

VOLUME 6 (2020) ISSUE 2

European Cybersecurity Journal

Strategic perspectives on cybersecurity
management and public policies

**Is Technology Bringing
Us Together or Pulling
Us Apart**

**Lawful Access
– Balancing Privacy
and Accountability**

**Grand Strategy:
Managing New
Geostrategic Projections in
an Interconnected World**

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

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 2, page reference



THE KOSCIUSZKO INSTITUTE

Published by:

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

Phone: 00 48 12 632 97 24

E-mail: editor@cybersecforum.eu

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

Is Technology Bringing Us Together or Pulling Us Apart

Pauline Neville-Jones

9

Lawful Access - Balancing Privacy and Accountability

Michael Malsch

16

Grand Strategy: Managing New Geostrategic Projections in an Interconnected World

Bonnie Butlin

29

Digitalisation - Opportunities for Development

Faustine Felici

40

Six Goals for the Digital Services Act

Daniel Castro
Eline Chivot

45

What Does Resilience-Building to Emerging and Disruptive Technologies Actually Look Like?

Kulani Abendroth-Dias

55

Training or Technology? The Key to CISO Success Is a Balanced Approach that Focuses First on what Matters Most

Adam Palmer, Oliver Hoare

61

5G Corridors, a Promising Investment in Europe's Technological Sovereignty

Arsenio Cuenca-Navarrete

68

From High Tech to High Politics: a Geopolitical Analysis of the European Approach to Secure 5G networks

Ségolène Milaire

79

Active Defensive Measures in Cyberspace - a Swiss Case Study

Bastien Wanner
Solange Ghernaouti

91

Social Media at War. The Case of Kurdish Fighters and Their Impact on the Perception of the On-Going Anti-ISIS Conflict in Western Countries

Ginevra Fontana

97

Cybersecurity of 5G Networks. EU Toolbox of Risk Mitigating Measures - Practical Consequences of the Approach Taken

Paweł Gruszecki

Editorial



Barbara Sztokfisz

Chief Editor of the European
Cybersecurity Journal

Dear Readers,

In these unprecedented times, I am honoured to hand over to you the very new issue of the *European Cybersecurity Journal*.

Nowadays, more than ever before in human history, we can demonstrate that technological tools serve the prosperity and well-being of our economies and societies. It is largely thanks to them we can continue working, maintaining relationships, and pursue the debate on the most strategic challenges of our times. But to keep the world running we need to deploy secure digital solutions.

As we are now approaching the digital future at an accelerated pace, it is worth highlighting that even though uncertainty is embedded in the process of technological change and future technologies are to a large extent unknown, we need to come together to prevent the world from having a rough ride coming to a dead end due to the win of adversarial technology use.

Following the words from UN Secretary General António Guterres: “we need to turn the recovery [from COVID-19] into a real opportunity to do things right for the future”. These words could not be more relevant for digital transformation itself. Technological tools should always empower humanity. Eventually, we must remember that it depends on people whether digital disruption is used for good or for adversarial purposes.

I sincerely hope that this issue of the Journal will enable our readers to gain deeper knowledge about the cybersecurity landscape and will contribute to intensifying the dialogue on the cybersecurity threats in the social and political discourse.

Enjoy the read!

Barbara Sztokfisz



CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

CYBERSEC GLOBAL 2020
6TH EDITION OF CYBERSEC

**TOGETHER AGAINST
ADVERSARIAL INTERNET**

DIGITAL-ONLY
28 - 30 SEPTEMBER 2020

#CSGlobal20

@CYBERSECEU



www.cybersecforum.eu

OPINION

Is Technology Bringing Us Together or Pulling Us Apart

BARONESS PAULINE NEVILLE-JONES

SENIOR ADVISOR, RIDGE-SCHMIDT CYBER; FORMER MINISTER OF STATE FOR SECURITY AND COUNTER TERRORISM OF THE UK

When, in 1522, Martin Luther published his translation into German of the New Testament, he set off an intellectual revolution in Europe which challenged established institutions in closely linked Church and State. Theological controversy was far from unknown in the Catholic Church but it was confined to the small minority who had both time and money to obtain access to handmade texts. What made Luther's ideas so powerful was them being printed soon after Guttenberg had invented the moveable type printing press. New technology brought the arguments to much wider circles who communicated with each other across national boundaries, the resulting intellectual tumult finally splitting Western Christendom into rival political

and faith camps. An example, one might argue, of a new technology causing major disruption and enduring divisive change in the established order.

