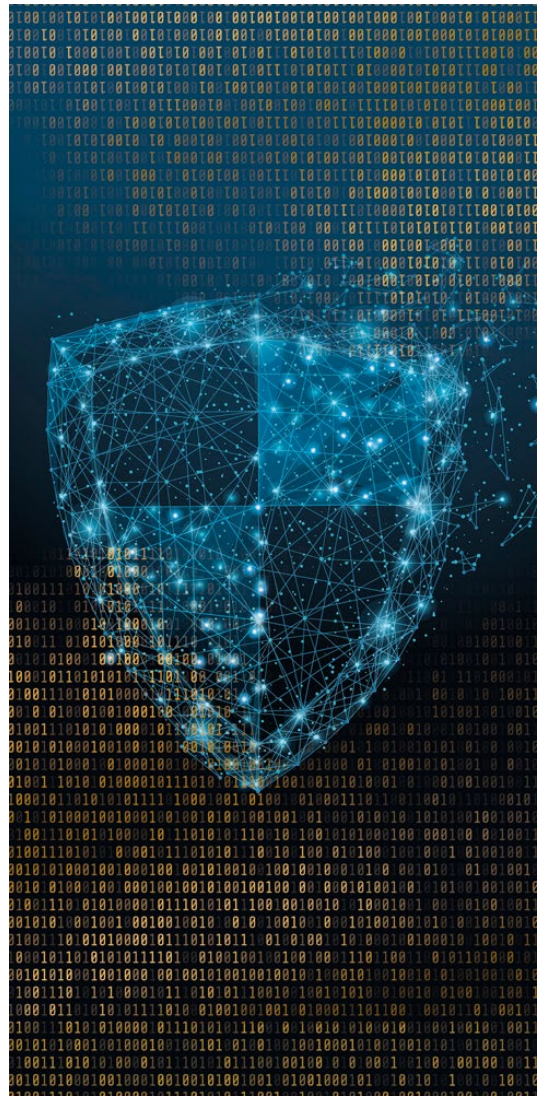
Second, Cybersecurity in the Defence Supply Chain. During the acquisition of new capabilities, threats can derive from abusing the imperfect exchange of information across the supply chain,

where vendors have to go through a number of steps to integrate and provide the required assets. The amount of risk taken in this process by the acquisition entity is extremely hard to determine - in a world where IT is a crucial function in any capability including military ones, it is of utmost importance to have a clear view of what the risks are, what mitigation options are available and what the residual risk at the end of the process is. There is enough room in this area to build one or more collaborative projects to analyse available mechanisms and produce tools and procedures that can be used by pMS in their acquisition processes, in order to provide a more unified approach.

Third, Advanced Threat Detection. While we have a project in place to address this issue, there is a strong consensus on the need to produce even more advanced tools, in order to counter threats using the latest technology available. Additional research projects could look for synergies with other running initiatives at EDA, such as the working group on AI. We see opportunities here to start other initiatives with a stronger focus on specific areas of APT detection (threat hunting, APT detection in specific areas, like low level software, IoT, etc…)

Furthermore, additional activities and projects under EDIDP, PESCO or other cooperation formats will most probably materialise. ■

Questions by Mackenzie Baldinger



Wolfgang Röhrig is the Head of Unit Information Superiority in the Capability, Armament and Planning Directorate of the European Defence Agency (EDA). He was born 1966 in Germany and entered the German Navy in 1985. After completing his studies at the University of the Federal Armed Forces in Hamburg with the degree of MBA in 1990. He served in several officer's positions in the German Navy and the German Joint Services including several operational deployments and service in NATO. March 2012 he joined EDA as Project Officer and became Programme Manager Cyber Defence beginning of 2014. In this position he developed and shaped the EDA Cyber Defence Programme, being inter alia responsible for the identification of capability gaps with respect to cyber defence in EU-led military operations, and the development and implementation of solutions for closing these gaps through cooperative projects with EU Member States. In February 2018 he returned to the German Armed Forces becoming a staff member of the new Cyber and Information Domain Services Headquarters dealing with International Cooperation in Cyber Defence. Since November 2018 he is leading the EDA Information Superiority Team in EDA. The EDA Information Superiority Team pools the EDA expertise on Capability Development in the Cyber Domain and the Space Domain as well as on ISR, Information Management and general CIS.

If sovereignty is the objective, strategic autonomy is a means

Interview with Paul Timmers, Visiting Fellow, Oxford University; Former Director, Sustainable & Secure Society Directorate, DG CONNECT, European Commission

"Strategic Autonomy is the ability, in terms of capacity and capabilities, to decide and act upon essential aspects of one's longer-term future in the economy, society, and their institutions". According to this definition, the unit for strategic autonomy may be understood to be the state, but it is equally valid to consider an alliance of countries. (...) The definition is non-normative, though identifying "essential aspects" is of course a subjective matter. (Timmers, 2019)

In May 2019 you published an article about strategic autonomy and cybersecurity in which you started by giving an overview comparison of both "strategic autonomy" and "sovereignty". Why do you think both terms are often confused by policy-makers and politicians? What are the reasons, in your view, that academics have worked little on differentiating both topics?

Policy-makers, politicians, and journalists tend to be quite creative with political terms. It is then up to academics to reflect on their scientific foundation and to provide more conceptual clarity. Philosophers of science may be able to explain why this is the case.

The confusion of sovereignty and strategic autonomy often reads as a confusion of means and ends. If sovereignty is the objective, then strategic autonomy is a means to realise that objective. Consequently, strategic autonomy is much more actionable than sovereignty. "Actionability" is what policy-makers usually are looking for. Strategic autonomy is about practical abilities to make sovereignty a reality. Sovereignty is an aspiration or for some a divine right or innate to collective identity (Biersteker, 2012).

Academics until recently did not much discuss the difference between strategic autonomy and sovereignty. The reasons probably are a lack of proper definition of strategic autonomy and the confinement of strategic autonomy to the domain of defence and military, which is only a part of the big world of interest to political scientists. Nowadays, however, strategic autonomy has escaped from that corner and is seen as being relevant to economy, society, and democracy at large. This is due to the confluence of pervasive digital transformation, cyberthreats, and international tensions.

The confusion of sovereignty and strategic autonomy often reads as a confusion of means and ends. If sovereignty is the objective, then strategic autonomy is a means to realise that objective. Consequently, strategic autonomy is much more actionable than sovereignty.

On strategic autonomy, which you define as "the ability, in terms of capacity and capabilities, to decide and act upon essential aspects of one's longer-term future in economy, society, and their institutions", what are those "essential aspects" governments should guard? Why do governments need digital strategic autonomy? And the EU? What would be the consequences of not doing so?

This definition has three elements: agency, future, and essential aspects. On purpose the definition does not spell out these essential aspects. Doing so would imply academically pre-defining the key aspects of one's future. Rather, this should be a political process, both to imagine "one's future" and to agree on its essential aspects. Nevertheless, we can try to identify a minimal set, based on widely shared perceptions of sovereignty. This would include safety, security, and healthy living; being free from fear of disastrous internal and external disruption; opportunities to an adequate income for all; inclusive knowledge and cultural development opportunities; and credible internal and external authority. All these qualia need to be present to an acceptable rather than to an absolute degree. Opinions are more divided whether to add: a democratic voice for all; supremacy of citizen's rights including diversity rather than state supremacy; internal and external integrity of the state. Contestation of these latter has been fuelling disagreement in cyber diplomacy at UN level.

Governments must keep strategic autonomy in mind as this is central to what they stand for: the people and the state. The same holds for alliances of states such as the EU. Pursuing strategic autonomy for national sovereignty is an acceptable means-end logic. Expressing the same at EU level and mentioning "EU sovereignty" still creates unease. At least that seems to be the case when reading reactions to European Commission's President Juncker's State of the Union speech in September 2018 that had the title "The Hour of European Sovereignty".

In current geopolitics, if governments drop the ball on strategic autonomy, they would put at risk the future of the people they represent and the institutions they are to maintain. This is the concern expressed nowadays from Washington to Brussels to Moscow and Beijing.

The notion of "digital strategic autonomy" is not defined but could be interpreted as the part of strategic autonomy that is related to the digital world. It is a fact, of course, that ever more of "the abilities, in terms of capacity and capabilities, to decide and act upon essential aspects of one's future" are digitally related. They include mastery and control of specific digital technologies (such as 5G, AI, quantum technologies) and abilities in critical areas of economic, societal, and democratic life that are very strongly digitally dependent, from energy networks to media.

In current geopolitics, if governments drop the ball on strategic autonomy, they would put at risk the future of the people they represent and the institutions they are to maintain. This is the concern expressed nowadays from Washington to Brussels to Moscow and Beijing.

One of the three pathways that you suggested in order to achieve a greater level of strategic autonomy is risk management, from a cyber resilience perspective. Risk management, as could be deduced from your article, needs a great level of cyberthreat awareness. Shouldn't this awareness be three-fold (governments, business, civil society)? How can governments promote cyber awareness in the civil society?

This is a very valid point and my answer is a qualified yes. Yes, because with the distributed nature of cyberincidents and the high interconnectedness of digital systems everyone gets exposed to cyberthreats. Threat awareness,

preparedness, and protection need to be similarly widespread and interconnected.

Still I would like to qualify this "yes" with a "but" as we need to also counter the downsides of this approach. Pursuing widespread awareness and attentiveness should not result in a surveillance society. It should not result in freeriding. It should not result in undue responsibility. It should not result in legitimising commercial collusion or government-private collusion. Nor stifle innovation.

We are starting to build up a body of experience within countries and within sectors in countries to best deal with cyber awareness and how to counter the negatives. The challenge now is to do the same across sectors and internationally. Good examples of such collaboration are in the global financial sector, e.g. SWIFT; in the energy sector, e.g. ENCS; between national cyber experts, such as the CERT collaboration under the EU's NIS Directive; and across national and private awareness initiatives, such as ENISA's Cyber Awareness Month.

Pursuing widespread awareness and attentiveness should not result in a surveillance society. It should not result in freeriding. It should not result in undue responsibility. It should not result in legitimising commercial collusion or government-private collusion. Nor stifle innovation.

Another policy recommendation was establishing strategic partnerships. In that specific topic, you pointed out that whereas only a few countries may be able to achieve a sufficient level of strategic autonomy (the People's Republic of China or the United States), the rest of the countries need to establish good quality strategic partnerships with like-minded partners, based on the notion that working together is a win-win situation. What do you think limits that win-win mentality while crafting accords on sensitive matters such as data sharing and cybersecurity? Can the pursuit of strategic autonomy create a new wave of digital protectionism and put an end to the joint global effort to advance technology?

The negotiation on the EU's NIS Directive was an instructive example of aiming to create a win-win while being constrained by national sensitivities, i.c. national security concerns. Formal limits in the EU's mandate as regards national security stem from the EU Treaties. Article 4(2) of the Treaty on the European Union states that the EU shall respect "essential State functions, including (…) maintaining law and order and safeguarding national security". National security remains the sole responsibility of each EU Member State. Consequently, EU legislation and policy often have a national security exemption clause.

The result is that the Network and Information Security Directive is less harmonised on information sharing for physical critical infrastructures than for digital infrastructures. The former is after all more bound to territory, think power plants, than the latter, e.g. cloud services (Timmers, 2018). So, national security is a limitation to data and information sharing. Obviously, national security is at the heart of sovereignty. Nevertheless, shared or pooled sovereignty is the hallmark of the success of the EU. Moreover, all EU Member States are acutely aware that cyber respects no borders. There is a clear willingness in Europe to collaborate in operational and strategic cyber matters. The shape this takes ranges from hard law like the 2018 Cyber Act to softer approaches like the 2019 Recommendation on Cybersecurity of 5G Networks.

Paradoxically, willingness to collaborate in cyber has been growing in the EU while internationally we have seen a growing polarisation and contestation (win-lose) rather than collaboration (win-win). The underlying reason is the fundamental change that cyber is creating a sovereignty gap (Kello, 2017). As digital technologies become ever more pervasive, this sovereignty gap concerns ever more of economy, society, and democracy (viz. the definition of strategic autonomy). States cannot afford to let this happen.

There is a clear willingness in Europe to collaborate in operational and strategic cyber matters. The shape this takes ranges from hard law like the 2018 Cyber Act to softer approaches like the 2019 Recommendation on Cybersecurity of 5G Networks.

Therefore, they pursue the three approaches that I outlined: 1) trying to keep the risks to their sovereignty manageable, 2) working in strategic partnerships of the like-minded, and 3) promoting the global common good and thereby moving certain risks to sovereignty out of the control of any single country. The fourth approach, "bowling alone", to quote Putnam, is at most for the US or the People's Republic of China, be it with dire consequences for global trade.

The three approaches are not exclusive. It is thinkable to pursue at the same time a risk management approach for cybersecurity in, say, the health sector underpinned by a UN norm to not harm each other's civilian critical infrastructures, and to invest in a strategic partnership in supercomputing or 6G as well as to promote a global common good approach for protecting the core of the internet.

In your article you mention multiple times the term cyber diplomacy, which can be the soft version of what Joseph Nye has defined as "cyber power". In his work, from a behavioural point of view Nye defines a cyber power as having hold of "three Cs": creation, control, and communication of information in the cyberspace. Can the EU be considered a cyber power? What are the differences between cyber power and cyber diplomacy? How can becoming a cyber-diplomacy power help the EU in achieving strategic autonomy?

Clearly today's foremost cyber power in the Nye sense must be the People's Republic of China, based on a coercive system that has been labelled the techno-security state (Cheung, 2018). It is not a model that most Europeans aspire to follow, even if the EU is behind China in terms of being a cyber power. The quest to be a matching cyber power risks reviving the kind of inter-state mistrust that has proven to be highly damaging, leading to trade blockages as early as the 19th-century UK Corn Laws and as recent as today's US-China tariff war. It also risks a (cyber-)arms race. Historically, diplomacy has played a beneficial role breaking such vicious cycles. It has enabled the world to establish some degree of peaceful coexistence, enabled the flourishing of international trade, and even establishing arms treaties.

Today, some of that appears to be breaking down (cf. the collapse of the INF Treaty). In my view now is the time that Europe can and should show again its strengths in diplomacy, applied to cyber diplomacy. Will that benefit Europe's strategic autonomy? Yes, as it would reduce the external risks to its critical infrastructures. It would create more openness to partnerships of the like-minded and help establish agreements for proper behaviour where the alternative otherwise would be a lose-lose, i.e. establish strategic interdependencies (Bendiek, 2018). It would facilitate positioning selected cyber challenges as a common cause for the good of humanity, to be pursued under global governance as a common good.

In my view now is the time that Europe can and should show again its strengths in diplomacy, applied to cyber diplomacy.

Your third policy recommendation is titled "promoting the global good". There you emphasised how humanity has been able to debate solutions once it had identified a risk that became a policy priority. On that specific topic, you open the door to extended debates that involve both private and public sectors as well as society. How can the strengthening of these improve the role of European cyber diplomacy? Can society participation through, for example, crowdsourcing, have a positive impact on working towards strategic autonomy?

First, pursuing this approach will need active cyber diplomacy itself. Cyber diplomacy engagement would be crucial in order to explain the open source approach in non-technical terms.

It will help us to build bridges between public/private sector and civil society at international level. Diplomacy will be essential to take the sting out of the most sensitive aspect of the global approach, namely that countries appear to relinquish some sovereignty. The argument would be that a global good approach means having a fair share in global governance and preventing domination by a single state or non-state actor.

Cyber diplomacy engagement would be crucial in order to explain the open source approach in non-technical terms. It will help us to build bridges between public/private sector and civil society at international level.

Second, Europe has a strong tradition in open source and is an active player in distributed security (e.g. in the International Blockchain Alliance). Europe's R&D programmes have for many years taken an open approach, governments mandate open source software, European e-government (e.g. the European Interoperability Framework) and standardisation are favourable to Free/Libre (sic!) and Open Source Software. Europe's diplomats would therefore be quite credible promoters of the global common good approach.

This route may require revisiting global governance: the global open source and internet community as a collective of non-state actors would have to be a recognised and major actor.

As said, some governments would not readily accept this, notably those that want to turn the clock of history backwards to revive a Westphalian state-centric world or seek a position of power fuelled by the politics of conflict. Participation of non-governmental actors *together with* government actors is the realistic way forward. As the open source movement shows, in such a setting technical development flourishes with non-government initiatives. Governments can stimulate such initiatives. In the forthcoming €100 bn Horizon Europe R&D programme, this would mean to give financial and programmatic priority to open source, distributed governance (including distributed security), crowdsourced and other non-governmental distributed initiatives that overcome the downsides of single-state control.

In your article, you often use the "Franco-European strategic autonomy" as an example of a win-win strategic partnership. Can that open the door to thinking of strategic autonomy in the EU as a complex network that comprises such alliances as member state to third state, member state to member state, member state to European Union?

This is a very interesting reflection, and, in my view, we need to see that in the broad sense, assessing how such alliances have worked so far, such as NATO, and evaluate the relationships maintained to both EU and other alliances by countries like France, Germany, and the UK (think Brexit). We should also keep in mind the conceptual and ideological differences that led to the bifurcation of the UN cyber dialogues into UN GGE and OEWG (Tikk, 2019).

The EU is sui generis, a unique entity in offering a house for many international linkages of its members and at the same time commitment to the EU itself. Imagine that the States of the USA or the provinces of China would pursue such a model… But this unique alliance of EU states has been severely tested and strained.

As regards cyber, these stresses are more external than internal and, interestingly, cyber increasingly seems to be a uniting rather than a dividing force in Europe; see the recent common quest for an approach to 5G security. Several international developments bring much external pressure. Some of these bring EU countries together, Brexit being a case in point, other external stresses are divisive indeed, migration being the counterpoint here. What is the net result of this in the EU? I would suggest that we will see a dynamically evolving set of relationships, based on common values that will continue to be subject to debate, with a strong dose of realism and pragmatism, yet on a solid foundation, namely the EU Treaties. Therefore, we should expect a rather dynamic evolution of EU countries with regards to their own and the joint EU strategic autonomy.

As for the future, we are on the brink of a new technological revolution that is going to greatly affect the cybersecurity environment. The second quantum revolution brings with it many cybersecurity risks, of which we can highlight two: cracking the most-used public-key cryptography and possibly creating a quantum vector for cyberattacks that would be devastating considering that our computational systems are archaic compared to quantum computation systems. Is the cyber resilience cycle enough to analyse and face these potential threats or does that qualitative leap require new creative ways of thinking about cybersecurity?

Cybersecurity is here to stay and will become even more challenging with the new technology developments. We cannot but confront this challenge. Ducking it means an unacceptable loss of voice in our own future. Yes, it will need qualitatively different and creative ways of thinking and of governance. In my view this includes proactive cybersecurity that anticipates large-scale misuse. It asks for openness to new forms of post-Westphalian and global governance. It asks for reflection on identity and participation as citizens, companies, and institutions on a vulnerable small planet.

Personally, I am inspired by hints of the future given by (Cowhey & Aronson, 2017), (Snyder, 2017) and (Bostrom, 2017), and indeed, by some of the young people that dare to take their concerns about the future to the streets. ■

Questions by Andrea Rodriguez

Cybersecurity is here to stay and will become even more challenging with the new technology developments. We cannot but confront this challenge.

Paul Timmers is a visiting fellow at the University of Oxford. His recent research is on cybersecurity, strategic autonomy and sovereignty. He is also visiting professor at Rijeka University, Senior Advisor to the European Policy Center, Chief Adviser to the European Institute of Technology/Health, and Supervisory Board member of the eGovernance Academy in Estonia.

He is a former Director at the European Commission for Digital Society, Trust & Cybersecurity, responsible for policy, legislation and innovation in cybersecurity, digital privacy, digital health and ageing, e-government, and smart cities/mobility/energy. He was member of the Cabinet of European Commissioner Liikanen.

He held various academic positions. He was manager in a large ICT company and co-founder of an ICT start-up, holds a PhD in physics from Nijmegen University in the Netherlands, an MBA from Warwick University in the UK, was awarded an EU fellowship at UNC Chapel Hill and completed executive cybersecurity education at Harvard.

References

Bendiek, A. (2018). No new Cold War: Give strategic interdependence a chance. Oxford Politics Blog.

Biersteker, T.J. (2012). State, sovereignty and territory. In W. Carlsnaes, T. Risse, & B.A. Simmons (Eds.), *Handbook of International Relations* (pp. 245-272). SAGE Publications.

Bostrom, N. (2018). Vulnerable world hypothesis. Oxford working paper.

Cheung, T.M. (2018). The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, 3(3), 306-326.

Cowhey, P., & Aronson, J. (2017). *Digital DNA*. New York: Oxford University Press.

Kello, L. (2017). *The virtual weapon and international order*. New Haven: Yale University Press.

Snyder, T. (2019). *The road to unfreedom*. Tim Duggan Books.

Tiik, E. (2019). Search for Cyber Norms – Where to Look? Blog #2National Views and Positions in the UN. ICT4Peace.org.

Timmers, P. (2018). The European Union's cybersecurity industrial policy. *Journal of Cyber Policy*, 3(3), 363-384.

Timmers, P. (2019). Strategic Autonomy and Cybersecurity. EU Cyber Direct Policy in Focus.

ANALYSIS

The weaponisation of social media

The use and abuse of human dispositions

JORIS VAN BLADEL
ASSOCIATE FELLOW, AUSTRIAN INSTITUTE FOR EUROPEAN AND SECURITY STUDIES
ARTHUR DE LIEDEKERKE*
EXTERNAL AFFAIRS OFFICER, CERT-EU

Disclaimer: Arthur de Liedekerke contributed to this article in a strictly personal capacity. The views and opinions expressed in this article are those of the author and should not be construed as reflecting the official policy or position of the European Commission.

People and War

Ever since war has been conceived as a political, social, and military phenomenon – this is, since the Napoleonic era – the influence of the *vox populi* has become increasingly significant during military campaigns. Public opinion, according to this view, shapes the dynamic and the outcome of battle. At the beginning of the 19th century, Carl von Clausewitz, for instance, declared "popular support" and the "exploitation of moral factors" to be among the main aspects of strategic effectiveness (von Clausewitz, 2007, p. 363). Antoine-Henri Jomini, a contemporary military theoretician, cited "public credit" as one of the necessary conditions to build strong nations and effective military institutions (Jomini, 2007, p. 37). In asymmetric warfare, small warfare, and counter insurgency operations, the battle for the hearts and minds is one of the main concerns of the military commander (Guran, 2013). Currently, in times of "war amongst the people" (Smith, 2005) and hybrid warfare (Armistead, 2004; Fevery, 2018; Fridman, 2018), achieving domination of the information sphere, including through targeted operations designed to manipulate the perception of the population, has become a standard objective for every strategist (Gerasimov, 2013; Korybko, 2015).

In asymmetric warfare, small warfare, and counter insurgency operations, the battle for the hearts and minds is one of the main concerns of the military commander.

Despite this generally accepted premise, there is still debate on the precise effect of public opinion on war. Some authors focusing on this theme claim that a population's view on the issue of war is dynamic, yet not volatile. Within this school of thought, two distinct strands compete: attitudes and beliefs about war are based either on a rational cost-effect calculation (Mueller, 1985) or imposed by elite opinions (Berinsky, 2009). Alternatively, especially for those who focus on the theory of "reflexive control" or those who emphasise the effectiveness of information warfare, the prevailing view is that it is possible to profoundly manipulate the thinking of the adversary, military and civilians alike, even to the point where they take decisions or assume opinions that are unfavourable for them (Leonenko, 1995; Komov, 1997; Thomas, 2004; Panarin, 2015; Giles, Seaboyer & Kerr, 2018). These approaches are based on the assumption that individual and collective thinking is both highly volatile and malleable and thus, if managed well, can be conveniently altered to one's advantage. Sophisticated theories have been elaborated to explain how to influence an opponent's behaviour, resorting to tactics such as distraction, overload, deception, division, suggestion, and provocation (Komov, 1997; Thomas, 2004; Snegovaya, 2015). On the basis of these premises, it becomes clear that the growing prevalence of social media has made the application of such tactics both easier and more effective than ever.

Social Media: Exploiting The Fallibility of Human Nature

Recent research has revealed some alarming findings regarding the impact of social media on public opinion. Indeed, a comprehensive study of Twitter users' behaviour has shown that falsehoods are 70% more likely to be retweeted than accurate news[1]. This means that false content travels further and faster than the truth. As a result, Twitter users, and by extension users of social media, seem to be particularly susceptible to spreading false news (Vosoughi, Roy & Aral, 2019).

Indeed, a comprehensive study of Twitter users' behaviour has shown that falsehoods are 70% more likely to be retweeted than accurate news. This means that false content travels further and faster than the truth.

There is much debate as to the reasons why social media users demonstrate such a behaviour. Featuring high among possible explanatory factors is a human inclination to engage with content that elicits an emotional response

1 This study is based on data collected in the period 2006–2017, including about 126,000 news cascades that were tweeted by 3 million people over 4,5 million times.

