

VOLUME 6 (2020) ISSUE 1

European Cybersecurity Journal

Strategic perspectives on cybersecurity
management and public policies

Addressing specific
Requirements for
Cybersecurity in the
Smart Grids at EU level

Designing Digital Safety
into the Smart City

The Technological
Sovereignty Dilemma –
and How New Technology
Can Offer a Way Out

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.

Editorial Board

Chief Editor:

Barbara Sztokfisz – CYBERSEC Programme Director, the Kosciuszko Institute

Executive Editors:

Faustine Felici – CYBERSEC Project Manager, the Kosciuszko Institute

Michał Rekowski – Strategic Partnerships Manager, the Kosciuszko Institute

Honorary Members Of The Editorial Board:

Dr James Andrew Lewis – Director and Senior Fellow of the Strategic Technologies Program, Center for Strategic and International Studies (CSIS)

Dr Joanna Świątkowska – Programme Director, European Cybersecurity Forum – CYBERSEC; Senior Fellow, the Kosciuszko Institute

Members Of The Editorial Board:

Alexander Klimburg – Director, Global Commission on the Stability of Cyberspace Initiative and Secretariat; Director, Cyber Policy and Resilience Program, The Hague Centre for Strategic Studies

Helena Raud – Member of the Board, European Cybersecurity Initiative

Keir Giles – Director, Conflict Studies Research Centre (CSRC)

Associate Editors:

Izabela Albrycht – Chairperson, the Kosciuszko Institute

Marta Przywała – Non-resident Research Fellow, the Kosciuszko Institute

Design & DTP:

Joanna Świerad-Solińska

Proofreading:

Adam Ladziński

ISSN: 2450-21113

Citations: This journal should be cited as follows: "European Cybersecurity Journal" Volume 6 (2020) Issue 1, 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

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute. Authors may have consulting or other business relationships with the companies they discuss.

© 2020 The Kosciuszko Institute

All rights reserved. The publication, in whole or in part, may not be copied, reproduced, nor transmitted in any way without the written permission of the publisher.

Contents

4

Togo's National Approach to Cybersecurity.
Interview with
Cina Lawson

12

Addressing Specific Requirements for Cybersecurity in the Smart Grids at EU Level
Stephan Lechner, Manuel Sanchez, Michaela Kollau

24

The Technological Sovereignty Dilemma - and How New Technology Can Offer a Way Out
Luukas Ilves & Anna Maria Osula

36

Designing Digital Safety into the Smart City
Robert Muggah

44

Multi-level Governance in Cybersecurity: What Role for the European Regions?
Milda Kaklauskaitė

52

Boosting the Role of Women in Cybersecurity.
Interview with
Nicole Wajer

57

Insider Threats in Cybersecurity: The Enemy within the Gates
Guerrino Mazzarolo & Anca D. Jurcut

64

Back to the Civilian Power Discourse: Can it Survive in Cyberspace?
Omree Wechsler

76

Piercing the Bubble with a Cyber Needle - Cyber Tools Application during a Possible Baltic States Defence Scenario
Dominik Skokowski

Editorial



Barbara Sztokfisz

**Chief Editor of the European
Cybersecurity Journal**

Dear Readers,

We are now at a decisive moment in European history. The election of a new European Parliament along with the appointment of a European Commission with a “geo-

political approach” opens grand development opportunities for the Union that strives for more. Digital matters are very high on the EU agenda and their security dimension should receive particular care. If we want to enjoy a future based on a peaceful and secure world order, we need to establish a peaceful and secure cyberspace. It needs to be based on trust, multi-stakeholder and multi-institutional cooperation.

We can already say that the year 2020 will mark milestones in this respect, in light of the digital agenda of the EU institutions aiming to adopt a set of new regulations and therefore, serve as an example for the rest of the world. We gladly welcomed the new digital strategy launched by the European Commission – Shaping Europe’s digital future – which is set to address key digital policy issues over the next five years. We strongly believe that EU countries can lead by example and show in their actions that ensuring an ethical development of technology, one that will serve the people and empower them, is absolutely necessary for a further inclusive digital transformation.

Through the CYBERSEC leitmotif – **Securing the World’s Digital DNA** – we are promoting an approach that puts the security aspects at the very core of the creation and the further development of our digital world. Because it is only by embracing cybersecurity that we will ensure resiliency and prosperity, now and in the future.

Securing the World’s Digital DNA is our shared responsibility.

I sincerely hope that this issue will contribute to our common goal of increasing awareness on the cybersecurity matters and promoting stable growth across cyberspace.

Enjoy the read!

Barbara Sztokfisz

SAVE THE DATE
FOR THE

6th

EDITION
OF CYBERSEC

CYBERSEC CEE

#CSCEE20

SPODEK, KATOWICE
3-5 NOVEMBER 2020

INTERNET
GOVERNANCE
FORUM

#IGF2020

MCK, KATOWICE
2-6 NOVEMBER 2020

@CYBERSECEU



www.cybersecforum.eu



Togo's National Approach to Cybersecurity

Interview with Cina Lawson, Minister of Posts, Digital Economy, and Technological Innovation of Togo

Madam Minister, thank you very much for accepting this interview and taking the time to talk with us about Togo's national approach to cybersecurity, it is an honour. As we enter a new decade, the pace of digital development will surely increase further, along with the landscape of cyberthreats. What are the biggest challenges Togo is facing nowadays in terms of cybersecurity and why is it a priority for the Togolese government to reinforce its cyberdefences?

It is a pleasure to speak to the *European Cybersecurity Journal* Team. Thank you for having me.

Africa is experiencing a boom in digital development, especially with regard to mobile penetration rates, access to the internet and acceptance of mobile payments. Togolese citizens increasingly have access to high-speed internet thanks to the rapid expansion of 3G and 4G networks across the country. Togo's internet penetration rate reached 61% in 2019, compared to barely 13% five years ago. Connectivity prices have also fallen over the same period as we continue to extend high-speed fixed and mobile internet across the country.

Consequently, more of our population can now reap the benefits of opportunities that the digital economy provides, including better communications, improved access to information online, and novel opportunities for business, including e-commerce.

One of the missions of the Togolese Government is to quickly deploy the required digital infrastructure across the country which will then allow us to provide services and solutions that will change people's lives for the better. We want to take advantage of the explosion in the use of mobile phones to create value in the lives of the entire population, particularly for the most excluded and disadvantaged people. At the Ministry of Posts, Digital Economy and Technological Innovation in Togo, I am fully dedicated to the monumental task of reaching this goal.

Indeed, under the leadership of HE Faure Essozimna Gnassingbé, the government has set out on National Development Plan (NDP) which aims to transform Togo into a logistics and services hub. Guaranteeing national digital sovereignty, particularly cybersecurity and the protection of citizens,

underpins our policy. As our digital economy develops, we need to put mechanisms in place to ensure that our citizens, companies, public institutions, and critical infrastructure are protected from cybercrime and other threats in cyberspace.

Shoring up our cybersecurity is therefore a matter of urgency, an obligation that we have to our people and to the investors who contribute to our economy by setting up their ventures here. Togo is also an important financial hub as several subregional financial institutions, such as the Central Bank of West African States, are based in the capital, Lomé. Therefore, boosting the legal and regulatory framework for cybersecurity at the national level is a critical economic objective.

We therefore set out to work on setting up the requisite framework which led to the adoption of Law No. 2018-026 of 7 December 2018 on Cybersecurity and the fight against cybercrime. This is a significant piece of legislation which finally provides Togo with a coherent strategy to monitor and defend against cyberthreats at the national level. In addition, it equips the national criminal justice system with the means to prosecute offences committed by cybercriminals.

Perhaps most importantly, the legislation instituted Togo's National Cybersecurity Agency (Agence nationale de la cyber-sécurité, ANCy) which is the national authority in charge of security of information systems and contributes to the definition and implementation of the national cybersecurity strategy. However, we neither have the necessary skills and nor want to create just another administrative body. Our focus was on achieving the vision to quickly establish an operational arm in charge of analysis, response, and remediation to cyberattacks. This is the main reason we adopted the PPP model, a point I will come back to.

In addition to the cybersecurity law and associated decree creating ANCy, we also passed a decree defining what we consider to be Essential Service Operators (ESO). ESOs operate critical infrastructure such as the port, airports, electricity grid, security services, public administration and the like, which the state considers fundamental to

the social order and the smooth functioning of the economy. Accordingly, the ESOs are obliged by law to have a certain level of maturity in their cyberdefences to protect themselves and infrastructure from cyberthreats.

Guaranteeing national digital sovereignty, particularly cybersecurity and the protection of citizens, underpins our policy. As our digital economy develops, we need to put mechanisms in place to ensure that our citizens, companies, public institutions, and critical infrastructure are protected from cybercrime and other threats in cyberspace.

Furthermore, Togo is committed to contributing to the continental effort to boost cybersecurity. In 2019, Togo became a signatory to the African Union Malabo Convention on Cyber Security and Personal Data Protection, which was adopted by the bloc in 2014. We therefore have an obligation as an AU member state to follow through with setting up the legislation, institutions, and infrastructure to enable ratification of this convention.

This is especially pertinent for Togo's integration in the era of the agreement on African Continental Free Trade Area (AfCFTA), which is expected to see a rapid rise in international trade between African countries, including via e-commerce.

Bearing these points in mind, it is obvious why we need to do handle cybersecurity systematically as a matter of urgency because just as you rightly hinted, with rapid advancement of and deepening reliance on digital technologies across all economic and social sectors, the stakes and sophistication of cybercrime are increasing daily.

In recent years, Togo showed a strong willingness to reinforce its position in cyberspace. What other steps are you taking – be it in terms of legislation or regarding other institutional frameworks – to boost Togo's cybersecurity level and cyber defences?

In addition to setting the legal foundation for cybersecurity, in 2019, the Togolese Government passed the law No. 2019-014 of 29 October 2019

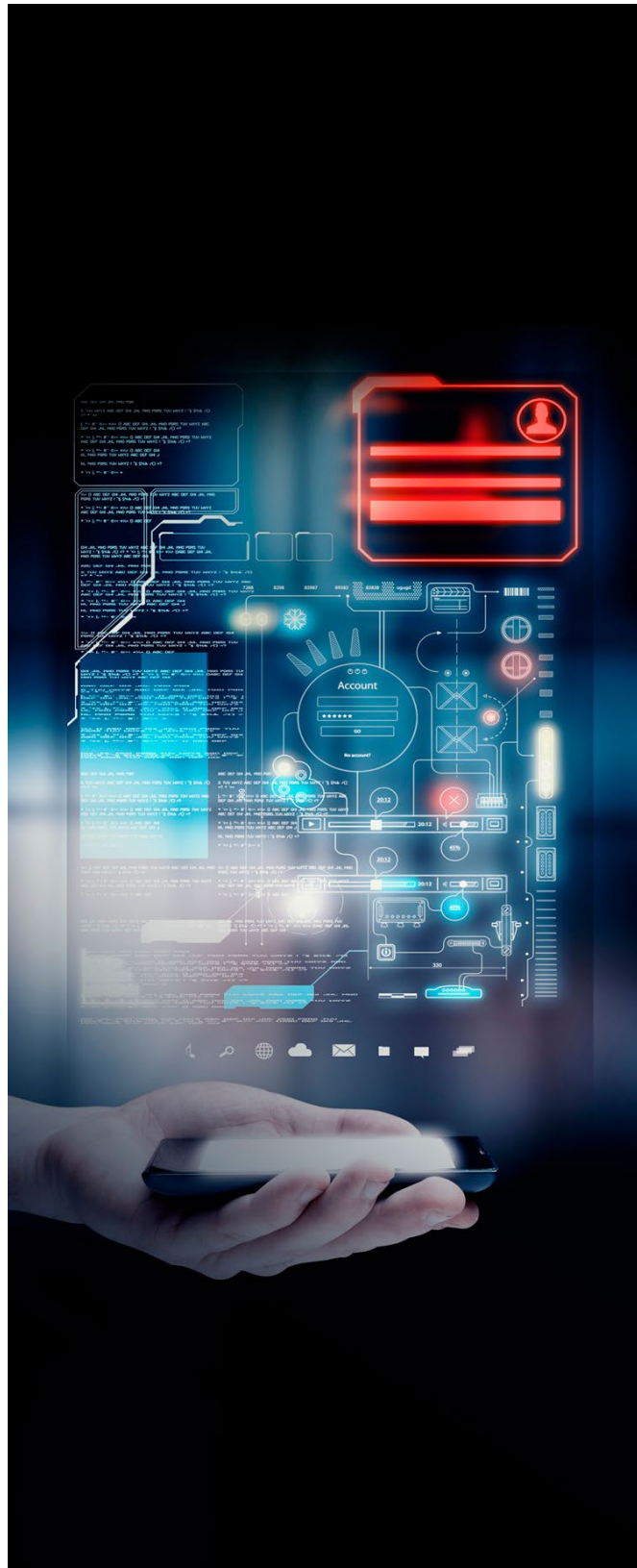
on the protection of personal data. This legislation confers every Togolese with the right to the protection of their personal data.

The data landscape has become incredibly complex since the early days of the internet. With the emergence of data-driven technologies such as artificial intelligence and big data analytics, we need to make sure that people’s personal data are processed, transmitted, and stored according to a set of standards that ensure data security, privacy, and trust. As digital platforms continue to make our societies more productive, people will continue to trust these platforms with their data. However, we need to make sure that people’s sensitive data are adequately protected from exploitation and misuse.

The Togolese law on protection of personal data, which is the first big step in our quest to guarantee data protection rights to citizens, will evolve in response to emerging needs and technologies. The legislation also established the Authority for the Personal Data Protection (Instance de protection des données à caractère personnel, IPDCP) to enforce compliance. It supports the underlying objective of developing our cyberdefences, which is to breed trust among users in the cyberspace to protect businesses, public agencies, and citizens.

In 2019, the Government of Togo established a public-private partnership with Assec Data Systems in order to create the first-of-its-kind institution responsible for cybersecurity in Togo, called “Cyber Defense Africa”. What is the purpose of Cyber Defense Africa and what makes it so unique?

In searching for a way to address these urgent cybersecurity needs, we needed to make sure that our approach guaranteed a high quality of service without it being prohibitively expensive to set up and operate. To be able to fully carry out its operational functions, the National Cybersecurity Agency (ANCy) was required by law to rapidly establish the necessary technical framework for the constant monitoring and implementation of proactive defence mechanisms in response to attacks.



Our joint venture with Asseco to create Cyber Defense Africa (CDA) was a direct response to our urgent need to establish this technical framework serving the operational arms of the ANCy. CDA's mandate is to build and operate this technical framework comprising a Computer Emergency Response Team (CERT) and a Security Operations Centre (SOC).

The CERT is offered as a predominantly free service to the public. Its work will alert the population of vulnerabilities and sensitise the public on how to protect against attacks. The CERT will also provide key information about patches to identified vulnerabilities. The SOC, on the other hand, is a paid end-to-end service which provides bespoke cybersecurity-as-a-service geared at the ESOs, businesses, public institutions, and other interested parties.

Our partnership with Asseco on CDA also allows us to not only mitigate the issue of finding the expertise to run this technical framework but also develop our local capacities to manage cybersecurity infrastructure. With both a CERT and SOC in its arsenal, CDA will be Togo's first line of defence against a host of cyberthreats such as phishing, ransomware attacks, denial of service (DDoS), spearfishing, etc.

Achieving a high quality of service requires a team of experts with several years of experience in the field. However, the lack of personnel in cybersecurity is a global issue. Several reports studying the issue have highlighted a lack of skilled personnel as a top concern – even more so than the lack of resources to carry out their jobs efficiently.

Togo, like many other African countries, is not spared by this global challenge. We do not yet have a local pool of cybersecurity professionals large and robust enough for our needs. Outsourcing has thus become a prevalent way for organisations in Africa to meet their cybersecurity needs. Unsurprisingly, one report conducted by analysts from Dataprotect, a Morocco-based data security firm, indicates that 55% of African financial institutions outsource their cybersecurity needs.

Furthermore, following an internal study of the experiences other African countries had when setting up CERTs and SOCs, we realised that the process typically took at least two to three years. We also observed that a lack of technical skills and appropriate procedures undermined the systems' effectiveness among the few countries that had attempted it.

Given our urgent need to make our newly established ANCy operational in the shortest possible time, we adopted a systematic approach, supported by legal and technical advisers, to find the best way to circumvent the challenges faced in other countries. It became clear to us that partnering with an established private sector player would be the best way to address our cybersecurity needs.

CDA is unique in that it combines the CERT with a national SOC, which immediately gives it economies of scale and synergies.

This eventually led to our unique partnership with Asseco, a leading Polish IT firm – sixth largest software producer in Europe – with operational expertise in cyberspace protection, to set up a joint venture called Cyber Defense Africa (CDA). Not only was this partnership to develop both the national CERT and SOC done in record time, it will also ensure that our needs are met effectively and at scale.

CDA is unique in that it combines the CERT with a national SOC, which immediately gives it economies of scale and synergies. It is unique because Asseco is not only a technical partner but also an investor in the joint venture. This is to ensure that the joint venture is operated efficiently and profitably.

In your opinion, what are the advantages of running a public-private cooperation in the field of cybersecurity?

This brings me back to my earlier point about the main reason we entered into a PPP model. Partnering with Asseco allows us to bring in experts with years of experience in this field to respond

adequately to our cybersecurity needs. Our role as government is to work on the institutional, legal, and regulatory framework to ensure that all stakeholders in the sector play their part to guarantee cyberdefence and set up enforcement mechanisms to fight against cybercrime.

With cybersecurity, we needed to get it right the first time because doing otherwise could be catastrophic for our national security. Inking a public-private partnership grants two key benefits: 1) high quality of service, and 2) sustainability.

The joint venture allows us to deliver a service with exceptional quality and performance right from the start. Quality of service is intrinsically linked to the profitability of this joint venture. The model devised with CDA places it in the position to provide the CERT as a mostly free service to the public and to provide the SOC service which is the main source of revenue ensuring the venture's sustainability.

We have positioned CDA to provide these services locally and with Asseco as a partner the company will serve businesses and public agencies with comprehensive solutions, specific to their respective sectors, to protect them from data breaches, phishing, ransomware attacks, and a host of other cyberthreats – and at competitive rates.

Cyber Defense Africa is designed to be a self-sustaining venture to serve Togo's needs as its digital economy evolves over a long time.

We do not yet have enough human resources locally to build and run this kind of service at the quality and at scale that we desire. But bringing in Asseco, with its proven track record of providing world-class IT software solutions and cybersecurity to clients around the world, will help build the local capacity we need.

As Cyber Defense Africa operates in Togo and builds its portfolio of subregional clients, we expect that local capacities in this all-important field will improve. It is noteworthy to mention that all the technical stuff of CDA are Togolese who are undergoing training according to stringent global standards as part of a deliberate knowledge and technology transfer programme.

Our ambition is for it to become a world-class centre of excellence for cybersecurity professionals in Africa. Cyber Defense Africa will be a centre of training for IT staff and non-IT personnel of its clients. In addition, CDA will embark on a civic education mission to instil the culture of security in our youth by holding workshops and seminars for students, young professionals, and officials, which should encourage young people to take up a career in cybersecurity.

Do you believe the innovative approach enshrined in the Cyber Defense Africa project can serve as an example – and maybe even a motivating force – for neighbouring countries which want to build or boost their cybersecurity? Would you say that Togo has a regional ambition in this field?

Absolutely! We believe that our approach to cybersecurity can be a model for other countries, especially for small countries that need to build cyberdefence capabilities at a rapid pace, at scale, and at a reasonable cost.

Through partnering with Asseco to establish CDA, we have been able to equip the country with an effective national Computer Emergency Response Team (CERT) and Security Operations Centre (SOC).

The national legislation on cybersecurity requires that companies demonstrate that they have taken adequate measures for cybersecurity within their organisations. The value proposition of signing up for CDA's SOC service is that it is an all-in-one solution at a fraction of what it would cost should they set up a dedicated cybersecurity team. The SOC carries out uninterrupted monitoring, real-time analysis of threats, proactive alerts, and the responses to cyberattacks.

From a regional standpoint, our plan is to nurture cybersecurity experts in Togo who can eventually work within organisations in other countries. Africa will need professionals in this field to staff CERTs and agencies providing cybersecurity services. Many African countries are drafting legislation and setting up cyberdefence infrastructure so it is only a matter of time before demand for experts in cybersecurity reaches sky-high levels.

We want to be ready with the supply of expertise when the time comes. We have a lot to learn from our partners in more developed markets, who have been doing this for years. Through cooperation and exchange with them, I think we will be able to grow our continent's capacity for cybersecurity which will in turn serve our local cyberdefence interests in the near future.

Your portfolio includes, among others, digital economy. What is the potential of e-services development in Togo and what assessment do you make of its possible impact on Togolese economic growth?

Togo may be a small country, but we have big ambitions for leveraging a diverse mix of digital innovations to address our local challenges. E-services result in significant benefits for social and economic development. They are a powerful tool to reduce poverty and improve social inclusion. In Togo, we have implemented digital interventions such as AgriPME – a mobile wallet solution which has facilitated the distribution of government subsidies to 250,000 vulnerable farmers towards the purchase of fertiliser; and ECO CCP – a pioneering interest-bearing mobile savings account aimed at the unbanked segment of the population. These are just two of several initiatives we are adopting in Togo to improve the livelihoods of our population. We are resolute in our objective to harness digital solutions to improve all aspects of Togolese society and the economy. This position underpins our sectoral policy for the 2018–2022 period and is the centrepiece of our National Development Plan.

Also, e-services development improves the business environment making our country more attractive to investment. Thanks in no small part to the digitisation of various processes such as starting a business or filing corporate and income taxes, Togo climbed up 40 places on the World Bank's Doing Business 2020 rankings and is now ranked among the Top 5 countries in Africa and Top 100 in the world for the ease of doing business.

Further, developing e-services has the strong potential to create stable jobs for our burgeoning youth population. There is good local demand for people with IT skills to not only build but also

operate the digital platforms that will revolutionise public service delivery. We have also committed to promoting the emergence of a dynamic business processing and outsourcing (BPO) industry which will create further job opportunities for Togolese.

In parallel, we aim to revolutionise our education systems by expanding high-speed internet access to public schools and hospitals. We continue our work to improve the efficiency of public administration by digitising a host of procedures. We will also launch a new national digital identification platform this year which will grant every Togolese a unique ID to improve their access to social and financial services provided by both the state and private service providers.

However, the reach and impact of any digital service is dependent on the deployment of sound digital infrastructure. Our plan is to accelerate and expand investments in digital infrastructure, particularly to improve access to high-speed internet across the country. Togo currently has an internet penetration rate of 61%. This effectively means that digital solutions that require internet access can theoretically reach just around half of the population. We need to ensure that we improve broadband availability across the country to increase the number of people who can benefit from all the interventions we have made and those to come.

Finally, a question regarding technological innovation which is also part of your portfolio. According to the UK's Intellectual Property Office, Togo is the world leader in terms of women inventors, with an impressive 57.14% of patent filers being women. Do you see the same enthusiasm and involvement of women in the technological and IT innovation field? How to further encourage women and girls to engage in cybersecurity?

As the report by the UK's Intellectual Property Office shows, Togolese women are doing a lot when it comes to invention and innovation. We were absolutely delighted to find out that Togo has set this record as the country with the highest proportion of women inventors in the world.

I am reminded of the illustrious days of the industrious market women of Togo during the second half of the 20th century. They were incredibly successful entrepreneurs who ruled the African trade at a time when the Lomé marketplace was a hot-spot. These women were so wealthy that they were the few in the country who could afford luxury Mercedes Benz cars earning them the name “Nana Benz”. The legacy of the Nana Benz is present in Togolese women today. We need to bring back those good old days but within the context of the digital age through encouraging more women to be involved in IT and innovation. Togolese women have immense potential to propel our innovation ecosystem to the heights we are aiming for.

While the report is great news for us, it also reminds us that we need to do more to unleash this potential. In Togo, our aim is to create an ecosystem that fosters innovation by providing young people with the skills and tools they need to be able to fully express their creativity. Our hope is that these young people can turn innovative ideas into viable businesses that address local challenges, serve the needs of their communities, and bring prosperity.

We need to improve the availability of the right resources, create adequate spaces and support for women and men to enable them to express their creativity and innovation to solve local challenges.

We need to bring back those good old days but within the context of the digital age through encouraging more women to be involved in IT and innovation. Togolese women have immense potential to propel our innovation ecosystem to the heights we are aiming for.

One way we are contributing in this area is through the Djanta Tech Hub project set to be launched in 2020. Djanta Tech Hub is a 3000 sq. metre technology hub located in the heart of Lomé, initiated by the Togolese government in partnership with private sector partners. Djanta aspires to become French-speaking Africa’s largest hub with supraregional reach in four specialist areas: fintech, e-government, impact tech



(agriculture, health, renewable energy), and logistics. The aim is to incubate digital initiatives that have the potential to positively disrupt key economic sectors. Women need to be part of leading the country to find solutions that address our societal and economic needs. That is why the Djanta Tech Hub will also have a dedicated space we are calling “NanaTech Hub”, which will provide women and girls with tailored programmes for training, mentorship, placement, and entrepreneurial support. We want to provide all the support we can to ensure that the Tech Hub also produces women founders of world-class start-ups that receive funding from the world’s most respected venture capitalists.