At the same time, Luther's New Testament and his German language Bible (1534) had a profound effect on the formation of the German language and helped create Germanic cultural identity across the borders of separate princely states in Central Europe. The same could be said of the effect of printing Tyndale's English language translation of the New Testament in 1525 on the development of English which led, by 1536, to the chaining of an English language Bible to the pulpit in every parish church in the land. The influence

on the political and cultural identity of the island population has been profound. Both are examples of bringing peoples together. But, of course, on the basis of breakup elsewhere.

Does any of this ring bells? Historical analogies are always open to objection as circumstances are never the same, especially not when comparing periods far apart. But periods in history when the onrush of ideas and technology is especially fast and far reaching can be identified and ours is one of them. And, once again, it is the enhanced ability to communicate which is spearheading change. By itself, technology will not move mountains. It is the ideas that go with it and the values that underpin it which give technology its power. And, as with other revolutionary periods in history, there is plenty of dry political tinder lying around today which needs urgent and careful handling for outcomes to be good – climate change, migration, equality and diversity challenges within democracies, the decline of longstanding alliances, and the rise of autocracies accompanied by abuse of information technologies and human rights. All combustible issues.

By itself, technology will not move mountains. It is the ideas that go with it and the values that underpin it which give technology its power.

It is widely argued, rightly I think, that COVID-19 is having a transformative effect. Some of measures it has brought into play, such as extensive working from home, are accelerating trends already visible but at such a jolting speed and extent that there is no time for normal compensating lifestyle adjustments. That said, without communications technology across continents it is hard to see how society would have been able simultaneously to keep going, even at low levels of economic activity, while giving priority to saving lives. The digital world has given us policy options not available to the victims of Spanish flu a hundred years ago. Equally, there is no likelihood that we shall return to the status quo ante.

While increasing our ability to communicate and revealing opportunities, our use of digital technology is also increasing social division and risk. Inability to access the internet, whether for technical reasons, lack of skills, or difficulty to pay, now becomes a powerful force for exclusion, one that widens existing inequality of opportunity. And the more dependent the exercise of daily life becomes on data, the greater the surface opened up to antisocial manipulation: to crime at scale, disinformation, and extremism, undermining trust and the stability of institutions.

Without communications technology across continents it is hard to see how society would have been able simultaneously to keep going, even at low levels of economic activity, while giving priority to saving lives. The digital world has given us policy options not available to the victims of Spanish flu a hundred years ago. Equally, there is no likelihood that we shall return to the status quo ante.

So, the answer to the question in the title – about technology bringing us together or pulling us apart – is both. Technology is assisting both revolution and reformation; creation and destruction; problem and solution. For democracies the interesting and challenging questions lie in whether our institutions can rise to the opportunity of increased productivity and wealth creation that a technologically driven society could bring us (not just digital technologies but new energy sources, biomedical therapies, and enablers such as quantum) while avoiding the social disruption and individual misery that they can cause, destroying political support for change.

In the sixteenth century, many established powers resisted the forces unleashed by printing which led over time to major changes in the balance of power in Europe accompanied by prolonged violence both civil and military. Not the best model to follow. But we should be under no illusion about the profundity of the consequences of the technological changes that are now being unleashed. They are long term

in their effect and require a strategic rather than tactical response. The issue is not just the shape of economic revival – whether V-, L-, or W-shaped – it is about new ways of manufacturing and delivering services causing permanent changes in the job market with huge social consequences which demand new approaches to education and social welfare.

For democracies the interesting and challenging questions lie in whether our institutions can rise to the opportunity of increased productivity and wealth creation that a technologically driven society could bring us (...) while avoiding the social disruption and individual misery that they can cause, destroying political support for change.

It is arguable that in democracies the severe shock and the accompanying uncertainties of COVID-19 have made populations aware that that return to the old normal is unlikely and that it would be more sensible to adapt agendas to ride the tide of change rather than resist it. This openness to change is however likely to be quite fragile and easily crushed by events. High orders of leadership will be required. The return of the big state has been prophesied by commentators and it is the case that austerity is unlikely to be tried again as a remedy to political shocks and that public expenditure is likely to rise and taxes to increase. But this cannot be the whole story. Unlike the Cold War, when investment in scientific research and technology was to a significant extent financed and conducted by the state, in twenty-first century democracies the private sector is now the mainspring of technology development and exploitation. To ensure acceptable social outcomes, this implies a partnership between public and private sectors – a coming together in a shared strategy. China, we should remember, finds long-termism easier than democracies.