(think of "clickbait"), which contributes to the viral spreading of false news. Moreover, there is good reason to believe that a specific mode of human thinking, the so-called "system 1", which emphasises fast, emotional, and instinctive thinking (Kahneman, 2011), is active when using social media. According to this hypothesis, human reasoning is subject to intrinsic fallacies and faulty ways of thinking. Indeed, a certain number of cognitive biases such as anchoring, availability heuristics, or confirmation bias are hardwired in our brain. With these innate mechanisms being unconsciously active, human beings, and in this particular case social media users, tend to overestimate their own critical faculties. This may explain the paradox whereby even the most discerning and educated users of social media, apparently counting on their critical skills, often prefer online resources to the printed press, TV, and radio, even despite their awareness of the fact that social media is likely to be more inaccurate and misleading than traditional news outlets (Matsa & Shearer, 2018).

A Perfect Storm: Multiple Factors Converge

Technological developments as well as political, economic, and sociological realities, in addition to the aforementioned psychological dispositions, contribute to the growing influence of social media on public sentiment and opinion. Among these:

- The growth of internet users and ubiquity of social media guarantees an ever-expanding online audience for these platforms which, in turn, has "democratized the dissemination and consumption of information, thereby eroding traditional media hierarchies" (Gangware & Nemr, 2019);
- The use of bots (software that can perform automated tasks like posting content based on pre-determined rules) and troll farms (also known as factories; multiple online commentators pushing a specific political agenda) are able to artificially amplify the popularity, to distort the tone, or to steer the direction of information feeds or conversations;
- The emergence of "deepfakes" (highly realistic and difficult-to-detect digital manipulations of audio or video material that benefit from technological developments in machine learning), which is rendering the detection of false news increasingly difficult, if not impossible (Wilkey Oh, 2017);
- The contemporary trend of post-truth politics where "fake news" and "alternative facts" have been explicitly endorsed by prominent public figures using social media platforms as their main communication tool (Gangware & Nemr, 2019);
- The observation that the most vulnerable targets in terms of education, age and social background are those most resorting to social media as part of their information ecosystem (Dreyfuss, 2018);
- The inability or unwillingness of social media companies to control the content of their platforms – for commercial or ideological reasons (Newton, 2019).

Clearly, these factors make the exploitation of vulnerabilities in our information consumption relatively easy and potent, turning the social media into a powerful weapon. Accordingly, the weaponisation of social media – its intentional use to dominate the information sphere with the aim to manipulate public opinion and to undermine society – poses a serious threat (Singer & Brooking, 2018; Rychlak & Pacepa, 2013).

Social Media Platforms: Dual-Use Technology?

The innate ambivalent nature of technology is a well-known and widely documented issue (Feenberg, 1990). Here ambivalence means that a technology can be used both for good and bad purposes. It is indeed the social praxis that will ultimately determine what the repercussions of a certain technology are on our personal lives and on society at large. The positive effects of social media on our societies are numerous, ranging from democratic benefits, such as increased civic engagement, to improved communication.

However, two recent examples demonstrate the possible malicious use of social media.

- The terrorist organisation Islamic State (IS) has used the most popular social media platforms such as Twitter, Facebook, and YouTube to spread their propaganda, radicalise, and recruit terrorists among their followers (Awan, 2017; Hoffman, 2017). IS's skillful (ab)use of social media has also shown how difficult it is to counteract in the "battle of ideas and imagery" (The Economist, 2015);
- Robert Mueller, America's Special Prosecutor who has investigated the Russian intervention in the 2016 US presidential elections, has meticulously documented the organised manipulation of public opinion among US voters through social media with the intention to support Donald Trump, to instill mistrust in the American political system, and to sow division in society (Mueller, 2019; Sanger, 2018).

These examples, among many others, beg the following question: should social media, to a certain extent, be considered a dual-use technology, particularly when it is deployed with malicious intent and in times of war?

The positive effects of social media on our societies are numerous, ranging from democratic benefits, such as increased civic engagement, to improved communication.

War Goes Viral

In order to illustrate the use of social media in military conflict, one can look at a region like the Levant, where dominating the cyber-social battle has long been a key preoccupation. Indeed, between 2006 and 2013, a period where the Arab-Israeli conflict witnessed several escalating moments, the fighting parties, state and non-state actors alike, innovated in how they turned social media into a strategic warfare tool.

- In the summer of 2006, during the July War (a.k.a. the Second Lebanon War), the effects of "cybercortical warfare" (Conway, 2005; Szafranski, 1997) became clearly visible. Hezbollah militias, bypassing the mainstream coverage of the war, surprised Israel by using real-time internet press and social media. Israel, despite its formidable cyber capabilities, was taken by surprise and could not prevent the demoralising impact of Hezbollah's narrative on the Israeli military and public (Schweitzer, 2006; Pahlavi, 2007, Shakarian, Shakarian & Ruef, 2013). Indeed, Israeli's poorly managed media strategy resulted in largely counter-productive effects, demonstrating the difficulty to counter a well-designed (social) media campaign (Winograd Commission, 2007; Kalb & Saivetz, 2007).
- In response to the deficiencies of the Second Lebanon War, Israel established the National Information Directorate that controls and unifies Israeli propaganda and public relations across different media outlets. During Operation Cast Lead, starting in December 2008, Israel organised a concerted informational campaign, combining traditional media, new media, and diplomacy. For instance, the Defense Force Spokesperson's Unit launched a YouTube channel that was viewed by millions as it was the only source of information available in the area. Several diplomatic missions abroad used Twitter to provide press briefings; blogs, written by immigrants recruited by the Israeli foreign ministry, were published in several languages, including Hebrew, Arabic, English, Spanish, French, and Russian. Students, recruited by the Interdisciplinary Center Herzliya, were tasked with spreading positive messages justifying Israel's military operation in social networking platforms and posting comments in Israel's favour on influential blogs (Shavit, 2016). In turn, Hamas managed a video-sharing platform so that citizens from Gaza were able to send tweets, videos, and images with their mobile phones. Additionally, Skype and mobile phones were used by Palestinian journalists to provide interviews to the international mainstream media outlets, while blogs and Flickr accounts were used

to report on events as they unfolded. Those who supported the Palestinians used the Qassam Count bot to report real-time events on the ground.

- In November 2012, operation Pillar of Defense started with a Twitter message. Indeed, Israel's declaration of war on Hamas was done via the social media platform, which promptly received a response of the Al-Aqsa Brigade. During this operation, Israel, managing more than 30 accounts on several platforms simultaneously, was able to organise a social media barrage, destined to shape, influence, control, and manipulate information for both foreign and domestic audiences. Social media was here fully integrated in this military operation as a distinct, modern information warfare function carried out by professional and dedicated teams.

Over the last decade, the Arab-Israeli conflict has revealed insights into the true nature of the information war, one that is partly waged using social media platforms. However, these developments are just the beginning of nothing less than a revolution that will fundamentally change the face of war. The effects of this weaponisation of social media are already visible in virtual skirmishes that have taken place in conflicts in Syria, Bahrain, Egypt, Libya, Kenya, and Somalia. Moreover, the "seven sisters of cyber power" – the United States, Russia, China, Britain, Iran, Israel, and North Korea (Sanger, 2018) – have a strong record of information operations, which stretches their power into the fifth dimension. For example, Russia, based on the Soviet tradition of reflexive control and *maskirovka*, and learning from its mistakes in the wars in Chechnya (1996/1999), has established an elaborate information doctrine, which it has allegedly applied in the Baltic States (2007), Georgia (August 2008), Ukraine (2014), and Turkey (2015). China for its part is widely believed to be conducting aggressive information campaigns against Taiwan, via social media, to influence the population in favour of unification with the mainland.

It is increasingly evident that we are living in turbulent times where information warfare has become an issue of permanent concern. As observed during the last decade, a maturation and sophistication of information operations has taken place.

It is increasingly evident that we are living in turbulent times where information warfare has become an issue of permanent concern. As observed during the last decade, a maturation and sophistication of information operations has taken place. Military doctrines and organisations have adapted accordingly. In the coming years, this learning process will continue with far-reaching effects on the battlefield and our societies alike. Indeed the clear-cut distinction between peace and war, combatant and non-combatant, state actor and non-state actors, truth and falsehood will become increasingly blurred.

Taking (Back) Control

The picture is bleak: disinformation, fake news, hoaxes are metastasising on social media, challenging the original DNA of our information ecosystems. The case studies discussed previously, and many other contemporary examples, show the potency of foreign, weaponised social media campaigns in manipulating the hearts and minds of a target population. Meyer, commenting on the impact of social media platforms, has said that they "… seem to systematically amplify falsehood at the expense of the truth, and no one – neither experts nor politicians nor tech companies – knows how to reverse that trend. It is a dangerous moment for any system of government premised on a common public reality" (Meyer, 2018).

Alarming signals aside, a number of promising solutions, at various stages of maturity, exist to tackle this pressing challenge:

- Civil society and the government are at the digital front-lines. Implementing and promoting digital media literacy programs – teaching citizens to verify which digital information is credible, to evaluate sources, and to understand how social media platforms work – is crucial to equip digital natives with the right critical skills to make sense of and discriminate between the vast amounts of information they are exposed to on social media;
- Social media actors have come under growing political and societal pressure to ramp up their efforts in combatting disinformation campaigns. Notable examples in this domain include the European Commission's Code of Practice against disinformation to which Facebook, Google, and Twitter have voluntarily signed up. In this context, private sector stakeholders have taken steps to improve the scrutiny of ad placements, identify and neutralise inauthentic accounts, and limit manipulative content. Elsewhere, legal measures have been passed in order for these companies to take action and manage the flow of disinformation by holding them responsible for the spread of misleading content (i.e. Singapore's Protection from Online Falsehoods and Manipulation Bill). However, attempts to legislate on these matters are controversial and raise serious ethical dilemmas, notably concerns about stifling free speech and the flow of ideas;
- Concepts, such as "dual-use technology" which we have briefly discussed, should inspire reflection on the responsible use of these technologies, emphasising the need for international cooperation. Indeed, states, should continue to engage in international debate on the dual-use of internet and notably social media, including in forums such as the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security;
- Technological solutions may also provide reasons to hope. For instance, in the fight against doctored images and "deepfakes", one of the more probing innovations is the concept of "digital provenance", which entails that "every time a photo or video is taken on any device, it is automatically tagged with a digital watermark specifying when it was captured", immediately embedding a time and geospatial tag on the image or footage (Dack, 2019).

Concepts, such as "dual-use technology" which we have briefly discussed, should inspire reflection on the responsible use of these technologies, emphasising the need for international cooperation.

The ultimate solution however will not come from a single sector nor will it be a quick fix. A convincing response to the growing weaponisation of social media will require a sustained, whole-of-society approach, where academia, government, media, cybersecurity experts as well as civil society come together to build up resilience in this rapidly evolving information landscape. Even then, it is unlikely that this will solve the underlying reasons behind the effectiveness and contagious spread of social media-enabled (dis)information campaigns in our societies: human nature. It is therefore worth reminding ourselves that our capacity to nurture critical thinking skills, a deliberate and slow mode of reasoning, is our last line of defence. ■

About the authors:

Joris Van Bladel studied Social and Military Sciences at the Royal Military academy in Brussels, Slavic Languages and Eastern European cultures at the State University of Ghent and holds a Doctor of Arts degree of the State University of Groningen. Currently, he is studying cyber security at the Thomas More College in Malines (BE). During and after his military career (1985–2006), he taught courses and guest lectures at several universities, including the Royal Military Academy in Brussels, the University of Amsterdam, Ghent University, Uppsala University, and the Technical University of Berlin.

Arthur de Liedekerke joined CERT-EU in 2018. He is currently working on External Affairs, Policy and Administrative matters. He previously worked in the European Parliament as an accredited assistant, on foreign affairs and security issues. He has collaborated with a number of corporate and strategic intelligence companies, based in the United States and Belgium. He holds two masters' degrees – in geopolitics and international relations – from King's College London and the University of Maastricht.

References

Armistead, L. (2004). *Information Operations, Warfare and the hard reality of Soft Power.* Dulles, VA: Brassey's Inc.

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. Society, 54(2), 138-149.

Berinsky, A. (2009). *In Time of War: Understanding American Public Opinion from World War II to Iraq.* Chicago, IL: University of Chicago Press.

Conway, M. (2005). Cybercortical Warfare: Hizbollah's Internet Strategy. In S. Oates, D. Owen, & R. Gibson (Eds.). *The Internet and Politics: Citizens, Voters and Activists* (pp. 100-117). London: Routledge.

Dack, S. (2019). *Deep Fakes, Fake News, and What Comes Next*. The Henry Jackson M. School of International Studies. Retrieved from the Jackson M School of International Studies Website on 28 August 2019: https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/

Dreyfuss, E. (2018, September 13th). Who Gets Their News from Which Social Media. *Wired*. Retrieved from the Wired Website on August 28th, 2019: https://www.wired.com/story/who-gets-news-from-social-media-sites/

Feenberg, A. (1990). The Ambivalence of Technology. *Sociological Perspectives*, 33(1), 35-50.

Fevery, A. (2018). *Hybrid Warfare: Secrets of the Revolution.* Independently published.

Fridman, O. (2018). *Russian Hybrid Warfare, Resurgence and Politization*. New York, NY: Oxford University Press.

Gangware, W. & Nemr, C. (March 2019). *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age.* Washington D.C., Park Advisors. Retrieved from Park Advisors Website on 28 August 2019: https://www.park-advisors.com/disinforeport

Gerasimov, V. (2013, March 5th). The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Voyenno-Promyshlennyy Kurier, pp. 2-5.

Guran, H. (2013). *Hearts and Minds: A People's History of Counterinsurgency*. New York NY: The New Press.

Heffner, A. (2019, June 30th). Greed Is to Blame for the Radicalization of Social Media, *Wired*. Retrieved on 28 August 2019: https://www.wired.com/story/greed-is-to-blame-for-the-radicalization-of-social-media/

Herzog, K. (2017, April 10th). The Dystopian Future of Fake News Is Being Developed in Seattle. *The Stranger*. Retrieved from The Stanger Website on 28 August 2019: https://www.thestranger.com/slog/2018/04/10/26025092/the-dystopian-future-of-fake-news-is-being-developed-in-seattle

Hoffman, A. (2016). The Islamic State's Use of Social Media: Terrorism's Siren Song in the Digital Age. In: Y. Schweitzer & O. Einav (Eds.) *The Islamic State: How Viable Is It?* The Institute for National Security Studies (INSS), 2016. Retrieved from the INSS Website on 28 August 2019: https://www.inss.org.il/wp-content/uploads/2017/07/10-The-Islamic-States-Use-of-Social-Media-Terrorism's-Siren-Song-in-the-Digital-Age.pdf

Jomini, A. H. de. (2007). *The Art of War*. Rockville MD: ARC Manor.

Kalb, M. & Saivetz, C. (2007). The Israeli-Hezbollah War: The Media as a Weapon in Asymmetrical Conflict. Washington DC: Brookings Institute. Retrieved from the Brookings Institute Website on 28 August 2019: https://www.brookings.edu/wp-content/uploads/2012/04/2007islamforum_israel-hezb-war.pdf

Komov, S.A. (1997). About Methods and Forms of Conducting Information Warfare. *Military thought* (English Edition), 4, 18-22.

Korybko, A. (2015). *Hybrid Wars, the Indirect Adaptive Approach to Regime Change.* Moscow: People's Friendship University of Russia.

Larson, E., Darilek, R.E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L.H. & Thurston, C.Q.(2009). *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*. Santa Monica, CA: RAND Cooperation. Retrieved from the Rand Cooperation Website on 28 August 2019: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf

Leonenko, S. (1995). Refleksivnoe upravlenie protivnikom [Reflexive control of the enemy]. Armeiskii sbornik (Army Collection), 8, 25-39.

Matsa, K.E. & Shearer, E. (2018, September 10th). News Use Across Social Media Platforms 2018. Washington DC: Pew Research Center. Retrieved from the Pew Research Center website on 28 August 2019: https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/

Mueller, J. E. (1985). *War, Presidents and Public Opinion.* Lanham, MD: University Press Of America.

Mueller, R.S. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election. Washington, DC: US Department of Justice. Retrieved from de US Department of Justice Website on 28 August 2019: https://www.justice.gov/storage/report.pdf

Newton, C. (2019, February 25th). The Trauma Floor, The Secret Lives of Facebook Moderators in America. *The Verge*. Retrieved from the Website of The Verge on 28 August 2019: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona?fbclid=IwAR0Lj37YakRW0r_mmRbp_hqLmKoM5p5nWRbZQPVAklvni7IwtzTMFog3P14

Oh, E. W. (2017, December 12). The Future of Fake News. *Edutopia*. Retrieved from the Edutopia organisation website on 28 August 2019: https://www.edutopia.org/article/future-fake-news

Pahlavi, P.C. (2007). The 33-Day War: An Example of Psychological Warfare in the Information Age. C*anadian Army Journal*, 10(2), 12-24.

Panarin, I. (2015). *Informatsionnaya voyna i kommunikatsii* [Information war and communications], Moscow: Goryachaya Liniya-Telekom.

Reid, C. (1987). Reflexive Control in Soviet Military Planning. In B. Dailey and P. Parker (Eds.), *Soviet Strategic Deception* (pp. 293–312). Stanford, CA: The Hoover Institution Press.

Robinson, M. (2018, March 8th). The Grim Conclusions of the Largest-Ever Study of Fake News. *The Atlantic*. Retrieved from the Atlantic Website on 28 August 2019: https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/

Sanger, D.E. (2018). *The Perfect Weapon, War, Sabotage and Fear in the Cyber Age.* London: Scribe Publications.

Schweitzer, Y. (2006). Hizbollah and the Morning After: Guerilla, Terror, and Psychological Warfare. The Institute for National Security Studies (INSS), University of Tel Aviv. Retrieved from the INSS website on 28 August 2019: https://www.inss.org.il/publication/hizbollah-and-the-morning-after-guerilla-terror-and-psychological-warfare/

Shavit, M. (2016). *Media Strategy and Military Operations in the 21st Century, Mediatizing the Israel Defence Forces*. London: Routledge.

Singer, P.W. & Brooking, E. (2017). *LikeWar, the Weaponization of Social Media*. Boston, MA: Eamon Dolan Returns to Houghton Mifflin Harcourt.

Smith, R. (2005). *The Utility of Force*. London: Allen Lane.

Snegovaya, M. (2015). Putin's Information Warfare in Ukraine, Soviet Origines of Russia's Hybrid War. Washington: Institute for the Study of War (ISW). Retrieved from the ISW website on 28 August 2019: http://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare

Szafranski, R. (1997 [1994]). Neocortical Warfare: The Acme of Skill? In J. Arquilla & D. Ronfeldt (Eds.). *Athena's Camp: Preparing for Conflict in the Information Age*. California: Rand Cooperation. Retrieved from the RAND Cooperation Website on 29 August 2019: https://www.rand.org/pubs/monograph_reports/MR880.html

The Economist. (2015, August 15th). The Propaganda War, The terrorists' vicious message is surprisingly hard to rebut. Retrieved from the Economist Website on 28 August 2019: https://www.economist.com/middle-east-and-africa/2015/08/15/the-propaganda-war

Thomas, T. L. (2004). Russia's Reflexive Control Theory and the Military. *Journal of Slavic Military Studies*, Vol. 17, 237-256.

von Clausewitz, C. (2007). *On War.* New York: Oxford University Press.

Vosoughi, S., Roy, D. & Aral, S. (2019, March 9th). The Spread of True and False News Online. *Science*, 359, 1146-1151. Retrieved from the Science Magazine Website on 28 August 2019: https://science.sciencemag.org/content/sci/359/6380/1146.full.pdf

ANALYSIS

Susceptibility awareness: domestic vectors for disrupting the kill chain of cyber-enabled influence operations

JAKOB BUND
RESEARCH ASSOCIATE, GLOBAL CYBER SECURITY CAPACITY CENTRE, UNIVERSITY OF OXFORD

Awareness Advantage: The Missing Piece

The impact of cyber-enabled influence operations has proven notoriously difficult to quantify. This challenge remains three years after the US Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) publicly called out the hack-and-leak operations targeting the Clinton presidential campaign and the campaign committees of the Democratic Party as intended to interfere with the 2016 US Presidential Elections and authorised at the senior-most level of the Russian government (US Department of Homeland Security, 2016). Former director of the CIA and NSA Michael Hayden (2018) has gone on record concluding that while these operations in 2016 affected the vote, "the effect itself is not just unknown but unknowable". Political communication scholar Kathleen Hall Jamieson (2018) in her account has been able to isolate concrete effects for select aspects of the interference efforts. Jamieson demonstrates the influence that leaks of the hacked material and its subsequent coverage by mainstream media exerted on the three televised Presidential Debates between the nominees of the Democratic and Republican Party, showing actual impact on the nature and framing of debate questions and on voter attitudes based on polling data that compares changes in candidate preferences.

From a policy perspective, public impact assessments might not even appear worth pursuing, to avoid giving credit and encouragement to outside manipulators. The priorities set in the approach that informed the joint statement by DHS and the ODNI are instructive in this regard. The statement focused on highlighting specific manipulation efforts and reinforced the severity of these actions by attributing them to a formidable foreign adversary operating with high-level authorisation.

Any impact of these influence attempts largely depended on their performance along three vectors, namely: (1) whether certain groups unwittingly became victims of manipulation because of predispositions that made them more likely to accept specific disinformation material as true or authentic; (2) whether certain actors

in deliberate opportunism spread the material despite knowledge of its illicit provenance and underlying manipulative intent; and lastly (3) whether certain actors inadvertently presented disinformation material in ways that dissociate it from the underlying influence operation (IO) so that it is more easily accepted by an audience that would not have trusted the original source but trusts the information vetting and publication decision of the intermediary outlet.

Issuing the joint statement before the elections testifies to the importance assigned to informing the US electorate of Russia's ambitions ahead of casting their votes in November 2016. Within the scope of the mandate of the participating agencies, these awareness efforts, however, were necessarily limited in breadth. Limitations specifically concerned the ability to raise awareness among domestic actors at risks of inadvertently enabling foreign influence operations and the endeavour to build broader public awareness about opportunistic domestic collaboration – the latter being a critical first step towards campaigning practices that would have candidates refrain from using illegally obtained or fabricated information on their opponents.

In the aftermath of the elections, the high-profile US response has concentrated on exerting costs on election interference attempts, mainly through sanctions and other legal action against Russian operatives at the Internet Research Agency (IRA) and the military intelligence service GRU. Still in 2016, the Obama administration announced it was sanctioning the GRU alongside the FSB, Russia's internal security service for attempts intended to undermine and interfere in US elections (White House, 2016).[1] The measures additionally designated four GRU officers and three companies for their role in carrying out and supporting these operations. Later indictments of IRA employees have focused on their role in producing and disseminating disinformation material intended to deceive and manipulate US voters in the run-up to the elections (US Department of Justice, 2018). Subsequent charges filed against GRU operatives have concerned the hack-and-leak operations that sought to undermine the National and Congressional Campaign Committees of the Democratic Party (DNC and DCCC) and the presidential campaign of Hillary Clinton (US Department of Justice, 2018a). During the 2018 US midterm elections, US Cyber Command for the first time deployed offensive measures to counter Russian interference attempts, temporarily disconnecting the IRA from the Internet, according to US officials (Nakashima, 2019). These responses all share an external bent focused on imposing consequences, which serves an important function in asserting the boundaries of acceptable behaviour (White House, 2016) but requires a balancing effort on the domestic side committed to enhancing societal resilience to shore up defences against influence operations.

Resulting from the Special Council Investigation into Russian interference in the 2016 US elections led by former FBI director Robert Mueller, both indictments and the investigation's final report itself (Mueller, 2019) document a detailed understanding of Russia's activities, tactics, techniques and procedures (TTPs). As additional indictments of former campaign officials and business associates of then-candidate Donald Trump make clear (Rodriguez & Jin, 2019), threat assessments cannot afford to neglect the role domestic collaborators play in enabling foreign influence operations. Touching on the nexus between foreign intelligence and homeland awareness, military strategist Sun Tzu cautioned that "[i]f you know neither the enemy nor yourself, you will succumb in every battle. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know the enemy and know yourself, you need not fear the result of a hundred battles".[2]

1 The Trump administration, after its first year in office, implemented additional rounds of sanctions, see: US Department of the Treasury. (2018, March 15), US Department of the Treasury. (2018, June 11), US Department of State. (2018, September 20), US Department of State. (2018, December 19).

2 Sun, T. The Art of War. As translated by Lionel Giles in 1910 and available at https://suntzusaid.com/book/3/18. Sentences of the cited passage are rendered in reverse order.