In 2019, the African startup ecosystem attracted a record amount of venture capital investment. However, over 80% of the recipient startups were made up of all-male founding teams. This shows that we have more to do on a continental level to foster the emergence of successful female tech entrepreneurs.

Recalling the Nana Benz era of Togo, we hope to incite the emergence of the NanaTech of Togo who will join Africa's growing pool of female tech entrepreneurs and we believe that the NanaTech Hub within Djanta should be a part of that story. ■

Questions by Faustine Felici

Cina Lawson is Minister of Posts, Digital Economy, and Technological Innovation of Togo. Drawing from her over 15 years of experience and expertise in telecommunications policy and regulation, she is leading Togo through a profound transition to an inclusive digital economy. Lawson began her career at the World Bank in Washington, DC where she worked on telecom restructuring projects in developing countries focusing on regulatory reforms. She went on to become a Manager of Corporate Strategy and Business Development at the Orange Group in New York City, and later at Alcatel-Lucent in Paris. Her initiatives as minister have included diversifying private participation in the telecoms sector, spearheading regulatory reforms for data protection and electronic transactions, setting up an innovation hub as well as pushing for the deployment of high-speed fibre broadband to link key institutions, including all public universities in the country. In 2012, Forbes magazine ranked her among the 20 most powerful young women in Africa and in 2019, Lawson became the first African woman political figure to receive the Harvard Alumni Public Service Award. She is a fervent advocate of innovative solutions to Africa's developmental challenges and sits on the advisory board of the Digital Identity, Trade and Economy Initiative of the United Nations Economic Commission for Africa. She is a graduate of Harvard University's Kennedy School of Government and Sciences Po Paris.

Addressing Specific Requirements for Cybersecurity in the Smart Grids at EU Level

STEPHAN LECHNER*

DIRECTOR, EURATOM SAFEGUARDS, DIRECTORATE-GENERAL FOR ENERGY, EUROPEAN COMMISSION

MANUEL SANCHEZ**

TEAM LEADER FOR SMART GRIDS, DIRECTORATE-GENERAL FOR ENERGY, EUROPEAN COMMISSION

MICHAELA KOLLAU**

POLICY OFFICER, DIRECTORATE-GENERAL FOR ENERGY, EUROPEAN COMMISSION

* European Commission, Directorate General for Energy, Luxembourg, Luxembourg

** European Commission, Directorate General for Energy, Brussels, Belgium

Introduction

The energy infrastructure is one of the most critical assets for modern society. Its effective operation is a pre-condition for securing energy supply to a wide range of economic and social activities and thus enables societal welfare and stability. The energy infrastructure is generally characterised by numerous interdependencies and a high level of complexity. Due to the overarching need to tackle climate change and the necessary transition to a low-carbon economy as well as the rapidly increasing digitalisation, the energy sector of today is undergoing a very rapid transformation in terms of infrastructure and market functioning, but also because of the active participation by citizens as consumers and decentralised producers of energy.

Traditional energy technologies, which are historically composed of control systems specifically tailored to operate the physical networks, are being more and more connected to modern digital technologies and components. The advancing digitalisation offers new opportunities but also creates new risks. It makes the energy system smart and enables consumers to participate actively in the energy market and to better benefit from the energy services. At the same time, it creates an increasing exposure to cyberattacks, jeopardising the security of energy supply or the data privacy of consumers.

The European energy sector is characterised by numerous physical interconnections in electricity, gas, and oil and is increasingly witnessing electricity and gas market coupling. In view of such increased interdependencies, new threats related to cybersecurity are likely to gain another dimension. The cascading effects that can be the consequence of a cyberattack may potentially not only affect several sectors in one Member State but also produce considerable damage across critical infrastructures and energy sectors in a number of Member States as well as beyond EU borders.

The power grid is the basis of our modern economy and society. It serves hundreds of millions of consumers, but its basic operational architecture is still broadly the same as it was

a century ago. Its layout goes stepwise from the producer to the consumer, foreseeing power generation, transmission, and distribution. Original operational elements such as cables, transformers, substations, and circuit breakers are still at the heart of the grid.

The rise of decentralised power generation, mainly from renewable energy sources, has now forced this grid to become “smarter”. However, the operational technology for conducting electricity still prevails. Making the grid smarter therefore primarily means adding digital technologies to the *control* levels of the grid, while mostly maintaining its existing operational technology.

As anywhere, digital technologies require thorough cybersecurity, but standard cybersecurity concepts will not necessarily be applicable everywhere in the smart grid. The grid’s traditional operational technology might simply not be suitable for the introduction of such measures. In addition, its particular architecture and its need to combine legacy technologies with the Internet of Things serve to increase the cyber risk.

Due to the high degree of interconnectivity in the EU power grid, cybersecurity issues are better addressed by collaboration at EU level than at national level alone.

Materials and methods

LEGISLATIVE ANALYSIS IN THE ENERGY SECTOR

After the European energy crisis in winter 2014/2015, the European Commission increased its activities to improve energy security all across the EU. The Energy Union Strategy [1], adopted by the European Commission in 2015, specified that security is an indispensable feature of the energy system of the future. Being aware of upcoming cyberthreats, the European Commission created an Energy Expert Cyber Security Platform (EECSP) in November 2015 with the purpose of analysing the specific needs of the energy sector in terms of cybersecurity. The EECSP issued its final report [2] in February 2017, suggesting a cybersecurity framework for energy and providing generic considerations.

Based on the findings of the EECSP and following the legislative proposal on risk preparedness in the electricity sector [3], the European Commission set up a Stakeholder Working Group in spring 2017 under the Smart Grids Task Force to focus on practical approaches and solutions to improve the energy network resilience, including cyber resilience. This group presented its findings in a report at the end of 2018, and its recommendations will be the basis for preparatory works on a future network code on energy-specific cybersecurity as defined in the recast of the electricity Regulation 2019/942 [4], under the Clean Energy package.

CYBERSECURITY STRATEGY REVIEW

The European Commission also considered energy-specific aspects of the topic when revising the EU Cyber Security Strategy of 2013 [5]. The European Commission services found few Member States with a structured, energy-specific approach to cybersecurity, one example being Austria, with an established Energy CERT [6]. Although there is a general acknowledgement that the power grid is at the basis of our modern economy and society, there have been hardly any specific political considerations about its need for cybersecurity. To increase awareness among the Member States about these issues, the European Commission included references to sector-specific considerations in its cybersecurity package of September 2017 [7].

INTERNATIONAL DISCUSSION

In May 2017, the European Commission held a *High Level Roundtable on Main Challenges for Cyber Security in the Energy System* on occasion of the 60th anniversary of the European Treaties during the Digital Day in Rome. More than 50 selected experts and top managers from the energy sector attending the conference confirmed the increasing importance of cybersecurity and underlined the necessity for European guidance in the conference conclusions [8].

Also in 2017, the G7 countries held a ministerial meeting dedicated to energy security in Rome, and agreed to continue discussions on different concepts of cybersecurity strategies in the energy

sector [9]. The European Commission services participated in a follow-up expert meeting of the G7 countries later the same year to ensure a good understanding of the global challenges for cybersecurity in the energy sector. Further, the European Commission participated with an EU-team at a G7 cybersecurity hands-on exercise focusing on the energy sector in Canada 2019.

TECHNICAL ANALYSIS

After an internal technical analysis, the European Commission services initially suggested two main specific properties of power grid for particular attention when discussing its cybersecurity.

One is that real-time performance requirements of the power grid's operational technology do not allow for overhead as implied by standard cybersecurity solutions, and the other is the speed with which the impact of a successful attack on energy security can spread due to cascading effects in the operational technologies.

When looking into the associated risks in detail, a third specific issue emerged from the spread of technologies in the smart grid. The classical power grid contains technology components with a lifetime of 30–50 years, while the smart grid requires introducing new paradigms (and connecting new devices) from the Internet of Things (IoT). The specific difference between legacy and emerging technologies increases the cybersecurity risk in the power grid.

STAKEHOLDER HEARINGS

In early 2018, the European Commission services summarised these three identified main strands of energy specific requirements in cybersecurity and sent short overview papers with associated questions to stakeholders. The intention was to understand if the energy and cybersecurity communities in the European Union would support the respective findings, challenge them, or complement them with additional issues. In addition, for each stakeholder group the catalogue of questions contained the possibility to express their particular requirements and priorities. In February 2018, the European Commission services collected the replies and held hearings with representatives

from the contacted stakeholders' groups to discuss and aggregate the answers. Hearings included European energy associations of electricity transmission network operators (ENTSO-E), gas transmission network operators (ENTSO-G), and distribution network operators (EDSO for Smart Grids, Eurelectric, GEODE, and CEDEC).

In addition, the European Commission services had a hearing with dedicated cybersecurity stakeholders at the EU level, i.e. with the European Network and Information Security Agency ENISA and with the public-private-partnership project of the European Cyber Security Organisation (ECISO).

The final hearing addressed the European Agency of Energy Regulators (ACER).

Recent stakeholders' hearings broadly confirmed three main areas of specific attention for cybersecurity in the energy sector: real-time effects, cascading effects and the mix of legacy technology with the IoT (Internet of Things).

The stakeholders' hearings broadly confirmed three main areas of specific attention for cybersecurity in the energy sector: real-time effects, cascading effects, and the mix of legacy technology with the IoT. One association suggested cyber-physical effects as a fourth element, but during the following discussion this proposal, from an energy security perspective, showed significant overlap with the area of cascading effects and was therefore not maintained as a stand-alone element during the initial considerations.

EU MEMBER STATES INVOLVEMENT

To link the activities on energy-specific cybersecurity requirements to the ongoing co-ordination on the implementation of the Network and Information Security (NIS) Directive [10], the European Commission suggested a dedicated work stream in the NIS co-operation group of the EU Member States. The NIS co-operation group established this work stream successfully with the first meeting in June 2018, and confirmed the need for EU guidance.

DEFINITION OF MITIGATION MEASURES

To further elaborate on technical mitigation and guidance on the three identified specificities, the European Commission tasked a working group of the Council for Economic Co-operation (Fr. *Conseil de Coopération Economique*, CCE), a think tank under the patronage of the governments of Spain, France, Italy, and Portugal, to provide technical input. The members of the working group were all subject matter experts, originating from energy operators and technology suppliers to assure the required sector-specific knowledge. The CCE issued an internal report to the European Commission in mid-2018, which in connection with the output of other expert groups served as the basis for further work. The European Commission services organised a review for applicability and correctness of the main CCE working group results by the cybersecurity experts of the European Commission's JRC (Joint Research Centre). The JRC broadly confirmed the effectiveness of the recommended mitigation measures.

Results

The following sections are describing the three main strands of specific energy-sector cybersecurity requirements in more detail, focusing on the power grid. Detailed mitigation measures are not the subject of this section, but have been communicated by the European Commission [11] and might be part of future activities by the European Commission, providing EU-wide guidance cybersecurity in the energy sector.

TECHNICAL FINDINGS

Real-time requirements

Some operational technology (OT) components of the power grid (e.g. circuit breakers, turbine and generator protections) need to react in milliseconds and have a specific design to guarantee the timely execution of their function, thereby preventing damage from the grid. Their communication protocols foresee limited or no security, as the components typically were operated in a protected environment and did not have any network connection to the outside world.

With the introduction of connected control systems and with the need to balance distributed generation and consumption all across the smart grid, the degree of isolation of sensitive real-time components in the power grid has been gradually decreasing. This has exposed real-time OT components to a cybersecurity risk, but the usual security mechanisms do not necessarily work for them. To verify authenticity and integrity of a sensitive command before executing it, other IT environments are using checksums, encryption algorithms, or challenge-response protocols. All of these standard security measures usually require computing time in the range of some tens of milliseconds when executed by commercially available components. As a real-time OT component needs to react almost immediately, its performance needs do not leave any room for computing security checks. The time constraint for tele-protection between substations can go down to 10 milliseconds, and peer-to-peer messages inside a substation, replacing hard wire, can go down to 4 milliseconds. Such real-time requirements clearly make the introduction of any additional standard security function unfeasible.

Cascading effects

There is a high degree of interconnectedness of electricity grids and gas pipelines across Europe and well beyond EU Member States. A cyberattack causing an outage in one part of the energy sector therefore might trigger far-reaching cascading effects into other parts. Especially the stability of a national power grid may depend on the integrity of the entire electricity grid in the neighbouring countries and beyond. A sudden failure of a single element in a power grid can induce a domino effect, leading to blackouts in large parts of the grid. Such cascading effects already led to cross-border blackouts in the US and Canada on 14 August 2003, in Sweden and Denmark on 24 September 2003 and in parts of Germany, France, Belgium, Italy, Austria, and Spain on 4 November 2006. In contrast to other environments, where a successful cybersecurity attack might create mostly local damage or disruptions, the cascading effects in the power grid are immediate and can be very far-reaching.

The “Nine-Substation-Problem” [12], based on a 2014 report by the US FERC (Federal Energy Regulatory Commission), claims that a destruction of only 9 of the 55.000 substations in the US could bring down the power grid in the whole country. This increases the potential impact of cyberattacks, which can physically damage grid components, as shown by the infamous Stuxnet worm discovered in 2010, or by the Aurora attack demonstrated in the Idaho National Laboratories in 2007.

Legacy technology combined with the Internet of Things

The energy sector of today is composed of two different types of infrastructure. On the one hand, there is the OT (operational technology) infrastructure, partly originating from a time well before cybersecurity considerations came into play and having a lifetime of 30–60 years. These legacy systems are not only about analogue technology but also – and more importantly – about digital technology designed prior to cybersecurity requirements. On the other hand, there are more and more recent IT (information technologies) connected to the basic OT infrastructure. These new technologies add greater flexibility, accommodate distributed energy resources, and thus help adapt to the changing energy market environment. The digital revolution enables new services and business models for operators and serves, at the same time ensuring higher reliability and security of supply. However, the number of devices from the IoT in the energy sector is growing rapidly, which creates an increased cybersecurity risk.

Traditional grid security concepts that assume limited external connectivity are no longer sufficient. Consumers can connect arbitrary smart controls to the grid. Smart home products are not subject to energy regulations, but – if not sufficiently secure – might be misused as a platform for a large-scale orchestrated cyberattack on the grid (e.g. by switching on and off millions of devices at the same time repeatedly). The smart grid needs to be protected against such attacks in the future.

RECOMMENDATIONS BY THE EUROPEAN COMMISSION

On 3 April 2019, the European Commission issued Recommendations on cybersecurity in the Energy Sector [11] and an accompanying Staff Working Document [13], addressing operators and technology vendors via the EU Member States.

The Recommendations summarise the specificities discussed above and suggest exemplary mitigating measures, mostly for system operators but also for technology suppliers. The Commission Recommendations are non-legislative and non-binding. They are aimed at drawing Member States' attention to the implementation requirements for cybersecurity in the energy sector, and are to be seen as guidance in a very technical expert area, combining operational technologies and information technologies.

The European Commission will follow up with the Member States on the Recommendations in a specific work stream dedicated to energy under the NIS co-operation group. The accompanying Staff Working Document explains the background, refers to existing standards, and mentions related EU-level activities without claiming exhaustiveness. It is meant to provide orientation on the subject matter of cybersecurity in the energy sector at EU level in general.

Discussion

EXISTING GENERIC CYBERSECURITY STANDARDS

For decades there have been numerous concepts and standards for cybersecurity, risk management, and business continuity. International standards such as the ISO 27000 series [14] define a full Information Security Management System (ISMS), and Risk Management standards can be found in the ISO 31000 series [15]. These existing generic approaches to cybersecurity and risk are not in contradiction to the three main strands identified as essential specificities for cybersecurity in the energy sector. On the contrary, it is advisable to develop any cybersecurity concept for the power grid on the basis of internationally acknowledged standards and to keep its specificities in mind when so doing.

The main difficulty in applying generic cybersecurity standards to the power grid is the fact that the choice of security architecture and mechanisms needs to respect significant side constraints.

The power grid is a combination of legacy operational technology distributed over millions of assets in the field, connected in a way that makes it very difficult to confine potential outages. The smart grid will have to develop its own security mechanisms, taking this legacy into account. In addition, the future smart grid will have to incorporate a large number of genuine software and IT devices not subject to any energy-specific regulation or standardisation. Simultaneously, it will have to introduce smarter controls for its own core components. Information technology – and cybersecurity issues – will thus surround the grid and penetrate it down to its operational technologies, which in technology terms are a different world.

Most current national cybersecurity strategies [16, 17] remain generic, i.e. they do not refer to sector-specific requirements or refer to them under the broader notion of critical infrastructure protection. This also holds for the EU Cyber Security Strategy of 2013. Many sector-specific efforts to protect critical infrastructures in turn have remained at a high level, without giving concrete guidance [18, 19]. Only in September 2017, the cybersecurity package [20] of the European Commission formally introduced sector-specific considerations.

Apart from specific standards as described in the following section, there currently is limited guidance on how to deal with cybersecurity in the energy sector. The stakeholder community has so far appreciated every effort to issue guidance and to raise awareness about the topic.

The power grid is a combination of legacy operational technology distributed over millions of assets in the field, connected in a way that makes it very difficult to confine potential outages. The smart grid will have to develop its own security mechanisms, taking this legacy into account.

SPECIFIC CYBERSECURITY STANDARDS FOR ENERGY COMPONENTS

Particular technology standards for cybersecurity in the energy sector also exist or are under development. Relevant IEC standards [21, 22] or similar technical efforts are good examples. However, new standards are not applicable to legacy technology in the field. There need to be certified products available in the market before specific standards can be implemented in the grid. Moreover, even if this is the case, not all components will be changed or upgraded immediately, and some components might never be updated at all.

In addition, cybersecurity standards are not available for those areas of the grid that simply do not allow for an integration of cybersecurity. These areas need to be protected by alternative approaches, for which there is limited specific guidance in the market.

COMPARISON OF ENERGY TO OTHER INDUSTRY SECTORS

When it comes to cybersecurity, the smart grid is different from other industry sectors in many ways. In contrast to other sectors like telecommunications and banking, confidentiality ranks comparably low in the power grid, whereas integrity and availability are essential. This perceived imbalance might change over time when smart components will process more and more personal data of individual users, but these processes have only started a few years ago.

Despite of a similar tree structure as in telecommunications, in the power grid technical time constraints are far more stringent. So standard security concepts from telecommunications (e.g. authentication or encryption) will not necessarily be applicable to the smart grid world of operational technologies.

Although having similar real-time requirements as industry automation, the smart grid cannot simply copy industry automation concepts for cybersecurity. The smart grid has its assets distributed all across the world, is fully connected and additionally will need to integrate billions of IoT consumer devices in the near future, whereas industrial

plants are usually under a single governance, have a limited number of components, and are located in rather confined environments.

Due to a rather unidirectional electricity flow, a node failure in the power grid might easily imply a total blackout in all lower levels. This makes the power grid different from other tree-shaped networks such as fixed-line telecommunications, where local calls are possible even if an international switch is out of service. The power grid might only establish a similar autonomy of parts or regions in the future, but unlike telecommunications, would always require sufficient production being available to cover the demand.

Finally, due to its physical connections being sensitive to voltage and frequency, a node outage in the power grid can jeopardise the stability of neighbouring nodes, which is not the case in telecommunications or on the internet. The internet has a particularly robust architecture by design, preserving message flow by automated re-routing in case of node outages. So availability considerations from other networks might not hold for the smart grid.

ADDRESSING ENERGY SPECIFICITIES

Out of the experience gained as described in this paper, the European Commission has provided formal, non-binding guidance on how to deal with the specificities of the energy sector when it comes to cybersecurity in [11]. The baseline principles are awareness about the specificities and collaboration.

Operators of transmission and distribution networks must be aware of the specificities of their technologies and networks and should not copy cybersecurity concepts from other industry sectors without adapting them carefully. Cybersecurity and risk management considerations under any generic standard need to keep the specific properties of the energy sector in mind.

Operational technology experts need to collaborate with IT security experts to complement each other where special OT requirements hamper the implementation of standard cybersecurity mechanisms or where there is not enough knowledge about cyberthreats in an OT world that used to have limited connectivity until recently.

Operators need to be aware that there are neighbouring operators that might suffer in case of outages or that neighbours even might even cause outages. In this multilateral dependency situation, a close collaboration is required.

Cybersecurity regulations or concepts for the energy sector do not cover the new IoT world, which is introducing risks of its own. The smart meter might be a clear delimiter of the area under control by a distribution network operator, but should therefore be able to signal any abnormal activity before any damage is done.

Bigger operators or technology providers in the energy sector are typically able to address cybersecurity requirements more thoroughly by an in-house cybersecurity organisation. Smaller operators, local power distribution companies, and small technology vendors might have more difficulties in this respect and could rely on a well-developed cybersecurity consultancy market. In any case, the special requirements of the sector need to be clearly addressed to avoid inefficient or incomplete security concepts.

Areas for future work

CYBERSECURITY CERTIFICATION

Cybersecurity certification has been a useful tool for increasing the trust in information technology devices for more than 25 years, and the “Common Criteria for Information Technology Security Evaluation” have paved the way for international recognition of cybersecurity certification since the early 1990s and have become an international standard [23].

The European Union has recently gone beyond this well-established standard and issued the Cybersecurity Act [24], entering into force on 11 December 2018. This act defines an EU framework for the development of cybersecurity certification schemes for products, services, and processes.

To deploy cybersecurity certification successfully in the energy sector, a coherent approach across the EU will be required. Such an approach will have to include broader topics like cybersecurity certification for general industrial automation and control

systems (IACS), a network code for cybersecurity as defined in [4], and cybersecurity certification for other products, services, or processes deployed in the energy sector of the future (e.g. cloud computing or 5G wireless communications).

The report of the Expert Group 2 under the Smart Grid Task Force of the European Commission is taking a high-level approach to the topic [25].

To achieve a comprehensive understanding of needs and benefits of cybersecurity certification in the energy sector, the European Commission has conducted stakeholder hearings during 2019. The results are expected to influence the scope of the upcoming European network code on cybersecurity, to be developed during the next two years.

OTHER SPECIFICITIES OF THE ENERGY SECTOR AND BEYOND

There might be more than three specificities of the energy sector when it comes to cybersecurity, and the presence of cyber-physical effects is clearly a candidate for further consideration. In addition, the technology supply situation, where many essential power grid components are custom-made and require months of lead time for replacement, requires further analysis. Studies have shown that it takes 6–9 months to replace high voltage transformers, which are customised to the client's needs and have a lead time for planning and specification of 3–4 months. Moreover, there is only a limited number of producers for high voltage transformers in the world, and a sudden rise in demand after a successful cyber-physical attack might increase delivery time.

In this context, it needs to be pointed out that cyber-physical attacks were most successfully demonstrated on devices with rotating elements, as seen by the 2007 Aurora generator test of the US Idaho National Laboratory or by the Stuxnet worm, targeting Iran's centrifuges in 2010. Nevertheless, cyberattacks have inflicted permanent damage to control systems by ransomware attacks without causing any physical damage, as seen in the 2017 WannaCry malware. The vulnerability of OT controls against both cyber-physical and ransomware attacks requires further research.

In the energy sector, the trend towards distributed power generation has raised serious concerns about cybersecurity, as the grid needs to open up for many small producers and is going to connect billions of IoT devices. However, a heterogeneous and distributed technology landscape also can be of a benefit, keeping attacks from spreading. Power supply decentralisation can also replace single points of failure, given that a certain degree of autonomy for parts of the grid. The overall long-term impact of decentralisation on cybersecurity is another area for further research. Many other sectors such as telecommunications or the internet have shown that a sound level of cybersecurity is achievable in a dynamic and vastly distributed environment.

Finally, specific cybersecurity requirements do not only exist in the energy sector. The transport sector, where autonomous mobility concepts are under development, also has its specific requirements. In future driverless vehicles, artificial intelligence might have to make the right decision in milliseconds to avoid incidents and fatalities. Such IT-based real-time mechanisms clearly need protection from cyberattacks as well. Also for other sectors such as finance or defence, specific cybersecurity requirements should hold.

Concluding remarks

High-level concepts for cybersecurity are often similar and have been successfully standardised internationally. However, when it comes to implementation, one size does not fit all. The selection of suitable cybersecurity measures is not laid out in generic standards and will be left to the respective operators of the smart grid.

The choice of security measures always needs to respect the properties and limitations of the target environment. This paper reasons that to provide suitable cybersecurity for the future smart grid, it is essential to understand the real-time requirements of the power grid, the risk of cascading effects, and the particularities when using legacy operational technology in combination with most recent consumer devices from the IoT.

The development of the smart grid in the EU started already a decade ago and it will gradually proceed over the coming years and so will the development of its cybersecurity and its cyberattacks. In this development process, it is essential to keep in mind that the smart grid is not a completely new, digital world but contains millions of technical elements that were constructed several decades ago when cybersecurity did not yet play an important role. ■

High-level concepts for cybersecurity are often similar and have been successfully standardised internationally. However, when it comes to implementation, one size does not fit all.