And what about the individual? As China has shown, but as democracies have also experienced, applications of data technologies pose fundamental challenges to basic social values. Get this wrong and we

As China has shown, but as democracies have also experienced, applications of data technologies pose fundamental challenges to basic social values. Get this wrong and we destroy what we stand for.



beyond paying taxes, the individual could expect to live a largely anonymous life in relation to the state. Collective security against such threats to the safety of the individual as terrorism necessarily exposes populations to personal identification by public authority without their knowledge. The ability of the state to track and trace its citizens is an everyday reality.

The state has also to provide, as best it can, a shield against organised crime, implying once again a more intrusive state. At the same time data technologies increase the reach of individuals in relation to each other, magnifying the consequences of good citizenship but also of malign activity such as online pornography and social grooming. The use and abuse of data technologies have the capacity to profoundly destabilise traditional patterns of social behaviour, destroying the trust on which democracies depend for their good functioning. Artificial intelligence will increase both the benefits and the risks inherent in data technologies. Here we are only in the foothills of understanding future complexities.

Much of the twentieth century has been spent by governments reducing the risks faced by individual citizens in their ordinary lives – road safety and public health to name but two, COVID-19 notwithstanding. Indeed, people are inclined to feel that the state is at fault if it fails to render their lives risk free. But a new reality awaits. Our use of the new technologies brings new risks of a systemic kind. Their management is not so much a matter of being well prepared for emergencies when these arise from time to time as an exercise in continuous mitigation of risk to ensure systems resilience. This becomes more difficult the more complex the systems we create – and they are becoming steadily more complex. In this situation, it is quite hard to see how any user, whether corporate or individual, can escape taking a share of responsibility in risk management. It is not just the whole of government that has to be involved. It is the whole of society.

Moreover, the challenges facing democratic leaderships are not only domestic. The sunny days of globalisation are over and technology – the one-time

unifier of the global economy – is now at the centre of the factors causing political division and rising hostility between major powers. It was Western banking able, as the result of digital technologies, to work 24/7 across the globe that opened up markets round the world to unprecedented levels of commerce. It was the transfer of manufacturing – but crucially also western intellectual property – to China which began the East-West trade and investment boom that is now threatened by growing political disagreement. Once again, as in the Cold War, fundamental values concerning human rights and social organisation lie at the root of divergence and separation between democracies and autocratic governments.

The challenges facing democratic leaderships are not only domestic. The sunny days of globalisation are over and technology – the one-time unifier of the global economy – is now at the centre of the factors causing political division and rising hostility between major powers.

China is a rising military power with a government which directs the economy, suppresses dissent, and increasingly applies technology for repugnant social purposes. But – and here is a difference from the Cold War – her challenge lies precisely in her economic prowess: the attraction of an economic model, heavily invested in technology, which at home has lifted millions out of poverty within a single generation and, in the Belt and Road initiative purports to extend that prospect abroad. The economic model represented by free enterprise is thus directly challenged and, with it, the soft power of democracies. The current focus of Western leaderships is on cheating and unfairness in international commercial exchanges and these have genuine national security and prosperity implications. Three recent political developments seem to me, however, to raise the stakes to a different level and to have long-range importance. The first is the American decision to forbid the use of American components in Huawei's telecoms equipment. The second is the Chinese coverup during the early stages

of COVID-19 which will have cost many thousands of lives. The third is the introduction by China of repressive security laws in Hong Kong. The first deliberately destroys a significant element of international economic integration while the second underlines lack of regard for individual human life. The third tells us that international agreements with China are not to be relied upon.

Political moves like these create momentum which is hard to slow down, let alone reverse. Misjudged actions and responses can lead the world towards replacing cooperation with hostile competition and then confrontation. At a moment when items on the international agenda like climate change

cry out for international cooperation, we face the possibility of an increasingly bipolar world of divided camps with the exploitation of technology at the heart of the competition. Pulling us apart in other words. Are we going to let this happen with no attempt at arresting the slide?