Sun Tzu's stratagem serves as a reminder that awareness efforts need to be holistic and cannot be confined to the threat alone. By the same token, domestic awareness efforts cannot be restricted to exposing criminal behaviour but rather unfold their potential if undertaken in advance as preventive measure and need to extend to the full spectrum of domestic collaboration.

Resulting from the Special Council Investigation into Russian interference in the 2016 US elections led by former FBI director Robert Mueller, both indictments and the investigation's final report itself document a detailed understanding of Russia's activities, tactics, techniques and procedures. As additional indictments of former campaign officials and business associates of then-candidate Donald Trump make clear, threat assessments cannot afford to neglect the role domestic collaborators play in enabling foreign influence operations.

Assessing the specific susceptibility of democratic societies to influence operations through the three vectors described above embeds analysis of interference efforts in a realistic dynamic environment. Dynamic analysis of this design can reinforce the comprehensive appraisal of how disinformation is introduced into the bloodstream of democracy as well as of which parts of the targeted body politic an influence operation seeks to incapacitate, and of how to responsibly regulate its messengers to effectively shield targeted receptors of disinformation.

Scrutiny of influence operations in this vein through the three enabling vectors of unconscious predispositions, opportunistic engagement, and inadvertent laundering of IO material raises challenges by itself. Turning the gaze inward to identify conditions and actors at home that wittingly or unwittingly support foreign-directed influence operations runs the risk of exacerbating the climate of polarisation and distrust on which many of these operations are feeding.

These risks associated with developing susceptibility awareness need to be assessed and managed but also have to be put into perspective. Influence operations retain a significant share of their leverage if defensive measures are narrowed to threat intelligence, counterintelligence, and disrupting the adversary's technical capabilities, which make the foreign actor the focus of analysis. Analysis of specific TTPs can make critical contributions if geared to inform awareness about enduring susceptibilities of open societies to influence operations. If tethered to the enabling domestic context, insights into TTPs help protect the openness and inclusiveness of democracies from exploitation through influence operations and strengthen public discourse in support of greater transparency and accountability.

Influence operations retain a significant share of their leverage if defensive measures are narrowed to threat intelligence, counterintelligence, and disrupting the adversary's technical capabilities, which make the foreign actor the focus of analysis.

On its own, TTP analysis not only remains ephemeral but also needs to consider the possibility that adversaries actively seek to trap defenders in a loop of analysing perpetually evolving TTPs, thereby obstructing the remediation of fundamental vulnerabilities and domestic susceptibility concerns, to ensure they remain available for continuous exploitation. Moreover, diverting resources and attention might actually be part of the adversary's win set and any meaningful interference in the elections themselves, if achieved, only a welcome byproduct. In this vein, enhanced susceptibility awareness brings focus to defence strategies that advance accountability and transparency in political campaigning and news reporting. Strengthening social trust and robust and respectful discourse by these means increases the resilience of open societies regarding influence operations. More importantly, the same measures are independent public goods and worthwhile investments in the core values of open societies, irrespective of any outside threats.

Deployed IO methods change depending on their cost-effectiveness and their ability to circumvent countermeasures intended to protect enduring susceptibilities that remain the ultimate and continuous target. This continuity in susceptibility puts technical solutions aimed at any specific method at a disadvantage, as they tend to address those manipulation efforts that have been registered in previous instances but are less well positioned to pre-empt or counter campaigns that have undergone tactical evolution or whose methods have avoided detection.

Susceptibility awareness in this sense offers a pathway to mitigate the priming of democratic openness and inclusiveness as vulnerabilities. In the assessment of the former CIA station chief in Moscow, John Sipher (2019), "what made this [interference in the 2016 US elections] most successful for the Russians is we [the US political landscape] were dry tinder – in the sense that our political dysfunction, our tribalism, and [US] hyper-partisanship was something that was really easy for them to stoke. So Russian active measures, they don't create these problems, they don't create these frictions. They exploit them and they amplify them."

This realisation offers comfort that the characteristics influence operations threaten to weaponise against open societies are also under the primary control of open societies. Estimates that the "translator project" alone – the IRA's efforts targeting the US population – was operating on a budget of USD 1.25 million per month by September 2016 (United States District Court for the District of Columbia, 2018, p 7), however, demonstrates the need for open societies to reassert control and understand how to marshal attention and resources to their greatest effect in self-aware defence. Exploring susceptibility awareness as a means to disrupt influence operations, this paper seeks to inform democracies in denying outside threat actors' attempts to commandeer the inherent strengths of open societies against them.

Sequencing the Kill Chain of Influence Operations

Originally a military concept, kill chain models are used to sequence the steps an attacker has to work through to achieve their objective. The structured understanding of these attack phases, facilitated by the kill chain approach, seeks to enable defenders to locate interception points for impactful disruption to frustrate an adversary's attack efforts. By the same token, kill chain analysis offers insights into dedicated susceptibilities that adversaries aim to leverage and that defenders can address to thwart the attack attempt. A 2011 Lockheed Martin white paper applied the concept to computer network defence. Building on this adaptation, Bruce Schneier (2019) has proposed a framework specific to the kill chain of cyber-enabled influence operations.

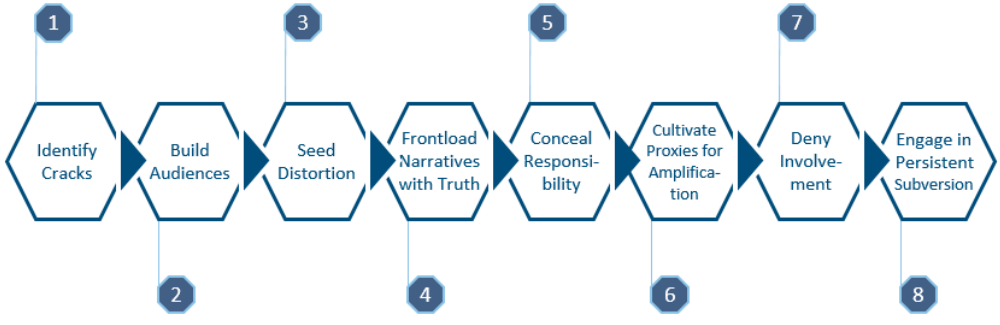


Fig. 1. Framework for an influence operation kill chain. Source: own chart based on Bruce Schneier, "8 ways to stay ahead of influence operations," 2019.

The following overview of a possible influence operation kill chain draws on the particular steps identified in Schneier's framework.

In step 1, adversaries seek to identify existing cracks in the social structure and public discourse that offer opportunities to gain a foothold in the targeted deliberation and decision-making processes. Political, social, demographic, economic, and ethnic divisions serve as instrumental entry points.

Step 2 sees attackers expand this beachhead by building audiences for the influence narratives that are to follow. Schneier specifically identifies bot networks on social media and fabricated online personas as well as less easily detectable measures such as microtargeting through individualised ads and the cooptation of influencers as outreach mechanisms. Sufficiently equipped threat actors might create their own platforms for engagement and distribution, fronting as media outlets.

Step 3 focuses on seeding distortion, the introduction of polarising narratives espousing "alternative truths" into political discussions that are intended to stoke a climate of doubt and suspicion and stifle compromise and dialogue. These "alternative truths" are purposefully crafted to exacerbate and exploit divisions within society, unaddressed social grievances, and perceived or actual disenfranchisement.

Step 4 concerns front-loading influence narratives with truth, providing them with a believable, verifiable core that connects to ongoing political debates to overcome initial scepticism of influence targets and complicate debunking efforts. These shell narratives can be charged with a variable payload of falsehoods and fabrications.

As part of step 5, threat actors conceal their responsibility for the activity conducted in the preceding steps, in particular fostering appearances that the inserted influence narratives emerged organically. In practice, this step would need to be taken in parallel with the specific measure that it seeks to cover up.

Step 6 addresses the development of a network of proxies for amplification. Acting of their own accord, proxies spread content in support of the influence operation's aims, without receiving any explicit direction from the actor orchestrating the operation (Helmus et al., 2018).

Step 7 consists in denying any involvement in the influence efforts; if needed, even in light of obvious facts to the contrary. Dissociation of this kind, even where implausible, serves the purpose of cultivating an atmosphere in which everything can be called into question and furthers "alternative truths" that undermine any common basis for discussion.

The kill chain leads up to step 8: play the long game. Lasting impact trumps short-term gains. Operations build up momentum through their cumulative effect. The next section explores success conditions for this phase under the title of persistent subversion.

The general cybersecurity kill chain and the influence operation kill chain are distinguished by one additional characteristic. In principle, the steps of the cybersecurity kill chain can be accomplished by attackers on their own. Depending on the target, an outside adversary might rely on unwitting assistance from an insider in a preparatory spear phishing attack to gain access to a particular network or system. Influence operations, by contrast, require advertent or inadvertent collaboration throughout most of their stages. This characteristic assigns critical importance to raising awareness for different actors about how influence operations may take advantage of them, about the actions of those collaborating wittingly, and – correspondingly – about mechanisms to hold the latter accountable. Securing collaboration at any of these steps already delivers first influence effects, signalling support at least among a subset of the target group. In this understanding, influence operations need not complete the entirety of eight steps to show adverse impact. Especially steps two to six exhibit this gateway character that offers an outside attacker increasing strategic leverage over select parts of public discourse. Decisions about at which stage of the kill chain an influence operation is to be disrupted need to consider the consequences of not intercepting manipulation efforts earlier, especially in light of cumulative effects (such as the build-up of proxy networks) that easily transfer between operations.

Depending on the target, an outside adversary might rely on unwitting assistance from an insider in a preparatory spear phishing attack to gain access to a particular network or system. Influence operations, by contrast, require advertent or inadvertent collaboration throughout most of their stages. This characteristic assigns critical importance to raising awareness for different actors about how influence operations may take advantage of them, about the actions of those collaborating wittingly, and – correspondingly – about mechanisms to hold the latter accountable.

Breaking down influence operations objectives and linking them to election calendars can shed light on which kill chain segments presently are a priority concern from the adversary's perspective. Kill chain focal points thus differ based on whether operations intend to (1) sway voters' minds ahead of elections or suppress turnout of specific groups, (2) assail the legitimacy of election outcomes, undermine support for the newly elected leader or specific policy projects, or (3) create an influence-operations enabling climate by sowing discord and confusion and corroding the integrity and inclusiveness of public discourse generally.

As step 8 indicates, influence operations derive their lasting and more pervasive effects not from the one-off completion of the kill chain but from working through the kill chain persistently to erode societal trust or take advantage of pre-primed issues that on select topics already provide the polarisation and disenfranchisement, perceived or real, for IO narratives to take hold.

Persistent Subversion

Exploiting Existing Weak Points: Primed Discourses and Tipping Points

Particular issues on which political debate is already polarised can serve as fertile ground for outside threat actors to seed disinformation or selectively plant authentic information to reinforce divisions. Influence operations take advantage of the fact that preceding media coverage and statements of officials or candidates have tied key words in these debates to clearly demarcated positions. In cognitive psychology, this process is referred to as priming. If influence narratives relate to primed content, priming can shape public interpretation of the material along the established fault lines, reducing the need for direction by outside manipulators. Less command and control lowers the profile of outside threat actors, making their efforts harder to detect.

Influence operations take advantage of the fact that preceding media coverage and statements of officials or candidates have tied key words in these debates to clearly demarcated positions.

Kathleen Hall Jamieson (2018, p. 40) describes priming as the process by which "exposure to a stimulus produces an effect on memory and hence on subsequent responses. By making them more cognitively accessible, priming is able to make some issues, candidate characteristics, or concepts more salient or focal than others in decision making".

One such case Jamieson identifies for the 2016 US presidential elections campaign where priming in connection with a Russian-led influence operation had a particularly notable impact concerned candidates' position regarding financial market regulation, which featured as a contentious issue during debates between Hillary Clinton and Bernie Sanders in Democratic Party primaries. Sanders on various occasions asked that Clinton release texts of speeches she had given to financial firms at Wall Street to prove that she was not advocating one position in public and making contradicting commitments in private. During the general election campaign, after Clinton had secured the Democratic nomination and was running against Republican nominee Donald Trump, WikiLeaks released excerpts from some of these speeches just ahead of the second presidential debate. Manuscripts of the speeches had been passed on to WikiLeaks as part of a larger trove of documents that GRU operatives had illegally obtained by hacking into the email accounts of Clinton campaign staffers. The published excerpts appear specifically chosen to reignite the issue of duplicity for Clinton that had been primed during the primaries and to create the impression that the Clinton campaign had kept these speeches deliberately secret because they showed Clinton recognising the need for "both a public and a private position," (Chozick, Confessore & Barbaro, 2018) albeit in a context unrelated to financial regulation.

This incident demonstrates the power of influence narratives that are carefully inserted into the framing of campaign issues. Studying existing priming allows influence operations to plant snippets of real or outright fabricated documents that on their own would garner little attention safe for the meaning they have attained in the campaign. The Clinton case shows the extent to which hijacked priming can facilitate distortion, as published speech excerpts were taken out of their original context and instead transplanted to the already polarised, yet unconnected, debate on financial regulation that had been primed earlier the campaign (Gardner, 2016). As Jamieson notes, these tactics become all the more effective if the suspected provenance of internal campaign documents from a foreign intelligence agency that would raise suspicions about the disclosure's ulterior motives is truncated in media reports to their publication by a self-styled whistle-blower clearinghouse, without acknowledgment of the illegal activity that led to their discovery.

Looking for leverage effects similar to the ones Russian-orchestrated hack-and-leak operations sought to take advantage of in focusing on priming to exploit existing divisions to drive a deeper wedge between Clinton supporters and wider potential Democratic voters, the IRA explored tipping point communities whose votes, if swayed, could have an outsized effect on election results. According to the February 2018 indictment of IRA employees, the agency in 2014 sent two researchers on a three-week-long discovery mission through nine US states to identify and better understand divisive issues (United States District Court for the District of Columbia, 2018, p 13). Members of the IRA also posed as Americans online to make contact with US political and social activists and "learned from the real US person that they should focus their activities on 'purple states like Colorado, Virginia & Florida.'" (United States District Court for the District of Columbia, 2018, p 13) The indictment notes that IRA members, following this exchange, made frequent references to "purple states" as they discussed priority targets for their operations (United States District Court for the District of Columbia, 2018, p 13), demonstrating interest in tailoring their efforts to tip the scales. Critically, the indictment concludes that the contacted Americans remained unwitting about communicating with Russian agents (United States District Court for the District of Columbia, 2018, p 4).

These findings of the indictment emphasise the role of susceptibility awareness as first line of defence and foundation for building resilience in open societies with respect to foreign influence attempts. Two contrasting accounts about GRU attempts to solicit US journalists' collaboration in the distribution of hacked material demonstrate that awareness about possible inadvertent complicity in the kill chain of such operations can make a tangible difference. Both cases concern the Guccifer 2.0 online persona – the July 2018 GRU indictment links them to the GRU – who offered journalists access to password-restricted

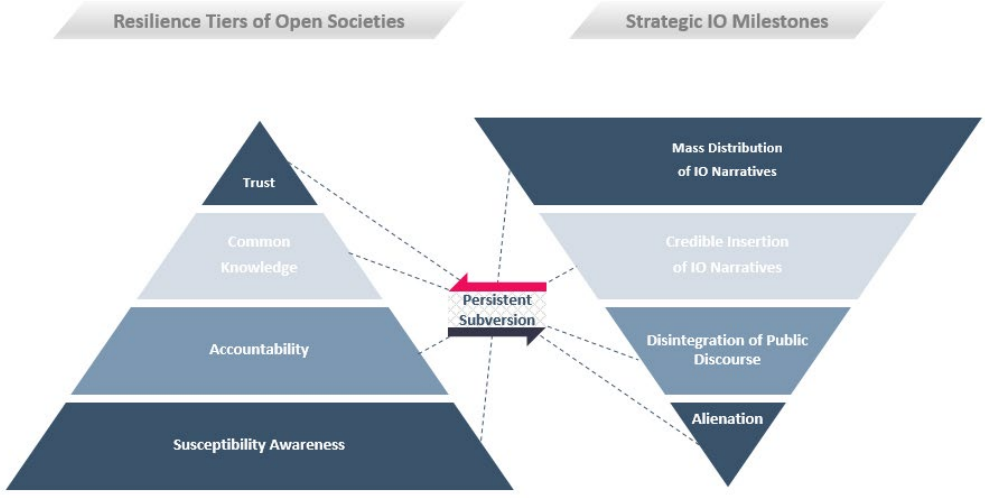


Figure 2. Persistent subversion. Source: own chart, 2019.

portions of DCLeaks – a website serving as repository for hacked campaign-related documents – with the objective to generate media coverage based on exclusive access. In the first instance, Guccifer 2.0 contacted the media organisation The Smoking Gun, which decided to accept the offer (United States District Court for the District of Columbia, 2018a, p 17, 45b; tsgnews, 2018) and in its coverage of the closed-off sections omitted any mention of DCLeaks or the privileged access that Guccifer 2.0 had facilitated (The Smoking Gun, 2016). Only in later reporting on its interactions with Guccifer 2.0 does the outlet openly address these shortcomings of the earlier article and highlight links between Guccifer 2.0, DCLeaks, and Russian intelligence services (The Smoking Gun, 2016a). The second case involved Mikael Thalen, at the time writing for InfoWars. When contacted by Guccifer 2.0, Thalen reportedly turned down leaked documents offered by Guccifer 2.0 over suspicions that they reached out to the person they thought "would best carry the story the way they wanted" (Fisher, 2017). Despite deviating initial approaches, both cases show that susceptibility awareness can be reconciled with a variety of editorial decisions and should not by default result in refraining from reporting altogether where risk of contributing to an influence operation is identified.

Creating New Weak Points: Subverting Common Knowledge

Through persistent execution of the kill chain, influence operations threaten to cause lasting damage to the institutions and fundamental beliefs of the targeted society, the protective fabric that holds society together and lets it embrace diversity. These institutional resilience mechanisms that in democracies preserve public confidence in the fairness of elections and general acceptance of their outcomes are crucial aspects of the common knowledge stock

of open societies (Farrell & Schneier, 2018, p 8). Common knowledge also encompasses the shared understanding of the forces shaping political processes, i.e. of who the "political actors are, what their interests are, and where they clash" (Farrell & Schneier, 2018, p 9). Through their persistent attempts at subversion, sustained influence operations cloud collective perspectives on who these actors are or should be, their interests, and how these relate to each other. Sustained influence operations repeatedly pressure targeted candidates and politicians to position and explain themselves. These continuous accountability challenges alone, even if readily dismissed as baseless and reported as such in the media, can cultivate perceptions that all is questionable and threaten to dissolve the basic consensus. A Pew Research Center survey of July 2019 (Rainie et al., 2019) found that already almost two-thirds of Americans find it hard to tell what is true when listening to elected officials. In the view of survey respondents, politicians are seen as the social group that creates most of made-up news and information, even outranking foreign actors (Stocking, 2019).

In washing out common knowledge, influence operations not only permeate higher resilience tiers. Inasmuch as the disintegration of common knowledge gives rise to voter resignation, it also reduces pressure for politicians to participate and explore voluntary accountability mechanisms, which might be seen as giving up a competitive edge in the absence of voter demands to make them general best practice. One such initiative, the Election Pledge of the Transatlantic Commission on Election Integrity asks candidates to commit, among others, to refrain from fabricating, using, or spreading material that was falsified, fabricated, doxed, or stolen for purposes of disinformation. The Election Pledge combines this commitment with measures to maintain an appropriate level of cybersecurity for their campaign resources and staff, including risk awareness to facilitate the detection and prevention of attacks (Alliance for Democracies, 2019). For the 2019 European Parliament elections, 179 candidates had signed on to the pledge by election night. This compares to 751 members of parliament, a figure that is yet significantly lower than the overall number of candidates participating in the election.

In washing out common knowledge, influence operations not only permeate higher resilience tiers. In as much as the disintegration of common knowledge gives rise to voter resignation, it also reduces pressure for politicians to participate and explore voluntary accountability mechanisms, which might be seen as giving up a competitive edge in the absence of voter demands to make them general best practice.

For reasons of cost-effectiveness, influence operations are more likely to take advantage of primed issues and tipping point communities, to exploit their resources to maximum effect. On the upside, this might reduce the likelihood that common knowledge is explicitly targeted for as long as these other openings remain.

Conclusion

A growing body of evidence suggests that debunking misinformation remains a lasting challenge (Ecker et al., 2014; Swire, 2017; Quattrociocchi, Scala & Sunstein, 2016; Chan et al., 2017). Preventing rather than countering influence operations is key. Yet, strategic thinking on what prevention looks like in the context of cyber-enabled IO needs to continue to adapt. It is not the operation as such that requires prevention but the influence that an operation seeks to exert. Focusing prevention on individual operations is not cost-effective. Technical solutions that raise the cost of maintaining influence networks notwithstanding, manipulation efforts remain comparatively easy to mount, perhaps even to detect, but still harder to dismantle.

With respect to harnessing awareness to move from the mere detection to the effective disruption of IOs, Ellen Weintraub (2019), Chair of the US Federal Election Commission, offers a healthy

baseline assumption: "When foreign governments seek to influence American politics, it is always to advance their own interests, not America's". Any opportunistic gains for domestic collaborators for their support of foreign influence operations are bound to remain inherently fleeting. The kill chain framework offers insights into how to conceptualise the different steps of influence operations. However, depending on the adversary's objective, influence operations can inflict harm even before the full kill chain is executed. Thus, not all interventions along all the steps are equal in their ability to deny influence operations in their effect. As with many other cyber-enabled security challenges, the human factor is at the core of influence operations. And as the kill chain concept illustrates, influence operations reverberate in the proxy network foreign actors establish on the ground in targeted societies. These proxies, wittingly or unwittingly, keep influence narratives alive even after foreign elements of the threat have been defused. These dynamics underscore the need to expand the set of available countermeasures to include protections that operate independently of outside threat actors. Awareness efforts along the three vectors for susceptibility – unconscious predispositions, opportunistic engagement, and inadvertent laundering of IO material – and related accountability improvements offer benefits in their own right and promise to raise the resilience of democratic processes independent of any interference efforts. ■

About the author:

Jakob Bund is a Research Associate at the University of Oxford's Global Cyber Security Capacity Centre (GCSCC), focused on the analysis of national cybersecurity postures. In this capacity, he is working closely with governments and representatives of civil society and the private sector to support the inclusive development of national cybersecurity strategies. At the GCSCC, he is also leading the development of a Cyber Harm Framework, funded by the British Foreign Office, to support nations in assessing the impact of cyber incidents in an all-of-society approach. Previously, Jakob worked as Associate Analyst at the EU Institute for Security Studies (EUISS), where he co-coordinated the Chinese Future Task Force that assessed international implications of China's military modernization industrial policies.

References

Alliance for Democracies. (2019). The Pledge for Election Integrity. Retrieved from https://electionpledge.org/

Chan, M. S. et al. (2017). Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation. *Psychological Science*, 28(11), pp. 1531-1546.

Chozick, A., Confessore, N., & Barbaro, M. (2016). Leaked Speech Excerpts Show a Hillary Clinton at Ease With Wall Street. *New York Times*. Retrieved from https://www.nytimes.com/2016/10/08/us/politics/hillary-clinton-speeches-wikileaks.html

Ecker, U. et al. (2014). Do People Keep Believing because They Want To? Preexisting Attitudes and the Continued Influence of Misinformation. *Memory & Cognition*, 42(2), pp. 292-304.

Farrell, H., & Schneier, B. (2018). Common-Knowledge Attacks on Democracy. *Berkman Klein Center for Internet & Society*, Harvard University. p. 8. Retrieved from https://cyber.harvard.edu/story/2018-10/common-knowledge-attacks-democracy

Fisher, M. (2017). Russian Hackers Find Ready Bullhorns in the Media. *New York Times*. Retrieved from https://www.nytimes.com/2017/01/08/world/europe/russian-hackers-find-ready-bullhorns-in-the-media.html

Gardner, L. (2016). Clinton: "Public and a private" position comment based on Lincoln biopic. *Politico*. Retrieved from https://www.politico.com/story/2016/10/2016-presidential-debate-hillary-clinton-abraham-lincoln-229474

Hayden, M. (2018). Remarks at StratCom 2018. *Atlantic Council*. Retrieved from https://www.atlanticcouncil.org/news/transcripts/former-cia-director-michael-v-hayden-s-remarks-at-stratcom-2018

Helmus, T. et al. (2018). Russian Social Media Influence Understanding Russian Propaganda in Eastern Europe. *Rand Corporation*. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf

Hutchins, E. et al. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Lockheed Martin Corporation*. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Jamieson, K. H. (2018). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President – What We Don't, Can't, and Do Know*. Oxford: Oxford University Press.