About the authors:



Dr Stephan Lechner, based in Luxembourg, is Director at the European Commission's Directorate General for Energy and co-ordinates the policy activities of the European Commission on cybersecurity in the energy sector. Before his appointment in July 2016, he was Director of the Institute for the Protection and the Security of the Citizen at the European Commission's Joint Research Centre in Ispra, Italy, for more than 8 years. Prior to joining the European Commission he held various management positions and spent more than 18 years in the hi-tech sector of private industries. He managed international expert teams in Germany and in China and has more than 30 years of experience in cybersecurity. Dr Lechner holds a degree in mathematics and computer sciences and a doctoral degree in cryptography.



Dr.-Ing. Manuel Sánchez Jiménez joined the European Commission in 1996 and launched the European Technology Platform "Smart Grids" in 2006. Since April 2009, he is the Team Leader for Smart Grids in the Directorate General for Energy and launched the European Task Force for Smart Grids in November 2009. Since 2015 he is contributing with key policy and regulatory solutions to the Electricity Market Design under the Clean Energy legislative package. Since January 2019, he chairs the DG ENER Task Force for digitalisation of the energy sector. He holds a degree in Engineering (University of Seville, Spain) and a doctorate in engineering (University of Kassel, Germany). Prior to working at the European Commission, he was the Director of the Plataforma Solar de Almería of the Spanish Ministry of Industry and Energy, the largest solar test centre in Europe.



MMag. Michaela Kollau is currently working for the European Commission at the Directorate General for Energy in the directorate for internal energy market. Within this context, she works in the unit dealing with security of supply in which her responsibilities cover cybersecurity in the energy sector as well as security of electricity supply including risk preparedness. Prior to her current position, she worked in in the Smart Grids Team on cybersecurity in the energy sector and chaired different expert groups like the Energy Expert Cybersecurity Platform (EECSP) and the Smart Grids Task Force – Expert Group 2 (SGTF EG2). She joined the European Commission in 2014 following a career in the Austrian Regulatory Authority for the electricity and gas market. Mrs Kollau studied in Austria (Graz), the US (New Mexico) and in France (Nice – Sophia Antipolis) and holds master degrees in economics and environmental system sciences.



References

- [1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy, COM/2015/080 final.
- [2] ENERGY EXPERT CYBER SECURITY PLATFORM, Cyber Security in the Energy Sector, Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP Report, February 2017. Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
- [3] Proposal for a Regulation of the European Parliament and of the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, COM/2016/0862 final - 2016/0377 (COD).
- [4] Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity, OJ L 158, 14.6.2016, pp. 54–124. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0943&from=EN>
- [5] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 07.02.2013, JOIN(2013)1.
- [6] Austrian Energy Computer Emergency Response Team (CERT). Retrieved from <https://www.cert.at/about/aec/content.html>
- [7] COM(2017) 477 final. The Cyber Act is part of the cybersecurity package of 2017: Proposal for a Regulation on ENISA, the “EU Cybersecurity Agency”, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”).
- [8] Minutes - High Level Roundtable on Main Challenges for Cyber Security in the Energy System, 24. March 2017, Rome, Terna S.p.A. Piazza Frua n. 2 - 00156 Roma, Organised by the European Commission. Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/detailed_minutes_rome_24.3_final.pdf
- [9] G7 Rome Energy Ministerial Meeting – Energy Security: from Rome 2014 to Rome 2017 – Rome, 9 – 10 April 2017 Chair’s Summary. Retrieved from http://www.g7italy.it/sites/default/files/documents/energy_chairs_summary.pdf

- [10] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, J L 194, 19.7.2016
- [11] COMMISSION RECOMMENDATION (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector (notified under document C(2019) 2400), Official Journal of the European Union L96 / 50, Brussels, 5.4.2019. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/F/?uri=CELEX:32019H0553&qid=1575654275937&from=EN>
- [12] Smith, R. (12 March 2014). U.S. Risks National Blackout From Small-Scale Attack - Federal Analysis Says Sabotage of Nine Key Substations Is Sufficient for Broad Outage. *Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/u-s-risks-national-blackout-from-small-scale-attack-1394664965?>
- [13] COMMISSION STAFF WORKING DOCUMENT Accompanying the document Commission Recommendation on cybersecurity in the energy sector [C(2019) 2400 final], SWD(2019) 1240 final, Brussels, 3.4.2019. Retrieved from https://ec.europa.eu/energy/sites/ener/files/swd2019_1240_final.pdf
- [14] ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, ISO/IEC JTC 1/ SC 27 IT Security techniques, 02/2018. Retrieved from <https://www.iso.org/standard/73906.html>
- [15] ISO 31000:2018 Risk management – Guidelines, ISO/TC 262 Risk Management, 02/2018. Retrieved from <https://www.iso.org/standard/65694.html>
- [16] Cyber Security Strategy for Germany, Federal Ministry of the Interior, published 2011. Retrieved from http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?blob=publicationFile and German Cyber Security Strategy, November 2016 (in German only). Retrieved from <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany/view>
- [17] HM Government, National Cyber Security Strategy 2016-2021, Published 1 November 2016, last updated 11 September 2017. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
- [18] Improving Critical Infrastructure Cybersecurity, US Presidential Executive Order 13636, The White House, Office of the Press Secretary, 12 February 2013. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
- [19] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union L 345, pp. 75–82, 23.12.2008. Retrieved from http://www.infrastrutturercritiche.it/aiic/images/DocArticoli/directive%20eepic%20en_12_01_2009.pdf
- [20] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final, 2017/0225 (COD), Brussels, 13.09.2017. Retrieved from <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF>
- [21] International Electrotechnical Commission, IEC 62351:2018 SER Series, Power systems management and associated information exchange - Data and communications security - ALL PARTS, 2018. Retrieved from <https://webstore.iec.ch/publication/6912>
- [22] International Electrotechnical Commission, IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Retrieved from <https://webstore.iec.ch/publication/7033>
- [23] ISO/IEC 15408-1:2009 [ISO/IEC 15408-1:2009] Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. Retrieved from <https://www.iso.org/standard/50341.html>
- [24] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, pp. 15–69. Retrieved from <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
- [25] Smart Grid Task Force Expert Group 2, Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management, Final Report June 2019. Retrieved from https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

ANALYSIS

The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out

LUUKAS ILVES

HEAD OF STRATEGY, GUARDTIME

ANNA-MARIA OSULA

SENIOR POLICY OFFICER, GUARDTIME; SENIOR RESEARCHER, TALTECH CENTRE FOR DIGITAL FORENSICS AND CYBER SECURITY

Over the past two decades, digitalisation has become the primary driver of globalisation and cross-border economic integration. New technologies and economic models promise to enable further integration in the coming decades. However, with geopolitical rivalry growing across the world, this open integration may have run its course. This article discusses how disruptive technology and “autonomy by design” may solve some of the technological sovereignty issues faced by the EU.

Governments across the world are making digital autonomy and sovereignty core parts of their economic, security, and diplomatic strategy, often at significant cost. The US-China digital “trade war” over 5G networking technology and mobile software that has been unfolding over the past year is the newest flashpoint.¹ And the new European Commission

is putting Europe’s “technological sovereignty” at the centre of its strategy for the next five years²

Behind this concern is a structural tension between the integrated nature of the global digital economy and the enduring responsibility of any sovereign government for security and domestic rule of law.

1 Fearing that equipment from Chinese manufacturers could serve as a Trojan horse for exploitation of its critical infrastructure, the US has effectively banned Huawei and other Chinese equipment from the core of its domestic 5G networks and encouraged its allies to take similar steps. Alarms have similarly been raised about Chinese tech companies doing the bidding of their government abroad (for instance taking down posts in the US about pro-democracy protests in Hong Kong). China, for its part, effectively bans many US cloud services from operating in China through its great firewall. Chinese companies have been working to reduce their dependency on US technology in everything from operating systems to chips.

2 Europe’s push for technological sovereignty began in earnest after allegations in 2013 of large-scale espionage by US intelligence services. Since then, several steps have been taken that point at the need for more autonomy, such as changing EU competition rules to favour European stakeholders, setting up an EU-wide payments system and discussions on new rules on digital taxation. Domestically, individual Member States have come up with options for alternatives to huge US cloud service providers. The new President of the European Commission, Ursula van der Leyen, specifically called for pursuing “technological sovereignty” in her inaugural agenda: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

No doubt, this problem is here to stay: the next generation of digital technologies and economic models will only highlight the issue.

Policy-makers' existing toolbox is not up to the challenge. Many current and proposed technological sovereignty measures force governments into a difficult and costly trade-off between taking advantage of the benefits of digital technologies and surrendering control. The ideas behind "security by design" provide an answer – we need products and services that enable a level of trust and verifiability functionally superior to what sovereign control promises. The good news is that the tools to solve this problem are available, waiting for governments and companies to broadly adopt them: new technologies and measures of transparency, audit, and control will enable governments and users to verify how their technologies and services are behaving and allay concerns over compromise and attack.

Many current and proposed technological sovereignty measures force governments into a difficult trade-off between taking advantage of the benefits of digital technologies and surrendering control.

The technological sovereignty problem

Policy-makers have good reasons to be worried about technological sovereignty and autonomy in the Internet era. Technologies connected to the Internet and new emerging business models have changed the way our societies function and are affecting relationships between states. Three main factors – dependency, concentration problems, and cross-border character – play a role in reshaping governments' policies towards digital autonomy. While this problem is global, we will focus in particular on the European dimensions of technological sovereignty.

Firstly, we have become more dependent on digital technologies. The "digital economy" is equivalent to 15.5% of global GDP and has grown two and a half times faster than global GDP over the past 15 years (Huawei, 2017). In many industries,

new entrants are disrupting long-standing incumbents. As cyberspace is increasingly also used for malicious purposes, countries' interest in controlling cyberspace has spiked.

Three main factors – dependency, cross-border character, and concentration problems – play a role in reshaping governments' policies towards digital autonomy.

Secondly, this digital transformation is shaping up to be a winner-takes-all phenomenon, with category-leading companies able to offer their products and services on a global scale. This allows them to reap economies of scale and spread innovations into all markets. The biggest technology platforms – now the world's most valuable companies – are offering essential digital infrastructure on a global level, frequently leaving no viable domestic alternative.

Finally, as jurisdictional boundaries begin to blur in cyberspace, the conventional territorial foundations of sovereignty are no longer as solid as they used to be. In the context of criminal investigations, service providers such as Google and Facebook are now required (under both the US CLOUD Act and the proposed EU e-Evidence framework) to share specific data with domestic and international law enforcement offices irrespective of the actual physical location of the data. This is a significant change from the previously prevalent "territorial" approach where data location was the main determining connecting factor to identify the foreign state with whom to initiate the Mutual Legal Assistance process in order to obtain access to the evidence (e.g. Osula, 2017).

It does not stop with digital evidence. The effective nexus for controlling large swaths of how a society functions – transport, housing, energy, health, food, financial services – is coming unmoored from the territorial jurisdiction where the service is provided, with the service provider subject to orders from their headquarters' home country or a third country. Further developments such as cryptocurrencies threaten states' classical monopolies in domains like monetary, taxation, and social policy.

The most capable and committed governments are keen to exploit their “cyber power” as a new form of power projection, sometimes employing companies under their jurisdiction and control as their agents. While their intentions can be benign and their actions can even seem necessary in a globalised world – e.g. the pursuit of terrorists or money laundering – such activity leaves most countries suffering from a “sovereignty gap” and concerned about domestic rule of law (Schaake, 2017). This is a gap new policies of technological sovereignty and autonomy are intended to fill (Nye, 2010; Kello, 2018).

There are two technological and economic trends which will have an effect on how governments are able to deal with further digitalisation.

The first of these – “software-defined everything” – describes the idea that computers now run everything, including the physical environment around us, from car brakes and door locks to factories and supply chains, complex transportation and energy systems. What was previously hard-wired or coded is now constantly modifiable, updateable, hackable – and, in effect, a black box for those who would certify or inspect the functioning of a device. And general-purpose machines replace specialised equipment (e.g. the smartphone, which functions as a GPS receiver, calendar, map, radio, telephone, metronome and piano tuner, voice recorder, camera, measuring tape, pedometer, sports watch, digital identity/smartcard, etc.).

The second – “servitisation” – describes companies moving toward offering services in lieu of products (for an exploration of the idea, see Osimo & Ilves, 2019: 28–29). Software-as-a-service is the prime example: Gartner predicts that by 2020, 80% of software will be subscription-based (Gartner, 2018). However, this extends well beyond digital products: Rolls Royce has introduced new “pay by the hour” models for its airplane engines, instead of the equipment itself, while car manufacturers are preparing for an era where individuals no longer buy automobiles but consume “mobility-as-service”. Instead of purchasing a clearly defined good, customers enter a long-term relationship with

their supplier and consume a product that is constantly being updated and changed.

The most capable and committed governments are keen to exploit their “cyber power” as a new form of power projection, sometimes employing companies under their jurisdiction and control as their agents.

Both of these trends exacerbate technological sovereignty challenges: the service you subscribe to today could change tomorrow, the software of your certified device can be reconfigured in minutes with an over-the-air update. This is generally a good thing, enabling convenience, responsiveness, quality, and continuous improvements. But this also opens a window – for malicious cyberattackers, including foreign governments – to reach straight into a country’s critical infrastructure, sensitive data, and overall economy.

Toolbox

The terms “strategic autonomy” and “technological sovereignty” have become a catch-all for measures to limit exposure to these risks. Governments are considering a broad policy toolbox, with measures generally intended to increase government control or promote domestic competitors.

Common proposals include (Leonard et al., 2019; Aaronson, 2018):

- industrial policy and domestic technology development programmes, including in new technologies such as 5G, AI, quantum computing;
- rules to limit foreign companies (e.g. rules on foreign ownership) or indirect measures (such as taxation and competition rules);
- preference for domestic technologies and services, expressed in procurement or legal requirements;
- forced localisation (e.g. data localisation, requirements for local staff or headquarters) or filtering and blocking non-domestic data and services;

- more aggressive jurisdictional concepts or universal jurisdiction, e.g. the US CLOUD Act and the EU GDPR and the proposed e-Evidence regulation;
- stronger cybersecurity rules and capacity, notably reporting, information sharing, and standards;
- “security by design”, e.g. requirements for testing and standardisation, opening source code for review.

This toolbox lays out the dilemma posed by “technological sovereignty”: measures that increase domestic control over technology have serious costs. Technological autarky and even simple localisation rules break global supply chains. New legal requirements create compliance costs also for domestic firms (e.g. Hohmann et al., 2014). Industrial policy can lead to costly technology choices. And *other countries’* policies can hurt one’s own firms. At worst, we risk escalating *beggar-thy-neighbor* policies leading to widespread “digital protectionism” and mercantilism (Denton, 2019). Studies of just one such practice, forced data localisation, have pegged the cost of current and proposed measures at 1% of global GDP (see Bauer et al., 2014; Bauer et al., 2016).

Perhaps the biggest cost of limiting foreign technology and services is its impact on broader technological adoption. The ICT industry itself forms narrowly 4–8% of the economy in most countries (see OECD indicators). Economic success comes from the speed with which the economy digitalises (and raises labour productivity) as a whole. Tomorrow’s digital leaders will be those who aggressively use today’s technology. Conversely, measures that make new technology harder or more expensive to use harm countries’ broader digital agendas.

This toolbox lays out the dilemma posed by “technological sovereignty”: measures that increase domestic control over technology have serious costs.

The European Commission’s internal think tank summarises the dilemma of technological sovereignty:

[I]n today’s interconnected world of globalised supply chains, no one can walk alone. From a strategic point of view, the issue is hence more complex than simply seeking to prevent, or eliminate, vulnerabilities in supply chains. In many respects, it appears more realistic to find ways to manage and reduce, when possible, these vulnerabilities. Likewise, some dependencies might be less critical than others, depending on the country of origin and the technologies involved (EPSC, 2019: 10).

Three core technologies (5G, Cloud, and AI) illustrate the tradeoffs behind the technological sovereignty dilemma and the challenge posed by the increasing pervasiveness of software- and services-driven offerings.

5G is the newest generation of mobile broadband technology, currently being rolled out across the world. Like 2-3-4G before it, 5G will bring faster mobile broadband, but its transformational effect arises from other characteristics – low latency and low power connections that will bring mobile connectivity to billions of IoT devices, from construction equipment and autonomous cars to small transmitters in clothing, medical equipment, and household goods. And along with this connectivity come all the risks of connected devices.

5G equipment relies on “software-defined” networking and radio equipment to handle the massive volumes and variations in the use cases the technology allows (Routray, & Sharmila, 2017). This in turn can only be accomplished through frequent updates and active management of the network by the manufacturer (European Commission, 2019). Traditional controls – thorough examination and certification of hardware and software before deployment – fail to effectively address this active management. In these circumstances, the US government determined that it could never be sure it could prevent the Chinese government from exploiting the presence of Huawei equipment in networks, and chose an outright ban on Huawei equipment as the most expedient solution (for a summary of US Government considerations: Defense Innovation Board, 2019). Other governments are arriving at similar conclusions.

This choice, however, carries significant costs. In the short term, many experts conclude that Huawei offers the operationally most effective (and cheapest) end-to-end solution for deploying 5G (GlobalData, 2019). In its absence, the market is basically confined to two providers, with limited competition potentially raising the cost of 5G (Barzic, 2019). Furthermore, a policy of excluding Huawei from 5G networks also requires previous equipment investments to be recouped, at a cost of billions of euros in the EU alone.³

Cloud computing, narrowly construed, is a service that facilitates the on-demand availability of computer system resources. But the promise of cloud computing goes beyond providing a more efficient infrastructure: enterprise functions that were previously provided in-house (e.g. human resources, accounting, training, internal and external communications, business intelligence, quality assurance, specialised services from monitoring aircraft engine performance to detecting financial crime) can now be consumed as cloud services (Bommadevara et al., 2018).

Today, the productivity benefits of digitalisation are delivered via cloud, which is also the easiest way to consume new technologies like AI and Blockchain without requiring specialised staff or major upfront investments. This disrupts the scale advantage of large firms and makes it easier for a startup or small business to scale rapidly.

European concerns about cloud computing highlight the sovereignty dilemma. European firms already lag significantly behind their American counterparts in adopting cloud services (Targett, 2018). Partly as a result, Europe also has far fewer cloud and software-as-a-service startups (e.g., Eurostat, 2018; Lorica & Nathan, 2018).

³ The only form of 5G networks that can currently be deployed by telecom operators are “non-stand-alone” – built on top of existing 4G networks by the same manufacturer. For telecoms operators whose 4G equipment is built on Huawei – including many in Europe – the choice not to use Huawei equipment for 5G networks means either waiting several years before deploying 5G or a bill in the hundreds of millions or in billions to replace significant components of their 4G network before they even begin 5G deployment. See GSMA, 2019. See also the balanced risk-based approach provided by the EU 5G toolbox, European Commission, 2020.

Data sovereignty concerns are leading European governments to launch costly new initiatives for cloud infrastructure that do not necessarily address the adoption question. Partly in response to the US CLOUD Act, which would allow the US federal law enforcement officers to demand data from the servers of American tech firms located anywhere in the world, the French and German government launched the “Gaia-X” project. Due to be established in spring of 2020, the initiative is a response to the “European economy urgently need[ing] an infrastructure that ensures data sovereignty” (Meyer, 2019). The infrastructure will be developed in cooperation with France and a number of private sector actors, and further activities will include establishing data warehouses, data pooling, and developing data interoperability. At the same time the EU is lacking a uniform approach in this question. For instance, in 2018 the Polish government launched the programme “Common Information Infrastructure of the State” which also includes setting up a “Public Computational Cloud” in cooperation with Google (Operator Chmury Krajowej, 2019).

The development of Artificial Intelligence has surged forward in the past decade. Driven by massive increases in data and computing power (via cloud computing), machine learning (ML) is enabling large swaths of human tasks to be automated, with major economic and social consequences.⁴

Using AI is a bit like hiring a person, requiring trust in a black box we cannot fully control. Tools built on ML and associated technologies are not static; their functionality is constantly evolving based on new data and learning cycles. They must be configured and set up properly to work well.

⁴ It is estimated that AI will add \$15.7 trillion to the global economy by 2030. At the same time, 15 percent of the global workforce – or about 400 million workers – could be displaced by automation. As in the case of 5G and cloud, the greatest returns will come from broad adoption of AI technologies across different economic sectors.



And – in the case of many deep learning models – their internal functioning is effectively a black box that even the designers of the specific algorithm cannot fully explain.⁵ Traditional approaches to testing and certification cannot track a dynamic system. Systems that use AI become unpredictable and can often produce unexpected effects – leading to the broad and far-reaching discussion on the ethics and human rights impacts of AI as well as design principles for safe, secure and reliable AI (Ilves, 2018).

Most cutting-edge applications of AI are being designed in the US and China, with core components provided by a limited number of companies, such as Google’s Tensor Flow and IBM’s Watson, increasingly baked into most enterprise AI products. We are seeing increasing concern about the provenance and trustworthiness of AI, analogous to existing discussions around Cloud and 5G (e.g. Renda, 2019). The dilemma policy-makers face will be similar – building a set of sovereign technologies while excluding US or Chinese technology on the grounds of national origin may be the only reliable way to address all trust concerns around a foreign-sourced technology, but doing so will come at immense cost – including possibly slowing down one’s own industrial and economic progress by years.

Security and autonomy by design

The notion of “security by design” points to a way out of the technological sovereignty dilemma. If we can design our digital products and services so as to preclude misuse and guarantee that services perform as promised, we can eliminate much of the risk that policies for technological sovereignty are trying to address. Effective control over the ongoing functioning of a product or service can make up for foreign provenance or control over the service provider. Ultimately, “security by design” should deliver “autonomy by design”.⁶

⁵ While there is significant research in the area of “explainable AI”, it has thus far not satisfactorily addressed the question.

⁶ To be sure, “security by design” measures cannot address all technological sovereignty concerns. Notably, they are silent on the question of reliability and do not reduce the industrial costs of long-term dependency on foreign suppliers. But they do give policy-makers more leverage, allowing them to focus on developing domestic technologies and supply chains in a more targeted manner.

The EU has steadily worked on enshrining the principles of “security by design” (and its cousin, “privacy by design”) in its legislative frameworks. For example, the new EU Cybersecurity Act establishes cybersecurity certification schemes which play an important role in enhancing trust and security in products, services, and processes by encouraging manufacturers or providers involved in their design and development to implement security measures at the earliest stages of design and development (EU Regulation 2019/881: Art. 13). The EU’s data protection rules (the GDPR) also clearly underline the relevance of “data protection by design and by default” (EU Regulation 2016/679: Art. 25). Other measures include adopting security standards, the use of ethical hacking and penetration testing for ensuring the security of the products, services, and processes as well as putting in place requirements for an assured supply chain (e.g. Eurosmart, 2019).

“Security by design” points to a possible way out of the technological sovereignty dilemma.

However, current approaches to security by design suffer from significant limitations that keep them from reaching the level of control technological sovereignty concerns demand:

- Security testing, certification, penetration testing, and auditing are expensive and labour-intensive. This approach will struggle to scale broadly.⁷
- They focus on initial design of a product or service, not the ongoing and dynamic processes that are common in the digital world today. Common practices in software engineering and service design, including extensive multi-party supply chains and continuous updates, break this paradigm (as described above for 5G and cloud). One software update and new release later the product may have changed entirely.

⁷ For instance, a regular penetration test costs anything between \$15,000 and \$30,000, while comprehensive audits can cost hundreds of thousands. See Tritten, 2020; Glover. For a list of Conformity Assessment Bodies, see ENISA 2019.

- Auditing and testing alone simply move the trust and provability burden elsewhere, to the question of “do you trust your testing lab or auditor?” “Security by design” will not solve our digital sovereignty dilemma if products and services still need to comply with multiple different standards and be audited, testified, or certified in each country they are used in.
- Many (in principle) highly secure systems are compromised because of user error in configuration and setup. Any approach to solving the technological sovereignty dilemma that relies on technology must also work in the real world.

However, new technologies and approaches can address these shortcomings to the point where many of the control questions raised in this article can be convincingly addressed. “Autonomy by design” relies on three fundamental functionalities to ensure that technology and its uses are free from outside influence: scalable data and process integrity, automated testing, and transparency. New trust technologies (e.g. blockchain) and forms of automation (e.g. AI) now make these realisable in practice.

1) Scalable data and process integrity⁸

Data integrity is a fundamental aspect of information security that deserves more attention in the context of security by design. The integrity of individual data objects is central to a wide variety of trusted processes, from log analysis to elections. And the stakes are rising: automated processes that rely on exponentially growing volume and speed need to be able to verify the integrity of their input in real-time.

How do I know, in real time, that my 5G base station, autopilot, or cloud service have not been compromised by the manufacturer or a third party? Can I prevent the risk scenarios described in this paper?