It is not only the case therefore that democracies need strategies at home to deal with the challenge posed by technological change. We badly, and indeed urgently, need a shared international strategy to identify and prioritise our goals and, in the process, successfully reduce the risks we may otherwise face. Do better, in other words, than Europe managed in the sixteenth century. ■



About the author:

Rt Hon Baroness (Pauline) Neville-Jones DCMG is a Conservative peer in the UK House of Lords. She sits on the Committee on the National Security Strategy. Until recently she was a member of the Lords Science and Technology Committee and the Engineering and Physical Sciences Research Council. She was David Cameron's National Security Adviser in Opposition becoming Minister for Security and Counter Terrorism and a member of National Security Council 2010-2011. She was the PM's Special Representative to business for cyber security until 2014. She has advised the Bank of England on cyber security.

Pauline has a background in foreign affairs and was a member of the UK Diplomatic Service from 1963 to 1991. She has since worked in the City; been Chairman of the technology company QinetiQ plc and has been the international Governor of the BBC.



ANALYSIS

Lawful Access – Balancing Privacy and Accountability

MICHAEL MALSCH

LEGAL ATTACHÉ FOR POLAND,
FEDERAL BUREAU OF INVESTIGATION (FBI)

One night while writing this article, I heard this line spoken in a movie I was watching: “Tonight. Policing a free Internet, personal rights versus public safety. This is the great question of our time. And the choices we make about this will determine our future” (Greengrass, 2016).

It was so on-point for the topic of this article, I had to re-check the date of the movie to ensure it was as old as I thought. After quickly consulting IMDb, I confirmed that the movie I pulled this from – *Jason Bourne* – was written during 2015 and released in theaters in the summer of 2016 (IMDb, n.d.). For context, the moderator says these lines as he is introducing the CEO of a global social media company, the Director of the US Central Intelligence Agency, and two other inconsequential speakers to a crowded audience at a technology conference in Las Vegas, Nevada. To avoid spoiling the movie, I will not share what happens next, except to say that the movie does not answer “the great question of our time” (Greengrass, 2016).

I believe most of us can agree: privacy is well established as a fundamental human right. A right to privacy is included either explicitly or by court interpretation and legal precedent in the constitutions of most countries of the world (Banisar, n.d.). In 1791, a provision protecting people from unreasonable searches and seizures without probable cause was officially added to the Constitution of the United States of America by amendment. This was the fourth among a group of the first ten amendments to the US Constitution, referred to as the Bill of Rights. Since ratification of this amendment, US courts have interpreted this provision broadly to protect citizens’ privacy. Nearly 200 years after the ratification of the US Bill of Rights, the United Nations codified the protection from arbitrary or unlawful interference into one’s privacy into the 1976 International Covenant on Civil and Political Rights. In 2018, the European Union passed into law the General Data Protection Regulation (GDPR), which provides for protection for everyone regarding the processing of their personal data.

I believe most of us can agree: privacy is well established as a fundamental human right. A right to privacy is included either explicitly or by court interpretation and legal precedent in the constitutions of most countries of the world.

As with all rights, their significance to those upon whom the right is bestowed comes from the balance between the personal interests and reasonable expectations of citizens and those of society – both private (e.g. corporate industry) and public (e.g. government). With regard to government, this equilibrium is due to the combination of restraint in the use of its authority to avoid infringing upon the rights of the private citizen; the private citizen’s lawful exercise of their rights with respect to the government’s policies, regulations, and laws; and the private citizen’s responsible behavior within their rights and with regard to the rights of other citizens. When the balance is disrupted, society suffers. In some cases, the imbalance is minimal and the reason for it is easily identified and simply restored. In other cases, the reason for imbalance is complex and the path to restoration of balance is anything but simple.

This analysis will look at the increasing imbalance between the private citizen, the government, and other citizens by the proliferation of encryption technology for mainstream use on the Internet. Specifically, I examine the issue from the perspective of law enforcement agencies losing their ability to investigate violations of laws, which have been enacted by elected representatives of the people, and to bring justice to the victims of these crimes. This issue has become known by some as “going dark”, or more broadly as “lawful access”.

It is important to acknowledge it is not universally accepted that an imbalance between private citizens rights to privacy and law enforcement’s lawful access even exists. Some believe an imbalance was corrected through the unauthorised disclosures of government surveillance programmes. Yet others believe the imbalance does not threaten the security of society. Researchers at the Center for Strategic and International Studies (CSIS) determined that “the risk to public safety created

by encryption has not reached the level that justifies restrictions or design mandates” (Lewis, Zheng, Carter, 2017, p. V). The data used in the report show the instances where encryption negatively impacts an investigation involving electronic evidence are relatively few when compared to total investigations involving electronic evidence. Still another position is that this is not a global issue at all, as some countries have either codified in their national laws a requirement to make all data transiting service providers’ networks operating on their territory accessible for intercept by the government, or the government has denied access to encryption technology and applications altogether.