Mueller, R. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. *US Department of Justice*. Retrieved from https://www.justice.gov/storage/report.pdf

Nakashima, E. (2019). US Cyber Command Operation Disrupted Internet Access for Russian Troll Factory on Day of 2018 Midterms. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

Quattrociocchi, W., A. Scala, & C. R. Sunstein. (2016). Echo Chambers on Facebook. Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2795110

Rainie, L. et al. (2019). Trust and Distrust in America. *Pew Research Center*. Retrieved from https://www.people-press.org/2019/07/22/trust-and-distrust-in-america/

Rodriguez, J. and Jin, B. (2019). The Mueller indictments so far: Lies, trolls and hacks. *Politico*. Retrieved from https://www.politico.com/interactives/2018/interactive_mueller-indictments-russia-cohen-manafort/

Schneier, B. (2019). Toward an Information Operations Kill Chain. *Lawfare*. Retrieved from https://www.lawfareblog.com/toward-information-operations-kill-chain; Schneier, B. (2019). 8 Ways to Stay Ahead of Influence Operations. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/

Sipher J. in Hennessey, S., & Wittes, B. (2019). The Report – Part I: Active Measures [Podcast]. 22:20 minute mark. *Lawfare*. Retrieved from https://www.lawfareblog.com/introducing-report-podcast-series-lawfare

Stocking, G. (2019). Many Americans Say Made-Up News Is a Critical Problem That Needs To Be Fixed. *Pew Research Center*. Retrieved from https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/

Sun, T. *The Art of War*. As translated by Lionel Giles in 1910 and available at https://suntzusaid.com/book/3/18

Swire, B. et al. (2017). The Role of Familiarity in Correcting Inaccurate Information. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 43(12), pp. 1948-1961.

tsgnews [The Smoking Gun]. (2018, July 13). "We're the 'U.S. reporter' referenced in para 45b of new Russian hacking indictment. 'Victim 1' is former Clinton campaign worker Sarah Hamilton. We first exposed the Guccifer 2.0/DC Leaks connection on 8/12/16: http://goo.gl/AZ6AVY" [Twitter Post]. Retrieved from https://twitter.com/tsgnews/status/1017838697268563968

The Smoking Gun. (2016). Hack Yields Clinton Campaign E-Mail, Records. Retrieved from https://thesmokinggun.com/documents/crime/hfa-gmail-attack-723571

The Smoking Gun. (2016a). Tracking The Hackers Who Hit DNC, Clinton. Retrieved from https://thesmokinggun.com/documents/investigation/tracking-russian-hackers-638295

US Department of Homeland Security. (2016). Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security. Retrieved from https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

US Department of Justice. (2018). Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System. Retrieved from https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere

US Department of Justice. (2018a). Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election. Retrieved from https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

US Department of State. (2018, September 20). Sanctions Under Section 231 of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA). Retrieved from https://www.state.gov/sanctions-under-section-231-of-the-countering-americas-adversaries-through-sanctions-act-of-2017-caatsa

US Department of State. (2018, December 19). Sanctions Announcement on Russia. Retrieved from https://www.state.gov/sanctions-announcement-on-russia/

US Department of the Treasury. (2018, March 15). Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks. Retrieved from https://home.treasury.gov/news/press-releases/sm0312

US Department of the Treasury. (2018, June 11). Treasury Sanctions Russian Federal Security Service Enablers. Retrieved from https://home.treasury.gov/news/press-releases/sm0410

United States District Court for the District of Columbia. (2018). United States of America v. Internet Research Agency LLC, et al. *US Department of Justice*. Retrieved from https://www.justice.gov/opa/press-release/file/1035562/download

United States District Court for the District of Columbia. (2018a). United States of America v. Borisovich Netyksho, et al. US Department of Justice. Retrieved from https://www.justice.gov/file/1080281/download

Weintraub, E. (2019). Statement Regarding Illegal Contributions from Foreign Governments. US Federal Election Commission. Retrieved from https://www.fec.gov/resources/cms-content/documents/Chair_Weintraub_on_Illegal_Foreign_Contributions.pdf

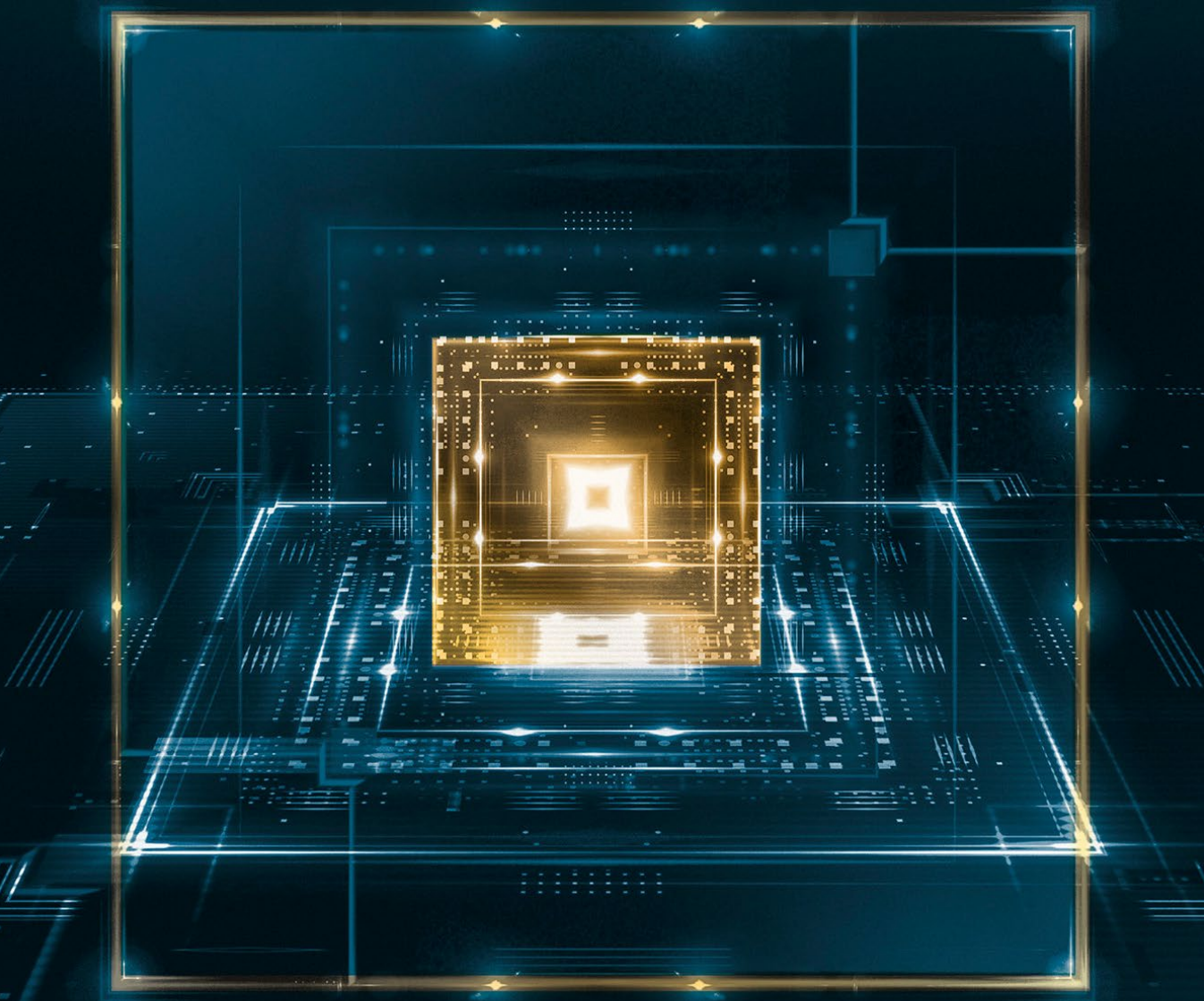
White House, Office of the Press Secretary. (2016, December 29). Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

ANALYSIS

Two reasons not to miss the quantum race

ANDREA G. RODRÍGUEZ

INTL. MASTER'S IN SECURITY, INTELLIGENCE AND STRATEGIC STUDIES PROGRAMME, UNIVERSITY OF GLASGOW, DUBLIN CITY UNIVERSITY AND CHARLES UNIVERSITY IN PRAGUE



CYBERSEC

YOUNG LEADERS

Different national cybersecurity strategies warn about the emergence of hybrid cyberthreats that pose a danger to our digital infrastructure. Among them is the use of infested vectors upgraded with artificial intelligence (AI), but also the development of quantum computation, that equips honest parties and adversaries with asymmetric capabilities.

Cybersecurity aims to protect hardware, software and information (Wallden & Kashefi, 2019) to prevent unauthorised parties having access to systems and conducting exercises of espionage, sabotage, subversion, or disruption. The applications of quantum mechanics in simulation and computation create new risk scenarios in the field of national security as well as opportunities for the national economy. The increased computation power stems from the properties of quantum bits or *qubits*. While classic computation systems store information in bits that have either a 0 or 1 value, qubits *are* both 0 and 1 in what is called the superposition principle. Both 0 and 1 happen at the *same* time and the state of the qubit can only be known once it is *read*. This specific nature of quantum bits allows for faster data processing, factorisation and problem solving.

The applications of quantum mechanics in simulation and computation create new risk scenarios in the field of national security as well as opportunities for the national economy.

Although the state of the matter is still in its infancy, advances in the field suggest that a quantum future is nearer than expected, where the *expected* was the unlikelihood for it to happen. Quantum computers are set to cohabitate with classic computation systems in about two decades due to the complexity and expensive environment qubits need to work; a temperature close to 0°K (-273°C), for instance.

Historical experience with classical computers provides enough examples to conclude that the possibility of everyone having access to a quantum computer must be considered (O'Regan, 2016). Hence, it is arguable that the quantum future can be divided into three phases: an initial phase during which quantum technologies will be monopolised by high-tech companies collaborating with governments that mostly fund and benefit from quantum projects, and a final phase in which quantum computation systems will be available to everyone. It is in the middle phase – during which the state of the matter is advancing but quantum technologies are only in few hands – when friction occurs, and security is compromised. The lack of international standards and legislation makes this mid-phase anarchic and chaotic.

The following analysis aims to give an overview of the matter by highlighting the main risks of quantum computing for national security as well as the opportunities for states that decide to invest in quantum technologies. It concludes that advances in the field are sufficient to declare that the creation of a universal quantum computer is possible. Universal quantum computers will be capable of inducing irreparable damage in cryptosystems, but the fact that the advent of Q-Day[1] is imminent, does not exempt the present from risks. A comprehensive quantum strategy must be bi-fold. On the one hand, following the cyber resilience cycle, it must prepare for the threat, protect the information that could be targeted, detect advances in the industry, and respond by acquiring the necessary capabilities to be able to repair the damage. On the other hand, it needs to innovate, be present in the industry to ensure its interests are not compromised and that it can comfortably lead and benefit from the quantum leap.

Advances in the field are sufficient to declare that the creation of a universal quantum computer is possible.

Protection of national security

The protection of national security has a physical and a nonmaterial form. Roughly speaking, the physical dimension involves the protection

1 According to the Hudson Institute Q-Day is "the day that a universal quantum computer will be able to hack into asymmetric encryption" (Herman, Friedson, 2018).

of critical national infrastructure, whereas the nonmaterial aspect includes the protection of securitised incorporeal assets such as the protection of values (Baldwin, 1997). Whereas the debate on the consideration of data as critical infrastructure is open and ongoing (Chapman, 2018), digitalisation puts the creation of data, transfer of data, and the use of data in the centre of a highly digitalised present and future.

National security concerns stem from the ability of universal quantum computers, that is, machines able to run "almost any type of algorithm and discover patterns in data that existing digital computers, including the fastest supercomputers cannot" (Herman & Friedson, 2018, p. 8), to break codes and breach into systems. The magnitude of the consequences can be as large as an integral blackout: paralysation, crippled and disabled fundamental systems, and even seemingly apocalyptical scenarios involving nuclear facilities, etc. The stealing of secrets is one of the biggest threats, which makes quantum a worry for the intelligence community.

While the first generation of universal quantum computers will need a thousand qubits or more to work effectively (Herman & Friedson, 2018), the most advanced quantum processor developed to date is Google's 72-quibit Bristlecone (Google AI, 2018) which amplifies computation power but does not assume big national security concerns.

The protection of national security has a physical and a nonmaterial form. (...) The physical dimension involves the protection of critical national infrastructure, whereas the nonmaterial aspect includes the protection of securitised incorporeal assets such as the protection of values.

In most cases, information is encrypted to ensure confidentiality, integrity and the authenticity of the message. As it happened during World War II with Alan Turing's "Bombe" used to decrypt Nazi messages encoded by the Enigma machine, the ability to read other's messages and to compile information is key for a nation's intelligence. Asymmetric, often called "public-key" and symmetric cryptosystems protect the message, so only the intended partner can read it. They do so *via* algorithms that encode and decode the information. Quantum algorithms, specifically Shor and Grover algorithms, are capable of breaking most asymmetric and symmetric cryptosystems (Bernstein & Lange, 2017). It will take 4,000 entangled qubits to break RSA and 2,500 qubits to do so with ECC, very popular and widespread algorithms (Herman & Friedson, 2018). With a looming future that puts communication in danger, governments are investing heavily in developing quantum-resistant algorithms, in which has been called post-quantum cryptography, core to post-quantum cybersecurity. The efforts of the US National Institute of Standards and Technology (NIST) in the development of quantum-safe algorithms, post-quantum cryptography and new programming languages are remarkable.

Quantum-enhanced technologies disrupt the intelligence cycle as it lessens the limitation of the focus – everyone can become a target, augments the possibilities of collection – most information is accessible, and, improves the processing and analysis of that information thanks to upgrading capacities simulation and pattern-finding of quantum computers. It has to be noticed that albeit Q-Day has not arrived yet, quantum is already disturbing the intelligence cycle as, since the creation of a universal quantum computer is only a matter of time, it is accelerating the download of encrypted data packages in what has been called the "download now, decrypt later" fashion, once the technology is available. The upgrade of current cryptography to flexible cryptography – albeit costly in time – should be considered (Mosca, 2016) to transition to post-quantum cryptography once available and avoid the disclosure of information, secrets and sensitive data as well.

Governments with access to post-quantum cryptography will be able to secure their communications while those without it will be subject to cyberattacks that are both hard to repel and destructive. The United States, China, Japan, Canada, the European Union and the United Kingdom are the ones investing the most into this

field, anticipating the upcoming friction between the holders and non-holders of advantageous quantum technologies.

Governments with access to post-quantum cryptography will be able to secure their communications while those without it will be subject to cyberattacks that are both hard to repel and destructive.

Economic growth

Development, international prestige, influence and power have traditionally walked hand-in-hand with access to technology. In the following decade, the market value of quantum technologies will multiply by ten, according to the IDA report (2017). Although technical limitations make the contribution of quantum to the national economy small at the moment, the possibilities in the fields of simulation, computing, communications, metrology and sensing have made governments notice the leap and promote investment.

Advanced quantum technology developers hold the opportunity to shape the future market and establish protocols and standards that new developers will need to follow, resulting in benefits worth millions of US dollars and competitive advantage. The influence over the market will not only have multiplier effects in the profits to come, as the industry gains prestige and space in the market and the demand of quantum products generate the need to satisfy new necessities and increase the offer, but it is also an opportunity for the job market to welcome new skilled and unskilled workers.

Moreover, global value chains (GVCs) are also affected by technological development. Some parts of the production chain, such as manufacturing, are relocated to developing countries. Whereas the risks that GVCs pose to them have largely been discussed (Wallerstein, 2004; Korn, 2008), it is arguable that manufacturing leads to industrialization (Rodrik, 2018), thus increasing the national GDP and, ideally, the purchasing power of the population who, also, become consumers of that technology. Nevertheless, knowledge rarely accompanies the invention. Macbooks are desirable objects whose components are manufactured in tens of countries, but the laptop is designed and assembled in California, which increases the price. There is another way to see it: the innovation required to produce a Macbook never leaves California.

The influence over the market will not only have multiplier effects in the profits to come, as the industry gains prestige and space in the market and the demand of quantum products generate the need to satisfy new necessities and increase the offer, but it is also an opportunity for the job market to welcome new skilled and unskilled workers.

Besides the opportunity to lead the market, to influence GVCs and to create new jobs, quantum technologies facilitate the growth of the existent tech-industry. In the fields of sensing and metrology, the application of quantum physics improves synchronization thanks to the entanglement principle, which can be relevant to financial markets or even for managing airport traffic (Ilo-Okeke, Tessler, Dowling, & Byrnes, 2018). Also, the increased computation power thanks to the application of the principles of quantum mechanics is a genuine push for the AI industry. Quantum superposition, one of the most important quantum mechanics principles explained above, allows for simultaneous simulation, advanced machine learning and deep learning processes. A quantum leap in the AI industry promises bigger breakthroughs in a shorter period of time than what classical instruments would need to achieve the same results.

Conclusion

The lack of international legislation on quantum technologies generate the basis for anarchic competition, also fuelled by the premise of enhancing simulation, metrology, computation, sensing and communication; the latter is essential for the functioning of the economy, defence

and national infrastructure. Anarchy, along with the uncertainty raised by the unpredictability of Q-Day and who will develop that, have created a sense of a race to dominate and lead this technological leap.

Although in actor terms, the initial and mid-phase of the full-quantum computer deployment are going to be centred in states and high-tech companies, the acquisition of this technology by not-state actors is a matter of time. However, this fact alone will not change the nature of the threat spectrum and is not going to reduce it.

The biggest threat to national security involving quantum computers is the dismantling of the current cryptosystems that encode and protect information. Being aware of this issue, the development of quantum technologies is accelerating the download of packages of encrypted data, unreadable at the moment, but decodable once a universal quantum computer is fully developed. Everything involving data and information must be adaptable to the quantum future, but this adaptation must start soon to diminish the consequences of the damage, such as the implementation of quantum-safe solutions or flexible cryptography (Mosca, 2016 & 2018). It also involves a mid-term adaptation of the intelligence cycle, when adversaries are equipped with some quantum instruments but do not have a universal quantum computer, and a long-term adaptation for a full quantum deployment.

A comprehensive quantum strategy must be bi-fold. On the one hand, following the cyber resilience cycle, it must *prepare* for the threat, *protect* the information that could be targeted, *detect* advances in the industry, and *respond* by acquiring the necessary capabilities to be able to *repair* the damage. On the other hand, it needs to innovate, be present in the industry to ensure its interests are not compromised and that it can comfortably lead and benefit from the quantum leap.

Although in actor terms, the initial and mid-phase of the full-quantum computer deployment are going to be centred in states and high-tech companies, the acquisition of this technology by not-state actors is a matter of time. However, this fact alone will not change the nature of the threat spectrum and is not going to reduce it.

In sum, preparations for the worst-case scenario as well as improved cooperation and communication with relevant quantum actors are vital to decrease the uncertainty and stop the myths surrounding quantum technologies. Although the initial phase and mid-term timeframes are dominated by state actors and companies, they both act as defenders and offenders. The cyber resilience cycle gives us an idea of where to start to secure our networks and our digital infrastructure. One thing is clear: besides the protection of national security and the economic benefits, there are many other reasons to embrace the upcoming quantum future. ■

About the author:

Andrea G. Rodríguez is a Spanish technology enthusiast. She publishes in different Spanish media and think tanks as well appears in radio and TV programs both in Europe and Latin America analysing the security implications of the rise of new technologies and geopolitical events in Far East Asia. Andrea holds a B.A. in International Relations from the Complutense University of Madrid with a dissertation on cross-strait relations which she finished during her stay at the National Taiwan University. She is currently finishing an International M.A. in Security, Intelligence and Strategic Studies in the universities of Glasgow, Dublin City University and Charles University in Prague.

References

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies, 23*, 5-26.

Bernstein, D. J., & Lange, T. (2017, Septiembre 14). Post-quantum cryptography. *Nature, 549*, 188-194.

Chapman, E. (2018, Apr 18). *Should data be considered critical infrastructure?* Retrieved from Austalian Strategic Policy Institute: https://www.aspistrategist.org.au/data-considered-critical-infrastructure/

Google AI. (2018, marzo 5). *A Preview of Bristlecone, Google's New Quantum Processor*. Retrieved from Google AI Blog: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

Herman, A., & Friedson, I. (2018). *Quantum Computing: How to Address the National Security Risk.* Washington DC: Hudson Institute

IBM. (n.d.). *Cyber resilience lifecycle*. Retrieved from IBM: https://www.ibm.com/services/business-continuity/cyber-resilience

Ilo-Okeke, E. O., Tessler, L., Dowling, J. P., & Byrnes, T. (2018, August 15). Remote quantum clock synchronization without synchronized clocks. *Nature Quantum Information, 4*(40).

Institute for Defense Analysis. (2017). *Assessment of the Future Economic Impact of Quantum Information Science.* Washington DC: IDA.

Korn, W. (2008). *Made on Earth: What we wear. Where it comes from. Where it goes.* London: Bloomsbury.

Mosca, M. (2016). *A Quantum of Prevention for our Cybersecurity.* Retrieved from Global Risk Institute: https://globalriskinstitute.org/research/cyber-security-fraud/

Mosca, M. (2018, Septiembre/Octubre). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy, 16*(5).

Murgia, M. (2018, November 9). *UK scientists build world's first quantum compass*. Retrieved from Financial Times: https://www.ft.com/content/e90f902a-e441-11e8-a6e5-792428919cee

NIST. (2016). *Post-Quantum Cryptography.* National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

O'Regan, G. (2016). *Introduction to the History of Computing.* Cham: Springer.

Rodrik, D. (2018). *New Technologies, Global Value Chains, and the Developing Economies.* Background Paper, University of Oxford, Blavatnik School of Government. Retrieved from https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2018-10/dani_rodrik_new_technologies.pdf

Symantec. (2014). *The Cyber Resilience Blueprint: A New Perspective on Security.* Mountain View CA.

Wallden, P., & Kashefi, E. (2019, April). Cyber Security in the Quantum Era. *Communications of the ACM, 62*(4).

Wallerstein, I. (2004). *World-Systems Analysis: An Introduction.* Duke: Duke University Press.

ANALYSIS

Rebooting the EU's cyberdiplomacy

PATRYK PAWLAK*
BRUSSELS EXECUTIVE OFFICER, EU INSTITUTE FOR SECURITY STUDIES

When cyber diplomacy entered the European Union's institutional vocabulary not so long ago[1], only a handful of officials in the European External Action Service (EEAS) and the Ministries of Foreign Affairs of the member states had an idea of what the concept meant. International events have quickly provided a much-needed reality check. The increasing use of cybertools for large-scale industrial espionage, ransomware, interference in democratic processes, or the attacks against the critical infrastructure capable of paralysing financial or transportation networks (often as an element of a more complex hybrid operation) have generated significant political interest. At the same time, the threat to international peace and security resulting from such malicious activities, the risk of their escalation into an international conflict, and the inter-state competition put cyber issues on the agenda of regional and international organisations such as the Organisation for Security and Cooperation in Europe (OSCE), Organisation of American States (OAS), or the ASEAN Regional Forum (ARF). Currently, almost all EU member states and the European External Action Service have a senior diplomat (or even teams) responsible for coordinating their country's positions on major issues such as digital affairs, cyberdiplomacy, or broadly defined hybrid threats. The focus on cybersecurity as an internal market issue – the policy area which lends itself to a broader

1 The first EU Cyber security Strategy was adopted only in 2013 and the Council Conclusions on Cyber Diplomacy in 2015.

* Dr Patryk Pawlak is Executive Officer for the Brussels office of the EU Institute for Security Studies and the Project Coordinator for the EU Cyber Direct – an EU-funded project aimed at supporting the EU's cyber diplomacy. He writes in his personal capacity.

interpretation when it comes to the EU's competence – has allowed the European Commission and the EEAS to spearhead a number of initiatives that resulted in a more dynamic progress in comparison to other areas linked to national security issues. As a consequence of these developments, cyberdiplomacy issues are regularly discussed among member states in Brussels and with international partners through cyberdialogues or other high-level bilateral meetings.

Despite the progress, however, this is not the time for complacency. The EU needs to make a better use of its regulatory power and throw its full diplomatic weight into the ring if it is serious about delivering a more resilient society envisioned by the NIS Directive, giving citizens more control over their data as promised by the GDPR, ensuring safety and security through adequate standards heralded in the EU Cybersecurity Act, or strengthening the commitment to responsible behaviour in cyberspace as anticipated in the Cyber Diplomacy Toolbox. While much is happening already, there is both a need and potential for a better version of EU cyber-diplomacy. In order to allow a new approach to cyberdiplomacy to take shape, the EU needs to let go of the elements that cause system freezes or slow down its performance. The following sections discuss how such a reboot could materialise in practice.

The EU needs to make a better use of its regulatory power and throw its full diplomatic weight into the ring if it is serious about delivering a more resilient society envisioned by the NIS Directive, giving citizens more control over their data as promised by the GDPR, ensuring safety and security through adequate standards heralded in the EU Cybersecurity Act, or strengthening the commitment to responsible behaviour in cyberspace as anticipated in the Cyber Diplomacy Toolbox.