This entails proving a negative – that no compromise of the system has occurred. Reaching a sufficient level of proof means real-time tracking,

⁸ Within the narrow context of information security, the term integrity means to protect the accuracy and completeness of information, see ISO standard (ISO/IEC 27000, 2014: section 2).

logging, and reporting millions of steps in complex processes, often over multiple computing environments, while generating cryptographic proof of this process. There are now scalable forms of blockchain technology in use in industrial applications, including in the US defence supply chain and mission critical industries such as shipping, that reach this standard (Linkov et al., 2018, Vestergaard & Umayam, 2019). Similar technology is being applied to cloud computing and AI training, providing process integrity at a scale sufficient for “hyper-automation”, where AI systems can act directly upon insights without human intervention (Kenyon, 2019: 2). Applied to cloud computing, this means real-time awareness of what is happening to cloud-based processes on a bits-and-bytes level, ongoing confirmation that a cloud deployment corresponds to the parameters of relevant certifications, and immediate alerts and automated action if something deviates from these parameters (e.g. insider compromise or an unauthorised access based on e.g. foreign e-evidence requests).

2) Automated testing

Where services are not configured to provide ongoing proof of data and process integrity, we should aim for ongoing, scalable testing that occurs at the speed of software. AI and autonomous agents promise to automate security and compliance testing. The 2016 DARPA Cyber Grand Challenge saw automated penetration testers outperform human teams. Applied broadly, such an approach enables a wide range of security and conformity tests to be performed at scale. Automated testing can serve to reduce the risks of the black box problem presented by AI, cloud, 5G, and other new technologies. For instance, a wide variety of cybersecurity startups now promise automated cybersecurity and penetration testing to discover vulnerabilities or configuration errors and to assess the security of a product or service.⁹

As a next step, increasingly sophisticated virtualised testing environments allow new software and updates to be tested before release, but in real time.

This allows testing and certification to be built into dynamic, quickly developing products and services without a significant compromise in usability or availability.

3) Transparency, accountability, and automated compliance

Of course, both process integrity and automated testing will only create confidence for policy-makers when these can be independently verified by third parties, including regulators and government cybersecurity centres.

Transparency is becoming the “new normal” both in private and public sectors. For example, the retail industry has discovered the merits of blockchain technology, allowing the consumer to track how products are sourced and providing transparency as well as traceability throughout the entire supply chain (Weinswig, 2018). Governments are also relying on providing transparency to users to engender trust in increasingly digitalised public services, especially when these involve sensitive personal data.¹⁰ For instance, Estonia’s e-health system provides an independent forensic-quality audit trail for the lifecycle of patient records, making it impossible for anyone who gains access to those records to manipulate information and cover their tracks (E-Estonia, 2016).

The last decade has also seen an explosion in region- or vertical-specific regulation centred around trust and auditability (notably around privacy and financial services). The burden of complying with these rules has spawned a new generation of services focused on simplifying and automating compliance (RegTech, short for regulatory technology). RegTech allows companies to manage and track their compliance and ultimately demonstrate to regulators that they have acted appropriately. By using automated and machine-readable reporting, compliance becomes an automated process.

Ultimately, we see a virtuous cycle of process integrity, automated testing, compliance, and accountability, providing the ability to ensure that digital

⁹ E.g. Aquascan, Pcysys, Security Scorecard.

¹⁰ See, e.g. the eGovernance Benchmark report showcasing the digital efforts in the EU: European Commission, 2018.

services and software function as promised.¹¹ These tools allow us to realise “continuous compliance”, whereby ongoing conformity of a system can be ascertained second-to-second. States, regulators, and users can reach a level of control and oversight over technology and services that are not designed and developed domestically or are offered from another jurisdiction, while achieving the same or greater level of oversight and trust as they would wish for in their own sovereign technology.¹²

In expanding the toolbox at their disposal, policy-makers should actively consider how new standards of evidence, proof, and compliance could be used to make products and services trustworthy and controllable, even where they are of foreign origin.

These capabilities are underpinned by recent technological developments (scalable blockchain and AI), but we emphatically do not propose that policy-makers should therefore simply mandate the use of these technologies. The technological sovereignty concerns outlined in this paper and elsewhere arise from functional concerns over the functioning of modern IT systems. The solution, too, should be specified in functional terms. In expanding the toolbox at their disposal, policy-makers should actively consider how new standards of evidence, proof, and compliance could be used to make products and services trustworthy and controllable, even where they are of foreign origin.

11 For example, the EU’s newly published toolbox for secure 5G networks covers functionalities such as strong security requirements, strict access controls, monitoring, reinforcing testing and auditing capabilities (European Commission, 2020).

12 Frequently, tools for oversight, PKI, etc. are called “trust services” and “trust technology”. This name gives insight into their limitations – they entail trusting another party. And the need to trust third parties is precisely the problem that is being put under stress with arguments for technological sovereignty, which basically say that “we cannot trust all the parties potentially involved in this process or supply chain.” So we need to move beyond trust to independent “truth”, verified frequently and by many parties.

This is an area that calls for EU leadership. Europe continues to be one of the largest exporters of digital goods and services (Eurostat, 2018). European manufacturers and technology companies will pay the price of the technological sovereignty dilemma, as Europe, the US, China, India, Brazil and other parts of the world impose new restrictions. Conversely, a broad adoption of “security and autonomy by design” measures would help European offerings thrive and shore up globalised, open markets. In short, the EU has good reasons to promote technological and design solutions to the technological sovereignty dilemma, both to support its own digital development at home and to set an example for the rest of the world.





About the authors:

Luukas Ilves is Head of Strategy at Guardtime. For the past two years, he also chaired the Council of Europe's Committee of Experts on human rights dimensions of automated data processing and different forms of artificial intelligence. He has previously held policy-making positions in the Estonian Government and European Commission, focusing on cyber security, digital government, and data flows.



Dr. Anna-Maria Osula serves as Senior Policy Officer at Guardtime and Senior Researcher at TalTech Centre for Digital Forensics and Cyber Security. During 2008-2018 she worked as a legal researcher at the NATO Cyber Defence Centre of Excellence.

References

- Aaronson, S. A. (2018). What Are We Talking about When We Talk about Digital Protectionism?. Washington, DC: George Washington University. Retrieved from <https://www2.gwu.edu/~iiep/assets/docs/papers/2018WP/AaronsonIIEP2018-13.pdf>
- Barzic, G. (7 June 2019). Europe's 5G to cost \$62 billion more if Chinese vendors banned: telcos. Retrieved from <https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3>
- Bauer, M., Ferracane, M. F., Lee-Makiyama, H., & Van der Marel, E. (2016). Research Report Unleashing internal data flows in the EU: An economic assessment of data localisation measures in the EU member states ECIPE Policy Brief. Retrieved from <https://www.econstor.eu/bitstream/10419/174802/1/ecipe-pb-2016-03-Unleashing-Internal-Data-Flows-in-the-EU.pdf>
- Bauer, M., Lee-Makiyama, H., Van der Marel, E., & Vershelde, B. (2014). Research Report The costs of data localisation: Friendly fire on economic recovery ECIPE Occasional Paper. Retrieved from <https://www.econstor.eu/bitstream/10419/174726/1/ecipe-op-2014-3.pdf>
- Bommadevara, N., Del Miglio, A., & Jansen, S. (2018). Cloud adoption to accelerate IT modernization. Retrieved from <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization>
- Defense Innovation Board. (April 2019). The 5G Ecosystem: Risks & Opportunities for DoD. Retrieved from <https://apps.dtic.mil/dtic/tr/fulltext/u2/1074509.pdf>
- Denton, J. (28 April 2019). Digital protectionism demands urgent response. Financial Times. Retrieved from <https://www.ft.com/content/0c360404-65ba-11e9-a79d-04f350474d62>
- E-Estonia. (February 2016). eHealth authority partners with Guardtime to accelerate transparency and auditability in health care. Retrieved from <https://e-estonia.com/ehealth-authority-partners-with-guardtime-to-accelerate-transparency-and-auditability-in-health-care>
- EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- EU Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
- European Commission. (2018). eGovernment Benchmark 2018: the digital efforts of European countries are visibly paying off. Retrieved from <https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2018-digital-efforts-european-countries-are-visibly-paying>

- European Commission. (2019). Member States publish a report on EU coordinated risk assessment of 5G networks security. Press release. Retrieved from https://europa.eu/rapid/press-release_IP-19-6049_en.htm
- European Commission. (2020). Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures. CG Publication. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468
- European Network and Information Security Agency (ENISA) (2019). List of conformity assessment bodies (CABs) accredited against the requirements of the eIDAS Regulation. Retrieved from <https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation>
- European Political Strategy Centre. (July 2019). Rethinking Strategic Autonomy in the Digital Age. EPSC Strategic Notes. Issue 30, July 2019. Retrieved from https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf
- Eurosmart. (2019). Towards European Digital Strategic Autonomy. Retrieved from <https://www.eurosmart.com/towards-european-digital-strategic-autonomy-digital-sovereignty>
- Eurostat. (August 2018). Trends in EU trade in goods and services 2000-2017. Retrieved from <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/WDN-20180827-1>
- Eurostat. (December 2018). Cloud Computing – Statistics on the Use by Enterprises.
- Gartner. (2018). Moving to a Software Subscription Model. Retrieved from <https://www.gartner.com/smarterwithgartner/moving-to-a-software-subscription-model/>
- GlobalData. (25 June 2019). Telecom Industry's First 5G RAN Competitive Analysis by GlobalData Reveals Huawei Leadership. Retrieved from <https://www.globaldata.com/telecom-industrys-first-5g-ran-competitive-analysis-published-by-globaldata-reveals-huawei-leadership/>
- Glover, G. How Much Does a Pentest Cost?. Retrieved from <https://www.securitymetrics.com/blog/how-much-does-pentest-cost>
- GSMA. (28 March 2019). 5G Implementation Guidelines. Retrieved from <https://www.gsma.com/futurenetworks/wiki/5g-implementation-guidelines/>
- Hohmann, M., Maurer, T., Morgus, R., & Skierka, I. (24 November 2014). Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013. Retrieved from <https://www.gppi.net/2014/11/24/technological-sovereignty-missing-the-point>
- Huawei. (2017). Digital Spillover: Measuring the true impact of the digital economy. Retrieved from https://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf
- Ilves, L. (October 2018). Briefing Note: Responsible, Safe and Secure AI. retrieved from <https://lisboncouncil.net/publication/publication/152-responsible-safe-and-secure-artificial-intelligence.html>
- ISO/IEC 27000. (2014). Information technology – Security techniques – Information security management systems – Overview and vocabulary.
- Kello, L. (2018). Private-Sector Cyberweapons, An Adequate Response to the Sovereignty Gap?. In: Lin, H., & Zegart, A. (Eds.). *Bytes, Bombs, and Spies*, Washington, DC: Brookings Institution Press, 2019.
- Kenyon, T. (2019). Data integrity critical in securing autonomous AI. Guardtime whitepaper. Retrieved from <https://m.guardtime.com/files/data-integrity-critical-in-securing-autonomous-ai.pdf>
- Leonard, M., Pisani-Ferry, J., Ribakova, E., Shapiro, J., & Wolff, G. B. (25 June 2019). Redefining Europe's Economic Sovereignty. Retrieved from <https://bruegel.org/2019/06/defining-europes-economic-sovereignty/>
- Linkov, I., Wells, E., Trump, B., Collier, Z., Goerger, S., & Lambert, J. H. (May 2018). Blockchain Benefits and Risks, Military Engineer. Retrieved from https://www.researchgate.net/publication/325385235_Blockchain_Benefits_and_Risks
- Lorica, B. & Nathan, P. (October 2018). Evolving Data Infrastructure, October 2018 <https://www.oreilly.com/data/free/evolving-data-infrastructure.csp>
- Meyer, D. (2019). Europe Is Starting to Declare Its Cloud Independence. Fortune. Retrieved from <https://fortune.com/2019/10/30/europe-cloud-independence-gaia-x-germany-france/>
- Nye, J. (2010). Cyber power, Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from <https://www.belfercenter.org/publication/cyber-power>

OECD. Key ICT Indicators. Retrieved from <https://www.oecd.org/internet/ieconomy/oecdkeyictindicators.htm>

Operator Chmury Krajowej. (2019). Press release of 27 September 2019. Google Cloud został strategicznym partnerem Operatora Chmury Krajowej. Retrieved from <https://chmurakrajowa.pl/partnership.html>

Osimo, D., & Ilves, L. (2019). Roadmap for a Fair Data Economy. Retrieved from <https://lisboncouncil.net/publication/publication/155-a-roadmap-for-a-fair-data-economy-.html>

Osula, A.-M. (2017). Remote search and seizure of extraterritorial data. Tartu: University of Tartu Press.

Oxford Economics and Huawei. (December 2019). Restricting Competition in 5G Network Equipment: An Economic Impact Study. Retrieved from https://resources.oxfordeconomics.com/hubfs/Huawei_5G_2019_report_V7.pdf

Renda, A. (February 2019). Artificial Intelligence: Ethics, governance and policy challenges. Retrieved from https://www.ceps.eu/system/files/AI_TFR.pdf

Routray, S. K., & Sharmila, K. P. (2017). Software defined networking for 5G. 4th International Conference on Advanced Computing and Communication Systems (ICACCS). Retrieved from <https://ieeexplore.ieee.org/document/8014576>

Schaake, M. (2017). Europe should give meaning to the rule of law online. Retrieved from <https://marietjeschaake.eu/en/europe-should-give-meaning-to-the-rule-of-law-online>

Targett, E. (2018). Just 26% of European Enterprises Are Using the Cloud: Eurostat Report. CBR. Retrieved from <https://www.cbonline.com/news/european-cloud-adoption>

Tritten, T. (15 January 2020). Defense Contractors to Face Added Costs with Cybersecurity Audit. Bloomberg Government. Retrieved from <https://about.bgov.com/news/defense-contractors-to-face-added-costs-with-cybersecurity-audit/>

Vestergaard, C., & Umayam, M. L. (November 2019). The Prospect of Blockchain for Stengthening Nuclear Security. IAEA Conference Paper. Retried from https://conferences.iaea.org/event/181/contributions/15812/attachments/8478/11247/FINAL_Prospect_of_Blockchain_for_Strengthening_Nuclear_Security_-_27_Nov_2019.pdf

Weinswig, D. (2018). Transparency Is the New Normal: Top Takeaways from the 2018 Innovation Series. Forbes. Retrieved from <https://www.forbes.com/sites/deborahweinswig/2018/05/25/transparency-is-the-new-normal-top-takeaways-from-the-2018-innovation-series/#4636a71a1e85>



ANALYSIS

Designing Digital Safety into the Smart City

ROBERT MUGGAH

PRINCIPAL, SECDEV GROUP;
CO-FOUNDER, IGARAPÉ INSTITUTE



All cities face digital opportunities and threats. From the wealthiest to the poorest, urban infrastructure, networks, and citizens are vulnerable to foreign and domestic cyber infiltration. Cities are increasingly at risk (Muggah & Goodman, 2019) as digital services expand and more and more devices are connected to the cloud. City residents are also vulnerable to smart city technologies that can be and are being used to conduct mass surveillance and curb their rights both online and off. If lacking adequate oversight and accountability, the hardware and software of digital cities can unfairly discriminate against minorities.

This article explores two basic questions: (1) What are the cyberthreats facing cities and their residents; and (2) How can cities and city networks work to improve their digital safety? These may be among the most significant – if under-appreciated – questions facing cities in the 21st century. Part of the reason is that most of the world’s population is living in cities. The explosive expansion of smart technologies in mature and emerging cities will redefine virtually every aspect of political, economic, and social life. Yet most city leaders and urban residents are only dimly aware of how big the risks are, much less how to deal with them.

The explosive expansion of smart technologies in mature and emerging cities will redefine virtually every aspect of political, economic, and social life. Yet most city leaders and urban residents are only dimly aware of how big the risks are, much less how to deal with them.

The world is currently experiencing two huge mega-trends that are dramatically reconfiguring the future of digital safety in cities and outside of them. The first is the exponential acceleration of technology development and deployment around the world. The global smart city market is expected to grow to over \$717 billion by 2023 (Markets and Markets, 2019). The second mega-trend is hyper-urbanisation and the growing concentration of power in cities. More than three million people are moving to cities every

week, and by 2050 they will be home to over two thirds of the world’s population. These trends are baked in. In the process, cities and city networks are beginning to rival nation states in power and influence (Muggah, 2020).

Technology transformation is occurring so fast – and across so many domains – that it is difficult for international, national, and municipal leaders and institutions to keep up. Indeed, cities around the world are experiencing (or are about to experience) quantitative shifts in IoT, 5G, AI, AR deployment that will transform how metropolitan areas are governed, deliver services, manage commercial exchange, and ensure the safety and security of citizens. Cities are the laboratories, with coalitions of private sector and academic-based institutions driving the process. Along the way, large consultancy firms are overstating many of the upsides of new technologies and downplaying the latent and future risks.

More than three million people are moving to cities every week, and by 2050 they will be home to over two thirds of the world’s population.

Meanwhile, turbo-urbanisation has accelerated over the last 50 years. In the 1950s there were just 3 megacities with populations over 10 million people: today there are almost 40. Mega-regions and large metropolitan areas are growth poles in the real and digital economies. Another 2.5 billion people are going to move to cities in the next three decades, albeit most of them in middle- and low-income settings. According to the UN, this is the largest and fastest demographic shift in history. Most of this growth (90%) will occur in Africa and Asia where cities will need to be redesigned, upgraded, or built from scratch. We’re seeing an explosion of “smart cities” and “techno hubs”: shiny, and often empty, cities in the sands.

These two trends – exponential urban technology expansion and massive urbanisation – are converging. A growing numbers of cities – especially but not exclusively in middle- and upper-income countries – are harnessing new technologies

(remote sensor systems, big data analytics, facial and biometric surveillance) with mixed effects. In some cases, they are developing what I call “agile security” solutions (Muggah, 2018). To be sure, all cities are on the way to becoming digital cities albeit at different temporal and spatial scales. The rules and regulations to manage these processes are evolving haphazardly, even as data protection groups are weighing in. Some cities like San Francisco and Oakland are banning certain technologies (O'Brien, 2019) like facial recognition (many more are using them – D'Onfro, 2019), while others such as those in China are doubling down on mass surveillance (Keegan, 2019).

So what are the big risks that cities are facing in the short-term? There are at least three big clusters: (1) cyberattacks, (2) mass surveillance, and (3) algorithmic bias and discrimination. I'll very briefly focus on these before turning to possible solutions.

The first major threat to making cities “digitally safe” is attack from external and domestic sources. We are already seeing a major escalation of cyberattacks – ransomware, phishing, DDOS attacks, kill-disk malware – targeting municipalities around the world (Muggah & Goodman, 2019). Most of the tools are off-the-shelf and sourced from the Deep Web. Think of them as the 21st-century automatic weapon – cheap, easy to use, and running 24/7. The increases in attacks globally are alarming. About 70% of all reported ransomware attacks in the U.S. in 2018 (Freed, 2019) targeted critical infrastructure – hospitals, schools, police, emergency hotlines, and businesses in counties and cities. At least 70 state and local governments were attacked involving over 620 digital extortion incidents in 2019 (Fernandez, Sanger, & Martinez, 2019 and Ng, 2019). The truth is no one knows how big these challenges really are – cities and insurance companies are reluctant to disclose details. Most cities cannot even tell if their IT systems are subject to breaches.



About 70% of all reported ransomware attacks in the U.S. in 2018 targeted critical infrastructure – hospitals, schools, police, emergency hotlines, and businesses in counties and cities.



An epidemic of cyber threats facing cities are global. London was hit by almost 1 million attacks a month in 2019 according to Centrifry's Freedom of Information request (Narendra, 2019). Ransomware jammed municipal trams in Dublin (Ms. Smith, 2019) and railway ticketing in Stockholm (Johnson, 2017) in recent years. City power plants were also targeted from Hyderabad (Pradhan, 2019) to Johannesburg (BBC, 2019) over the past year. Kiev has become a testing site or even a battleground for all manner of cyber malfeasance, drawing state intelligence units, state-sponsored advanced action groups, and various types of white and black hat hackers (Greenberg, 2017). The costs of these digital incursions are soaring. It is not just the costs of extortion, but the knock-on effects of repairing systems, lost productivity, and rising insurance premiums that are over-burdening local governments. Cities are being targeted because they are soft targets – awareness is low, systems are outdated, and skills are limited.

The truth is that cities globally are poised at the very beginning of a dangerous cyberattack escalation. The coming digital economy and expanding automation of the public and private sectors are a nightmare for cities. Metropolises will soon be managing hundreds of billions of hackable, unpatchable, and unupgradable devices connected to subnational, national, and international grids. So far, most cyberattacks have targeted urban legacy infrastructure, including systems that are either forgotten or poorly managed by IT departments. It is useful to recall that despite the hype, most cities are still generally “dumb”. The real concern is what happens when the attack surface increases dramatically and oil production, electricity grids, transportation systems, water supplies, and all manner of basic services that citizens depend on are exposed?

The second big obstacle to digital safety is mass surveillance. The rising capacity for surveillance is an intrinsic property of “smart cities” – data collection technologies and systems are used for everything from traffic lights and parking to energy use, water management, and policing. Indeed, there has been a sharp rise in the deployment of connected cameras, facial recognition, biometric and scanning systems at the borders of – and across – cities.

But when such technologies are persistent, unaccountable, exploited, and unidirectional, they raise legitimate questions about citizen safety and civil liberties both online and off. Some analysts fear that smart cities themselves are a crucible of “pan-opticon” society where surveillance is mediated by selective biases of its operators.

Metropolises will soon be managing hundreds of billions of hackable, unpatchable, and unupgradable devices connected to subnational, national, and international grids.

Predictably, there are of course some parts of the world where mass surveillance in cities is more intensive than in others. For example, authoritarian and autocratic systems tend to be early adopters of surveillance technologies. Roughly 8 out of the 10 most heavily monitored cities in the world (Zhang, 2019) are in China (the others are Atlanta and London). The city of Chongqing has 2.6 million cameras – one for every six residents – beating out even Beijing, Shanghai, and Shenzhen. There we see a combination of “sharp eyes” monitoring (AI-enabled facial, gait, and biometric surveillance; Denyer, 2018) and the infamous “social credit score” (Marr, 2019). Whether made in China, Israel, or the US, similar technologies are being exported around the world.

While government surveillance in democratic and non-democratic societies is typically cast as a desire to “protect citizens”, this is not always welcomed by local residents. Indeed, there are obvious ways that intrusive technologies can reduce people’s sense of autonomy or privacy and undermine their digital safety. For one, even when surveillance is anonymised, it can reveal “personally identifiable information” that may be protected by privacy laws. The overly broad application of certain technologies (like biometric surveillance) without a “pressing social need” may even violate the International Covenant on Civil and Political Rights. These concerns are voiced more prominently in Western European and North American constituencies than elsewhere.

A third and related challenge involves biases and discrimination in urban digital hardware, software, and their application. As machine learning tools and data-driven software play an increasingly important role in how city governments make decisions, the concerns with how these algorithms are designed and used keep rising. There are real and justified concerns that using data stained with prejudiced policing, judicial practices, or (potentially unconscious) biases of developers will discriminate against minorities and others (Aguirre, Badran, & Muggah, 2019, p. 8–9). Some technology companies recognise the risks that such tools generate (not least to their bottom line), but as noted above, these tend to be downplayed.

While government surveillance in democratic and non-democratic societies is typically cast as a desire to “protect citizens”, this is not always welcomed by local residents. Indeed, there are obvious ways that intrusive technologies can reduce people’s sense of autonomy or privacy and undermine their digital safety.

While the digital challenges facing cities are real, there are also unexpected opportunities. Indeed, the dizzying spread and lowering costs of new technologies mean that fast-growing cities in Africa and Asia may have the second-mover advantage (Aggarwala, Hill, & Muggah, 2018). If urban leaders, planners, and developers take the right decisions early as cities are being designed and developed, they can potentially avoid making the mistakes of their counterparts in other parts of the world. These cities can be designed with digital safety and security in mind from the beginning, not mid-way through or at the end of the process. They will also have tremendous opportunities to leap-frog legacy systems and adopt more efficient options.

If urban leaders, planners, and developers take the right decisions early as cities are being designed and developed, they can potentially avoid making the mistakes of their counterparts in other parts of the world.

First, cities need to adopt a digital safety mindset. A smart city is a digitally secure city. This means having plans, protocols, and personnel in place before, during, and after attacks occur. It means having the right intelligence-led systems in place to detect, mitigate, and contain threats before they spread and having cyber risk insurance in place for when cities are hit, as they surely will be. It means reducing attack surfaces in the city and segmenting networks so that a single point of entry doesn't end up bringing down the entire system. It also requires ensuring city intelligence is informed by the wants and needs of citizens, and not just ICTs.

Second, city executives need to assume a leadership role in digital safety and security. Just like we have mayors coming out in defence of climate and migration, we need our top officials championing digital safety. This is important. Most technology experts say that city mayors and managers don't take cyber security seriously enough. Our mayors, city managers, CIOs, CTOs, and utility executives need to work with partners across society to adopt a whole-of-city approach aligned with the smart city strategy. Building a "joint venture" approach can reduce the likelihood of adversarial relationships between governments and city residents.