Encryption strengthens the ability of a private citizen to ensure their privacy. Today’s technology enables individuals using inexpensive, and in many cases free, applications to encrypt their stored data and their communications. This is a good thing. As discussed previously, privacy is generally accepted as a basic human right. Another net-positive development is the increase in the number of providers building this end-to-end encryption technology into their applications. This further decreases the barrier to entry, allowing even more private citizens to use encryption technology to protect the privacy of their data and communications. For example, according to a report by Juniper Research, WhatsApp – the most popular messaging application in the world, which also happens to be end-to-end encrypted – has approximately 1.6 billion active users on a monthly basis (Woodford, 2020). Another recent example is the explosion in the use of another end-to-end encrypted application – Signal. The combination of a global pandemic and social unrest in May and June 2020 caused a surge of downloads of the secure messaging application. Signal saw over one million downloads of its application in May 2020 alone and the total number of installed applications world-wide currently stands at just under 33 million (Nguyen, 2020). Statistics showing the rapid increase in adoption of these end-to-end encrypted applications are frequently used to suggest that society believes the imbalance should tilt towards more privacy for the private citizen.

Encryption strengthens the ability of a private citizen to ensure their privacy. Today’s technology enables individuals using inexpensive, and in many cases free, applications to encrypt their stored data and their communications.

However, when in the exercise of their right to privacy the private citizen infringes upon the rights of others, there must be a remedy. When the infringement violates laws, society has agreed to entrust the government with the responsibility of applying the remedy. In democratic society, citizens elect government representatives who propose and enact laws that grant law enforcement agencies the authority to investigate criminal activity. Law enforcement officers use all available investigative techniques to gather evidence to build and strengthen their case against the suspected criminal. The more intrusive of these investigative techniques generally require authorisation by a court. Once approved, law enforcement officers can use the investigative technique in strict compliance with the terms approved by the court. Examples of these intrusive techniques are search warrants and surveillance. On the Internet, these investigative techniques are conducted electronically and remotely, but still require court authorisation. Today’s encryption technology effectively eliminates electronic search and surveillance techniques from the law enforcement agency’s toolbox. Even when an individual has been identified and the location and method of data storage and communication has been discovered; and the law enforcement authority has provided a truthful and substantive statement regarding the reason they believe there is probable cause the account was used, is being used, or will be used in criminal activity; and a court has approved the use of an investigative technique, encryption still prevents law enforcement from gaining any useful information from the results of a search warrant or from electronic surveillance. With modern encryption, the equilibrium is disrupted – as US Attorney General William P. Barr said (2019):

this form of “warrant proof” encryption poses a grave threat to public safety by extinguishing the ability of law enforcement to obtain evidence essential to detecting and investigating crimes.

It also allows the right to privacy of the private citizen to trample the rights of other citizens and disables the law enforcement’s ability to ensure justice for the victims of these crimes.

Some may think the last statement seems extreme or overly dramatic. But allow me to illustrate using a real-world problem. This will illustrate the imbalance and emphasise why it is important to restore equilibrium. There are many possible examples to choose from – individuals using darkweb sites to plot murder-for-hire schemes; criminal groups organising and coordinating financial frauds; and terrorist organisations using private online forums to plan attacks, to name a few. For this discussion, however, online child sexual abuse and child exploitation will provide sufficient context to highlight the scale and scope of the imbalance. This criminal activity poses significant and increasing risk to the most vulnerable in our society. In 2019, 18.4 million reports of child sexual abuse imagery were made to online service providers (Keller & Dance, 2019). Those reports included over 45 million images and videos of child sexual abuse. Many of those images were posted and shared on the open Internet. More disturbing still is the volume of content not reported because it is hidden using impenetrable end-to-end encryption technology. The same *New York Times* article describes a darkweb site with over 30,000 members and over 3 million images made available for viewing, and another darkweb site with over one million members. In addition to the child sexual exploitation content, the article says, the operators of these sites provide how-to information to help contributors keep their identities secret:

Offenders can cover their tracks by connecting to virtual private networks, which mask their locations; deploying encryption techniques, which can hide their messages and make their hard drives impenetrable; and posting on the dark web, which is inaccessible to conventional browsers.... the forum had dedicated areas where users discussed ways to remain