Adapting to a new global operating system

Over the past five years the international digital environment has changed dramatically. The reliance by states on cyber operations to pursue their national security and foreign policy objectives is no longer a taboo. In 2019 alone, we have seen a range of high-profile cyber operations that seriously challenged the notion that cyberspace should be used only for peaceful purposes. The use of cyber operations to defy existing foreign policy tools such as the reliance on ransomware for fund generation and evasion of existing sanctions by the Pyongyang regime highlights another challenge in the technology–foreign policy tandem. At the same time, cybersecurity has become a significant issue for foreign policy. The debate surrounding 5G technology and its implications for the EU's and the member states' bilateral relations with China illustrate this point well. Finally, the proper development, functioning, and openness of our societies and economies is dependent on the levels of vulnerability to digital threats posed by cyber criminals.

Steering the change requires identifying the right questions. In the case of the European Union's role in the global cyberpolicy debates, the following set of questions and issues would be a good starting point.

a) What cyber-specific norms, values, and principles should the EU promote?

The European Union has constantly expressed its support for the UN-led debate about norms, rules, and principles of responsible state behaviour in cyberspace. The discussion on international norms of responsible behaviour in cyberspace has come a long way since 2010, when states acknowledged for the first time that a lack of shared understanding of international norms pertaining to state use of cyberspace might have a negative impact on cooperation between states in cases of major incidents (United Nations, 2010). Consequently, back then, much of the debate focused on sharing best practices, managing incidents, building confidence, reducing risk, and enhancing transparency and stability.

Fast forward to 2019, the debate about responsible behaviour in cyberspace is more mature. Five different UN Groups of Governmental Experts (GGE) that gathered between 2005 and 2017 have generated a set of concrete norms of state behaviour that have been endorsed by the UN General Assembly. Parallel norm development processes led by different policy communities (Paris Call, Prague Proposals, Tech Accord, Charter of Trust, Global Commission on Stability of Cyberspace) have supplemented the existing acquis with new proposals. The conversation about norms is now entering a new stage under the UN aegis (i.e. with another GGE, a novel format of the Open-Ended Working Group, and the Agenda for Disarmament launched in May 2018).[2] Regional organisations such as the OAS and ARF are also engaged in norm-shaping processes.

Several Council Conclusions and other policy documents adopted by the EU have endorsed the set of norms proposed by the UN. But little effort has so far gone into mapping the EU's indigenous norms and promoting them through broader international cooperation. While individual services of the European Commission have focused on beefing up their cooperation with international partners in an effort to promote EU's solutions and good practices, there still needs to be a more significant effort to use diplomatic channels to the same effect. In addition to clarifying and explaining their own normative stances, the EU institutions and member states need to do more to promote the rules and norms of behaviour that are already engrained in the EU's laws and policies, notably security by design and privacy by design. The Union's role as a regulatory and standard-setting actor gives it additional tools for ensuring that such norms are respected. *But how does the current international agenda support the EU objectives? What are the "made in the EU" norms that are critical for EU's security and foreign policy? Which of them should be prioritised and promoted by "uploading" them to the global level?*

2 The implementation Action Plan states in one of the points that the Secretary-General will engage with Member States to help foster a culture of accountability and adherence to emerging norms, rules, and principles on responsible behaviour in cyberspace.

In addition to clarifying and explaining their own normative stances, the EU institutions and member states need to do more to promote the rules and norms of behaviour that are already engrained in the EU's laws and policies, notably security by design and privacy by design.

b) What strategic goal for EU's cyber diplomacy?

In light of the evolving security landscape – in terms of both the complexity of attacks and their origins – the EU has progressively advanced in its thinking on the role of cyber diplomacy as an aspect of its international posture. The adoption of the Cyber Diplomacy Toolbox in 2018 is the latest addition to the range of EU's instruments and policies adopted over the past five years. What is missing, however, is an overall framework that provides guidance and a comprehensive narrative about the EU's objectives for a global cyberpolicy and a clear definition of the role that the EU wishes to play in cyberspace: preventing potential conflicts, serving as a mediator or maybe enforcer of norms? The vision of a free, open, safe, secure, and rules-based cyberspace often referenced in the public documents has neither clarified what *specific* objectives the EU wishes to achieve nor provided a *comprehensible* narrative that could serve as a unifying force for the EU's external action in the cyber domain. Rather than clarifying what *concretely* the EU stands for, it created additional confusion among its international partners by leaving ample room for interpretation. Because of these shortcomings, the EU's credibility is often challenged. Almost simultaneously, as the policy space of the normative debate has become more crowded and more dynamic, the national security and foreign policy community became hungrier for results in delivering a peaceful and secure digital environment.

Faced with the growing number and complexity of malicious cyberactivities, the EU member states adopted different, sometimes divergent, approaches towards that objective: strengthening

resilience or imposing consequences on malicious actors. Recognising that simply making it harder for adversaries to inflict damage in cyberspace is not enough, the United Kingdom adopted a doctrine of deterrence against cyberattacks that aims to impose a price on perpetrators of malign cyberactivity by identifying state or other actors that were behind it, responding by naming and shaming, prosecuting the perpetrators, and taking further steps in accordance with international law (Hunt, 2019). In the past, the British Government had already exposed the Russian cyberattacks in Ukraine, North Korea's ransomware campaign that affected thousands of computers around the world, and the theft of commercial data by hackers linked to the China's Ministry of State Security. The focus on "deterrence by punishment" resembles the doctrine adopted by the United States that presumes increasing the costs and changing the decision calculus of the adversaries through "persistent presence, persistent innovation, and persistent engagement". The "defend forward" philosophy adopted by the US is based on the premise that a Cyber Command engages in fighting against and hunting for adversaries on another state's networks. EU's reflection on the preferred strategic posture will no doubt also be affected by the commitments member states made in the 2016 NATO's Cyber Defence Pledge and the subsequent decision of some states to make their cyber capabilities available to NATO.[3]

EU's reflection on the preferred strategic posture will no doubt also be affected by the commitments member states made in the 2016 NATO's Cyber Defence Pledge and the subsequent decision of some states to make their cyber capabilities available to NATO.

Such approaches differ from doctrines developed by other countries such as France, for instance. In January 2019, Florence Parly, Minister of the Armed Forces, presented the French Cyber Military Strategy, which in addition to defensive aspects, for the first time included a new doctrine for offensive military cyberoperations that explains the way in which the country uses offensive cybertools and the interaction with conventional forces (Delerue, Desforges, & Géry, 2019). This model, however, is substantially different from the UK and US models in that it foresees a strict partition between agencies with offensive capabilities and their defensive agency counterparts dealing primarily with "cyber protection".[4] Through its actions, France has also demonstrated a clear preference for "red phones over the megaphone" (Laudrain, 2019).

These two approaches entail a set of concrete choices about the policies and instruments to be adopted. These choices will then influence where the centre of gravity of the EU's cyber posture should lie. *How can the EU reconcile the image of a peaceful actor focused on strengthening resilience at home and abroad with the focus on deterrence – the approach that in its nature assumes and assigns negative intentions and puts a relationship between states on the path of conflict rather than cooperation? Is there a role for the EU when it comes to cyberdefence or should it abdicate and find a suitable "division of labour" arrangement with NATO?*

c) How do we make EU's voice on preventing conflict in cyberspace better heard?

While the EU's posture to cyber diplomacy is still a patchwork of approaches, the EU does have a unique combination of instruments and resources ranging from law enforcement, development, trade, regulation to diplomacy that altogether contribute to preventing conflict in cyberspace. The establishment of the European Cybercrime Centre within Europol, the laws on cross-border access to evidence and bringing cybercriminals to justice, and the EU's support for the Budapest Convention have made the EU

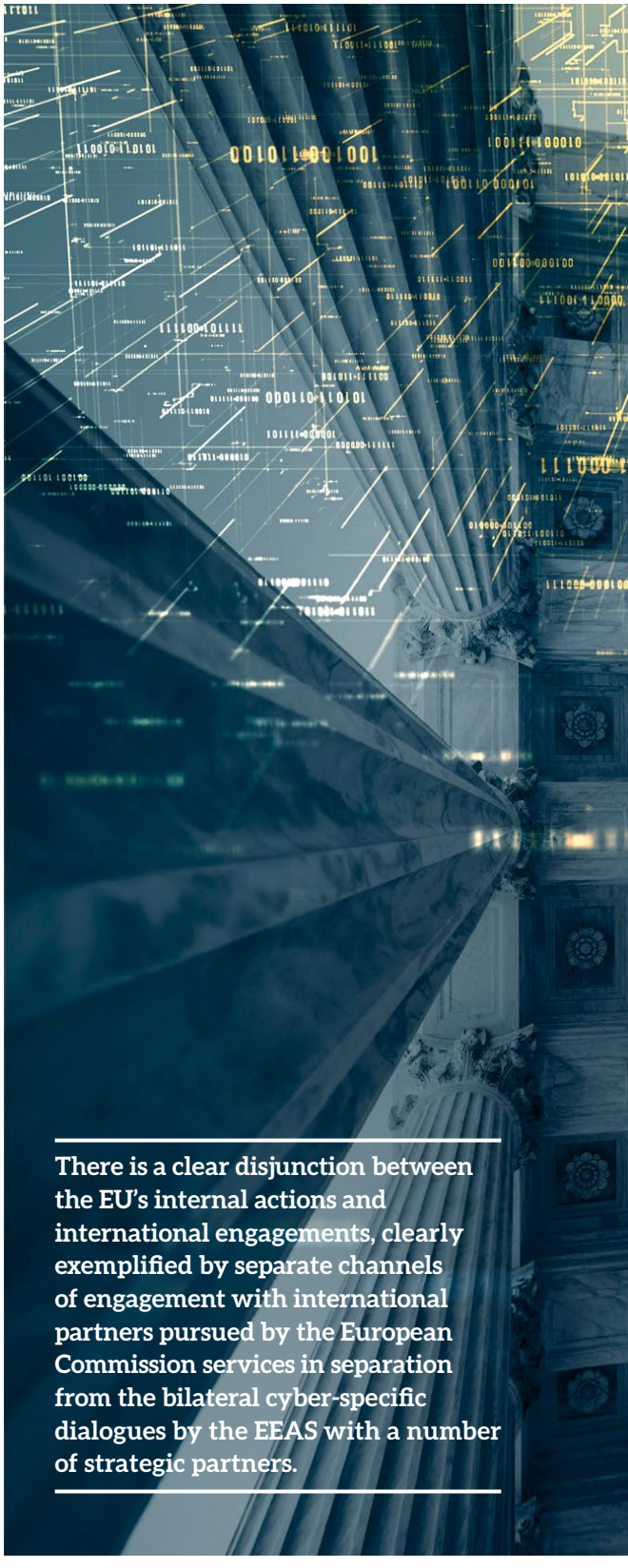
3 Several Allies have made declarations to commit specific resources towards cyberdefence, including Denmark, Estonia, Germany, Lithuania, the Netherlands, Norway, the UK and the US.

4 Other countries (such as the Czech Republic) have adopted similar approach whereby the responsibilities are delineated between cybersecurity (NÚKIB) and cyberdefence (military intelligence). The latter is supposed to be able to conduct active operations in cyberspace.

one of the key players on cybercrime. The EU's efforts to bring all member states to a similar level when it comes to cybersecurity and the support it provides towards strengthening member states' capacities through harmonisation and legal approximation made the EU's approach a point of reference across the world (even if countries like China or India perceive the extraterritorial effect of such laws as undermining their sovereign right to regulate as they wish). Finally, the Cyber Diplomacy Toolbox offers a whole range of tools and instruments to promote the adherence to norms of responsible behaviour, promoting international law and reducing the risks of conflict escalation in cyberspace.

However, the existing fragmentation and the lack of a guiding international strategy means that the EU often punches below its weight. There is a clear disjunction between the EU's internal actions and international engagements, clearly exemplified by separate channels of engagement with international partners pursued by the European Commission services in separation from the bilateral cyber-specific dialogues by the EEAS with a number of strategic partners. This is not surprising given that the EEAS engagement with third countries is taken hostage by the lack of real competences in the digital domain (most of them lie with the European Commission) and the member states' control over the most critical aspects of the cyber diplomacy portfolio (such as decisions about attribution and imposing consequences). As the most impactful pieces of European legislation have extraterritorial effects – in particular the GDPR, the NIS Directive, and the EU Cybersecurity Act – there is a clear need for a more holistic stance in explaining the value of the EU's approach through a more extensive and better use of cyberdiplomacy tools and instruments, including the EU Delegations around the world.

More importantly, there is a clear need for addressing the question of the division of labour between the member states and the European Union institutions when it comes to cyberdiplomacy. The EU has made significant progress in cyberpolicy over the past years. But it is partly because it has avoided the issue of communitisation and instead



There is a clear disjunction between the EU's internal actions and international engagements, clearly exemplified by separate channels of engagement with international partners pursued by the European Commission services in separation from the bilateral cyber-specific dialogues by the EEAS with a number of strategic partners.

pursued a harmonisation strategy. However, the Union now needs to hit some of the questions heads on when it comes to international security in cyberspace. One may observe a certain paradox: on the one hand member states keep repeating that the issues of war and peace and national sovereignty and international law belong to the member states while at the same time increasingly looking for answers towards the European Union. The recent decision to put a cybersanctions regime in place is an example. The question on strategy is therefore also a question on the member states' willingness to pursue some of their foreign policy objectives through a common action at the EU level. *What is the EU's added value in supporting EU member states? How should the division of labour between the EU and the member states look?*

Closing the unfinished business

The story of the European Union's cyberdiplomacy is filled with initiatives that have not seen their completion. There are at least three concrete initiatives that could contribute to significantly improving the way in which the EU conducts its cyberdiplomacy and consequently serves European interests.

1. **Appoint a Special Representative for International Cyberspace Policy.** For quite some time now, the European External Action Service has been toying with the idea of establishing an envoy on cyber affairs with a similar role to that of the EU cyber ambassadors/coordinators. That idea has not been applied for several reasons, including the lack of political will at the highest levels of the EEAS. However, establishing a position of an EUSR for international cyber policy may have several advantages. While decisions about war and peace are the sovereign decisions of EU member states, member state governments increasingly look towards the EU to act as a force multiplier on the international stage. In addition, most of the EU's cyberdialogue partners – such as China, India, and the United States

– have established such positions already and having one point of contact on the EU side for international affairs would bring value. Placing this dossier in the hands of a capable and experienced diplomat directly under the EU High Representative (as is the case with other EUSRs) – with a privileged link to the Political and Security Committee and working in close relationship with the Security and Defence Directorate in the EEAS, the Commission services, and the counterparts in member states – would send a strong signal to allies and perpetrators and give cyberpolicy the political attention it deserves.

2. **Adopt an EU Cyber Diplomacy Strategy.** The appointment of a "cyber tsar" to represent the EU interests globally notwithstanding, the EU needs a proper strategy for its international engagement on cyber-related issues. Such a strategy should put forward a clear message regarding the EU's role as a "forward looking" cyber player by bringing together all aspects of digital policies, including conflict prevention, international law, internet governance, 5G, norms, data economy, AI, research, innovation, skills, etc. Substantial work in that respect is already done in the context of UN processes, the implementation of the Cyber Diplomacy Toolbox or other sectoral digital strategies. But there is a clear need for streamlining all these efforts while preserving a certain level of flexibility, including through digital and sectoral strategies being developed, projects, and programmes with different funding mechanisms. Such a strategy should be developed through a close cooperation between different institutions and in close consultation with the member states in order to provide more clarity on conceptual issues and on the use of resources. Rather than being yet another bureaucratic exercise, drafting such a strategy should be conducted with the support of a Reflection Group working closely with stakeholders from academia, private sector, and civil society.

The appointment of a "cyber tsar" to represent the EU interests globally notwithstanding, the EU needs a proper strategy for its international engagement on cyber-related issues. Such a strategy should put forward a clear message regarding the EU's role as a "forward looking" cyber player by bringing together all aspects of digital policies, including conflict prevention, international law, internet governance, 5G, norms, data economy, AI, research, innovation, skills, etc.

3. **Further strengthen the joined-up approach and the capacities of the EU.** EU's voice is louder on the international stage when it is more than the sum of its parts. With cyber-issues pervasive across various areas of European policies, there is a clear need to streamline ongoing efforts and various aspects of cyberdiplomacy. Such coordination is currently only partly provided through the Working Party on Cyber Issues in the Council of the EU with discussions about the external aspects of European policies coordinated by the Commission still taking place primarily in the issue- or region-specific working groups. Many of these services do not even consider themselves to be a part of the EU's foreign policy and external relations agenda. However, as the method used to prepare the EU's position on China has demonstrated, closer coordination provided by the EEAS can have its benefits and a joined-up approach should become a standard working method. Issues that could be addressed through such a method – either in respect to specific countries/regions or as cross-cutting horizontal items – include defining the EU's indigenous norms to be promoted globally, the strategic objectives for cyber capacity building, or regional priorities for digitalization and security. Such a joined-up approach also requires close cooperation with the member states, some of whom are already spearheading important initiatives: Netherlands and Estonia

on capacity building, international law and norms; Estonia on resilience building and cyber defence; Germany on data protection and resilience; and France on international norms and state response. It is clear that the EU cannot do it alone and that its influence comes through working together. At the same time, there is no doubt that the biggest strength of EU's cyber diplomacy is its people – in both the EU institutions and the member states. It is a sad truth, however, that under the layer of political declarations and statements, there is another layer of often under-staffed and under-resourced departments across the governments.

There is no doubt that cyberpolicy has been one of the most dynamic policy areas in the past decade of the European foreign and security matters. When it comes to cyberdiplomacy, despite the lack of a clear voice, weak political commitment, and under-resourced departments, the EU has managed to project the image of a reliable partner in shaping cyberspace. Where its vision and commitment were clearly defined, the EU has set the tone of the global debate (e.g. the EU's support for the Council of Europe Budapest Convention or the commitment to the Confidence-Building Measures process in the OSCE). But the grace period is slowly coming to an end. With powers like China, United States, or India aspiring to play a more active role in shaping the digital environment, the EU needs a powerful voice. We are now reaching a point where the dilemmas that have stifled the progress in other policy areas are increasingly present in the cyber-related debates: Should there be more European integration when it comes to digital issues and cyberdiplomacy? What role should the EEAS and the Commission play when it comes to defining and promoting norms of responsible behaviour in cyberspace? How do we balance national interests with the common good for the European Union? Answering these questions and ensuring a real progress in the European project will require strong political will. With digitalisation featuring permanently on the new Commission's agenda, there is a unique window of opportunity to ensure that the EU's norms and practices proliferate and help us find a stronger voice for Europe. Like with any system-wide upgrade, there is a need and suitable time for a reboot. For EU's cyberdiplomacy this time is now. ■

About the author:

Dr Patryk Pawlak is Executive Officer for the Brussels office of the EU Institute for Security Studies and the Project Coordinator for the EU Cyber Direct – an EU-funded project aimed at supporting the EU's cyber diplomacy. He writes in his personal capacity.

References

Delerue, F., Desforges, A., & Géry, A. (23 April 2019). A close look at France's new military cyber strategy. *War on the rocks*. Commentary. Retrieved from https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/

Hunt, J. (2019). Deterrence in the cyber age: Foreign Secretary's speech. Retrieved from https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary\

Laudrain, A. P. B. (26 February 2019). France's new offensive cyber doctrine. *Lawfare*. Retrieved from https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

United Nations. (30 July 2010). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/65/201. Retrieved from https://undocs.org/A/65/201

ANALYSIS

A model proposal for financial services security risk coordination in Europe

ADAM PALMER
GLOBAL HEAD OF CYBERSECURITY RISK MITIGATION & CONTROLS, SANTANDER BANK
JOHN MORGAN SALOMON
REGIONAL DIRECTOR, FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER

The European financial services sector would benefit significantly from a European stakeholder-driven initiative to create a centralised coordination group for security risk identification, mitigation strategy, and risk prioritisation. In 2002, the United States successfully created a similar financial sector cooperation body known as the FSSCC (Financial Services Sector Coordinating Council).[1] Despite the success of the FSSCC, Europe currently lacks a similar regional sector risk coordination group. This article outlines a proposal for a similar group, but designed to meet the unique requirements and needs of European banking firms.

While several smaller, task-specific, either regional or national risk coordination initiatives exist, there is not a broadly inclusive and centralised European risk coordination group. This is primarily the result of the significant differences between sector risk strategies across different European countries. This challenge is contrasted with the relative ease of designing the FSSCC coordination group within the single nation of the United States. The FSSCC also had close support from the US Government which was active in the foundation of the FSSCC. This close government engagement contrasts with the more passive support by European institutions to sector risk coordination.

1 The Financial Services Sector Coordinating Council (https://fsscc.org) is an industry-run forum for protecting the US financial sector from physical and cyberattacks, as part of US critical infrastructure resilience. It works with US government agencies through public-private partnerships, and provides guidance to the sector as a whole on how to accomplish risk reduction goals.

Background

The need for the creation of a European financial services risk coordination body is highlighted by recent challenges in the EU security of network and information systems (NIS) directive development process. The NIS Directive is a major EU-level policy statement related to risk and security across Europe. Because no single sector coordination focal point existed, the NIS review process included the creation of a public-private platform consisting of three working groups. These groups' task was to comment on European Commission recommendations for cybersecurity. One of those working groups, related to security risks, saw significant fluctuation in membership and a lack of clarity in messaging. A single sector risk coordinating body that includes as members the most critical financial firms, financial trade associations, and financial services partners/service providers, would have provided a far more efficient forum for collecting inputs from relevant sector stakeholders.

The goals of this proposal are:

1. Avoid duplication in focal areas for cyber and physical risk coordinated by other entities.
2. Share and track information about ongoing efforts to mitigate systemic cyber/physical risk.
3. Optimise coordination with partners as well as key stakeholders on risk identification, mitigation, prioritisation, and strategy.
4. Provide strategic guidance to operational security risk initiatives within EU financial services community and partners.
5. Provide a unified point of contact for discussion with regulators and external stakeholders on cyber and physical risk issues.

Risk-Focused, Not for Technical Coordination

The strategic nature of a sector coordination council makes it an ideal platform for cyber and IT risk leaders to harmonise risk strategy. While many external cyber defence groups focus on technical or operational coordination, there is a need for strategy and risk prioritisation. This commonly may occur in the first line of security at a financial institution. However, risk strategy and prioritisation is commonly found at the second security defence line level in the financial services sector. A single coordination council could be designed as a unique platform for this strategy-level discussion. A key objective would be to identify and prioritise risks in a way that guides priorities across the European Financial Services sector.

While many external cyber defence groups focus on technical or operational coordination, there is a need for strategy and risk prioritisation.

A Risk Coordination Model Designed for European Members

A successful EU risk *coordination* model should be a risk coordination group, not a *control* group. A European coordination model can only be successful if there is flexibility and openness. This allows for different multi-jurisdictional member requirements. While the US FSSCC can more easily adopt a single public-private management model, this is not feasible for the European sector where different national laws create conflicts and challenges. The proposed solution is to facilitate voluntary sector coordination *without* any binding restrictions or requirements.

It is also important to emphasise that the sector risk coordination council should be designed to complement, not replace, current work by sector stakeholders. The European Union Agency for Network and Information Security (ENISA) has a mandate under the European Cybersecurity Act to act as "European Cybersecurity Agency". ENISA conducts sector-wide exercises, issues good practices and recommendations, it also supports policy-making and implementation. Similarly, areas like threat intelligence-based Ethical Red Teaming is a framework developed originally by the Dutch National Bank, and subsequently issued by the European Central Bank (ECB). These initiatives provide unique value. However, they are not risk

strategy and prioritisation coordination bodies for the financial services sector. Sector interaction with these, and other European/national entities, has often been on an individual and *ad hoc* basis that is not always representative for the entire sector's needs. Similarly, stakeholders such as the European Banking Federation (EBF) are focused primarily on policy. EBF is not focused on security risk strategy. A new centralised risk coordination council could be uniquely placed to ensure a coordinated platform for the European financial sector to collectively identify and reduce the systemic risk to this industry.

A successful EU risk coordination model should be a risk coordination group, not a control group. A European coordination model can only be successful if there is flexibility and openness.

Public-Private Partnership for Financial Services Operational Risk Resilience

While this proposal is not designed to suggest creating a policy group (duplicative of EBF), a critical goal of a risk coordination council should be to support strong public-private partnership. The objective of this would be to maintain a robust and resilient financial services sector across Europe. The focus of this activity should be to provide strategic operational guidance and risk prioritisation coordination to government stakeholders. Additionally, this could include collaboration with government stakeholders to share ideas and feedback on policy to improve the resilience of the sector. To effectively provide this guidance, a coordination council would create and maintain relationships with key government stakeholders. These relationships would be used to support the sector's coordinated response to cybersecurity risk issues. However, it should be emphasised that while a risk coordination council may act as a focal point for policy discussion with stakeholders, the goal is to avoid becoming a policy-focused group.