Third, cities need to recruit the right personnel to adapt to fast-changing challenges. This means attracting the right talent – including engineers, coders, and hackers. Cities can also outsource some of their needs – some are even issuing RFPs to hire ethical hackers to test city networks and assets. This isn't easy for cities with shrinking budgets and ballooning deficits. But recruitment, together with regular training for all city staff and associated service providers is key. It's often the most basic human errors that cause the biggest problems. Sometimes it's just the simplest of patches – software upgrades, up-to-date firewalls, frequent backups, and multi-factor authentication – that make all the difference.

Fourth, cities should more actively incubate digital safety solutions. Of course the legal frameworks at the international, national, and state levels matter – but cities have more discretion than they

often realise. Cities can crowd-source and help nurture solutions from the global to the municipal scale. For example, they can create open data portals – as many have done – to allow researchers and residents to build apps to improve safety. They can accelerate innovation through incentive competitions or bug bounties. This is a win-win for cities, since by building local innovation ecosystems they also reduce reliance on outside vendors.

Fifth, cities should increase citizen involvement in decision-making and design processes involving digital safety. This is critical, since citizens are increasingly rejecting technologies that are seen as intrusive and opaque. One way to build awareness is through what researchers call the "triple helix" – the combined efforts of government, business, and universities working together. Activities such as smart citizen labs and ICT tasters can help spread understanding and optimise residential uptake of new innovations.

Sixth, cities may wish to set out guidance or standards for algorithmic transparency in decision-making platforms used by the government and related service providers. While the legal case will vary from jurisdiction to jurisdiction, cities could explore ways to improve the explainability, responsibility, accuracy, auditability, fairness, and privacy of their key technologies impinging on safety and security (especially as it relates to, say, issues of crime control, criminal justice and probation, provision of public and financial services).

Finally, cities need to initiate a conversation about the necessary national and global rules and standards to improve digital safety. They cannot wait for nation states or international organisations to take the lead, nor can they rely on business to save them. To do this, urban centres and citizens need to be digitally literate and practice good digital hygiene. Some cities and states are also experimenting with legislation to require all tech devices to have reasonable security features that prevent unauthorised access, modification, and information disclosure. Such norms are more effective if city residents are part of the process of developing such laws to begin with.

Ensuring cities are digitally safe and secure is a comprehensive and complex agenda. But the truth is that the seven priorities identified above are the minimum that must be done. City governments, public utilities, service providing agencies, commercial entities, and digital rights groups will need to learn from one another, share experiences,

and start thinking about more agile norm setting. They will need to be pressing governments and intergovernmental bodies to take bolder action. After all, cities are bearing the brunt of digital insecurity. And the situation is about to get a whole lot worse before (if) it gets better. ■

About the author:



Robert Muggah is a globally recognized specialist in cities, security and new technologies. He is a principal of the SecDev Group – a digital risk consultancy working at the interface of the digital economy and urbanization. At SecDev Group, Muggah helps city, corporate and non-profit leaders improve their future preparedness through high resolution data-driven diagnostics, strategy development, exponential leadership training, and public talks. In addition to his work at SecDev, he is also research director of the Igarapé Institute - a think and do tank - known for developing award-winning data visualizations and technology platforms to improve public safety.

Muggah has spend decades tracking past and future trends in urban risk. He is faculty at Singularity University, senior adviser to McKinsey and Company, a fellow and adviser to the World Economic Forum, chair of the Global Parliament of Mayors, and a regular consult to the United Nations and World Bank. Muggah is the author of seven books and hundreds of peer-review and policy-oriented studies, including *Impact: Maps to Navigate our Past and Future* (Penguin, with Ian Goldin, out in 2020). His research is featured in global media, including the BBC, CNN, Economist, Financial Times, Guardian, New York Times, USA Today and Wired. He has given several TED talks viewed by millions, and speaks regularly at the Davos Summit. Muggah received his DPhil from the University of Oxford and his MPhil from the University of Sussex.

References

Aggarwala, R. T., Hill, K., & Muggah, R. (October 2018). Smart city experts should be looking to emerging markets. Here's why. Retrieved from <https://www.weforum.org/agenda/2018/10/how-the-developing-world-can-kickstart-the-smart-cities-revolution/>

Aguirre, K., Badran, E., & Muggah, R. (July 2019). *Future Crime: Assessing twenty first century crime prediction*. Retrieved from https://igarape.org.br/wp-content/uploads/2019/07/2019-07-12-NE_33_Future_Crime.pdf

BBC. (July 2019). Ransomware hits Johannesburg electricity supply. Retrieved from <https://www.bbc.com/news/technology-49125853>

D'Onfro, J. (July 2019). This Map Shows Which Cities Are Using Facial Recognition Technology—And Which Have Banned It. *Forbes*. Retrieved from <https://www.forbes.com/sites/jilliandonfro/2019/07/18/map-of-facial-recognition-use-resistance-fight-for-the-future/>

Denyer, S. (January 2018). China's watchful eye. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/>

Fernandez, M., Sanger, D. E., & Martinez, M. T. (August 2019). Ransomware Attacks Are Testing Resolve of Cities Across America. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html>

Freed, B. (August 2019). Report: Two-thirds of ransomware attacks in 2019 targeted state and local governments. Retrieved from <https://statescoop.com/report-70-percent-of-ransomware-attacks-in-2019-hit-state-and-local-governments/>

Greenberg, A. (June 2017). How an Entire Nation Became Russia's Test Lab for Cyberwar. Retrieved from <https://www.wired.com/story/russian-hackers-attack-ukraine/>

Johnson, S. (May 2017). Swedish local authority says hit by cyber attack. Retrieved from <https://www.reuters.com/article/us-britain-security-hospital-sweden/swedish-local-authority-says-hit-by-cyber-attack-idUSKBN1882OI>

Keegan, M. (December 2019). Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled. *The Guardian*. Retrieved from <https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled>

Markets and Markets. (2019). *Smart Cities Market by Smart Transportation, Smart Buildings, Smart Utilities, Smart Citizen Services, and Region* [TC 3071]. Retrieved from <https://www.marketsandmarkets.com/Market-Reports/smart-cities-market-542.html>

Marr, B. (January 2019). Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids?. *Forbes*. Retrieved from <https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/>

Ms. Smith. (January 2019). Hacker posts ransom demand on Dublin's Luas tram system site. Retrieved from <https://www.csoonline.com/article/3330651/hacker-posts-ransom-demand-on-dublins-luas-tram-system-site.html>

Muggah, R. (June 2018). How smart tech helps cities fight terrorism and crime. Retrieved from <https://www.weforum.org/agenda/2018/06/cities-crime-data-agile-security-robert-muggah/>

Muggah, R. (January 2020). Look to cities, not nation-states, to solve our biggest challenges. Retrieved from <https://www.weforum.org/agenda/2020/01/cities-mayors-not-nation-states-challenges-climate/>

Muggah, R., & Goodman, M. (September 2019). Cities are easy prey for cybercriminals. Here's how they can fight back. Retrieved from <https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/>

Narendra, M. (August 2019). #privacy: City of London hit by nearly one million cyber-attacks each month. *PrivSec Report*. Retrieved from <https://gdpr.report/news/2019/08/23/privacy-city-of-london-hit-by-nearly-one-million-cyber-attacks-each-month/>

Ng, A. (December 2019) Ransomware froze more cities in 2019. Next year is a toss-up. Retrieved from <https://www.cnet.com/news/ransomware-devastated-cities-in-2019-officials-hope-to-stop-a-repeat-in-2020/>

O'Brien, M. (December 2019). Why some cities and states ban facial recognition technology. *The Christian Science Monitor*. Retrieved from <https://www.csmonitor.com/Technology/2019/1218/Why-some-cities-and-states-ban-facial-recognition-technology>

Pradhan, S. D. (November 2019). Cyber-attack on Kudankulam Nuclear Power Plant underlines the need for cyber deterrent strategy. *The Times of India*. Retrieved from <https://timesofindia.indiatimes.com/blogs/ChanakyaCode/cyber-attack-on-kudankulam-nuclear-power-plant-underlines-the-need-for-cyber-deterrent-strategy/>

Zhang, P. (August 2019). Cities in China most monitored in the world, report finds. *South China Morning Post*. Retrieved from <https://www.scmp.com/news/china/society/article/3023455/report-finds-cities-china-most-monitored-world>



Multi-level Governance in Cybersecurity: What Role for the European Regions?

MILDA KAKLAUSKAITĖ

POLICY MANAGER, EUROPEAN CYBER SECURITY ORGANISATION (ECSO)

Introduction

In its first ever cybersecurity strategy adopted in 2013, the European Union (EU) stated that it aims to “make the EU’s online environment the safest in the world” (European Commission, 2013). Since then, a number of policy measures have been implemented to strengthen the EU’s cybersecurity capabilities and resilience against cyberattacks, including the Directive on security of network and information systems (NIS Directive), Digital Single Market Strategy, the proposal to create the European Cybersecurity Competence Centre and Network, the EU Cybersecurity Act, as well as the Digital Europe and the Horizon Europe programmes. While cybersecurity’s place at the top of the EU’s political agenda raises no doubts, the question of key actors in charge of strengthening the EU’s cybersecurity requires wider debate at both strategic and operational levels.

The concern regarding the key EU cybersecurity actors is a primary focus on the European and national level. The current EU policy suggests that in the context of cybersecurity the principal players are Member States’ national governments, supported by the dedicated EU bodies, such as the European Union Agency for Cybersecurity (ENISA). The role of European regions is largely omitted. However, the regions are what has the biggest potential to connect the technology with the end users, assist local small and medium enterprises (SMEs), and provide them with business support and access to innovative technologies. In order to achieve an effective cybersecurity posture, the EU must realise that national governments and EU institutions are not enough and that more structured inclusion of the regions and the definition of their strategic role

in Europe's cybersecurity is needed. Therefore, this paper argues that the multi-level governance model needs to be established to include European regions in the EU cybersecurity policy implementation.

The regions are what has the biggest potential to connect the technology with the end users, assist local small and medium enterprises (SMEs), and provide them with business support and access to innovative technologies.

Cybersecurity and the changing roles of the state

The traditional approach to security highlights the state as the main referent object of security and the key actor in implementing security politics. Historically, and especially after the establishment of Westphalian sovereignty, the states have had an exclusive authority within their territory and the right to legitimate exercise of power to ensure its security against any external threats. Such security-sovereignty nexus has become deeply enshrined in international and domestic political discourse, making it difficult to include other actors in the traditionally state-dominated field of security. However, the emergence of cybersecurity as a political and security issue suggests the changing role of the state as the key security actor.

The emergence of cybersecurity as a political and security issue suggests the changing role of the state as the key security actor.

Because of its multifaceted and all-encompassing nature, cybersecurity policy requires a diversification of the actors involved in its implementation. The increasing digitalisation and the resulting security challenges place cybersecurity at the top of the political agendas across the globe. Unlike the previous "hot" security challenges that have dominated the political agendas for years (e.g. a classic example of nuclear proliferation during the Cold War), cybersecurity cuts across different policy areas and affects the daily social, economic and political life

of entire society.¹ This new security environment changes the role of the state, making it not only the sole security guarantor, but also the security partner (Dunn Cavelty & Egloff, 2019, pp. 42–49). For example, critical infrastructure protection requires the state to cooperate with the private sector, and to raise cybersecurity awareness the state needs to directly involve society. Sharing the authority and responsibility of cybersecurity with the new actors becomes a prerequisite.

The ensuring of cybersecurity becomes barely possible without close cooperation with the non-state or semi-state actors, including private sector representatives, different levels of government, and NGOs organisations. The cooperation with the private sector has been recognised as an important step in strengthening the EU's cybersecurity, resulting in the contractual public-private partnership on cybersecurity signed with the European Cyber Security Organisation (ECSO) in 2016 (European Commission, 2016). At the same time, European regions still lack recognition as important cybersecurity actors. However, it is the regions that can ensure the cohesive EU cybersecurity policy by linking the local users, research centres, and suppliers of cybersecurity solutions with the national and the European levels.

The (in)visible role of the regions

The main advantage of the regions is their proximity and their ability to build trust among the local cybersecurity stakeholders. Unlike national governments, which tend to (and actually must) have a bird's-eye view of the country's cybersecurity posture, regions enjoy much closer connection to the local cybersecurity stakeholders: from end users and integrators to research and innovation (R&I) centres, product and service providers. The *Pôle d'excellence cyber* initiative, launched under the auspices of the

¹ There is no doubt that the disruptive potential and the far-reaching impact of the cyberattacks are widely recognised. However, in the political discourse cybersecurity is not associated with the "doomsday" and all-out war scenarios which are often considered for "hot" security issues and give the state an exclusive authority to act. As a current security policy priority, cybersecurity is more a matter of the "normal", everyday politics and policy practices rather than the politics of emergency.

French Ministry of Armed Forces and the Brittany Region, is a good example of how the state can benefit and advance its cyber readiness by involving the regional authorities in cybersecurity (Pôle d'excellence cyber, n.d.). This privileged position allows regions to effectively address the cybersecurity innovation and industry development issues which could be difficult to manage by national authorities due to their lack of knowledge about regional cybersecurity environment and its dynamics.

The Pôle d'excellence cyber initiative, launched under the auspices of the French Ministry of Armed Forces and the Brittany Region, is a good example of how the state can benefit and advance its cyber readiness by involving the regional authorities in cybersecurity

The regions could play an important role in strengthening national and European cybersecurity posture. In recent years, European regions have become a frequent target for cyberattacks. The ransomware attacks against a Rouen hospital in France (BBC, 2019) and the city of Frankfurt in Germany (Cimpanu, 2019) that happened at the end of 2019 are just a few examples among many others. The regional preparedness against cyberattacks can serve as a litmus test to identify national strengths and weaknesses. Being in a direct contact with the end users, CISOs (Chief Information Security Officers), critical infrastructure operators, and national governments, regional authorities can establish effective response mechanisms and preventive measures, thus contributing to the increased cybersecurity awareness. Likewise, the ignorance of the regional dimension of cybersecurity could harm the national cohesion, as a cyberattack against the region could be as destructive and costly as an attack against the entire state, with far-reaching repercussions on its economy as well as socio-economic stability. The role of the regions in the EU cybersecurity architecture is paramount.

More specifically, the regional authorities can play an important role in rising cybersecurity awareness among the local SMEs. Representing 99%

of all businesses in the EU and providing two-thirds of the total private sector employment, they are of particular importance to the EU (European Commission, *Entrepreneurship...*, n.d.). Unlike large corporations, SMEs often lack resources or expertise to implement both the digitalisation of their operations and the appropriate cybersecurity measures to protect them. They also too often rule out the possibility of a cyberattack because they assume that they are too small to draw the cybercriminals' attention. The local authorities can effectively address the poor cybersecurity practices by tailored initiatives. The Keep IT Secure (KIS) initiative by Digital Wallonia (Belgium) and Basque Industry 4.0 by the Basque Country (Spain) serve as very good examples. Both programmes have been designed to help local SMEs assess different cybersecurity threats and take the appropriate measures to protect their businesses.

The ignorance of the regional dimension of cybersecurity could harm the national cohesion, as a cyberattack against the region could be as destructive and costly as an attack against the entire state, with far-reaching repercussions on its economy as well as socio-economic stability.

In terms of the EU cybersecurity market development, regions can significantly contribute to the development and deployment of European cybersecurity products and services, thus reducing the EU's reliance on cybersecurity solutions coming from the third countries. Even if the Union has a sufficiently solid cybersecurity landscape with dedicated strategies and financial instruments, it still largely depends on non-European providers. The European regions can play a significant role in escaping this cul-de-sac by leveraging their knowledge of the local cybersecurity ecosystem and adopting national and European resources to solve region-specific challenges. By providing business support to the local cybersecurity SMEs, regions can help to facilitate the commercialisation of European cybersecurity solutions. For example, the Institute for Business Competitiveness of Castilla y León (Spain) has developed a pre-commercial

public procurement programme, which promotes the acquisition of cybersecurity solutions starting with the research, innovation, and development (R&I&D) phase, thus providing the local cybersecurity companies with the financial support and incentives to work on innovation and technological development (ECOSO, 2019). For these reasons, regional authorities should be recognised as a thriving force for the digital transformation of the EU.

Regions can significantly contribute to the development and deployment of European cybersecurity products and services, thus reducing the EU's reliance on cybersecurity solutions coming from the third countries.

Finally, the key role of the regions should be recognised not only in the implementation but also in the design of the European cybersecurity programmes. Having a knowledge of the local cybersecurity ecosystem, regions have a great potential to contribute to accelerating the cybersecurity innovation. The cybersecurity research projects would benefit from involving regional representatives. Such involvement would help to ensure the sustainability and applicability of the research projects to market needs. To achieve this, the future European technology research programmes, such as Horizon Europe, would need to clearly integrate the regional dimension and establish practices for more robust involvement of regional research bodies.²

The existing regional cybersecurity initiatives in the EU

The EU has recognised the importance of regions to its cybersecurity posture, and thus economic stability and growth, which reflects at the strategic and policy levels. Unlike its previous version, the updated 2017 cybersecurity strategy, titled *Resilience, Deterrence and Defence: Building strong*

cybersecurity for the EU, stated that the regional dimension of cybersecurity readiness is very important to ensure the EU's readiness to effectively prevent and react to cyber incidents. The document also underlined the importance of facilitating "more targeted capacity building in different regions" (European Commission, 2017). In addition to conferences and tailored workshops to address the role of the regions, few key European initiatives have been launched to support regional cybersecurity building.

The CYBER project has been initiated under the EU Interreg Europe programme and the European Regional Development Fund (ERDF) financial instrument to strengthen the local cybersecurity SMEs and to boost interactions among the European regional cybersecurity ecosystems (Interreg, n.d.). The lack of cooperation among different cybersecurity stakeholders and different ecosystems is identified as one of the challenges preventing local cybersecurity SMEs from scaling up and internationalising their business. The CYBER involves nine institutional partners, representing different EU countries and regions: Bretagne Development Innovation agency (France), Institute for Business Competitiveness of Castilla y León (Spain), Tuscan Region (Italy), Digital Wallonia agency (Belgium), Brittany Region (France), Kosice IT Valley (Slovakia), Chamber of Commerce and Industry of Slovenia (Slovenia), Estonian Information System Authority (Estonia), as well as the European Cyber Security Organisation (Belgium). To address the cooperation challenge, project partners work together to develop and implement regional action plans and concrete policy instruments to improve the inter-regional cooperation.

The European Cyber Valleys pilot project is another EU initiative launched to address regional cybersecurity aspects (European Commission, *Smart...*, n.d.). Just like CYBER, it recognises the interregional cooperation as a key enabler for facilitating the development of the European cybersecurity value chain, reducing market fragmentation, as well as boosting the investment and commercialisation of the European cybersecurity solutions. Currently, the project involves the European regions which

² The involvement of regional research centres to such programmes as the Horizon Europe would allow the actors to better manage the cascade funding for the SMEs to uptake or develop digital innovation, as the regional authorities would be able to serve as intermediaries between the EU funds and the local cybersecurity companies that seek funding.

identify cybersecurity as a strategic smart specialisation priority, namely Estonia and the regions of Castilla y León (Spain), Brittany (France), North Rhine-Westphalia (Germany), and Central Finland (Finland). One activity recently implemented under the European Cyber Valleys framework was the mapping of European regional cybersecurity ecosystems, which helped to identify the European cybersecurity capabilities provided by 470 regional cybersecurity players. The project continues developing the operational strategy which would allow further development of the EU's regional cybersecurity ecosystems, a.k.a. cyber valleys.

The CYBER project and the European Cyber Valleys pilot action are two fine examples of the targeted initiatives aimed to reduce European cybersecurity market fragmentation and to strengthen its competitiveness on a global stage by involving the regions. However, such time-bound initiatives for the regional involvement are not sufficient. The regions should be institutionalised and become a permanent feature of the EU cybersecurity-building efforts. For this, multi-level governance, involving the European, national, and regional levels, should be established.

Multi-level approach to the EU cybersecurity governance

The application of the multi-level governance approach to the EU cybersecurity policy implementation would allow European regions to play an active role in strengthening the EU cybersecurity posture. Multi-level governance is defined as the dispersion of central political power and the delegation of decision-making processes between governments and non-governmental actors at various territorial levels (Bache & Flinders, 2004, p. 3). Due to the ever-evolving risks and far-reaching implications of cybersecurity, the European regions cannot be left in a wait-and-watch position. To establish the effective multi-level governance, the vertical and the horizontal dimensions of regional involvement in the EU's cybersecurity governance should be recognised: responsibility-sharing across different levels of government (i.e. European, national, and regional) as a vertical dimension and interregional cooperation as a horizontal dimension.



Placing the European regions next to the EU and the national government as one of the key actors in the EU cybersecurity governance provides a territorial perspective on cybersecurity issues.

The vertical dimension of multi-level governance is important because it allows the European regions to take an active role in the cybersecurity policy formulation and implementation. Placing the European regions next to the EU and the national government as one of the key actors in the EU cybersecurity governance provides a territorial perspective on cybersecurity issues. The European regions are better placed to initiate and coordinate certain types of cybersecurity initiatives. They also possess a more intimate grasp of the cybersecurity developmental needs, on-the-ground policy issues and the state of cybersecurity in their respective territories. By representing regional perspectives, policy efforts undertaken at the regional level can effectively complement pan-European (as well as international) discussions on cybersecurity. Likewise, the regions can help to build awareness of the policy outcomes in their respective territories and be the strategic drivers in the implementation of the internationally agreed decisions.

The cooperation among the regions as the horizontal dimension of multi-level governance is important for its potential to reduce cybersecurity market fragmentation, which remains one of the biggest challenges for the EU. The interregional cooperation helps to break down regional silos and establish trustworthy communication channels which in turns incentivises sharing good practices and exchanging information on the regional challenges and needs. The creation of such linkages between the regions not only can help to optimise the EU's cybersecurity coordination but also benefit the local cybersecurity SMEs. These companies can have more opportunities to scale up their business outside their local market and facilitate the commercialisation of their cybersecurity solutions abroad. The interregional cooperation is also fundamental for developing regional innovation ecosystems, because the less the regions are fragmented, the more they can exploit their cybersecurity innovation potential.

In lieu of conclusions


This article argued that to have a truly effective EU cybersecurity, European regions should be recognised as important players and involved in the policy formulation and implementation. The key strength of the regions is their proximity to the local cybersecurity market players and their familiarity with the local cybersecurity ecosystems. As an intermediate governance level between the national and the European, they can significantly contribute to the enhanced EU's cybersecurity posture in a more effective and sustainable manner. They have instruments to reduce policy overlaps, create synergies among different stakeholder groups, and enhance the innovative performance and commercialisation of European cybersecurity companies.

Despite the regional cybersecurity initiatives fostered by the EU and some clearly successful examples of the local initiatives implemented by the regions themselves, their role is not well recognised. The territorial perspective on the EU cybersecurity policy formulation and implementation is rather rudimental. European regions often find themselves confined to the roles of mere consultation and feedback providers but never rise to the positions associated with negotiations and decision-making.