“safe” while posting and downloading the imagery. Tips included tutorials on how to encrypt and share material without being detected by the authorities. (Keller & Dance, 2019)

To further exacerbate the issue, currently unencrypted platforms are poised to become encrypted, which will put more of similar illicit material and illegal activity out of the reach of law enforcement authorities as they seek to investigate and prosecute those responsible for producing and distributing it. This state of imbalance, as expressed by Christopher A. Wray, Director of the US Federal Bureau of Investigation, *cannot be a sustainable end state for us to be creating an unfettered space that’s beyond lawful access for terrorists, hackers, and child predators to hide. But that’s the path we’re on now, if we don’t come together to solve this problem. (Wray, 2019)*

The problem is not confined only to the realm of child sexual abuse, other criminal activity is happening beyond the reach of law enforcement on these encrypted platforms. The problem is not contained within national boundaries as individuals and organised groups from all around the world are conducting criminal activity and impacting victims, regardless of where they are located. It is not a problem for only the government to solve, it will also require cooperation between both public and private sectors to develop a solution.

It is important to take a step back and look at how we arrived at where we are today. For this we need to look at a specific piece of legislation regarding the Federal Communications Commission – United States Code Title 47, Section 230(c)(1) Treatment of Publisher or Speaker, taken from the Communications Decency Act of 1996 – which states the following: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” (US Code, n.d.). This sentence is sometimes referred to as the “26 words that created the Internet.” At its core – this section of the United States Code provides for a separation between the creators of content from the services that make it available to the public.

The problem is not contained within national boundaries, individuals and organised groups from all around the world are conducting criminal activity and impacting victims, regardless of where they are located. It is not a problem for only the government to solve, it will also require cooperation between both public and private sectors to develop a solution.



The reasoning behind this is also included in the legislation as the findings of Congress, those being in summary: the Internet is rapidly advancing and provides educational and informational resources to US citizens; the services offering the information have significant control over the information made available; the Internet offers a forum for political discourse, cultural development, and intellectual activity; the services making these resources available benefit US citizens with a minimum of government regulation; and US citizens are increasingly relying on interactive media for political, cultural, educational, and entertainment purposes. As a result, the US lawmakers adopted as policy to promote the continued growth of the Internet and the services that make it possible while still acknowledging its responsibility to enforce federal criminal laws. A fair and noble posture, when one considers that most people use the Internet services for legitimate and legal purposes. However, in the early 1990s when the Internet was emerging as a disruptive technology, the authors of this legislation could not have seen the full ramifications of the protection it extends to service providers nor the tools which have emerged to hide illegal activity. Furthermore, the interactive computer service providers Section 230(c)(1) sought to protect when initially written are no longer at risk of succumbing to the burden of undue regulation. The interactive computer service providers are valued in the hundreds of billions of dollars. Yet, because of the protections afforded under the Communication Decency Act, they are largely not exposed to liability for the content posted on or transiting their services.

Where do we go from here? As was discussed earlier in this article, the imbalance between private citizens' rights to privacy, the government, and other private citizens due to widely available advanced encryption technology is not going to be easy to correct. The imbalance is increasing in severity with no rebound on the horizon. To rebalance, it will require trust, innovation, and effort from both the government and the companies who develop the technologies and provide the services people use on the Internet. But the protections codified in the Communications Decency

Act that allowed the major providers operating on the Internet today to flourish should not simultaneously allow criminal activity to continue unfettered while also making it impossible for law enforcement to vigorously combat that activity. There are numerous arguments raised in defense of maintaining the status quo regarding encryption. Among the most popular are: technologically difficult/impossible, too costly, undermines security, reduces privacy. While there are merits to these arguments, the result is a shift in the burden of risk and expense entirely onto the victims. Due to the civil immunity protections provided by the Communications Decency Act, the victim does not have any legal recourse through civil lawsuits against the interactive computer service providers. Instead the victim turns to law enforcement seeking a last chance at justice. In increasingly more instances, law enforcement is powerless to investigate due to an inability to gather the kind of evidence necessary to prosecute these crimes as a result of impenetrable encryption.