Critical Infrastructure Protection and Financial Services

Another key function of a risk coordination council should be to coordinate risk strategies and priorities to protect financial services as part of the critical national infrastructure (CNI) ecosystem. Country-specific differences or sensitivities related to CNI often complicate collaboration. One unique need for a risk coordination council is to strengthen the resiliency and coordination of the financial services sector against threats interconnected to critical infrastructure. This can be accomplished by including the voice of financial services as part of CNI protection issues. The function of the risk coordination council in this regard would be to coordinate across the sector to proactively identify risks, promote joint action, drive preparedness, collaborate with regional government stakeholders, and support the sector's crisis response. This would be designed to support critical infrastructure risk awareness and help member firms understand how to mitigate CNI-related risk issues.

One unique need for a risk coordination council is to strengthen the resiliency and coordination of the financial services sector against threats interconnected to critical infrastructure.

Oversight and Strategic Guidance of Financial Services Sector Risk Mitigation Activity

In 2018, the European division of the FS-ISAC established the European Cyber Resiliency Centre (ECRC) with a permanent European office in The Hague, The Netherlands, and London, UK. The ECRC is the operational security focal point for FS-ISAC in the EMEA region, and coordinates intelligence and community cyber risk operational mitigation activities. The ECRC has already established operational relationships with law enforcement agencies, CERTs / CSIRTs across Europe, partner organisations (industry federations, sector sharing groups), has placed analysts in joint intelligence centres (e.g. UK NCSC Industry 100)

and worked with intelligence staff seconded from member firms and financial CERTs. The ECRC is the operational "other side of the coin" of this proposal. This proposal compliments the ECRC by providing strategic guidance of risk priorities, reviewing risk mitigation plans, and confirming the effectiveness of ECRC risk mitigation activities. This function is similar to the second line of defence concerning security risks at financial services firms. While the ECRC functions as a first-line operational implementation and mitigation team, the risk coordination council could guide prioritisation and review effectiveness.

Final Comments

The purpose of this article is to encourage discussion, seek input for guidance on ideas, and gather the support of the financial services community in Europe to make this type of effort successful. This proposal is not designed to duplicate or interfere with existing efforts in the sector. Risk coordination should be voluntary and non-binding on member participants. However, there is significant value in having a centralised risk coordination group in Europe.

In April 2019, the European Banking Federation, the FS-ISAC, AFME, and a group of EU financial services firms created the Cyber Resilience Forum-European Financial Sector (CRF-EFS). This effort is in its earliest stages. It is aimed at achieving the goals discussed in the preceding paragraphs. The CRF-EFS appears to be a unique opportunity to develop a pan-European model for financial services sector risk coordination. The FSSCC model in the US demonstrates the value and potential of such efforts. This points to a bright future if there is member support, agreement, and active participation. It is hoped that the CRF-EFS can mature and achieve success, or at least be a significant positive step towards successful risk coordination for the European financial services sector. ■

DISCLAIMER: This is not an official statement or policy position of Santander Bank Group.

About the authors:

Adam Palmer is based in Madrid, Spain as the Global Head of Cybersecurity Risk Mitigation & Controls at Santander Bank. Adam is a former US Navy officer and also led the UN Global Programme on Cybercrime.

John Morgan Salomon is the regional director for the Financial Services Information Sharing and Analysis Center (FS-ISAC). John is Swiss, lives and works in Spain, and has over 20 years of experience in most aspects of the global information security industry.

Welcoming the digital as a new agora

ROB VAN KRANENBURG
@ROBVANK
FOUNDER OF COUNCIL IOT AND #IOTDAY

Picture the current situation: a table full of delicacies, linen as white as snow, beautiful cutlery; you've invited your friends to dinner. Everyone is happy and deep in conversation. All realise, however, that nothing on that table is yours. You only (still) own the house in which you throw the party. GAFA: Google, Apple, Facebook and Amazon, and BAT: Baidu, Alibaba and Tencent, play on that table and they get richer every minute from our very own feedback. They build new services on top of that. You realise that at some point soon they will take over your house. They already offer to pay the rent of the patio, and do you really need the attic? You are in an uphill battle. You have no tools to fight off the invaders as you are only now, when it is too late, beginning to realise these friends you have invited are taking reality itself, what is "normal" to another level. And as the peasants learned how to tumble the knights from their horses, the world was never the same again.

Our current conceptual toolbox is no longer equipped to address new challenges: "We grasp reality through concepts. When reality changes too quickly and dramatically, as it is happening nowadays because of ICTs, we are conceptually wrong-footed." (Gligoric et al., 2017)

Goods, persons, houses, situations,[1] and industrial processes radiate data trails and create digital twins. These twins exist as sets of properties in an analytic layer that is in many hands at the moment, but not really under multi-stakeholder control. Whoever or whatever gains agency in and on that layer (which defines governance of the everyday) must grasp the practice and theory of assigning, withdrawing, validating, and defining the entitlements and their very nature: who/what exists when/where/how and why? The term "entitlements" is vague but it points to the fact that "identity" as a term to designate actions, attributes and location of a person has become problematic. Andrea Servida, "father" of eIDAS (Electronic Identification and Trust Services), for example uses it in the following way (Servida, 2019): "where eIDAS matters; data-minimisation; use of trusted attributes, credentials and entitlements (such as age verification, proof of residence, etc.)"

The situation is hybrid in the sense that digital twins actually begin to influence back in analogue objects. This is the moment of ontological change, decisive for leadership in the 21st century. It demands a new toolset for the notion of identity itself. Uncoupling identity in thinking of "entitlements" opens up a new field of value and services. In the case of self-driving cars, for instance, this way of thinking could argue for liability resting not with real person-identities but with entitlements – any combination of a particular driver (with particular points on a passport and certain characteristics) and a particular car. This reasoning can be extended to any service in the network.

1 The public review of Classification of Everyday Living Version 1.0 CSPRD03, announced in https://lists.oasis-open.org/archives/coel-comment/201805/msg00000.html, closed on 23 May 2018. No comments were received.

Goods, persons, houses, situations, and industrial processes all radiate data trails and create digital twins. These twins exist as sets of properties in an analytic layer that is in many hands at the moment but not really under multi-stakeholder control.

There is a simple reason for this emancipation and agency: Internet. Psychologists specialising in the behaviour of larger groups of people try to explain the relative ease with which one is able to exert influence over masses by assuming "a causal force which bears on every member of an aggregate, and also for each individual there is a large number of idiosyncratic causes" (Stinchcombe, 1968, p. 67-68). He continues: "Now let us suppose that the idiosyncratic forces that we do not understand are four times as large as the systematic forces that we do understand.... As the size of the population increases from 1 to 100, the influence of the unknown individual idiosyncratic behavior decreases from four times as large as the known part to four tenths as large as the known part. As we go to an aggregate of a million, even if we understand only the systematic one-fifth individual behavior as assumed in the table, the part we do not understand of the aggregate behavior decreases to less than 1 percent (0.004)."

This shows how top-down power works and why scaling itself has become such an important indicator in such a system of "success". Imagine you want to start a project or "do something" with your friends or neighbours, say five people. This means to take into account before you do anything – state a goal, negotiate deliverables, or even the first date on which to meet for a kick-off – that all five people are impacted by huge idiosyncrasies and generic forces that have to be aligned or overcome before you can even say hello. This shows how difficult it is to "start something". It also explains why you are always urged to "get bigger" and why you need to "grow". It is only then *and through the process of getting bigger itself* that the management tools can operate, lying in waiting for you to discover them. To be decisive, to make a difference, to set about a course for change, is in no need of growth, nor of scaling.

Understanding the nature of these social relations in the above terms shows how difficult it is to script moments of systemic change, as hierarchical systems – due to the very fact that they are top down –are able to maintain the status quo with relatively little effort. That which they cannot predict or control are still dissident, strange, or abnormal lone voices, or "sudden events". With the Internet such elements have been assembling and intensifying, and the Internet of Things will only help reinforce the trend, bringing individuals the sensor network data sets they can handle on their devices. This acceleration of weak signals into clusters, organised networks, and flukes cannot be managed anymore by formats that are informed by and that inform systemic forces as *the nature of these forces has changed.*

Authorities can never again talk at people. They must develop policies in conversation with people and re-negotiate on equal footing the balance between accountability and anonymity and entitlement versus identity.

China, India, and now Russia[2] have already made this a priority and have taken to centrally coordinate the design of the future online/offline architecture as it will apply to their territory and population.

Authorities can never again talk at people. They must develop policies in conversation with people and re-negotiate on equal footing the balance between accountability and anonymity and entitlement versus identity.

The hegemony that used to enable authorities to facilitate the continuity of peace is at its breaking point. Political populism, lack of digital agency, lack of aligning techno-reality in any kind of domain and service with its full absence at the most important decision-making level: the political model of voting representatives organised in the party format (paid to be an organisational form by the same state structures) once every four years, lack of long term visions on jobs vs robots, lack of education on generational issues of having grown up in commercial connectivity, the erosion of trust in the current financial toolsets versus strong moves towards and adoption of central authority-less crypto-currencies, further regionalisation (Brexit, Catalonia, Poland, Hungary) – they all point to immanent breakdown of the current economic, social and political toolsets.

I posit a living ecosystem of the best possible balance between extreme centralisation (of infrastructure, protocols, and identity management) and extreme decentralisation (of data, applications, services), focussing on resilience and self-healing properties as radically new concrete functionalities of a digital ambient infrastructure, and legible interfaces to those properties that matter for citizens – stability, solidarity, reciprocity, fairness – in an inclusive sustainable environment.

In general and popular imagination there is no available alternative to the real-world situation: Google, Amazon, Facebook, Apple (GAFA) have won the winner-takes-all paradigm and seem to be eternal. With Libra[3], Facebook is set to fulfil the killer retail application of IoT: full dynamic pricing on any good, any service, any human want or need. The Facebook whitepaper on LIBRA (May 2019) specifies under The Libra Association purposes: "An additional goal of the association is to develop and promote an open identity standard. We believe that decentralized and portable digital identity is a prerequisite to financial inclusion and competition" (Libra Association Members, 2019).

There are too many dependencies to real-world violence and discrimination in the current governments to fully back nationalisation of all data

2 "As reported by Russia's TASS news agency on Wednesday, 'Russian President Vladimir Putin has signed the law on providing stable operation of the Russian Internet (Runet) in case it is disconnected from the global infrastructure of the World Wide Web.'" (Doffman , 2019).

3 Interestingly our proposal involving the Zenroom protocol was engendered in the same EU project DECODE from which Facebook "acqui-hired" the UCL team from to build LIBRA, basically validating the commercial impact of the protocols.

assets or run a Chinese form of platform politics that integrates the industrial Internet, sharing clouds across value chains and aligning that with the Honest Shanghai app that pulls data from over 300 databases scoring citizens on trust and thus credit rates.

In between the commercial model of the US data lakes and the fully integrated top-down Chinese approach, Europe should find *a new balance with new leading actors* between centralisation and decentralisation, anonymity and accountability, and investments in innovation and maintenance and repair.

We are in a new conceptual space and should co-create notions of solidarity (economics), privacy (self), security (trust), assets (potentials), risks (resilience), and threats (competition), tailored to a reality of today.

The most important feature of this approach is that identity becomes an activity dispersed over and managed by the person and his or her attributes profile, the object, machine, or robot that performs the service, and the enabling connectivity harnessed in an architecture.

We are in a new conceptual space and should co-create notions of solidarity (economics), privacy (self), security (trust), assets (potentials), risks (resilience), and threats (competition), tailored to a reality of today.

Accountability over anonymity characterises this approach as it underlies society in the 21st century itself. Tokenised trust is a key feature but only in the actual locality where face-to-face interaction can occur and communities of people work and live together.

This approach that builds reciprocity not over two, but three actors, is the only way to counter and overcome the incongruities that are currently eroding trust: fake news, synthetic data (information artificially manufactured, created algorithmically), fake passports and passports for sale by national source signers.

This approach builds on the fixed identities of human beings in nationally signed passports, of goods in GS1 type of repositories (and scenarios of behaviour in taxonomies such as coelition.org and face and gait recognition capabilities) and reorganises them as "event" identities.

In the Technical Report entitled *Self-Sovereign Identity: A Comparison of IRMA and Sovrin* (Nauta, Joosten, 2019), authors state "Over a decade ago, Kim Cameron and others dreamed of what was called an Internet Identity Layer; it would do for (the exchange of) (identity) data what IPv4 had done for network transport: make sure that all local solutions could live together to form a globally connected infrastructure. could be exchanged throughout the world in the same way. (…) Today, we see tens if not hundreds of initiatives that work with these principles. However, it is still quite difficult to satisfy all of them: surveyed some 50 of them, and identified the three that came closest: uPort, IRMA and Sovrin."

Identity is thus distributed over architecture, service, and phone, signed in digital signatures, federated and attribute-based only. A large number of technical (IoT), financial (blockchain) and semantic (AI) experts see the need to move from the present fixed-identity paradigms to more flexible or fluid frameworks of "entitlements", to allow the formulation of context-specific and attribute-based identities. Let's focus on that vision and build a new smart social contract. It will bring hope and hope is what drives real change and society forward. Technically it can be operationalised in a fully open-source hardware and software environment. The hardware part needs to be procured from the EU industry. The operating system, zenroom,[4] is being developed in the EU project DECODE.[5] It forms the heart, a virtual machine running embedded in a chip in the triangle: device (EU passport), embedded SIM cards in services (wearables, home, connected car, and smart city), and infrastructure (routers, 5G base stations).

4 https://zenroom.org – Dyne.org also is the content partner in the EU Blockchain NGI RIA LEDGER.

5 https://decodeproject.eu

A large number of technical (IoT), financial (blockchain) and semantic (AI) experts see the need to move from the present fixed-identity paradigms to more flexible or fluid frameworks of "entitlements", to allow the formulation of context-specific and attribute-based identities.

We thus need an inclusive identity framework that is able to name, validate, and build services on identities that will become a process between a device/controller of some kind (now smartphone), services (energy, mobility…) and the architecture.

That capability should be European.
It does three things:

- it gradually fades out GAFA;
- it creates European services through EU-unified protocols that could be locally permission-less deployed, thus winning us the third battle – after losing data and platform we cannot afford to lose "meaning" (AI running off and on Big Data), as we don't care where the "original" data resides;
- it restores European dignity, a vital belief in our agency to build meaningful and value creating infrastructures, which is what leaders should do.

I received an invitation to talk about the Internet of Things from the GFF and the Italian Intelligence community, Transformational Technologies #4: Implications for an Expanding Threat Environment September 17-18, 2012 Rome, Italy. In the afternoon, five breakout groups (senior intelligence, police, and military) came back with five scenarios of major threats: one was military, two were about DIY bio-weapons and two were about the "total breakdown of society" because of the inability of current institutions to deal with the digital (Van Kranenburg, 2012). This was 7 (seven!) years ago.

Explaining the current drivers of the Digital Transition to a lay audience is difficult even if the effects are visible and present in everyday life: fake news, depression among youngsters, addiction to social media, sexting, and on a more economic scale, fear of job loss because of robotic automation, lack of systematic and technical agency on a political level (fining innovative companies or legally trying to regulate data protection, GDPR).

We lack positive stories and examples. We also miss out on formats that reach young audiences like Instagram and YouTube. In China citizens "are beginning to push back against some kinds of surveillance. An Internet company that streamed closed-circuit TV footage online shut down those broadcasts after a public outcry. The city of Shanghai recently issued regulations to allow people to dispute incorrect information used to compile social-credit records. 'There are rising demands for privacy from Chinese Internet users,' says Sammy Sacks, a senior fellow in the Technology Policy Program at CSIS in New York. 'It's not quite the free-for-all that it's made out to be'" (Larson, 2018).

Like China that has a strong business-policy coherence, GAFA[6] and the pre-bitcoin payment industry in the US is also closely aligning itself with traditional Chamber of Commerce activities to lobby against local data storage laws. US technology giants intensify lobbying efforts against stringent Indian data localisation requirements[7] "which they say will undermine their growth ambitions in India", sources told Reuters. Technology firms worry the mandate would hurt their planned investments by raising costs related to setting up new local data centres.

What I propose runs counter to the grain of thought and praxis in current western political frameworks and mental imageries. It is not relevant to *also* have a technical agenda, the full agenda has to be techno-political. A concrete action plan and our third step (after *GDPR* and *Digital Signatures*, see further) is to quickly regain agency over data, platforms, and the AI value layer.

6 Google, Amazon, Facebook, Apple.

7 https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-india-panel-wants-localization-of-cloud-storage-data-in-possible-blow-to-big-tech-firms-idUSKBN1KP08J

What I propose runs counter to the grain of thought and praxis in current western political frameworks and mental imageries. It is not relevant to also have a technical agenda, the full agenda has to be techno-political.

Roadmap

In the workplan of the Next Generation Internet CSA NGI FORWARD we propose a concrete three-step process to build a vibrant, inclusive, democratic Internet ecosystem by 2025.

The first step is being taken: regulating data in GDPR.

The second is regulating digital signatures for persons, which has been achieved (2014 EU eIDAS Regulation).

Future Internet services composition we propose to develop on the basis of digital signatures to be achieved in Taskforce Services (TS), and resilient architectures to be achieved in digital signatures in Taskforce Infrastructures (TI).

Digital Signatures for services (banking, payment, energy, education, care, mobility, connectivity…) and Digital Signatures for architectures (virtual and analogue enablers of connectivity) are a tool to complement current actions on procurement and local agency, as in this kind of Service Level Agreements it does not matter that the original data sets and analytical platforms are not under your control. In this manner local stakeholders are a priority part of building the next layer of value, namely the new entities that are formed when AI-inspired intelligence starts to see patterns unrecognisable before.

The third step is to embed signatures for persons, services, and architectures into a sustainable framework for access and identity. This could be brokered by:

- substituting the passport for a device (a successor to the Estonian e-card) which talks to friendly servers, platforms, and clouds running public algorithms and ethical AI, enabling direct democracy through local referenda and embedding contributions from taxpayers in a rich value layer that foster innovative public and private services in a comprehensive sovereign framework;
- adding security, framework and architectural checks for any device when it receives the electrical appliance label that is mandatory in Europe for any device as the instance to validate compliance with zenroom;
- produce a European router (dowse.eu) running zenroom;
- new notions of search and new notions of discovery are needed in real-time hybrid environments; Pearse O'Donohue explained these terms in the 2019 Future Internet Conference in Brussels[8] as follows: 1. We are in seamless connectivity 2. We face instant reprogrammable software defined networks that are with 5G not reprogramming system rules only but going straight into instantly adjustable applications in verticals (also or mostly through networked slicing in 5G).

We are experiencing the last potential zone of transition with humans in agency. The current policy situation requires the convergence of immediate (re)cognition of real-time reputation scores of people and their skills, machines and services

8 Opening Session: Rethinking the future of the Internet – Objectives, priorities, opportunities. The possibilities that digital technologies now offer up seem truly limitless and are at the core of Europe's socio-economic growth. A number of threats have however emerged in our increasingly connected digital world – from personal data misuse, digital exclusion, fear of job losses, to fake news – having had negative impacts on the uptake of innovative technologies and services. Looking ahead, it is therefore vital that future developments around the Internet and its governance enhance its role as a key driver for innovation, economic growth, inclusiveness and social progress. Moderator: Rob Van Kranenburg, Founder, Council. Panellists: Pearse O'Donohue, Director, Future Networks, DG CONNECT, European Commission; Maria Rautavirta, Director, Data Business Unit at Data Department, Ministry of Transport and Communications, Finland; Elena Plexida, Vice President, Government and IGO Engagement, Internet Corporation for Assigned Names and Numbers.

and infrastructure repairability.[9] In moments of crises the readiness of all relevant actors is immediately visible. Only then can planning begin on the basis of the actual level of response.

The current policy situation requires the convergence of immediate (re)cognition of real-time reputation scores of people and their skills, machines and services and infrastructure repairability.

We want to investigate embedding these signatures for persons, services, and architectures into a sustainable framework for conflict management that also includes social media, big data, pattern recognition, AI. With disasters come conflict. In *The Social Order of a Frontier Community*, Don Harrison Doyle writes there is a danger to equate conflict with social disorganisation. Jason Dykstra states social conflict is normal, inevitable, and a format for community decision-making (Doyle, 1983). Sociologist Lewis Coser advises that, instead of viewing conflict as a disruptive event signifying disorganisation, "we should appreciate it as a positive process by which members of a community ally with one another, identify common values and interests, and organize to contest power with competing groups" (Doyle, 1983).

The most challenging task will be to develop a common language and vocabulary that puts us on a par with machines that are able to learn, becoming more like equal partners in a relationship.

There is a strong tendency to also want to control data and information on top of owning media production capabilities. There is no need for this. We can envisage "locality" as a centralised protocol of coherent actions that can be executed in a full decentralised way. We move away from democracy as we know it to a new political democratic system that is tuned to the reality of what is happening in every domain of human activity; to live together and alongside real-time data streams of sensor input, to bring big data and analytics into the heart of decision-making and to eventually run territory (not "country") as a service for all.

The most challenging task will be to develop a common language and vocabulary that puts us on a par with machines that are able to learn, becoming more like equal partners in a relationship.

It takes a strong mental effort to realise that it is your own situation, *the very model that supports you*, that needs changing instead of a hypothetical situation thought of as more suitable. Even more difficult is to realise that it is possible to build similar pragmatic cybernetics and to start working towards that with like-minded people. A successful Digital Transition is the best possible feedback on our physical and mental health, the best possible deal based on real-time resource allocation monitoring, the best possible decision-making based on real-time data and information from open sources, and the best possible alignment of local providers with the global potential of wider communities.