To take the full advantage of the regions' potential, their role in the EU cybersecurity governance should be institutionalised. The vertical and the horizontal engagement of the regions would help establish the multi-level governance of the EU cybersecurity. To achieve this, responsibility-sharing among the European, national, and regional levels of government and the interregional cooperation mechanisms should become inherent components of the EU cybersecurity governance. ■

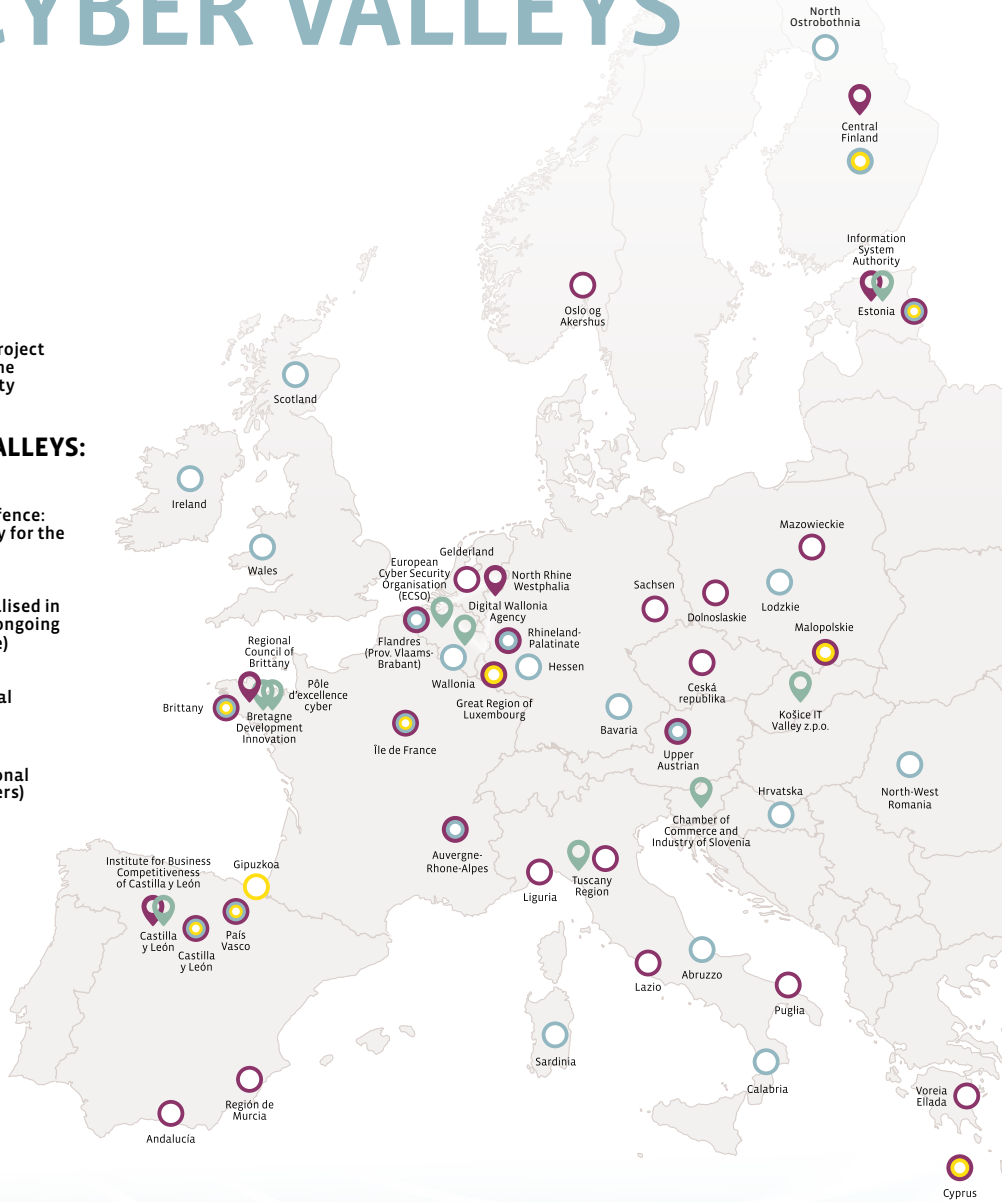
CONNECTING EUROPEAN CYBER VALLEYS



 An interregional cooperation project to enhance public policies for the competitiveness of cybersecurity companies

EUROPEAN CYBER VALLEYS: PILOT ACTION

-  Resilience, Deterrence and Defence: Building a strong cybersecurity for the European Union
-  Digital Innovation Hubs specialised in cybersecurity (established or ongoing process based on JRC database)
-  Smart specialisation or regional strategy on cyber security
-  ECSO Regional members (Regional authorities and regional clusters)



About the author:



Milda Kaklauskaitė is a Policy Manager at the European Cyber Security Organisation (ECSO). She works on such issues as cybersecurity market analysis and investment promotion, competitiveness and scaling up opportunities for the European cybersecurity startups and SMEs, as well as European regional cooperation on cybersecurity. Before joining ECSO, she worked at the Brussels-based political thinktank, at the Lithuanian Parliament as an assistant to MP and the Lithuania-based communications agency. She holds master's degree in international relations from Central European University (CEU) and bachelor's degree in political science from Vilnius University Institute of International Relations and Political Science (VU IIRPS).

References

Bache, I., & Flinders, M. (2004). Themes and Issues in Multi-level Governance. In Bache, I., & Flinders, M. (Eds.), *Multi-level governance* (pp. 1–11). Oxford/New York: Oxford University Press.

Cimpanu, C. (19 December 2019). Frankfurt shuts down IT network following Emotet infection. ZDNet. Retrieved from <https://www.zdnet.com/article/frankfurt-shuts-down-it-network-following-emotet-infection/>

European Commission. (2013). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001>

European Commission. (5 July 2016). *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2321

European Commission. (2017). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Retrieved from <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450>

European Commission. (n.d.). *Entrepreneurship and Small and medium-sized enterprises (SMEs)*. Retrieved from https://ec.europa.eu/growth/smes_en

European Commission. (n.d.). *Smart Specialisation Platform: Cybersecurity*. Retrieved from <https://s3platform.jrc.ec.europa.eu/cybersecurity>

European Cyber Security Organisation (ECSO). (2019). *The Role of the regions in strengthening the European Union's cybersecurity*. Retrieved from <https://ecs-org.eu/documents/publications/5dc043279c3fd.pdf>

Interreg Europe CYBER. (n.d.). *Regional policies for competitive cybersecurity SMEs: Project summary*. Retrieved from <https://www.interregeurope.eu/cyber/>

Dunn Cavelty, M. and Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing different roles of the state. *St Antony's International Review* 15 (1). 37–57.

Pôle d'excellence cyber. (n.d.). *Présentation du Pôle*. Retrieved from: <https://www.pole-excellence-cyber.org/presentation-du-pole/>

Rouen hospital turns to pen and paper after cyber-attack. (21 November 2019). BBC. Retrieved from <https://www.bbc.com/news/technology-50503841>

CYBERSEC *Women*

Women in Cybersecurity – A Bit of Context

- The actual number of women working in the cybersecurity field is still a matter of debate. Research carried out by Reed et al. in 2017 indicates that only 11% of the global cybersecurity workforce is female and that this figure is as low as 7% in Europe, while according to the 2019 (ISC)² Cybersecurity Workforce Report the number of women in cybersecurity has reached almost one quarter (24%) of the overall workforce.
- Women's underrepresentation in STEM has deepened imbalances in the labour market with an estimated **one million unfilled IT security vacancies worldwide**. Therefore, the sector is not able to develop to its full potential and to wholly reap the benefits of innovation.
- Diverse workforces perform better in decision-making, financial, and competitive matters. These are skills that are highly required in cybersecurity. Diversity in cybersecurity contributes to both **efficiency of teams and sustainability of solutions**, making it important for national security and imperative for business.
- The **gender pay gaps** are quite significant in STEM, with women making on average \$5,000 less than men in security management positions. The positive note is that younger women face less severe pay discrepancy than older women.

Sources: Reed, J., Zhong, Y., Terwoerds, L., & Brocaglia, J. (2017), *The 2017 Global Information Security Workforce Study: Women in Cybersecurity*; (ISC)². (2019). *Women in Cybersecurity*; McKinsey&Company (2015), *Why diversity matters*.





Boosting the Role of Women in Cybersecurity

Interview with Nicole Wajer,
Technical Solutions Architect, CISCO

Thank you, Ms Wajer, it is an honour to have the opportunity to conduct this interview. To begin with and to set the scene, could you briefly give us an overview of how big the gap between the number of male and female cybersecurity professionals is? What is the extent of the current women's scarcity in cybersecurity?

Anecdotally, women are awfully scarce in the cybersecurity field; except for a limited set of countries (Sweden, Romania, and Poland come to mind), it's quite rare to run into a female colleague. To a large extent, I guess, this is a remnant of traditional gender roles, but the STEM field is unfortunately also still considered largely devoid of human interaction and therefore slightly boring by many – a stereotype that continues to require a lot of effort to shake off.

The STEM field is unfortunately also still considered largely devoid of human interaction and therefore slightly boring by many – a stereotype that continues to require a lot of effort to shake off.

Would you say girls' reluctance to go for a job in cybersecurity is also linked to the perception of this field that you've just touched upon? What is the perception of a girl going to work in cybersecurity nowadays?

From experience I've noticed that girls see everything/everybody as equal before they reach the age of 12. There is no difference between boys and girls. However, when it's time for decisions, of course the people that are close to you, parents, have a great influence on them. If the parents are in IT, the perception of cybersecurity is positive and viewed as a normal job you can get. If the parents aren't IT versed, then it can somehow be painted in a way that is not close to reality.

In your opinion and based on your experience, what are the main causes of women's underrepresentation in cybersecurity and ICT sectors? Did you personally encounter any obstacles when it comes to embracing a career in these fields?

The main obstacle does seem to be the gloomy reputation of the IT industry in general as a bit of an old boys' club that involves lots of screen-staring

and very little interpersonal contact. This stereotype is of course far from generally applicable, and many companies are doing their utmost best to be different. On the other hand, I have encountered actual difficulties in advancing my career because of organisational issues in dealing with people that don't fit in with the establishment, so I do understand the hesitation of new entrants into the field.

The question on how to attract and retain individuals in the IT or cybersecurity sphere often regards young people leaving their country to work abroad. I would like to ask you the same question but referring to women. How can we make this field attractive and encourage women to pursue a career in it?

In my opinion, the only way to do this is to lead by example: women, and especially young people about to decide on their post-secondary education path, need to be able to see plenty of role models that show IT to be the exciting and rewarding line of work that it is. Of course, for such role models to exist, the industry needs to step up its efforts at inclusiveness, and there is also much work that remains to be done at the primary and secondary education levels to prevent women from prematurely tuning the STEM field out. But in general, people need to be shown, not told.

Women, and especially young people about to decide on their post-secondary education path, need to be able to see plenty of role models that show IT to be the exciting and rewarding line of work that it is.

Do you believe that educating young children (under 12 years old) in cybersecurity and computing technology would help with reaching out to more girls and break the stereotypes in the field?

You can't start young enough. A girl can wear a princess dress or be dressed as an alien, it doesn't matter, she can still crush the stereotypes. Teaching them at an early age what is possible with computer technology just tears down these perception barriers other people are putting up that these jobs are only for men.

What goals, in terms of workforce diversity, would you like to see companies striving toward? What concrete measures could be implemented?

Every company that is serious about workplace diversity should continuously be identifying the obstacles that keep minorities from making practical use of the theoretical options available to them, and then work on removing those as much as possible. Although the exact process will vary by company and even department, I've found that mentoring and internship programmes at every level (allowing people to get comfortable with job roles that they may not have considered before) and explicit career ladders (that do not rely on insider knowledge of the available options or lots of negotiation) are helpful in this regard.

Every company that is serious about workplace diversity should continuously be identifying the obstacles that keep minorities from making practical use of the theoretical options available to them, and then work on removing those as much as possible.

What are the effects of women's underrepresentation in cybersecurity in ICT, or in other words what are the advantages of gender diversity in a cybersecurity team?

Both my own personal experience and numerous studies have shown that a diverse workforce performs better. This is especially true for cybersecurity, where insights from team members with dissimilar backgrounds frequently lead to identifying threats that had been previously overlooked or allow use cases to be addressed that are specific to non-mainstream user groups.

Despite the scarcity of women representatives in the field, we can notice that, compared to men, a higher percentage of women cybersecurity professionals are reaching positions such as chief technology officer (7% of women vs 2% of men), vice president of IT (9% vs 5%), IT director (18% vs 14%)



and C-level / executive (28% vs 19%).¹ **Would you say that there is no glass ceiling in the digital sphere or maybe that women finally broke it?**

In my opinion, the lack of career advancement for women in IT in general is more of a supply-side issue than an actual glass ceiling, with the situation slowly improving over time. Given that cybersecurity is a relatively recent specialisation, it's quite plausible that women got in on the ground floor on a more equal basis, and that this has resulted in a naturally more diverse executive suite. It will be interesting to see whether these numbers hold and to what extent they can be replicated in other IT sectors.

What women role models can you think of, to inspire young girls and women?

Youngsters nowadays use YouTube and Instagram a lot. Until recently it was more Snapchat (that is still being used but less popular). The role models would come from this industry like vloggers and photographers. Mind you, the best role models for these young girls would be their own parents. They have been around them for a lifetime and discuss life and jobs constantly. Hence I guess, besides educating the kids, it's also key to engage the parents too if they are not in IT yet.

Nowadays, there is no doubt that women's participation in cybersecurity, STEM, and ICT has to be fostered. Could you briefly explain to our readers what the purpose of Cisco's Women in Cybersecurity group is? What concrete results did you achieve?

Informal groups are an important part of Cisco culture and are quite helpful for both newcomers and long-time employees to navigate the opportunities available in such a large organisation. As with other groups (such as Early in Career Network and the more general Women in Tech), the focus with Women in Cybersecurity is on sharing experiences and information. I've been present at several coffee talks about the opportunities within the security field, as a result of which several people have

¹ (ISC)², Women in Cybersecurity, <https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx>, p. 3.

applied for new positions within the company. External presentations are typically more general but have convinced at least a few women to settle on a STEM study they had been considering.

Another question related to perception of the IT and cyber spheres again. Why do we have the image of hacker as a man, and how to make things change?

Have you ever seen a house burglar as a woman? This is probably the same reason hackers are thought of as men. Yet there are loads of examples of famous women that hacked major systems. Mata Hari is a good example of a spy² yet nobody expected this from a woman. The same goes for Cyber Hacking – one does not simply expect that a woman would do such a thing. In order to make this change we must go into the gender-neutral stage.

² For a more comprehensive biography of Mata Hari, see for instance: <https://www.britannica.com/biography/Mata-Hari-Dutch-dancer-and-spy>

In the Netherlands, for example, the announcements in the train are nowadays gender neutral – I still have to get used to it, as when I hear the little announcement sound before the voice starts to speak, I automatically wait for “ladies and gentlemen”, yet now they say “dear traveller”. Again, it will take time before no one notices the difference anymore.

Finally, if you could give advice to the cyber-enthusiast women reading us, what would it be?

Go for it! Cybersecurity is a relatively new and exciting field with lots of opportunities and great demand for resources across all disciplines, be it architecture, sales, implementation, support, or engineering. Don't be afraid to ask around, and if you can find someone willing to mentor you, use the opportunity. ■

Questions by Faustine Felici

Nicole Wajer is based in Amsterdam, The Netherlands and has a global role for the security part of SDA (Software Defined Access) and SD-WAN in the Enterprise Networking team as a Technical Solutions Architect (IBN Security). She graduated with a degree in Computer Science from the Amsterdam University of Applied Sciences and specializes in Security, the Internet of Things (IoT) and IPv6.

Her career in Cisco started in Routing and Switching and Network Security, but since fighting spam and malware turned out to be in her DNA since her first day on the Internet, a move to Content Security was an obvious progression. Recently she joined the Enterprise Networking team to continue her Security passion. Some side activities Nicole is the EMEAR lead for the Women in Cybersecurity trying to get as much female talent attractive into the world of STEM. Nicole is also known in Cisco as the 'Chief Stroopwafel Officer'.

As people who have met her in person will attest, Nicole is very friendly and talkative, as well as quite active on social media. She also acts as the social secretary for Koala, her stuffed marsupial travel companion and conversation starter.



Insider Threats in Cybersecurity: The Enemy within the Gates

ANALYSIS

GUERRINO MAZZAROLO

PHD STUDENT AT UNIVERSITY COLLEGE DUBLIN (UCD)

ANCA D. JURCUT

ASSISTANT PROFESSOR, SCHOOL OF COMPUTER SCIENCE, UNIVERSITY COLLEGE DUBLIN

Introduction

The 2019 Capital One data leakage – as the latest instance of exploitation carried out by the actions of an insider threat – “involves the theft of more than 100 million customer records, 140,000 Social Security numbers and 80,000 linked bank details of Capital One customers, allegedly stolen by a single insider, according to court filings in Seattle” (Kate Fazzini, 2019). Cybercrime continues to exhibit rising trends. According to a study provided by Ponemon Institute and Accenture (2019), there was an 11% increase in the average annual number of security breaches in 2018. A data breach is an incident in which protected data has been accessed or disclosed in an unauthorised fashion. Those kinds of incidents can be caused by internal

or external actors. Internal ones are either malicious or careless users. The external threat category includes hackers, cybercriminals, and state-sponsored actors. The data breaches that appear on the news are typically carried out by outsiders. Attacks coming from the outside generally expose threats that have been addressed with traditional security measures through a “defence in depth” approach. The hazards that originate from inside are more difficult to prevent and detect because insiders pose a high danger as they are familiar with the organisation’s network topology, systems, directives, and policies, and they have access to confidential information with relatively low restrictions. When we analyse cybercrime, we

often underestimate the dangers of the internal threat. Insiders present a significant risk to organisations and, even if they were not the most common source of attacks in past years, they were the most expensive and difficult to recover from.

Definition

There are two main types of insiders: malicious users (those that intentionally harm the institutions, as described above), and unintentional insider users (those that accidentally expose confidential data, as described below). These activities endanger confidentiality, integrity, and availability of a business.

Different definitions of malicious insider threat could be found. The one from CERT US provides a comprehensive explanation. “A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and *intentionally* exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems” (Capelli, Moore, & Trzeciak, 2012). Motivators behind malicious insiders could include: monetary gain, a disgruntled employee, entitlement, ideology, or outside influence with the consequences of fraud, sabotage, espionage, and theft or loss of confidential information.

“A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems”.

The official working definition from the report *Unintentional Insider Threats: A Foundational Study* states that an *unintentional* insider threat is: “a current or former employee, contractor, or business partner who has or had authorized access

to an organization’s network, system, or data and who, through action or inaction *without malicious intent*, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems” (CERT Insider Threat Team, 2013, p. 2).

Insider threats could be considered the biggest cybersecurity danger to firms, organisations, and government agencies. According to the security company Clearswift, “Organizations report that 42% of IT security incidents occur as a result of their employees['] actions” (Clearswift, 2017).

Current concerns

The dangers posed by insiders have multiple variables that must be considered when the risk is assessed. The following list provides an outline of the most important tasks that need to be addressed in order to be aware of the hazard introduced by internal actors.

Firstly, an insider can easily bypass existing physical and technological security controls through legitimate rights. Employees, in fact, need to access the organisation’s data for their daily tasks. Spotting the malicious activity is extremely difficult and time consuming. In addition, members of staff with sufficient technical knowledge can elude security controls currently in place.

Another factor that needs to be considered is that technology alone is not enough. Controls can detect and block malevolent actions; however, if we want to prevent indiscriminate users, we need additional information. Human values have a huge influence on comportment and sometimes can provide indications that help to identify a person’s further actions. Emerging techniques are focusing on sentiment analysis. Monitoring and identifying disgruntled employees could greatly increase chances of isolating promiscuous activity.

In order to prevent malevolent activities, we need data from different controls. The availability of this information is often jeopardised within an entire organisation and by being available to a different business owner. The difficulty is to have the approval



of different stakeholders in order to have legal access to the data. Once these are aggregated, it is important to add correlation rules to the raw data so that it can give us significant information to help our Security Operation Center (SOC) to be alerted in case of any infraction or suspicious behaviour.

Safeguarding the privacy of the data in accordance with the law is mandatory for every firm and organisation. It is necessary that insider threat analysts follow laws regarding privacy, civil liberties, and legal guidance, including the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016).

Preventing data leakage does not stop at the boundary of a firm's network and it goes further beyond. The continued interaction with different business partners exposes systems to another threat. It is difficult to control the cybersecurity standards of affiliates. If not monitored properly, dishonest employees could use this as an entry point to an organisation's data and system, and misuse it.

Preventing data leakage does not stop at the boundary of a firm's network and it goes further beyond.

Types of insider activities

A study conducted by NATO's Cooperative Cyber Defense Centre of Excellence (Kont, Pihelgas, Wojtkowiak, Trinberg, and Osula, 2015) categorises threats into five different main areas:

1. Fraud – consisting of the use of the company's information and data for personal gain.
2. IT sabotage – which is a major and unpredictable action against the firm and could seriously impact the availability of the overall infrastructure.
3. Intellectual property theft – which is a remunerative action that permits insiders to exfiltrate copyrights, patents, trademarks, and trade secrets without permission.

4. Espionage – the practice of illegally obtaining information about the plans and activities from industrial or international government entities.
5. Unintentional – employee that have no malevolent intent, although their actions, or behavior, occasionally affect the organisation.

Unintentional actors can, due to carelessness, also lead to a major security breach. This could cause as much damage as malevolent actions. Disclosure of classified information in the public domain and social media, accidentally replying to phishing campaigns, or downloading malicious code off the Internet are all examples of negligent activities that could have serious consequences for the organisation. A famous example within this category was the breach perpetrated on the American security company RSA in 2011. Four employees were targeted through a phishing email campaign, one of them clicked on the attachment that used a zero-day exploit, targeting a vulnerability. The intruders succeeded in exfiltrating confidential information related to the company's SecurID two-factor authentication products (Zetter, 2011).

As technology grows and develops, malicious actors are constantly evolving and impacting our society. "Hacktivist" is a term used since 1994 (Hamann, 2019). Recently, this threat category has been popular in the media. According to Adam Meyers, CrowdStrike's Vice President of Intelligence, the first quarter of 2019 has registered an increase in hacktivism (Lily Hay Newman, 2019). The word "hacktivism" combines "hacker" and "activist". It consists of gaining unauthorised access to ICT systems and carrying out a variety of disruptive actions as a means of achieving political and social goals. In cases such as those of Chelsea Manning and Edward Snowden, thousands of classified documents were leaked, and a large amount of confidential information was revealed. Those incidents involve a number of distinct forms of cybercrimes – sabotage, espionage, intellectual property theft – and mark the difficulties of preventing a malicious actor from dispersing data even if sophisticated controls are in place (MacAskill, 2017).

Proposed remediation guidelines

To increase the chances of preventing, detecting and responding to insider threats, the overall security of the organisation must be well structured and organised.

Every project needs an executive-level manager's leadership. In a company, a chief information security officer (CISO) must provide a long-term vision, engage with all departments, and finally promote and build a strong insider threat program (InTP). An effective InTP must include participation from different stakeholders. Mandatory departments that could contribute actively to the project are human resources, information assurance, legal, and cybersecurity.

Best practices for an InTP should take into consideration at least the following areas in order to decrease the overall risk: administrative controls, technical controls, physical controls, security awareness, and incident response.

1. Administrative controls such as policies, directives and regulations must be clearly documented and enforced. It is important to show the acceptable use of an organisation's system, network, and information. It is relevant to remark what is expected from employees and also the possible consequences of violations. This is a valuable deterrence method.
2. Technical control is generally considered the backbone of every InTP. Data loss prevention, email monitoring, web proxy, rogue device detection, endpoint analytics, security information and event management (SIEM) are safeguards that can detect and prevent data leakage. In recent years, security has developed a new capability called User and Entity Behaviour Analytics (UEBA). This includes a behavioural analysis of entities other than the users, such as routers, servers, and endpoints. UEBA is much more effective since it can analyse the behaviour across multiple users and ICT devices in order to detect complex attacks.

3. Physical controls are also well-founded in assigning the least privilege, i.e. only enough access to perform the required job, and in implementing a segregation of duty when more than one person is required to complete a critical function. Physical controls are also used to control and minimise the risk of unauthorised access to physical assets and information systems.
4. The employees in a company need to have security awareness training, with a specific chapter dedicated to insider threat in order to explain what is expected from them and which threats they might be exposed to. Unintentional insider threat may be recruited from outside through social engineering. It is important to make all employees knowledgeable about such hazards and to train them how to avoid being the weakness in the organisation's security barrier.
5. Finally, the organisations must be ready to respond to an incident involving a malicious or unintentional insider threat. The incident response (IR) workflow should be part of an existing plan. However, the process should also include the escalation of the reporting, the notification to management, and submission to an investigation officer.

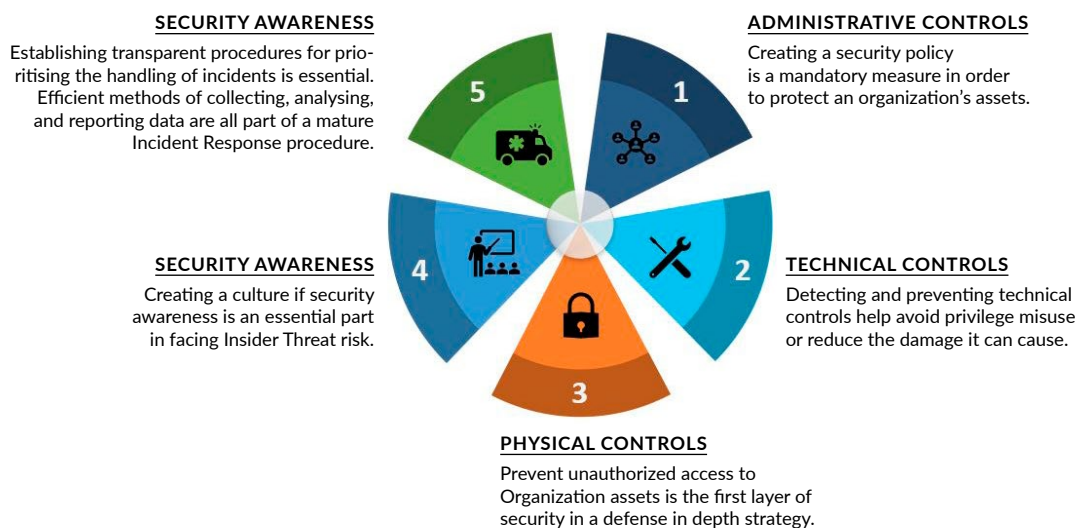
Future challenges

A new challenge has appeared in the recent years. This concerns the adoption of cloud and mobile technology in companies, and it transformed the IT infrastructures considerably. Physical boundaries of corporate networks and digital assets are becoming less clearly defined than they used to be in the past. Therefore, new challenges are calling for new approaches.