Since the advent of the Internet, the will to innovate online has overcome myriad financial and technological barriers at every turn. Developing a mechanism that will continue to preserve the privacy and security of citizens in their everyday communications, while creating a path to access only the communications identified as being related to criminal activity when ordered by a court, is something well within the capabilities of the global technology sector. As Bill Gates emphasised in a recent interview:

The companies need to be careful that they're not... advocating things that would prevent government from being able to, under appropriate review, perform the type of functions that we've come to count on... There's no question of ability; it's the question of willingness. (Allen, 2018)

Coupling access with strict oversight and accountability of law enforcement agencies' requests by the courts who approve this level of access can be accomplished. In the United States, the Communications Assistance to Law Enforcement Act (CALEA) is one example of how

this has been successfully implemented in an analogous technology – telephone communications. CALEA was passed in the United States Congress in 1994 and has provided a solid framework between law enforcement, courts, and telecommunications providers to offer limited access to communications for investigation of criminal activity. Similarly, legislative proposals regarding compelling Internet service providers to take more responsibility for illegal content on their platforms are currently being reviewed in both the US and the European Union (Pop & Schechner, 2020). I believe a similar combination of technological innovation coupled with well-crafted legislation and rigorous oversight is possible, but, as US Attorney General William Barr pointed out, *the time to achieve that may be limited.... As this debate has dragged on, and deployment of warrant-proof encryption has accelerated, our ability to protect the public from criminal threats is rapidly deteriorating. The status quo is exceptionally dangerous, unacceptable, and only getting worse.... It is time for the United States to stop debating whether to address it, and start talking about how to address it. (Barr, 2019)*

There is a solution which will bring the current situation back into a more balanced state. The personal right to privacy and the pursuit of public safety do not need to be diametrically opposed to one another. Both can coexist in balance with one another given the right technological and legal environment. It will require cooperation and trust; adaptability and flexibility; focus and determination; and most of all, the will to fix what is broken and answer “the great question of our time” (Greengrass, 2016). ■

About the author:



As the Head of the U.S. Federal Bureau of Investigation (FBI) Warsaw, Poland Office, Special Agent **Michael C. Malsch** cooperates with Polish Law Enforcement and Security Agencies to address criminal, cyber, and terrorism threats of mutual concern to Poland and the United States. Mr. Malsch began his FBI career in 2004. During the past 16 years, he has worked a variety of investigations across many of the FBI's programs, including international assignments in Poland and Central Asia. Mr. Malsch earned a Master of Science degree in Strategic Intelligence from the National Defense Intelligence College; a Master of Business Administration from University of Illinois at Chicago; and Bachelor of Science in Computer Science from the University of Illinois at Urbana/Champaign.

References

- Allen, M. (2018, 13 February). Bill Gates: Tech companies inviting government intervention. Retrieved 15 July 2020 from <http://www.axios.com/bill-gates-warns-big-tech-1518515340-fa3aa353-6078-405b-b3aa-8252bd06c1fc.html>
- Banisar, D., & Davies, S. (n.d.). Privacy and Human Rights - Overview. Retrieved 15 July 2020 from <http://gilc.org/privacy/survey/intro.html>
- Barr, W. P. (2019). *International Conference on Cyber Security - July 2019* (pp. 4-15). Washington, DC: US Department of Justice, Federal Bureau of Investigation.
- Barr, W. P. (2019). Lawless Access Summit: Warrant Proof - October 2019. (pp. 26-34). Washington, DC: US Department of Justice, Federal Bureau of Investigation.
- Greengrass, P. (Director), Greengrass, P., Marshall, F., Weiner, J. M., Smith, B., Damon, M., & Goodman, G. (Producers), & Greengrass, P., & Rouse, C. (Writers). (2016). *Jason Bourne* [Motion picture on DVD]. United States: Universal Pictures.
- IMDb. Jason Bourne (I) 2016 Release Info. Retrieved 15 July 2020 from https://www.imdb.com/title/tt4196776/releaseinfo?ref_=tt_dt_dt
- Keller, M. H., & Dance, G. J. X. (2019, 29 September). The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? *New York Times*. Retrieved 15 July 2020 from <http://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html>
- Lewis, J. A., Zheng, D. E., Carter, W. A. (2017, February). *The Effect of Encryption on Lawful Access to Communications and Data*. Retrieved 15 July 2020 from <http://www.csis.org/programs/technology-policy-program/intelligence-surveillance-and-privacy/effect-encryption-lawful>
- Nguyen, N. (2020, 14 June). Signal: The Pros and Cons of a Truly Private Chat App. *Wall Street Journal*. Retrieved 15 July 2020 from <http://www.wsj.com/articles/signal-the-pros-and-cons-of-a-truly-private-chat-app-11592127002>
- Pop, V., & Schechner, S. (2020, 5 July). Tech Giants to Face EU Legal Push on Content, Competition, Taxes. *Wall Street Journal*. Retrieved 15 July 2020 from <http://www.wsj.com/articles/tech-giants-to-face-eu-legal-push-on-content-competition-taxes-11593967270>
- US Code Title 47 § 230 - Protection for private blocking and screening of offensive material. (n.d.). Retrieved 15 July 2020 from <http://www.law.cornell.edu/uscode/text/47/230>
- Woodford, S. (2020). What's up WhatsApp? Trends for Messaging in 2020 (Rep.). Retrieved 15 July 2020 from Juniper Research website: <https://www.juniperresearch.com/document-library/white-papers/whats-up-whatsapp>
- Wray, C. A. (2019). *International Conference on Cyber Security - July 2019* (pp. 16-25). Washington, DC: US Department of Justice, Federal Bureau of Investigation.