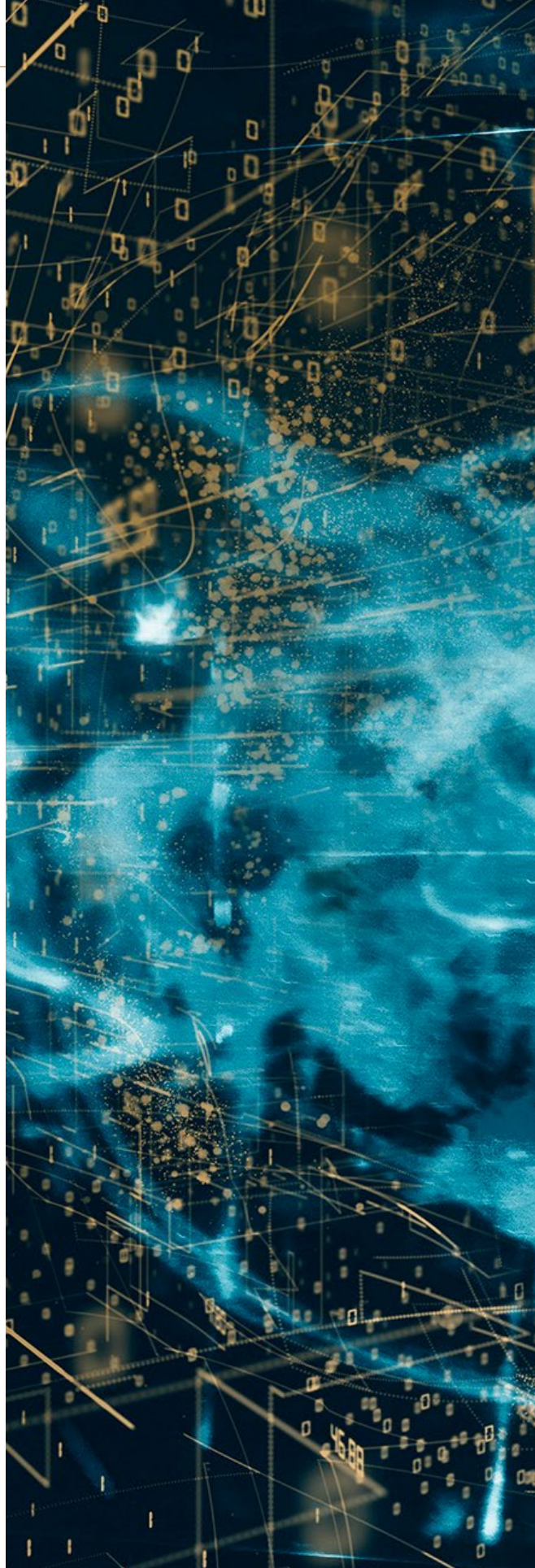
The journey we have to undertake resembles that of people going into exile. For "people" read our particular kind of embodied intelligence. It has a tremendous idiosyncratic variety; we are all different and unique, yet we also share characteristics that make us part of the human species. Foresight and planning as part of collective decision-making have been until now solely our domain. As we see another kind of foresight intelligence (that we call artificial) evolving and working in the key players as regards everyday (leisure)

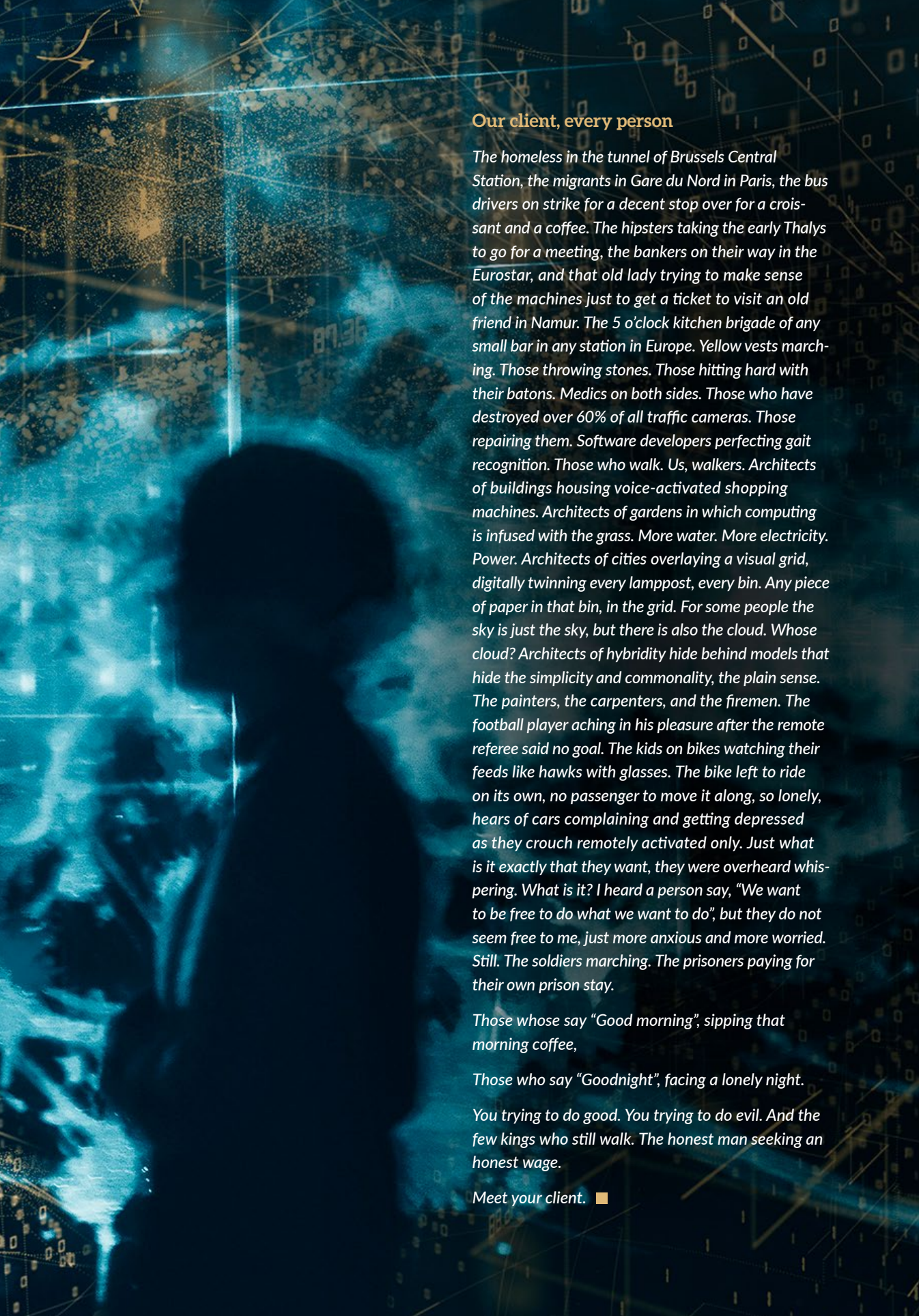
9 People are a set of properties and radiate data. Goods are a set of properties and radiate data. Machines and smart objects like lantern-poles are a set of properties and radiate data. At some point these data sets are mixed in order to address specific situations or provide shortcuts to services. For example: In a car accident with an autonomous self-driving car all the involved entities (from the driver to the tree to the rock to the water in which the car crashes) are awarded temporary identities in order to determine liability, accountability, and damages. The question then becomes: Who awards the identities? What organisation? These temporary identities will build new services.

activities and mundane tasks (Airbnb, Amazon Prime, Uber), in distinct domains (BAN: wearables/health, LAN: smart homes/retail, WAN: connected and electric car, mobility in general, planning patterns, and VWAN: the smart city and large grids), and in horizontal services such as fintech and ICOs (which compete and co-evolve with traditional financial tools), it is only a matter of time before AI works its way into public decision-making on a large scale. We have to prepare for this situation.

History has seen many botched revolutions and would-be patches to bring political reality in line with mental models, new business patterns, and emancipatory trajectories of individual human beings.

One of the most interesting and relevant in the current crypto-craze context is the 1825 Decembrist uprising against feudal Russia. It was not planned well. The officers had fought to free France alongside their French officers, only to return to see the soldiers they fought and died with go back into serfdom. It was more of a romantic then strategic uprising. The czar found it hard to hang them, so he sent them to Siberia. And as they went they formed *artely*, artels, just like any other convoy before them had. In these *artely* the convicts grouped together through all kinds of *self-organised smart contracts*. It was possible to change name (and punishment), to buy and sell goods, comfort, and protection. The *artely* leaders made deals with the wardens and officials. They were in chains in the cities and villages. In the open fields, as they marched, they took them off. It is well-documented that prisoners who escaped during such a deal were flogged harsher and longer by their fellow inmates than the officials. After all, they had broken not just the social contract with the state but with their own "family". This betrayal is always worse. This tactical leadership – temporary smart contracts – after coming together in *artely* is what we have to do along every stretch of the journey from here to the world as an integrated zone of operation. Against the grain at times, against our very own wishes, simply chained together in the belief that breakdown of the current and early integrators is far worse.





Our client, every person

The homeless in the tunnel of Brussels Central Station, the migrants in Gare du Nord in Paris, the bus drivers on strike for a decent stop over for a croissant and a coffee. The hipsters taking the early Thalys to go for a meeting, the bankers on their way in the Eurostar, and that old lady trying to make sense of the machines just to get a ticket to visit an old friend in Namur. The 5 o'clock kitchen brigade of any small bar in any station in Europe. Yellow vests marching. Those throwing stones. Those hitting hard with their batons. Medics on both sides. Those who have destroyed over 60% of all traffic cameras. Those repairing them. Software developers perfecting gait recognition. Those who walk. Us, walkers. Architects of buildings housing voice-activated shopping machines. Architects of gardens in which computing is infused with the grass. More water. More electricity. Power. Architects of cities overlaying a visual grid, digitally twinning every lamppost, every bin. Any piece of paper in that bin, in the grid. For some people the sky is just the sky, but there is also the cloud. Whose cloud? Architects of hybridity hide behind models that hide the simplicity and commonality, the plain sense. The painters, the carpenters, and the firemen. The football player aching in his pleasure after the remote referee said no goal. The kids on bikes watching their feeds like hawks with glasses. The bike left to ride on its own, no passenger to move it along, so lonely, hears of cars complaining and getting depressed as they crouch remotely activated only. Just what is it exactly that they want, they were overheard whispering. What is it? I heard a person say, "We want to be free to do what we want to do", but they do not seem free to me, just more anxious and more worried. Still. The soldiers marching. The prisoners paying for their own prison stay.

Those whose say "Good morning", sipping that morning coffee,

Those who say "Goodnight", facing a lonely night.

You trying to do good. You trying to do evil. And the few kings who still walk. The honest man seeking an honest wage.

Meet your client. ■

About the author:

Rob van Kranenburg is the Founder of Council IoT and #iotday. He wrote *The Internet of Things*. A critique of ambient technology and the all-seeing network of RFID, Network Notebooks 02, Institute of Network Cultures. Together with Christian Nold he published Situated Technologies Pamphlets 8: The Internet of People for a Post-Oil World. Rob is co-editor of Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model, Springer Open Access. He works as Ecosystem Manager for the EU project Next Generation Internet, Strategy CSA NGI FORWARD. He is a DeTao Master IoT.

References

Doffman, Z. (2019). Putin Signs 'Russian Internet Law' To Disconnect Russia From The World Wide Web. Forbes. Retrieved from: https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#50c7c8a51bf1

Doyle, H. (1983). The Social Order of a Frontier Community. Jacksonville, Illinois, 1825–70, University of Illinois Press, p. 11

Gligoric, N., Hennebert, Ch., Krco, S., Lopez, C., Elicegui I., OReilly, C., Nati, M., Van Kranenburg, R., Stembert, N., Serra, A., (2017), Making Onlife Principles into Actionable Guidelines for Smart City Frameworks and# IoT Policies. In: Designing, Developing, and Facilitating Smart Cities (editors: Vangelis Angelakis, Elias Tragos, Henrich C. Pöhls, Adam Kapovits, Alessandro Bassi). Springer.

Larson, C. (2018). Who needs democracy when you have data? *MIT Technology Review.* Retrieved from: https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/

Libra Association Members (2019). An Introduction to Libra. White Paper. Retrieved from: https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US-1.pdf

Lomba, D. (2019). Change Misnomer - Information Age and inevitability of automation and AI in: Information, Control and AI. Retrieved from: https://chinggary.blogspot.com/2019/05/information-control-and-ai.html?m=1

Nauta, J., Joosten, R. (2019). Self-Sovereign Identity: A Comparison of IRMA and Sovrin. Report number: TNO 2019 R11011.

Ramli, D. and Bergen, A. (2018). This Company Is Helping Build China's Panopticon. It Won't Stop There. *Bloomberg*. 19 November 2018. Retrieved from: https://www.bloomberg.com/news/articles/2018-11-19/this-company-is-helping-build-china-s-panopticon-it-won-t-stop-there

Andrea Servida (2019). Let's go eIDAS: building trust online. Towards Trustworthy Digital Identities in Europe. European Commission, Unit R3, "Knowledge Management & Innovative Systems".

Stinchcombe, A. (1968). Constructing Social Theories. The University of Chicago Press

Van Kranenburg, R. (2012). Identifying the Real and Absolute Enemy, *Cyberspace, Malevolent Actors, Criminal Opportunities, and Strategic Competition*, 457-477. Retrieved from: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1319

ANALYSIS

Discussing smart cities: stakes, challenges and initiatives

ALICE DECEUNINCK

STUDENT AT THE SCHOOL OF PUBLIC AFFAIRS OF SCIENCES PO, MASTER PUBLIC POLICIES - SOCIAL POLICY AND SOCIAL INNOVATION

Introduction

In the recent years, smart cities became a dominant paradigm of urban development that is part of thousands of innovative urban projects and smart strategies around the world. However, the concept that emerged as a necessary response to the unceasing growth of population and urbanisation receives as many comments as it raises questions and concerns.

Even though "smart cities" progressively entered the mainstream policy vocabulary in both academics and industrial fields – following the precedent concepts of information city or digital city – the term is still perceived as elusive. Therefore, it seems important to recall its definition before entering the accompanying discussion. The term "smart city", apart from the basic understanding referring to a superior state of urbanity, is unspecific and vague. Consequently, it refers to a broad range of ideas and concepts, in permanent evolution. It is difficult to find one exhaustive definition. There is neither a single template of framing a smart city, nor a one-size-fits-all definition of it (O'Grady and O'Hare, 2012). However, they are all going in the same direction: the essence of smart cities is the rationalisation of cities by improving and optimising urban services and city operations intelligently through the application of ICT (Information and Communication Technologies) but more specifically IoT (Internet of Things) and a wide array of advanced technologies. Any area of city management can become a smart city initiative if it aims at maintaining sustainability and improving people's quality of life: i.e. public transportation, IT connectivity, water and power supply, sanitation and solid waste management, e-governance, agriculture, banking services, health, manufacturing, and even citizen participation.

The essence of smart cities is the rationalisation of cities by improving and optimising urban services and city operations intelligently through the application of ICT but more specifically IoT and a wide array of advanced technologies.

This universalisation of the smart city concept can easily make consensus within the world – especially in our contemporary societies in which the shared ambition of development and growth leads to searching solutions to optimise and new innovations enabling progress. However, this new model for urban management and policing raises new concerns and demands reflection on the needs necessary to accompany this transition in the city management and organisation the best. Moreover, it also encounters practical challenges in its realisation. In this article, we will highlight the main points of discussion around the concept of smart cities, the challenges the actors in those cities will have to face to reach their ambition, and the cities the most active in the realisation process – by highlighting their performance and initiatives.

The frontrunners

Encouraged by the various commercial smart city technologies widely available on the market, governments promote smart cities with enthusiasm through funding programs and policy agendas. The European Union has been a particularly strong proponent of smart cities through the Smart Cities and Communities program of the European Commission's Horizon 2020,[1] even if these ambitions are shared by the majority of the developed countries' national governments such as the United States, Singapore, or China. As for developing countries, many may be tempted to see in the smart city the magic solution to catch up with their delays.

The European Union has been a particularly strong proponent of smart cities through the Smart Cities and Communities program of the European Commission's Horizon 2020.

The assessment of smart cities is complicated because of the variety of cities' visions and priorities worldwide. Although the action categories are theoretically the same for every city, the extent of the issues encountered

1 The Horizon 2020 Work Programme for 2018–2020, p. 105-109.

and the solutions are going to be specific to each urban landscape and its technological, economical, and governing barriers. One of the most famous reference ranking of the world's smartest cities is the IESE Cities in Motion Index (CIMI) prepared by the Center for Globalization and Strategy and the IESE Department of Strategy. The ranking is based on nine dimensions which are deemed crucial to a city's progress: human capital, social cohesion, economy, governance, environment, mobility and transportation, urban planning, international outreach, and technology. The top 10 is dominated by London, New York, Amsterdam and Paris. In the ranking, Western Europe is the best geographical area followed by North America and Asia Pacific.[2] However, looking only at the innovation criteria, the top innovative cities in the world aren't located in the United States or in Europe, but in Asia, especially in China – which its multifaceted approach helps explain. According to the United Nations, by 2050 over 68 per cent of the world population is expected to live in cities, with close to 90% of this increase taking place in Asia and Africa.[3] The Asia-Pacific region is therefore anticipated to be the fastest-growing region in terms of smart technology by 2025.[4]

When focusing on smart city governance – such as the necessary development of a smart city strategy and a digital inclusion plan, the public funding of initiatives, the experiment of smart hubs, the sharing of data with citizens – the city of London performs the best.[5] However, we still find Singapore and Seoul in the second and third position, illustrating their understanding of the necessity to have good governance with a dedicated city leadership steering smart city projects to develop a sincere, people-first design of the future city. In this matter, London and its Smart London Board, followed by Helsinki and Barcelona, could be considered the smartest "smart city" in Europe.

Internetworking technology – the pillar of smart city implementation

The concept of smart city is centred on the use of technology to improve the quality of life in cities and their management. It has the unique property of being less an idea to realise than a set of technologies to develop and exploit (Choplet, 2018). The key champions of the smart city agenda now include technical standards agencies, such as the International Organization for Standardization.[6] The application of the IoT, which works with a network of connected physical devices such as cars or home appliances that are exchanging real-time data, was a necessary precursor to the smart city. It allows a convergence of the physical and the digital to occur, which enables the analysis useful for achieving this goal of conducting better, data-driven policies. The IoT isn't the only technology used in smart cities, but the best one to aggregate information using sensors, cameras, and other smart devices. This technology can be combined with the use of other solutions, like cloud and edge computing, geospatial technology, and of course Artificial Intelligence (AI) to process the data and the blockchain technology to secure the data flow. Improving the connectivity and the technological infrastructures, with innovations like the AMI (Advanced Metering Infrastructure), appears therefore to be a condition achieving a degree of "smartness" in a city. Networks must be able to provide robust public safety communications for emergency services to keep people safe in these new "smart" environments. The deployment of 5G, combined with edge computing and the cloud, will be a catalyst that will

2 IESE Cities in Motion Index 2019, by cities in motion. Retrieved from https://blog.iese.edu/cities-challenges-and-management/2019/05/10/iese-cities-in-motion-index-2019/

3 According to the 2018 Revision of the World Urbanization Prospects, published by the Population Division of the United Nations Department of Economic and Social Affairs (UN DESA).

4 According to the experts of the market research company Frost and Sullivan in "Global Smart Cities to Raise a Market of Over $2 Trillion by 2025", retrieved from thetechnologyheadlines.com

5 According to the 2019/19 Top 50 smart city government rankings by Eden Strategy Institute and ONG&ONG Pte Ltd., cf. https://www.smartcitygovt.com

6 ISO and smart cities, ISO, 2017.

drive mass IoT adoption in the smart city and will help eliminate latency, bandwidth, and computation issues, which is key to connecting systems that cannot fail or be delayed, such as autonomous vehicles. Moreover, smart cities must integrate open-access software and gather technologies, systems, services, and capabilities into an organic network that is sufficiently multi-sectorial and flexible for future developments (Albino, Berardi, & Dangelico, 2015).

The deployment of 5G, combined with edge computing and the cloud, will be a catalyst that will drive mass IoT adoption in the smart city and will help eliminate latency, bandwidth, and computation issues.

Protection of citizen's data – combining the smart and the cybersafe city

Smart cities are built on an information network. Open data is therefore an essential component of smart cities: data points from sensors are being shared on a large scale across powerful data centres to collect, transfer, store, analyse, and learn from them in real time. Large quantities of data are being generated at unprecedented rates. The personal data of users can also be uploaded to and shared in the cloud.

Various studies have proven that these emerging technologies providing real-time information are enabling city managers to improve their operations. Braun et al. (2018) affirms that cities improved their resilience and safety indexes. However, if smart cities infrastructures can enable safer cities, they are also opening up new avenues for up-to-date cyberattacks. How to guarantee that hackers can't access the sensors and manipulate the data? Since vulnerabilities commonly exist in each layer of a smart system, security and privacy issues remain to be carefully addressed. Indeed, the IoT devices could become primary targets for attackers. Taking control of the traffic control infrastructure could delay law enforcement as it is reaching a crime scene, data manipulation can cause an evacuation in panic, tampering with smart farming sensors may even cut off food for the population. Those security problems aren't only speculations: to name only one example, nearly 230 thousand Ukrainian citizens suffered a long blackout in 2015 because of the power grid system hacking (Zetter, 2016). With the advent of smart cities, the responsibility of authorities is also increased with regard to tort litigation at the intersection of producer liability and municipal liability. To prevent mass panic, cities shouldn't let their sensors' vulnerabilities remain unpatched and need to safeguard users' data with effective countermeasures that can't be the traditional cybersecurity protection strategies such as encryption, biometrics, or anonymity since smart city IoT systems are characterised by their heterogeneity, scalability, and dynamism and since smart devices have limited computational power. The first and probably the easiest step cities can take is to appoint not only Chief Data Officers (CDO) but more importantly Chief Information Security Officers (CISO), with the former responsible for the use and management of data and the latter leading cybersecurity teams, working on modernising technology, partnerships, and training. Recently, Boston Mayor Marty Walsh has appointed the city's first Chief Information Security Officer, Gregory McCarthy, for whom this position is "the opportunity to lead the City into a new chapter of maturity in how we protect our systems, data, and constituents" (Wray, 2019). He will be working in collaboration with the Chief Data Officer, but his role will be dedicated to tackling cybersecurity issues. Appointing Chief Data Officers seems to be an effective and concrete way for a city government to prove that the concerns around the privacy of citizens data are taken seriously. Another way to respond to the concerns of citizens is to propose publicly a clear privacy plan for tackling data governance each time a new smart city project is communicated to the citizens. In Toronto for example, Sidewalks Labs stated that the data gathered through their project of redeveloping the city's waterfront will be kept by an independent "civic data trust" and will not be sold, used for advertising, or shared without people's permission. Overall, officials, even without having all the answers, are

making visible efforts to invest in cybersecurity and anonymise data in order to avoid a lack of acceptance of these technologies by citizens, who tend to be more and more informed of the risks, worried about the governance of their data and, therefore, wishing to expand their digital rights.

With the advent of smart cities, the responsibility of authorities is also increased with regard to tort litigation at the intersection of producer liability and municipal liability.

What is increasing this lack of trust is the experts' tendency to get enthusiastic about the benefits and possibilities of new technologies without being clear about their intentions and the deployment conditions. They forget that "the community of a smart city needs to feel the desire to participate and promote a (smart) growth" as well (Albino et al., 2015). This behaviour can worry the citizens, already concerned over the privacy of their data, potentially collected by service providers and third parties, as well as over the intersection of software with the physical world. Physical injuries or property damages could happen after a bug – accidental causalities – or a hacking. For example, a failure of sensors designed to protect infrastructure could result in the collapse of a building, or the hacking of an autonomous vehicle could threaten life safety. The response to this concern might be that accidents always happen and can't all be avoided; however, it will be always possible to claim that the harm could have been prevented or mitigated if the systems had been better designed.

Last but not least, no matter how much effort is put into using the security-by-design approach, there will always be concerns with data collection. The best answer might be education and transparency. Each citizen must know what data is collected and how it will be used: aware of the benefits of data collection, citizens will be more willing to give up personal data, considered to be a new type of "common good" generating public value. It is what we call a trade-off between utility and privacy, but this theory works only if biometric detection will only be used in the future to constantly optimise services for citizens. "Building transparency and accountability into services is the central mechanism to build trust. However, there is no single way of doing this – it requires a multidisciplinary approach that includes user research, systems and interaction design, technology and policy," Richard Pope reminds us rightly (2018). In some countries, like Singapore, where the amount of faith in the public institutions is high, citizens are less concerned by the use of their data – they really perceive the government as "a source of security and material comfort" (Poon, 2017) – whereas in the US smart cities, citizens seem more willing to give up their data to companies like Google, Facebook, and Apple than to the government.

New challenges for the private sectors – the necessity of a new mindset

The business dimension is inherent in the concept of smart cities: optimising urban services will result in significant long-term cost savings for the government authorities. The concept itself emerged from the high-tech companies in Silicon Valley. Marsal-Llacuna and al. (2014), include this business dimension explicitly in their definition of smart cities by writing that the goals are "to monitor and optimize existing infrastructure, to increase collaboration among different economic actors, and to encourage innovative business models in both the private and public sectors". A research firm estimates that Barcelona will save billions of dollars a year in energy costs by installing smart systems such as smart street lights ("on" only when sensors detect motion), parking sensors (real-time information about free parking spots), or even rubbish sensors (with an underground waste storage to lower noise and smell pollution). It is also not unusual for smart city initiatives to be spearheaded by economic development agencies or innovation agencies rather than by traditional planning departments. How to ensure that the business dimension doesn't overshadow the main goal of improving public utilities?

It is estimated that the market value of investments in IoT tools and platforms to modernise cities around the world will exceed $135 billion by 2021.[7] A leading IT company, Cisco, announced[8] in 2017, during the Smart City Expo World Congress in Barcelona, a one-billion-dollar investment in smart cities, describing such solutions as "an area that has previously been perceived as too new and, therefore, too difficult to finance" to justify the timing of this major investment. Much like private companies, governments are racing to infuse technology into their cities and gain the smart label – a major branding tool, giving the city a modern image and attracting investments. China alone has more than 200 smart city projects in progress (Li, Lin, & Geertman, 2015). Some authors, such as Adam Greenfield in his work *Against the smart city* (2013), criticise the corporate dimension since companies have no expertise, according to him, on how cities function. To be sure that this business dimension doesn't overshadow the main goal of improving public utilities, an increased collaboration between the private and the public sectors as well as between all municipal bodies is needed, following a mode of cooperation that differs from the existing ones. No one can deliver a full smart city solution alone. A smart city must propose a favourable environment for innovation directed to improve its inhabitant's life, like for example New York City – often considered the smartest city in the world in rankings – which is a real hub for businesses, startups and tech companies. The city of Dallas in the US is a good example of the important role the private sector plays in smart cities development. In 2015, the city, acknowledging the necessity to adopt smart technology with the help of the private sector, launched the Dallas Innovation Alliance, a public-private partnership lab.[9]

However, to partner with cities and operate effectively, companies will need to adopt the mindset of serving people and not just the market. Smart cities are much more than an opportunity for technology developers to position cities as primary marketplaces for their products. Technologies can empower citizens if adapted to their needs.

To be sure that this business dimension doesn't overshadow the main goal of improving public utilities, an increased collaboration between the private and the public sectors as well as between all municipal bodies is needed.