Since it is difficult to stop an insider threat at the boundary, early detection is the key. In modern ICT infrastructure, several technical controls are implemented and could identify suspicious activities such as unauthorised access, violation of organisation policies, internal reconnaissance, abuse of rights, and data loss. However, cybersecurity should not concern technology only. This approach can prevent and control the possible damage, but nowadays this approach is not enough; it should be integrated with an additional layer. Guarding information and systems against insiders with illegitimate intentions requires a multidimensional defensive strategy.

Analysing user personalities through social media and combining the information with the technical domain could represent a dynamic approach to decrease the likelihood of such threats.

Figure 1. Proposed Remediation Guidelines.



Marwan Omar remarks: "Organizations need to implement multi layered defensive approaches to combat insider risks" (2015, p. 162).

Nowadays, technical controls are already present in most organisations' security programs. However, because of an increasingly threatening landscape, they cannot be solely relied upon. New technologies are periodically proposed, which potentially offer the malicious employees new opportunities to strike. Using innovative know-how as a countermeasure should be the main priority.

Technologies based on machine learning and artificial intelligence are to be implemented in order to assist with prevention and detection of insider threats before they can cause irreversible damage. The future development chapter of cybersecurity has yet to be written, particularly with the coming power of quantum computers.

New technologies are periodically proposed, which potentially offer the malicious employees new opportunities to strike. Using innovative know-how as a countermeasure should be the main priority.

Conclusion

Insider threat employees represent a wolf in sheep's clothing. Daily, real examples clearly show that insider threats create a significant hazard to every company, institution, and organisation. A potential

malicious insider can cause millions of euros in damage by stealing intellectual property, sabotaging facilities, or disclosing information that can irreparably compromise the organisation. However, an unintentional insider can cause irreversible damage as well.

Enterprises will never be able to fully make sure that employees have no malicious intentions, or that they won't ever fall for phishing email campaigns. Meanwhile, although the elimination of all risks is not possible, the overall risks could be reduced and the residual risk controlled. Too often, the security strategy is dedicated to the edge security layer and ignores that a conspicuous threat might come from within the organisation.

To conclude, defending your enterprise from insider threats is a vital part of information security best practices. It is essential that your company's highly valuable classified data and assets are protected from its greatest threat: the enemy within the gates. Every mature cybersecurity program nowadays should contain an insider threat assessment and a comprehensive insider threat program to protect a corporation's people, facilities, networks, and intellectual property. ■

Disclaimer: The views and opinions expressed in this article are those of the authors' and do not necessarily reflect the official policy or position of any other institution, employer or company.





About the authors:

Guerrino Mazzarolo is a PhD Student at University College Dublin (UCD). His research interests focus on Information Security. He has over 20 years of experience working on IT security with leadership positions in industry, government and international organization.



Anca D. Jurcut received a bachelor of Mathematics and Computer Science from West University of Timisoara, Romania (2007) and a Ph.D from University of Limerick, Ireland (2013). Since 2015, she has been an assistant professor with the School of Computer Science, University College Dublin, Ireland. Her research interests focus on network and data security & privacy, security for internet of things (IoT), security protocols, formal verification techniques and applications of blockchain technologies in cybersecurity.

References

- Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT Guide to Insider Threats*. Retrieved from <https://www.semanticscholar.org/paper/The-CERT-Guide-to-Insider-Threats%3A-How-to-Prevent%2C-Cappelli-Moore/10d66c35f1322ab883bf32a425ce9f4e2b6deebe>
- CERT Insider Threat Team. (2013). *Unintentional Insider Threats: A Foundational Study* (CMU/SEI-2013-TN-022). Retrieved from <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744>
- Clearswift. (2017). Insider Threat: 74% of security incidents come from the extended enterprise, not hacking groups. Retrieved from <https://www.clearswift.com/about-us/pr/press-releases/insider-threat-74-security-incidents-come-extended-enterprise-not-hacking-groups>
- Fazzini, K. (2019). The Capital One breach is unlike any other major hack, with allegations of a single engineer wreaking havoc. *CNBC*. Retrieved from <https://www.cnn.com/2019/07/30/capital-one-hack-allegations-describe-a-rare-insider-threat-case.html>
- Hamann, N. (2019). "Hacktivism": about the origins, meaning and history of online Activism. Retrieved from: <https://www.firstlinepractitioners.com/hacktivism/>
- Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2015). Insider Threat Detection Study. Retrieved from https://ccdcoc.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf
- Lily Hay Newman (2019). Hacktivists Are on the Rise – but Less Effective Than Ever. Retrieved from <https://www.wired.com/story/hacktivism-sudan-ddos-protest/>
- MacAskill, E. (2017). WikiLeaks publishes 'biggest ever leak of secret CIA documents'. Retrieved from <https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance>
- Omar, M. (2015). Insider threats: Detecting and controlling malicious insiders. In Dawson, M., & Omar, M., *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, pp. 162–172. Hershey, PA: IGI Global.
- Ponemon Institute LLC and Accenture. (2019). The cost of cybercrime. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
- Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). General Data Protection Regulation. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- Zetter, K. (2011). Researchers uncover RSA phishing attack, hiding in plain sight. Retrieved from <https://www.wired.com/2011/08/how-rsa-got-hacked/>

ANALYSIS

Back to the Civilian Power Discourse: Can it Survive in Cyberspace?

OMREE WECHSLER

SENIOR RESEARCHER, YUVAL NE'EMAN WORKSHOP FOR SCIENCE, TECHNOLOGY AND SECURITY, TEL AVIV UNIVERSITY

CYBERSEC

YOUNG LEADERS

Introduction

The rise of state-sponsored cyberthreats to government networks, critical infrastructure and services along with the theft of technological and trade secrets and the disruption of economic sectors have brought to major changes in the way states perceive their strategic and defensive posture. Many cybersecurity incidents in recent years have turned worldwide attention towards cyberspace and the potential risks it involves. According to the US (United States) DNI (Director of National Intelligence) from 2017 to 2019, Daniel Coats, cybersecurity threats have risen to the top of the nation's national security concerns and became one of the most important priorities for the DNI and the intelligence community (MeriTalk, 2017).

One of the more interesting, in fact crucial trends in the last couple of years is the change that has

taken place within the national cyberstrategies of states which had traditionally refrained from the use of hard power in particular, and the change in their defensive postures in general. In June 2019, a leaked internal document of the German government described the planning of a new strategy, which would allow Germany to hack and disrupt the functionality of IT systems used for an attack, as well as to take servers down (Prager, 2019). Also Denmark, Greece, and Sweden have shown interest in developing military offensive cyber capabilities (Danish Ministry of Defence, 2018; Defense New, 2017; Jacobson, 2017).

This article deals with the question how the new threats from cyberspace change the strategic and defensive postures of traditionally peaceful states. Given that the term "pacifism" may not

fully fit states which employ standing armies and are members of security alliances, the article goes back to the old international relations concept of a “civilian power” and discusses its relevance in cyberspace. Furthermore, this article uses the case studies of Germany and Japan as examples for traditionally restrained powers that are moving in a more pro-active direction in cyberspace. Both Germany and Japan are central targets for cyberattacks due to their diplomatic and economic background. Both are leading members in their respective regions and are allies of the US. Both are also two of the world’s strongest and largest developed economies that rely on industries such as automobiles, chemicals, electronics, and machinery, which makes them subject to the threat of commercial and technological espionage. Additionally, both were defined as civilian powers in previous works, due to their economic strength and reluctance to use force.

The main argument in this paper is that despite the fact that state-sponsored cyberthreats are mobilising states which could be defined as “civilian powers” to take up a more pro-active stance in cyberspace, thus increasing their preparedness to use force in cyberspace, yet visible transformations are not enough to erode their civilian power postures.

The first part of this article provides the definition of a “civilian power” in international relations and a model of benchmarks, discusses its validity for both case studies and follows its adaptations to new international challenges after the Cold War. The second part tracks strategic changes in Germany and Japan’s traditional defensive approach in cyberspace, and includes the analysis of these changes vis-à-vis the civilian power model.

Civilian power as a foreign policy role in international relations

THEORETICAL BACKGROUND

The concept of “civilian power” was defined during the Cold War and was used to describe a new trend in projecting influence. The term was first developed by François Duchêne in the early 70s and referred to the international posture of

Europe. Duchêne argued that the superpower and nuclear stalemate of the Cold War had brought the rise of civilian forms of influence with which Europe may remain a centre of influence despite its decline as a military power. Thus, Europe, as a civilian power, influences international affairs by using its economic power, rather than the military one, in order to spread civilian and democratic standards (Duchêne, 1973, pp. 19-20). In terms of wielding influence and the means of power, one can outline Duchêne’s civilian power as an actor who uses economic power, namely resources, and what could be perceived although not mentioned, sanctions, embargos, and trade bans.

In 1990, Hanns Maull has further expanded Duchêne’s definition of “civilian power” and added some other components. According to Maull, the concept implies: 1. the acceptance of the necessity of cooperation with others in the pursuit of international objectives, namely acting multilaterally; 2. the concentration on non-military, primarily economic, means to secure national goals (though military power must remain to safeguard other means of international interaction); 3. willingness to develop supranational structures to address critical issues of international management. Developing supranational structures requires a partial transfer of sovereignty, which in turn allows the development of an international rule of law (Maull, 1990, p. 92, 106).

Maull has further explained that the term “civilian power” derives not from the prohibition on the use of military power or from its irrelevance, but from the will of the civilian powers to “civilise” international relations along the lines of democracy and domestic politics. In other words, the main goal of civilian powers is to change international relations in a way – they will be characterised by a more “civilised” and less violent manner and will resemble societies under democratic polity (Maull, 2005, pp. 779-780). That being said, civilian powers’ role is clear and their means of influence are the power of their markets, resources, technological superiority and the attractiveness their way of life holds. This paper uses Maull’s civilian power model, namely to define civilian powers as states

which: 1. focus on cooperation to pursue international objectives; 2. prefer to use soft means of power, such as, however not limited to, economic means in foreign policy; 3. support the establishment or strengthening of supranational bodies, while sharing sovereignty, as means to promote international rule of law and in order to address international problems.

HISTORICAL COMPARISON AND THE CHOICE OF CASE STUDIES

Historical developments in the 19th and 20th centuries have drawn the attention towards some political, historical and economic similarities between Japan and Germany as well as their roles and positions in international relations. Both countries saw some major political events which led to their unifications in the second half of the 19th century. In both, national reconstruction produced imperial states that promoted industrialisation in favour of military expansion (Anderson, 1991, p. 11). Both became revisionist, expansionist, and militarist powers who had been handed a catastrophic defeat in WWII, after which both fell under Western occupation, which sought to democratise and reintegrate them into the Western community (Inoguchi and Bacon, 2006, p. 4; Dobbins, Poole, Long & Runkle, 2008, pp. 11, 27-35).

In his work from 1990, Maull extended the term “civilian power” to depict the foreign policies of Germany and Japan, in order to claim that both had gone through a profound transformation which emphasises an abstention from power politics combined with significant economic strength. According to Maull, Germany and Japan’s civilian power postures turn them into prototypes of a promising future, therefore representing peaceful nations, which prefer to project influence through economic rather than military means. He further pointed out that the end of the Cold War has marked a shift in the dynamics of international relations from the military-political sphere to economic and social developments, a shift that favours both countries and one which will dictate a change in American foreign policy as well (Maull,

1990, p. 93). Given that both countries still employ armies, it is not to suggest that civilian powers will refrain from using military force for the purposes of self-defence, collective security or humanitarian intervention, but will rather seek to “civilise” or “domesticate” international relations as relations within a democratic international community.

GERMANY AND JAPAN’S “CIVILIAN POWER” ROLE AFTER 1990

Since the 1990s the “civilian power” role conception was met with changes within the global system and new challenges, such as ethnic conflicts and global terrorism, which saw both countries struggling to maintain their foreign policy principles. Since 1990, Germany, whose traumatic past had led its leadership to avoid the use of military power, intervened militarily in Kosovo in 1999 (Hyde-Price, 2001, pp. 21-23), took part in counter-insurgency missions in Afghanistan starting from 2007 (Noetzel, 2011, pp. 399-400)¹ and sent reconnaissance aircrafts to support the coalition against ISIS in Syria in 2015 (Peifer, 2016, p. 268). Japan, on the other hand, managed to avoid the use of force, though not without taking steps that throw its pacifist stance into question. Such steps include the Abe government’s resolve to revise Article 9 in the Japanese constitution which renounces war as a sovereign right (Kajimoto and Sieg, 2018) and its plan to convert its helicopter carrier *Izumo* into an aircraft carrier, which could hardly be perceived as a defensive weapon system (Gady, 2018).

However, despite such challenges, observers maintained that the two states still managed to uphold their civilian power postures. According to Adrian Hyde-Price (2001, p. 32), Germany remained a civilian power after the participation in the Kosovo war, due to its overriding concern to stop human suffering while avoiding civilian casualties. Hans Maull (2000, p. 71-73) has also examined the German participation in NATO operations in Kosovo. According to Maull, several

¹ Starting in 2002, Germany participated in reconstruction and stabilisation missions in Northern Afghanistan. However, with the security situation deteriorating in 2007, German troops got more involved in counter-insurgency missions against Taliban fighters.

shifts in the global arena have caused changes in Germany's security posture, however, those are not representing a departure from its civilian power posture. Judging by Maull's own model, it appears that Germany acted as a part of a cooperative NATO operation, used force after the exhaustion of all other non-military means, while providing large-scale humanitarian assistance to refugees in Albania and Macedonia.

Demirtas and Mazlum (2018, pp. 40-54) examined Germany's use of force during the participation in ISAF (International Security Assistance Force) in Afghanistan and in coalition operations against ISIS in Syria. In both cases, Germany has again acted as a part of a coalition of partners, under resolutions of the UN Security Council and against global terrorism which in both cases also posed a threat to European security.

Both the change of Germany's security and foreign policy posture and the more subtle change within Japan's security stance represent a security policy reorientation in both countries' traditional post-WWII foreign policy identity and an attempt to reframe their security and foreign policy roles in the face of new expectations and challenges. In Germany's case the drivers of change were the rise of global terrorism, conflicts with implications to European stability, and its allies' expectations that it should contribute more to international efforts. In Japan's case, it is the deterioration of the East Asia security environment which stems from North Korea's nuclear and ballistic missile programmes as well as China's growing military investment and its aggressiveness in the East China Sea. Despite these challenges, it seems that in the years since 1990, both countries have mostly maintained their civilian power postures.

Civilian powers in cyberspace

THREAT PERCEPTION AND CHANGES WITHIN GERMANY AND JAPAN'S NATIONAL CYBER POLICIES

Many countries, including Germany and Japan, have acknowledged in recent years the nature and scale of cyberthreats and the critical risk they

pose to national security, stability and democracy, and to public order and critical economic sectors. A central change in threat perception could be seen when comparing Germany's national cyber-strategy documents from 2011 and 2016. While the 2011 document presented cyberthreats in fairly general terms, the 2016 document has already indicated the complexity of the threat and its implications to German economy, public safety, and democracy and recognised the wide spectrum of potential attackers and their motives (Wechsler, 2018, p. 56-57).

Also Japan's 2018 national cyber policy strategy and the 2018's National Defense Program Guidelines acknowledge the growing cyberthreats to Japan and represent its preparations to secure the 2020 Olympic and Paralympic Games, which will take place in Tokyo (Japan Times, 2018). Large-scale cyberattacks on Japan's government networks and critical infrastructures, such as the 2011 attack on Japan's largest defence contractor, Mitsubishi Heavy Industries, and the 2014 attack on the Monju nuclear power plant have pushed the government to move forward and update its cybersecurity policy to face current threats (Dardenne, 2018).

Germany's Cyber and Information Space Command, CIR (German: *Cyber-und Informationsraum*), was established as part of the German army (*Bundeswehr*) in November 2015 and turned fully functional in April 2017. Its tasks are defined as passive and active defence in cyberspace. Within CIR, the Bundeswehr has begun developing offensive cyber capabilities which are designed to collect intelligence from foreign networks and systems and to interfere in or disrupt their operation. These offensive capabilities are being developed under the responsibility of the CNO (Computer Network Operations) team, whose manpower, authority, and capabilities have been extended (Kahl, 2013; Skierka, 2016). In September 2017, the German government announced the creation of a federal agency named the Central Office for Information Technology in the Security Sphere (ZITiS). ZITiS is a civilian agency, responsible for analysing digital forensics, however is also tasked

with developing surveillance strategies, exploits, malwares, and innovative techniques to break into encrypted communications (Knight, 2017). Another step that may imply Germany's striving for independence in the development of both defensive and offensive cyber capabilities is the launching of a new cybersecurity research and development agency, which was approved by the cabinet in August 2018. The new agency's purpose is to equip the security agencies with new technologies and capabilities. However, many critics within the German Parliament (*Bundestag*) have expressed fear that the new agency will focus on offensive capabilities for the intelligence and military agencies (Sprenger, 2018).

Also **Japan** has been showing signs of changing course towards a more pro-active posture in cyberspace. In its revised National Defense Program Guidelines, Japan has expressed its will to "employ flexible deterrent options and other measures" (Cabinet Secretariat, 2018, p. 11). Additionally, Japan has set the objective to deter opponents by making them realise that their deeds will be "consequential" (Cabinet Secretariat, 2018, p. 8), therefore punishable. Punishing adversaries in cyberspace requires full knowledge of their systems, networks, and vulnerabilities as well as having exploits and malwares ready at hand. Furthermore, Japan's 2018 Cybersecurity Strategy document stated that the government would promote the policy of pro-active cyberdefence, which would enable the use of technologies to induce attacks in order to collect information on attackers (National Information Security Centre, 2018, pp. 22-23). In May 2019, Japanese local media cited an unnamed government source which had admitted that the Ministry of Defense contacted private companies in order to create malware, including viruses and backdoors, to be used as deterrents (Cimpanu, 2019; Japan Times, 2019).

These steps by both countries imply a policy change from a purely defensive posture into a more pro-active, deterring posture, by expanding and modernising their militaries to achieve superiority in cyberspace as well as by developing offensive means.

PROACTIVITY IN CYBERSPACE: ARE GERMANY AND JAPAN STILL CIVILIAN POWERS?

In order to answer the question of Germany and Japan's civilian power posture in cyberspace, there is a need to analyse their strategic cybersecurity components, means, and goals vis-à-vis the three aspects of civilian power, namely, multilateralism, emphasis on non-military means, and promoting international law by supporting the development of supranational structures.

Multilateralism: In terms of multilateralism, a civilian power is expected to cooperate with other states and regions to solve international problems. Cooperating and negotiating with partners is perceived as a way to prevent actors from returning to what Maull called "old politics" (1990, p. 97). An examination of Germany and Japan's foreign and defence policies in cyberspace shows that both countries comply with the civilian power expectations. In that sense, Germany's role within NATO, and specifically within NATO's CCDCOE (Cooperative Cyber Defence Centre of Excellence), and its contribution to the sense of collective security can be seen as a multilateral way to face the challenge of cyberthreats. In February 2019, Germany announced that it would provide NATO with its national cyber capabilities in order to defend the allies against cyber and electronic warfare (Paganini, 2019). This sharing of capabilities, either offensive or defensive, implies a loss of autonomy for the benefits of interdependence, thus may prevent countries from acting unilaterally. This setup is even more relevant in cyberspace due to the nature of cyber weapons. From the attacker's perspective, cyber weapons are considered to be single use. Once they are employed, the adversary is very likely to perform an investigation, locate the used vulnerability and fix it, rendering the exploit useless. A capable adversary could also perform reverse engineering and repurpose the exploit (Smeets, 2018, pp. 8-9). These unique features of cyber weapons render the sharing of offensive cyber capabilities even more limiting, thus preventing states from acting one-sidedly or aggressively.

Japan's national cybersecurity strategy states that the government will contribute to various international discussions and work for sharing information and expertise with foreign countries and promote specific cooperation and collaboration (National Information Security Centre, 2018, pp. 40-41). In that sense, Japan has been strengthening its regional cooperation with the ASEAN (Association of Southeast Asian Nations) members. Japan's cooperation with ASEAN states in the field of cybersecurity has been an ongoing effort in the past several years. In February 2017, a Japanese information security company, NEC, announced that it would train government officials from Indonesia, Vietnam, the Philippines, Myanmar, Laos, and Cambodia as part of a contract signed with Japan's International Cooperation Agency (Parameswaran, 2017). In September 2018, the Cybersecurity Capacity Building Centre was established in Thailand with Japanese funding as part of an agreement between ASEAN and Japan's representatives, according to which more than 700 cybersecurity personnel from Southeast Asia were expected to be trained in cyberdefence, digital forensics and malware analysis (Tanakasempipat, 2018). Japan's initiatives and growing cybersecurity cooperation with the ASEAN states is a part of a wider effort to boost regional resilience and promote economic, security and business interests through development and capacity building. According to Maull, the ability to shape international processes depends on technological and economic capabilities and strengths. Those are manifested in Japan's regional cooperation in the field of cybersecurity. Another interesting aspect that is opposed to Japan's efforts to become an independent pro-active player in cyberspace is its will to preserve its reliance on the US and its dominance in cyberspace, especially in the realm of deterrence. In April 2019, after a meeting between American and Japanese defence officials, US Secretary of State Mike Pompeo declared that a cyberattack on Japan could in certain circumstances constitute an armed attack under Article 5 of the US-Japan Security Treaty. This declaration could serve as a deterrent message to China, as it states that a cyberattack on Japan may in some cases draw an American response (Wolfe, 2019).

Preference to use non-military means in foreign policy: While there is no example of a German or Japanese major offensive cyber operation known to the public,² the discussion has to revolve around building offensive capabilities and the manner and purpose of their use. Some may say that cyber weapon development programmes and the establishment of cyber warfare military teams may indicate the will to use force. However, looking at various strategy documents and officials' comments, it does seem that both nations are putting a strong emphasis on self-defence. In Japan's National Defense Program Guidelines, it is clearly stated that the Japanese SDF (Self-Defense Forces) will focus on identifying incidents, limiting damage and on recovery. Additionally, in the case of an ongoing cyberattack, the SDF will "block and eliminate the attack", thus using its capabilities for self-defence (Cabinet Secretariat, 2018, p. 12). While Japan seems to be focused on self-defence, Germany seems to be lacking a strategic plan on how and when to use its offensive cyber capabilities. Having no strategic plan in place may indicate a lack of will to use these capabilities and that the "culture of reluctance" that came to describe the reluctance to use force may still be present in Germany's strategic mindset (Schulze, 2018).

While Japan seems to be focused on self-defence, Germany seems to be lacking a strategic plan on how and when to use its offensive cyber capabilities.

In terms of the ability to use the newly acquired or future capabilities, both nations face constitutional hurdles which severely limit their operations.

Japan's most prominent challenge facing its ability to use force in cyberspace is the aforementioned Article 9 of the constitution that renounces war and prohibits Japan from initiating any offensive actions as well as allows it to employ only the minimum necessary level of defence capabilities.

² German military did hack an Afghan mobile operator in 2016 in order to locate the whereabouts of a kidnapped German woman. Due to the circumstances, this could not fit into the pure definition of projecting influence by force.

Japan's initiatives and growing cybersecurity cooperation with the ASEAN states is a part of a wider effort to boost regional resilience and promote economic, security and business interests through development and capacity building.



As of July 2019, Prime Minister Abe's ruling party has failed to gain the two-thirds majority needed for amending the constitution (Kyodo News, 2019). Germany also suffers from constitutional barriers. As part of the country's aforementioned "culture of reluctance", the German constitution states in Article 87a that any use of military force for purposes that are not purely defensive requires a parliamentary mandate. A report from the German Ministry of Defence states that the need for the parliamentary mandate is also valid for operations in cyberspace (Bundesministerium der Verteidigung, 2016). However, due to the complexity of this space, where it is not always possible to distinguish between defensive and offensive moves, questions arise as to how and in which cases the army must turn to parliament for its approval. It appears that the section in the constitution requiring parliamentary approval for active defence operations or a pre-emptive strike could pose a challenge to cyber operations, particularly in the instances where rapid, covert responses are needed. The means for bridging these gaps have not yet been found.

Judging by the current constitutional situation in both countries as well as their will and purpose to use force as shown in their self-defence strategies, or lack thereof in Germany's case, it appears that both are hesitant and would apparently use force only as a last resort. A characteristic which is compatible with the definition of a civilian power.

Promoting international rule of law by transferring sovereignty to supranational bodies: From Germany and Japan's international behaviour, both seem to be focused on promoting the establishment of international norms and principles for a responsible state behaviour in cyberspace as well as fully applying international law in cyberspace.

Germany's national cyberstrategy document from 2016 repeats Germany's commitment to lead the discussions within international organisations, such as the OSCE (Organization of Security and Cooperation in Europe) and the UN. More specifically, Germany is committed to enhancing compliance with international law in cyberspace, closing loopholes in international law with regard

to cybersecurity, developing norms, regulations, and principles regarding a responsible state-conduct, and reinforcing the capabilities and authority of the UN in cyberspace (Bundesministerium des Innern, 2016, p. 41).