Governing smart cities – the emergence of a new shared responsibility

The concept of the smart city is far from being limited to the application of technologies to cities (Albino et al., 2015). To try to understand the challenges that the society and the governments will have to face during this re-organisation of cities, we must firstly ask ourselves: what new role must citizens and urban managers embrace in the context of the smart city? People "are the protagonists of a smart city, who shape it through continuous interactions", Albino et al. (2015) remind us again. Smart cities convey the message of the emergence of collective – rather than artificial – intelligence, digital citizenship, and the direct relationship established between the elected and their citizens (characteristic of what is called an "e-democracy"). In short, "living together". New technologies put more information into the hands of the users, who are making choices and holding the government entities accountable for the results of their choices. This demands a willingness from citizens to participate in this process and to get involved in public decisions and city planning, in order to improve the efficiency and information transparency. In this domain, the city of Seoul really makes an effort to create a culture of citizen participation. Educating people on how to better take part in their partnership governance system is a mission of the Seoul Innovation

7 According to IDC's Worldwide Semiannual Smart Cities Spending Guide.

8 More information can be found on: https://newsroom.cisco.compress-release-content?type=webcontent&articleId=1895705

9 More information about the partnership project can be found on: http://www.dallasinnovationalliance.com/news/2015/9/11/dallas-innovation-alliance-launched-to-execute-smart-cities-strategy

Bureau fulfilled by providing physical spaces for collaboration through different organisations such as the Seoul Social Economy Centre, the Seoul Community Support Centre, or even the Seoul Youth Hub. In the same vein, Tel Aviv launched five years ago DigiTel[10], for which the city won the first prize at the Smart City competition in Barcelona. Using the annual budget planned, the city launched a platform to increase citizen engagement and trust in the municipality. Since starting as a pilot in 2013 the DigiTel Residents Club has spread citywide[11].

Smart cities convey the message of the emergence of collective – rather than artificial – intelligence, digital citizenship, and the direct relationship established between the elected and their citizens.

The second important question to ask ourselves is: should government entities rely on private actors to collect and analyse the private data of citizens (income, crime, etc.)? When a city like Singapore – which added many cameras and sensors to monitor crowd density, cleanliness of public spaces, and the exact movement of every locally registered vehicle – stores most of the collected data into its Virtual Singapore online platform, the government of the city gets the possibility to better understand its functioning in real time. However, those data points are also valuable insights into population patterns and consumer behaviour that could be easily monetised or misused. The uncertainty around data usage is clearly felt as a major reason of the public resistance. Ensuring legal certainty to all stakeholders through functional privacy law that would apply to most data collected by smart city infrastructure is not only a question of citizens' protection but is also the only way to encourage the cities and manufacturers to invest in the development of smart cities. However, regulating data usage for companies will not be sufficient. Data policies should also be adopted to prevent, in case of public use, the concerns about surveillance of individuals that can also be raised (i.e. with cameras embedded in light bulbs).

Ensuring legal certainty to all stakeholders through functional privacy law that would apply to most data collected by smart city infrastructure is not only a question of citizens' protection but is also the only way to encourage the cities and manufacturers to invest in the development of smart cities.

Conclusion

The concept of smart cities is an innovative response to the challenge of an increasingly urbanised world, envisioned to serve the well-being of citizens in an intelligent and sustainable way. However, despite its laudable aim and the economic growth that its development might bring, one should be aware that the theoretical concept encounters numerous practical barriers: no miracle solution exists. First and foremost, the widespread use of smart applications is causing many security and privacy issues. In the coming few years, mitigating the presented challenges will be the primary task of smart city-related studies. Despite the various protection mechanisms and strategies that have been developed in recent years, there is still a long way to go to satisfy the multiple security requirements of these rapidly developing smart technologies. ■

10 More information can be found on: www.forbes.com/sites/gilpress/2018/03/22/6-lessons-from-tel-aviv-for-successful-digital-transformation-of-smart-cities).

11 More information can be found on: https://newsroom.unsw.edu.au/news/science-tech/how-does-city-get-be-smart-how-tel-aviv-did-it

About the author:

Alice Deceuninck
Recently graduated with a Bachelor of Arts in social sciences and humanities at the Political Institute of Paris (Sciences Po), Alice Deceuninck spent the 2018-2019 academic year in exchange at the Jagiellonian University in Cracow and worked as an intern and project assistant at the Kosciuszko Institute during this time. Her research at the Institute focused on smart cities with problematics such as challenges related to their development, innovative hubs and the implementation of technologies to facilitate public services.

References

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, *22(1)*, 3–21. doi: 4.10.1080/10630732.2014.942092.

Allam, Z. (2019). The emergence of anti-privacy and control at the nexus between the concepts of safe city and smart city. *Smart Cities*, *2(1)*, 96–105. doi: 10.3390/smartcities2010007

Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society*, *39*, 499–507.

Chopplet, M. (2018).

Dubai Plan 2021: Dubai's smart city strategy. (2018, January 04). Retrieved from https://www.tanaza.com/blog/dubai-is-becoming-a-leading-global-smart-city/

Gui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities, *IEEE Access*, *6*, 46134-46145. doi: 10.1109/ACCESS.2018.2853985

Li, Y., Lin, Y., & Geertman, S. (2015). The development of smart cities in China. In J. Ferreira, Jr., & R. Goodspeed (Eds.), *Proceedings of the 14th International Conference on Computers in Urban Planning and Urban Management* (pp. 7–10). Cambridge: MIT.

Marsal-Llacuna, M.-L., Colomer-Llinàs, J., & Meléndez-Frigola, J. (2014). Lessons in urban monitoring taken from sustainable and livable cities to better address the Smart Cities initiative, *Technological Forecasting and Social Change*, *90*, 611–622.

O'Grady, M., & O'Hare, G. (2012). How smart is your city?. *Science*, *335(3)*, 1581–1582.

Poon, L. (2017, April). Singapore, city of sensors. *CityLab*. Retrieved from https://www.citylab.com/life/2017/04/singapore-city-of-sensors/523392/

Pope, R. (2018). A right to the digital city, a response to the Smart London 'new deal for city data'. *Medium*. Retrieved from https://medium.com/@richardjpope/a-right-to-the-digital-city-ce487a52353

Smart City Expo World Congress. (2018, November). Retrieved from http://www.smartcityexpo.com/en/home

Smart city projects & leaders to watch in 2018. (2018, April 10). Retrieved from https://apiumhub.com/tech-blog-barcelona/smart-city-projects-leaders-barcelona/

Wray, S. (2019). Boston appoints first Chief Information Security Officer. Retrieved from https://www.smartcitiesworld.net/news/news/boston-appoints-first-chief-information-security-officer--3908

Yang, F., & Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's cybersecurity law. *Asia and the Pacific Policy Studies*, *5*, 533–543. doi: 10.1002/app5.246 https://doi.org/10.1002/app5.246

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*. Retrieved from http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

ANALYSIS

Zero Trust: security beyond the perimeter

LOTHAR RENNER
MANAGING DIRECTOR, CISCO'S SECURITY SALES

The invisible line that we draw between what belongs to the enterprise and what doesn't – servers, desktops, networks, applications, and logins – traditionally depends on firewalls and endpoint security software for protection. But the headlines are full of examples where that simply wasn't enough. At the same time, the idea of getting rid of the perimeter is generally too scary for organisations to contemplate, especially if they've only recently solidified one. So, let's not think of it as doing away with the boundary, but rather as tightening security on the inside so that the network perimeter isn't the only thing keeping the attacker at bay. And it's now within practical reach for many more organisations to consider implementing this strategy with Zero Trust Security.

Access can happen anywhere – and new threats emerge

Over the last years we have seen a shift in the IT landscape, as users, devices and cloud move outside the traditional network. Organisations have different types of users – contractors, third-party vendors, and remote workers – connecting to their corporate network. They're increasingly using their own devices, such as smartphones, tablets, laptops to connect to applications and networks. Meanwhile, applications, servers, containers, and workloads can be found communicating with each other across both cloud infrastructure and data centres. Smart devices connected to the Internet of Things (IoT) are another entry point of access to networks.

In this new IT landscape, new threats have emerged that target:

- **Identity** – Primary account credentials (username and password) are often stolen through phishing attacks or compromised third parties, and re-used by attackers from remote locations, including botnets. Nearly one-third of breaches involved compromised credentials, which shows that password capturing is an effective way to get past traditional perimeter defences and get access to applications, undetected (Verizon 2019).
- **Applications** – 54% of web app vulnerabilities have a public exploit available to hackers, meaning if servers and applications aren't patched, they're left open to known flaws that can be exploited by an attacker to get access to your systems. An attacker exploiting application vulnerabilities can then move laterally to compromise critical systems (Avital 2019).
- **Devices** – Kaspersky Labs found a 370% rise in new IoT malware variants from year 2017 to the first half of 2018, proving that connected devices are being targeted more than ever by attackers that know they can leverage smart devices to get access to your network (Ali 2019). Another study showed that 59% of businesses have had security incidents stemming from network printers (Fernandes 2019).

Taking it all into account, security at the perimeter is no longer enough. This is where Zero Trust Security comes into play.

Why Zero Trust?

When you compare traditional security approaches to a zero-trust approach, you will find that in the old approach, trust is based solely on the network location the access request originates from, while in a zero-trust approach, trust is more dynamic and adaptive. It's established for every access request, no matter where it comes from. This approach prevents attackers from moving laterally within your network to get to your data – it secures access across your apps and networks and only allows the right users and devices to get access. In addition to a better access security, a zero-trust approach also supports modern enterprise models with BYOD, cloud apps, hybrid cloud/on-premises environments and more.

(...) in the old approach, trust is based solely on the network location the access request originates from, while in a zero-trust approach, trust is more dynamic and adaptive.

With the zero-trust model, organisations gain better visibility across their users, devices, containers, networks, and applications, because they are verifying their security states with every access request. They can reduce their attack surface by segmenting resources and only granting those permissions and traffic that are strictly needed. And by using more authentication factors, adding encryption, and marking known and trusted devices, they can make it harder for attackers to acquire what they want (user credentials, network access, and the ability to move laterally). Finally, users can get a consistent and more productive security experience regardless of where they are located, what endpoints they are using, or whether their applications are on-premises or in the cloud.

Security is not a one-size-fits-all proposition, even within the same enterprise environment. For example, continuous authentication is a great idea until it conflicts with users having a low-friction workflow: if they have to authenticate with multiple factors too often, they'll resent it (and try to evade the controls that require it). Software itself, on the other hand, doesn't mind frequent authentication, so workloads that communicate with one another can support those interactions. IoT devices, such as medical or manufacturing equipment, can have both safety and availability implications that affect how they are connected to a network. That's why there are three pillars of zero-trust security:

- **Zero Trust for Workforce** – employees, contractors, partners, and vendors accessing work applications using their personal or

corporate-managed devices. This pillar ensures only the right users and secure devices can access applications, regardless of location.

- **Zero Trust for Workloads** – applications running in the cloud, in data centres, and other virtualised environments that interact with one another. This pillar focuses on secure access when an API, a microservice, or a container is accessing a database within an application.
- **Zero Trust for Workplace** – this pillar focuses on secure access for any and all devices (including IoT) that connect to enterprise networks, such as user endpoints, physical and virtual servers, printers, cameras, HVAC systems, kiosks, infusion pumps, industrial control systems, etc.

Let's take a closer look at those three pillars.

Zero Trust for Workforce

The Zero Trust for Workforce implementation rests on the combination of validated users using validated endpoint devices. This combination is further locked down with end-to-end encryption between these devices and the resources they access. Finally, users are allowed only the bare minimum access needed for their roles (which is also known as "least privilege"). As long as the user is authenticated with the right number of factors and is using an endpoint that has been enrolled and inspected for security vulnerabilities, they can access exactly those resources that they are allowed by a centralised proxy.

How do you verify trust for the workforce?
To prevent breaches caused by stolen passwords, verify users' identities using multi-factor authentication (MFA). This adds another layer of security to ensure your users are who they say they are before they're granted access. To gain visibility and insight into the security hygiene of users' devices, ensure they're running up-to-date software and they're encrypted or passcode-protected. To respond to potential breaches of trust, enforce access policies for every application that limits access to trusted users and devices and block any access attempt that doesn't meet your security standards.

Zero Trust for Workload

Enterprise systems tend to grow in functionality and add connections and dependencies in response to business needs. In order to facilitate this growth, system designers and developers can sometimes trend towards the most permissive and flexible security configurations. This creates excessive trust which attackers may exploit as they move laterally to access sensitive resources. The textbook answer to this challenge is segmentation – to a point where trust is defined by the application's unique requirements, not by the network location.

Achieving this micro-segmentation requires three technologies which have, up until recently, been out of reach.

- **Deep and pervasive visibility into network communications.** Distributed network sensors instead of traditional centralised monitoring have made such visibility possible at scale.
- **Accurate and real-time application modelling.** Big data analytics has significantly reduced the manual effort in documenting applications, thus enabling up-to-the-moment understanding of traffic patterns and dependencies.
- **The ability to apply policy to multiple devices across multiple environments.** A high-level policy engine that manages the ongoing sprawl of access control devices across multi-cloud environments simplifies the steps required to act on the application visibility and analytics.

Combined, visibility, analytics, and policies reduce the excessive trust in application ecosystems. When the velocity of change exceeds the capacity of people, the move to automation becomes inevitable. This is the state segmentation efforts find themselves in today. Adopting a zero-trust mindset enables system designers and developers to come at the problem in new ways. With better visibility, quicker analytics, and a deeper understanding of application communication, Zero Trust for Workloads redefines the perimeter around expected behaviour. Then, malicious activity, from

initial compromise to lateral movement to data exfiltration, becomes apparent and preventable.

In order to facilitate this growth, system designers and developers can sometimes trend towards the most permissive and flexible security configurations. This creates excessive trust which attackers may exploit as they move laterally to access sensitive resources.

Zero Trust for Workplace

The modern workplace is enabled by campus, data centre, WAN, branch and cloud networks, with trust extended to any user, device, and application, linked wired or wirelessly, to connect to other users, devices, applications, and other parts of the workplace. Zero Trust for the Workplace is enforcing trust when any kinds of devices are authenticating and communicating on the enterprise networks.

The rapid growth of networked devices has strained our ability to manage, patch, and protect them against rogue actions. IoT gets much of the attention due to the explosion in network-enabled devices in recent years. IoT is often built on consumer-grade platforms, lacks enterprise-level security controls, and may not be patchable. The result is we have more of these devices, which have comparably more vulnerabilities per unit, and IoT is comparably more difficult to secure. While IoT is in the spotlight, we cannot overlook fairly traditional business equipment such as printers, videoconferencing, security cameras, and VoIP telephony, which continue to be a viable avenue for criminals to compromise enterprises. Then, we also have medical equipment and OT to consider. These are often on platforms that security teams cannot patch or secure due to a number of operational, functional, and technical factors. Broadly speaking, a Zero Trust for the Workplace strategy must address authenticating, authorising, segmenting, and monitoring trust across all equipment.

The approach assumes the network is inherently insecure. We need to protect the network from the users, devices, and applications connected to it, and vice versa. In a zero-trust network, any exploitable device has to be shielded or segmented to reduce the likelihood of a criminal finding and exploiting it. Moreover, in a zero-trust network, the remaining devices have to be protected from other compromised and exploited devices. These protections go hand in hand. Both require a known inventory of the entities using the network, and visibility into the security posture of the devices.

IoT is often built on consumer-grade platforms, lacks enterprise-level security controls, and may not be patchable.

The access control decision occurs when equipment attempts to connect to the network. Traditionally, network engineers accomplished this with fixed attributes such as a combination of network switch location and IP address. In this model, we trust equipment without knowing whether the equipment is vulnerable or exploited; the traditional trust is also based on easily spoofable attributes. When moving to zero trust, the decision must be made on a number of factors, including identity and behaviour, and it must be verified regularly based on device operations and any changing factors. In particular, the organisation must be able to respond to newly discovered threats and vulnerabilities by limiting the original network access or cutting it off altogether.

Network Access Control (NAC) forms the foundation of a zero-trust implementation. The equipment must authenticate to the network before it is trusted to connect and communicate. The ideal is software-defined access control built with the IEEE 802.1X standard and certificate-based authentication.

The next level of a zero-trust network is group-based segmentation where network connections are authenticated. When making the access decision, the network identifies the equipment as belonging to one or more roles and one or more groups. These roles are irrespective of IP addressing or physical location. In fact, in most complex enterprises, these roles include multiple subnets

and multiple buildings. We then define segmentation policies based on which groups of entities can talk to which network resources, including the internet. Based on the behaviour of the equipment, we can ascertain trust, and further restrict its interaction when there is cause for concern. We can continue to reduce the assumed trust and strengthen security in the network through continuous monitoring of communications and continuous improvement of policy sets.

The multiplication of employee-driven devices has led to a corresponding increase of devices within our enterprise networks. From IoT to printers, from OT to medical devices, more equipment than ever is powering our organisations. Consequently, the attack surface is now larger than ever. A Zero Trust for the Workplace strategy enables security operations and network engineers to have better visibility into all hosts and communications, provide tighter restrictions on network communications, and implement adaptive policies based on trust. We can then reduce the risk of malicious activity exploiting these devices and respond quicker to any suspicious traffic.

Summary

A zero-trust approach secures access to everything across the entire IT environment. It allows companies to prevent a data breach before it happens by enabling policy-based controls for every access attempt to applications, workloads, and networks. With this approach, organisations can gain visibility into who and what is accessing them and thus identify risks and indicators of a breach of trust. Finally, they can reduce their overall attack surface, contain breaches, and stop the attacker's lateral movement by enforcing granular controls, allowing them to segment networks and workloads.

Cisco's approach to zero trust covers the workforce, workloads, and workplace, as it allows its users to:

- Secure the workforce by ensuring only the right users and secure devices access applications. We do this by verifying user identities with multi-factor authentication (MFA) and ensuring their devices are trustworthy by checking their security hygiene and posture.

- Secure the workloads by securing connections within the applications across the multi-cloud. We do this with application micro-segmentation that ensures the right applications, servers, databases, containers, and more can access or speak to each other within a data centre and cloud infrastructure.
- Secure the workplace by securing connections across the local network, including interconnected devices and operational technology appliances such as printers, cameras, badge scanners. We do this with network segmentation by ensuring only the right users and devices can access components across a given network.

Finally, Cisco Zero Trust provides comprehensive visibility, policy enforcement, and reporting capabilities across workforce, workloads, and workplace to help better prevent, detect, and respond to any risks in order to provide secure, trusted access across the entire IT environment. ■

About the author:

Lothar Renner is Managing Director of Cisco's Security Sales, leading the EMEAR security sales specialists across Europe, Middle East, Africa, and Russia. In this role, he is responsible for creating and delivering the security strategy and sales growth. Together with his team, he is focused on securing customers in an increasing threat landscape. Prior to his current role, Lothar led the Services business for Central Europe. He joined Cisco 21 years ago in Germany and has held numerous leadership positions in Cisco in Germany and Central Europe in Sales and Business Development.
Lothar is a keen observer of life-changing technology. During his career, he has enjoyed playing his part in enabling Cisco to transform businesses, cultures, and societies. Lothar is an active ambassador for inclusion and believes in the true power of diverse teams. He holds an MBA from VWA Stuttgart, Germany, lives in Frankfurt, and enjoys travelling, skiing, running, and yoga.

References

Ali, Z. (30 March 2019). Cybersecurity in the IoT era: Why you need to protect your IoT solutions. Retrieved from https://www.scnsoft.com/blog/cybersecurity-in-iot

Avital, N. (9 January 2019). The state of web application vulnerabilities in 2018. Retrieved from https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/

Fernandes, L. (2019). *Quocirca global print security landscape.* Excerpt retrieved from https://quocirca.com/wp-content/uploads/2019/04/Quocirca_PrintSecurity2019.pdf

Verizon. (2019). Summary of findings. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/ (part of 2019 *Data Breach Investigations Report*)

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

Readers' profile

- European-level representatives, sectoral agencies of the European Union, International Organisations Representatives;
- National-level officials of the Euro-Atlantic alliance, Government and Regulatory Affairs Directors & Managers;
- National and Local Government Officials as well as diplomatic representatives;
- Law Enforcement & Intelligence Officers, Military & Defence Ministries Officials;
- Legal Professionals, Representatives for Governance, Audit, Risk, Compliance, Industry leaders and innovators, active investors;
- Opinion leaders, specialised media, academic experts.

Types of contribution:

- Policy review / analysis / opinion – a Partner's article or a series of articles on crucial issues related to cybersecurity;
- Interview with Partner's representative;
- Research outcomes and recommendations;
- Advertisement of a firm, product or an event (graphical);
- Promotional materials regarding a cybersecurity conference / event (invitation, advertisement – graphical).

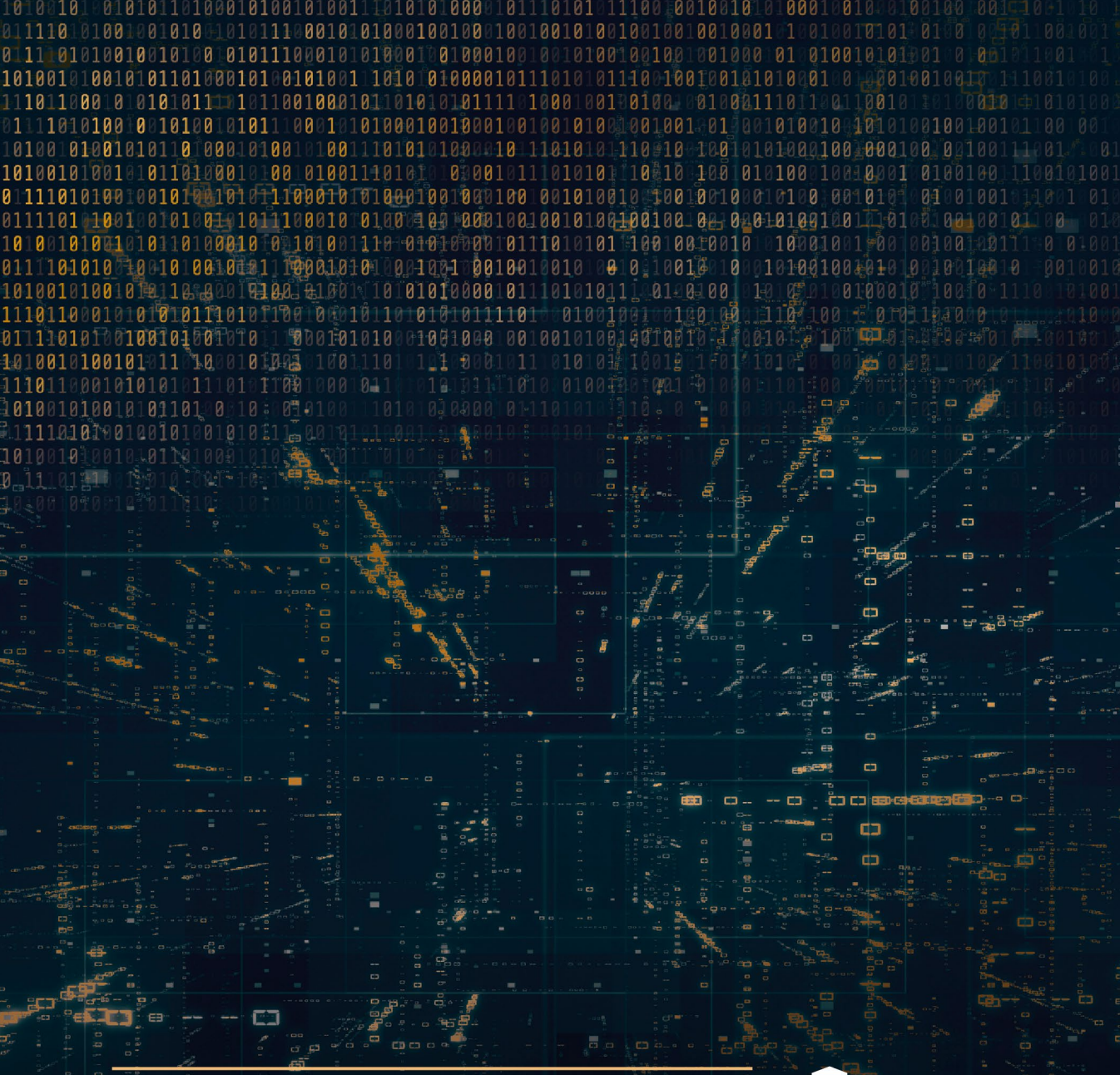
Do you want to share your opinion on national or European policies regarding cybersecurity? Do you want to publish outcomes of your research? Do you want to advertise?

The European Cybersecurity Journal is the right place to do it!

Prices of contribution

	PRICE (EUR)
Written contribution *Analyses, Opinions, Policy Reviews, Interviews, Research Outcomes*	100 / 1 page
Graphic contribution *Advertisement*	200 / 1 page
Graphic contribution *Advertisement*	350 / centerfold (2 pages)
Graphic contribution *Promotional campaign of an event*	250 / 1 page
Written contribution *Promotional campaign of an event*	400 / centerfold (2 pages)

CONTACT US: editor@cybersecforum.eu



The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship project in the field of cybersecurity, within which the CYBERSEC Forum is organized.

We invite you to follow our initiatives and get involved.

THE KOSCIUSZKO INSTITUTE
is the publisher of
European Cybersecurity Journal