Japan's Ministry of Foreign Affairs has also published a document, named "Japan's Cyber Diplomacy", which portrays the three pillars of Japan's cyber diplomacy. While the first pillar hinges on Japan's bilateral dialogues, the second pillar mentions Japan's role within the UN GGE (United Nations Group of Governmental Experts) and its push towards applying international law in cyberspace as well as confidence-building in cyberspace within the framework of the UN (Ministry of Foreign Affairs, 2018, p. 4).

Using Hans Maull's criteria as benchmarks for the definition of civilian powers, it is clear that both Germany and Japan may still be regarded as civilian powers. While Maull did not condemn civilian powers for employing a standing army or the use of force for mere self-defence or in the pursuit of civilian power ends, the conclusion may well be that even the striving for offensive cyber capabilities, as long as those will be used for these purposes, does not render these nations incompatible with the civilian power definition.

However, there does seem to be a subtle change. While Germany and Japan's security needs were largely provided by the alliance with the US during the Cold War and while their non-intrusive, mostly defensive posture allowed them to avoid military conflicts, cyberspace's special characteristics have brought new challenges. Both Germany and Japan's economies, industries, technological prowess and central position in their respective regions make them lucrative targets for crime organisations and state-sponsored cyberattacks. Understanding the magnitude of the threat, along with the failure to defend themselves, are driving both nations to adopt a more pro-active posture in cyberspace. While the change may still be subtle, growing challenges may strengthen the trend and both nations' determination to adopt a more offensive posture.

Both Germany and Japan's economies, industries, technological prowess and central position in their respective regions make them lucrative targets for crime organisations and state-sponsored cyberattacks. Understanding the magnitude of the threat, along with the failure to defend themselves, are driving both nations to adopt a more pro-active posture in cyberspace.

Conclusions

Analysing both Germany and Japan's national cyberstrategies along with recent changes in the way the use of force is rethought has shown that current changes are not enough in order to deny both nations' role in international relations as civilian powers. More specifically, both nations maintain multilateralism and cooperation with other actors, allies and regional cooperation bodies as pillars of their security and foreign policies. Both nations emphasise and promote the application of the rule of law in cyberspace within international and supranational platforms, such as the UN and the EU. Regarding the use of force and despite recent attempts to acquire offensive cyber capabilities, it seems that both nations still face constitutional barriers which will be difficult to either amend or settle with the special rules of engagement in cyberspace. Both also put the emphasis on the use of force for the sole purpose of self-defence or on subjecting it to full parliamentary oversight. This parliamentary oversight may hinder pro-active cyber operations against parties involved in cyberattacks, and will therefore bind the hands of the military in cases such as Germany's new planned strategy. Another problem is the lack of a specific plan on how and when to use offensive cyber capabilities, what their objectives are, and how they shall be used to convey a message to the attackers, especially when attribution problems persist.

More broadly speaking, one may also conclude that despite the decades that have passed since the establishment of the term "civilian power", the term still seems to be relevant to describe

foreign and security policy roles, also in cyberspace. However, as the use of cyberspace for crime, espionage, elections meddling, disruptions, and sabotage increases, so may the willingness of more pacifist and peaceful nations to use force in order to defend themselves. The higher the number of nations employing offensive cyber capabilities, the greater the threat of further destabilisation of cyberspace, along with nations' temptation to use them. As mentioned, using offensive cyber capabilities to disrupt adversaries' malicious activity or as a punishment requires reconnaissance and intelligence gathering which consist of network infiltration operations, which in turn may be detected, thus increasing the chances for a conflict, in cyberspace or in the physical realm.

A way to address the threat should consist of several elements. The first area to focus on is the strengthening of cyber defence. This will have to include forming more regional alliances and cooperation with like-minded states, along with deeper contributions from the private sector. The second focus area is the promotion of international norms and principles of behaviour in cyberspace. To achieve that, and given the stagnation at the UN GGE, like-minded states should decide on norms and principles within the scope of regional blocs, such as the EU and ASEAN, as well as promote and negotiate them with other regional blocs, such as the African Union.

(...) despite the decades that have passed since the establishment of the term "civilian power", the term still seems to be relevant to describe foreign and security policy roles, also in cyberspace.

Yet another area for action is to reduce the incentive to use cyberattacks by decreasing plausible deniability and improving attribution capabilities. This should go along with naming and shaming as well as sanctioning malicious states behaviour in cyberspace. ■



About the author:

Omree Wechsler is senior researcher for cybersecurity policy and strategy at the Yuval Ne'eman Workshop for Science, Technology and Security in Tel Aviv University. His research fields include information operations, states' cyberstrategies and cyber weapons proliferation. Omree holds an MA degree from the interdisciplinary European Studies program in the Heinrich Heine University of Düsseldorf, Germany, and graduated with honours, a double major BA in Political Science and Middle Eastern Studies from Tel Aviv University. He has worked as a research intern at the Israeli Institute for National Security Studies (INSS) in the Arms Control research program which dealt with nuclear arms control and the Iranian nuclear program, and participated in the Executive Training Program for diplomats at the Diplomatic Academy in Vienna. He served three years in the military intelligence branch in Israel Defense Forces.

References

- Anderson, P. (1991). The Prussia of the East?. *Boundary* 2, 18(3), 11-19. doi:10.2307/303200
- Bundesministerium der Verteidigung. (2016). Abschlussbericht Aufbaustab Cyber- und Informationsraum. April 2016, p. 5. Available at: http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf
- Bundesministerium des Innern. (2016). Cyber-Sicherheitsstrategie für Deutschland 2016. P. 41.
- Cabinet Secretariat. (2018). National Defense Program Guidelines for FY 2019 and beyond (Provisional Translation). December 18, pp. 8, 11. Available at: http://www.cas.go.jp/jp/siryou/pdf/2019boueikeikaku_e.pdf
- Cimpanu, C. (2019). Japanese government to create and maintain defensive malware. *ZDNet*, May 5. Available at: <https://www.zdnet.com/article/japanese-government-to-create-and-maintain-defensive-malware/>
- Dardenne, A. (2018). *Cybersecurity: the potential for Japan-India cooperation*. Asia Dialogue. May 30. Available at: <https://theasiadialogue.com/2018/05/30/japanese-cybersecurity-and-the-potential-for-japan-india-cooperation/>
- Dobbins, J., Poole, M., Long, A. & Runkle, B. (2008). *After the War: Nation-Building for FDR to George W. Bush*. Santa Monica, CA; Arlington, VA; Pittsburgh, PA: RAND Corporation. Pp. 11, 27-35.
- Duchêne, F. (1973). The European Community and the Uncertainties of Interdependence. In: M. Kohnstamm and W. Hager, ed., *A Nation Writ Large? Foreign Policy problems before the European Community*, 1st ed. London and Basingstoke: Palgrave Macmillan, pp.19-21.
- Gady, F. (2018). Japan to Convert Izumo-Class Into F-35-Carrying Aircraft Carrier. Retrieved 7 August 2019, from <https://thediplomat.com/2018/12/japan-to-convert-izumo-class-into-f-35-carrying-aircraft-carrier/>
- Hyde-Price, A. (2001). Germany and the Kosovo war: still a civilian power?. *German Politics*, 10(1), pp. 21-23.
- Inoguchi T. and Bacon P. (2006). Japan's emerging role as a 'global ordinary power'. *International Relations of the Asia-Pacific*, 6(1), p. 4.
- Japan Times. (2018). *Japan crafts new cybersecurity strategy for 2020 Tokyo Olympics*. July 25. Available at: <https://www.japantimes.co.jp/news/2018/07/25/national/japan-crafts-new-cybersecurity-strategy-2020-tokyo-olympics/#.XU6YdeMzblU>

- Japan Times. (2019). *In first, Japan to develop computer virus to defend against cyberattacks*. April 30. Available at: <https://www.japantimes.co.jp/news/2019/04/30/national/first-japan-develop-computer-virus-defend-cyberattacks/#.XVLFE-gzaUk>
- Kahl, C. (2013). Vom Kampf in der fünften Dimension. *Bundeswehr Journal*. May 3. Available at: <http://www.bundeswehr-journal.de/2013/vom-kampf-in-der-funften-dimension/>
- Kajimoto, T., & Sieg, L. (2018). Japan's Abe aims for constitution change in bid for extended term. *Reuters*, September 10. Available at: <https://www.reuters.com/article/us-japan-politics/japans-abe-aims-for-constitution-change-in-bid-for-extended-term-idUSKCN1LQ0AU>
- Knight, B. (2017). Hacking for the government: Germany opens ZITIS cyber surveillance agency. *Deutsche Welle*, September 14. Available at: <https://www.dw.com/en/hacking-for-the-government-germany-opens-zitis-cyber-surveillance-agency/a-40511027>
- Kyodo News. (2019). Abe wins upper house poll but suffers constitutional reform setback. July 22. Available at: <https://english.kyodonews.net/news/2019/07/7daa3eb5fd2b-voting-begins-in-japans-upper-house-election.html>
- MariTalk. (2017). *Cyber Looms as Top National Security Threat, DNI Says*. Available at: <https://www.meritalk.com/articles/cybersecurity-national-security-threat-dni-daniel-coats/>
- Mauil, H. (1990). Germany and Japan: The New Civilian Powers. *Foreign Affairs*, 69(5), p. 92-93, 106.
- Mauil H. (2000). Germany and the Use of Power: Still a 'Civilian Power'?. *Survival*, 42(2), pp. 71-73.
- Mauil, H. (2005). Europe and the new balance of global order. *International Affairs*, 81(4), pp. 779-780.
- National Information Security Center. (2018). *Cybersecurity Strategy (Provisional Translation)*. July 27, pp. 22-23, 40-41. Available at: <https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf>
- Ministry of Foreign Affairs. (2018). Japan's Cyber Diplomacy. P. 4. Available at: <https://www.mofa.go.jp/files/000412327.pdf>
- Noetzel, T. (2011). The German politics of war: Kunduz and the war in Afghanistan. *International Affairs*, 87(2), pp. 399-400.
- Paganini, P. (2019). Germany makes its cyber capabilities available for NATO alliance. *Security Affairs*, February 15. Available at: <https://securityaffairs.co/wordpress/81125/cyber-warfare-2/germany-nato-alliance-warfare.html>
- Parameswaran, P. (2017). Japan-ASEAN Cyber Cooperation in the Spotlight. *The Diplomat*, February 24. Available at: <https://thediplomat.com/2017/02/japan-asean-cyber-cooperation-in-the-spotlight/>
- Peifer, D. (2016). Why Germany won't be dropping bombs on Syria, Iraq or Mali. *Orbis*, 660(2), p. 268.
- Schulze, M. (2018). Germany develops offensive cyber capabilities without a coherent strategy of what to do with them. *Council on Foreign Relations*, December 3. Available at: <https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them>
- Skierka, I. (2016). Bundeswehr: Cyber Security, the German Way. *Digital Frontiers (blog), Observer Research Foundation*, October 20. Available at: <https://www.orfonline.org/expert-speak/bundeswehr-cyber-security-the-german-way/>
- Smeets, M. (2018). A matter of time: On the transitory nature of cyberweapons. *The Journal of Strategic Studies*, 41(1-2), pp. 8-9.
- Sprenger, S. (2018). German Cabinet approves new cybersecurity agency. *Fifth Domain*, August 31. Available at: <https://www.fifthdomain.com/global/europe/2018/08/31/german-cabinet-approves-new-cybersecurity-agency/>
- Tanakasempipat, P. (2018). Southeast Asian cyber security center opens in Thailand. *Reuters*, September 14. Available at: <https://www.reuters.com/article/us-asean-cyber/southeast-asian-cyber-security-center-opens-in-thailand-idUSKCN1LU1GO>
- Wechsler, O. (2018). Germany's cyber strategy – government and military preparations for facing cyber threats. *Cyber, Intelligence and Security*, 2(1), pp. 56-57.
- Wolfe, D. (2019). A cyber-attack in Japan could now bring the US into war. *Quartz*, April 20. Available at: <https://qz.com/1600574/a-cyber-attack-in-japan-could-now-bring-the-us-into-war/>



During two days of the European Cybersecurity Forum – CYBERSEC 2019, around 100 speakers discussed how to secure the world’s digital DNA. The CYBERSEC team has prepared the recommendations by following closely the statements made by CYBERSEC 2019 participants.

[Download the publication HERE](#)

ANALYSIS

Piercing the Bubble with a Cyber Needle – Cyber Tools Application during a Possible Baltic States Defence Scenario

DOMINIK SKOKOWSKI
EXPERT, THE KOSCIUSZKO INSTITUTE

In 2019 Jamestown Foundation published a report detailing a probable scenario of a Russian invasion of the Baltic States and their possible defence. The report contained several key objectives to be accomplished for the defence to be successful. One of them was suppressing the A2/AD systems currently deployed in Kaliningrad. To achieve this goal, the report recommended joint Polish-American land invasion of the Russian exclave. It is obvious that invading the Russian land would carry immense risks of casualties and escalation, including a nuclear attack (Hooker, 2019, p. 28).

The aim of this article is to investigate whether there are less drastic, ideally non-kinetic ways to achieve this objective, and, if the use of kinetic force would prove necessary, how cybertools can help achieve objectives on the ground.

A2/AD – Anti Access/Area Denial

A2/AD technology enables one party to effectively deny its adversary the freedom of entrance to and operation within a certain domain in a given area. E.g., an anti-aircraft missile system with a 200 km range can create an A2/AD bubble around the centre of its deployment, and the enemy aircraft flying into the range of the system risks being shot down. Although many A2/AD systems have a stated nominal range, their true effectiveness can vary due to many factors, e.g. weather, local topography, and the characteristics and behaviour of the target.

The importance of Kaliningrad

Kaliningrad is a Russian exclave, a piece of land squeezed between Poland and Lithuania, with access to the Baltic Sea. It is home to a variety of surface-to-air missile (SAM) systems, including the famous S-400 – with a nominal range of 400 km. Along with anti-sea and anti-land systems they create a bubble encompassing the three Baltic States, a large portion of Poland and a considerable part of the Baltic Sea. In the scenario of an armed conflict between NATO and Russia, the A2/AD systems deployed in Kaliningrad could greatly complicate maintaining supply routes to the Baltic states by either sea or air.

In the scenario of an armed conflict between NATO and Russia, the A2/AD systems deployed in Kaliningrad could greatly complicate maintaining supply routes to the Baltic states by either sea or air.

A2/AD systems vulnerabilities

The A2/AD systems consist of many interrelated parts – each with distinct vulnerabilities. The anti-aircraft system can be neutralised in a number of ways. The attacker can try to evade the defender's systems by means of camouflage, electronic jamming, application of decoys, etc. – these are called soft-kill countermeasures. Direct, hard-kill countermeasures depend on breaking the system's kill chain, which is find, fix, track, target, engage, and assess (Tirpak, 2000). It is often enough to eliminate a subsystem responsible for one of the above functions to render the whole anti-air defence useless.

Furthermore, even advanced anti-aircraft and anti-sea systems have limited visibility of the targets due to the Earth's curvature. A low-flying aircraft can stay undetected within tens of miles from the S-400 anti-aircraft unit (Stratfor, 2019). To tackle this problem, additional, forward-deployed or airborne radars can be integrated into the system, enabling it to "see beyond the horizon" – this is called cooperative engagement capability (CEC). However, according to the experts, such capability is easier to be achieved against naval units than against aircraft or missiles. Russia is unlikely to be able to demonstrate CEC in the air domain in the foreseeable future. It is important to note, however, that integration of additional elements into the system increases its complexity, creating new vulnerabilities that could be exploited in a cyberoperation. For example, eliminating an airborne, drone-mounted radar of the anti-sea unit deployed on the shore could limit its visibility from hundreds to just tens of miles into the sea.

Elements of S-400 system – how it acquires information and what are its vulnerabilities

The crux of modern Russian anti-air capabilities is the famous S-400. By the end of 2019 Russia is said to have deployed six S-400 battalions totalling

48 launch trucks (Domańska et al., 2019, p. 75). An S-400 battalion consists of two batteries. Four launch trucks, coupled with a command centre, a target acquisition radar, a fire control and engagement radar (92N6, known as Grave Stone by NATO) constitute one battery. These are supported by auxiliary vehicles, e.g. for reloading and power supply. Battalion is normally connected to additional sensors and command functions at the regimental level, as well as to territorial search radars, electronic listening stations, and the air defence command-and-control network (Dalsjö, Berglund, and Jonsson, 2019, p. 28).

Eliminating, for instance, the target acquisition radar would effectively take out the four launch trucks within the battery, thus knocking out the *find* link in the kill chain. The same holds true for the engagement radar – even though the short- (9M96) and medium-range (9M96DM) missiles of the S-400 system are partly autonomous, they still require target updates from the ground station.

Tactical considerations

A potential for the use of cyberweapons in the defence of the Baltic States greatly depends on the circumstances, and can play a considerable role before and during the conflict.

We should bear in mind that the consequences of a direct cyberattack on the military systems may be short-lived and difficult to ascertain at a distance. The targeted system could be switched to an emergency or backup mode, or otherwise brought back to functionality. In the case of anti-ship systems, even if an airborne radar has been eliminated, a missile may be fired on lower quality information, such as satellite-provided information or obsolete data (Dalsjö, Berglund, and Jonsson, 2019, p. 57). Unless the decisive suppression of the system (ideally through physical destruction) is assured, sending aircraft or ship to the contested zone entails considerable risk.

We should bear in mind that the consequences of a direct cyberattack on the military systems may be short-lived and difficult to ascertain at a distance. The targeted system could be switched to an emergency or backup mode, or otherwise brought back to functionality.

Therefore, applying cybertools along with a kinetic attack is worth considering. A potential cyberattack aimed at systems providing defence for the anti-aircraft batteries (Pantsir missile system in the case of S-400) could give a short window of opportunity for the ballistic missiles to reach the launch trucks and decisively neutralise the system. In reality, several surface-to-air missile (SAM) systems would be deployed on the ground – short- and medium range 9M96/9M96DM-missile-equipped S-400 launching platforms, but also mobile units with SA-15 or SA-17 systems. Therefore, taking down one system wouldn't nullify the defence, but could rather bring down the costs of a saturation attack (possibly employing drones and cruise missiles; 2019 attacks on Saudi Arabia oil facilities demonstrated the inability of many sophisticated SAM systems to deal with these kinds of aircraft). Nevertheless, there is a potential for synergy. Such a scenario seems to be in line with the current Multi-Domain Battle (MDB) concept – a new doctrine of the US Armed Forces. MDB puts emphasis on the simultaneous application of force in all domains to overwhelm the enemy instead of, as has often previously been the case, engaging the enemy in various domains sequentially (War on the Rocks, 2019).

Targeting civilian infrastructure

A cyberattack may be carried out well before any direct hostilities begin as means of strategic communication and deterrence. That applies not only to the military networks, but also to the general infrastructure of the Kaliningrad oblast. The energy facilities come to the fore as particularly vulnerable. Kaliningrad, lacking land connection to either Russia or Belarus, must be self-sufficient once the region is cut off from its neighbours' grids at the beginning of the conflict. Even though such an action doesn't target the A2/AD systems directly, skilful leveraging of Kaliningrad's isolation could affect the risk calculation on the part of Russia before the hostilities begin. This vulnerability should not be underestimated in the broad discussion of neutralising the Kaliningrad A2/AD bubble.

Even though the electricity shortage would not in all probability affect the military defence systems, in the event of a drawn-out conflict, this could undermine the exclave's self-sufficiency. Applying pressure through cyber means at various points could weaken the overall defence of the adversary.

Strategic implications

Here a strategic question presents itself: would the United States consider a potential conflict in the Baltics seriously enough to use up a considerable advantage in what would probably be a one-time operation? A successful cyberattack on the Russian military systems would surely prompt a vigorous investigation and subsequent patching, thus nullifying the advantage that could be well used should the conflict escalate, say, into nuclear domain. It's also worth noting that S-400 systems are used by China as well. If the same vulnerability in the system could in fact be used against China in another conflict – would that fact affect the decision to employ a cyberattack?

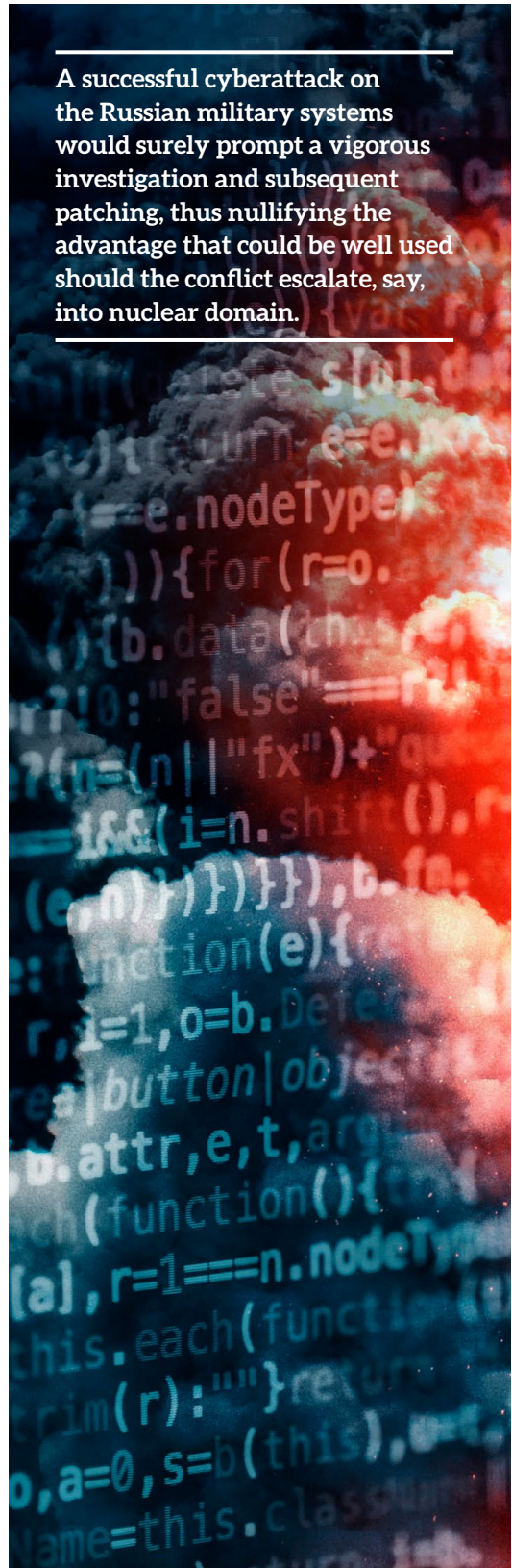
As attacks on Iranian or Estonian critical infrastructures demonstrated, a successful cyberattack can bring short-term advantage, but it also mobilises the victim to patch its systems and boosts the development of its cybersecurity capabilities in the long run.

Conclusion

The question of applying a cyberattack in any given conflict is influenced by a variety of factors beyond pure technical means to do so. Using cybertools most probably would not suffice to bring down the Russian A2/AD capabilities in Kaliningrad, but they present an opportunity to lower the cost of suppression. In a scenario where the US resources are strained and have to be deployed at multiple conflict zones around the world, the use of cyber weapons could prove a deciding factor.

Most certainly we should make an effort to integrate our current knowledge of the cybersecurity field in thinking about the traditional domains of the battlefield, not only in general terms, but with application to specific scenarios, like the Baltic States defence. ■

A successful cyberattack on the Russian military systems would surely prompt a vigorous investigation and subsequent patching, thus nullifying the advantage that could be well used should the conflict escalate, say, into nuclear domain.





About the author:

Dominik Skokowski graduated from the Drilling, Oil & Gas faculty at the AGH UST in Kraków. He is the Kosciuszko Institute collaborator within the cybersecurity and energy & climate research areas.

References

Dalsjö, R., Berglund, C., & Jonsson, M. (2019). *Bursting the Bubble. Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*.

Retrieved from <https://www.foi.se/rest-api/report/FOI-R--4651--SE>

Domańska, M., Kardaś, S., Menkiszak, M., Rogoża, J., Wilk, A., Wiśniewska, I., & Żochowski, P. (2019). *Fortress Kaliningrad. Ever closer to Moscow*. Retrieved from <https://www.osw.waw.pl/en/publikacje/osw-report/2019-11-07/fortress-kaliningrad>

Hooker, R. D. Jr. (2019). *How to Defend the Baltic States*. Washington, DC: Jamestown Foundation. Retrieved from <https://jamestown.org/wp-content/uploads/2019/10/How-to-Defend-the-Baltic-States-full-web4.pdf>

Stratfor. (2019). Why the S-400 Missile is Highly Effective – If Used Correctly. Retrieved from <https://worldview.stratfor.com/article/why-s-400-s400-missile-long-range-turkey-russia-syria-effective>

Tirpak, J. A. (2000). Find, Fix, Track, Target, Engage, Assess. *Air Force Magazine*, 83(7), 24–29.

War on the Rocks. (2019). How is the Air Force Adapting to Great Power Competition (podcast).

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



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**