ANALYSIS

Grand Strategy: Managing New Geostrategic Projections in an Interconnected World

BONNIE BUTLIN

CO-FOUNDER & EXECUTIVE DIRECTOR, SECURITY PARTNERS' FORUM

Recent tensions over 5G, cyber attacks and influence operations, targeted attacks on Russian expatriates, and new laws in China that have resulted in unrest in Hong Kong may have commonalities in escalating divisions within the International Order. Dissatisfaction and differences in interpretation within the rules-based International Order, including within the Public International Law (IL), International Investment Law (IIL) and trade regimes, have been growing for decades. Russia and China, particularly over the past two decades, have developed unique and divergent *sub-orders* and *grand strategies* within the existing rules-based International Order.¹ These sub-orders have quietly emerged amid rapidly changing technology,

a more sophisticated and strategic-level treatment of traditional security disciplines, and with novel geostrategic projections into other states and spheres of influence – all of which are informing the grand strategies of Russia, China, and the US.

Russia and China have developed comprehensive grand strategies and have been relatively open about their intentions. President Vladimir Putin's Munich speech in 2007 signalled defence of its near-abroad against NATO expansion, and President Xi Jinping's Foreign Affairs Work Conference (FAWC) speech in 2014 signalled an ambitious, security-focused strategic foreign policy (Swaine, 2015). Yet, dissatisfaction with and fracturing within the International Order has largely been dismissed as aggression or rule-breaking, rather than management of turbulence within the International Order itself. The US has been stretched in countering the unique grand strategies and ambitions of both Russia and China, which have

¹ Grand strategy is the "...collection of plans and policies that comprise the state's deliberate effort to harness political, military, diplomatic, and economic tools together to advance that state's national interest" (Feaver, 2009).

recently been acting in strategic partnership, rather than as competitors (Westerlund, 2018, p. 39). Russia and China have engaged in new geostrategic projections outside of their own spheres of influence so as to achieve greater control and further multipolarity within a changing International Order. In response, Russia, China, and the US appear to be defensively isolating and insulating themselves from these projections, counter-projections, and other negative effects and consequences within the increasingly complex and interconnected global landscape.

These new forms of geostrategic projection are in some ways similar to airpower projection, and are changing the meaning of geopolitics and borders. The geostrategic projections and push-back among the three great powers have caught multiple other states in the middle of new technology/5G and legal “shatterbelts” – in some cases regardless of location, partnerships, or alliances. Canada, for example, has been caught in a 5G dispute between China and the US, despite bordering on the latter and being a Five Eyes intelligence alliance member. Isolating or insulating from these larger projections and counter-projections across borders has been more challenging for those caught in the middle.

This has resulted in a mutually defensive and increasingly distrustful stand-off posture among Russia, China, and the US, one that risks escalation. All three have tried to prevent unnecessary escalation to military conflict, while enhancing their own military and non-military capabilities and strengthening their postures in the interim, including through strategic innovation.

The geostrategic projections and push-back among the three great powers have caught multiple other states in the middle of new technology/5G and legal “shatterbelts” – in some cases regardless of location, partnerships, or alliances.

There is a limited window of opportunity to de-escalate and build trust, stability, and more flexibility into the international system, and prevent further slide towards increasing conflict or new Cold War.

There is new urgency in addressing the underlying issues, as divergent international sub-orders and grand strategies have recently gained momentum, military and intelligence crises have become more frequent, and new geostrategic projections into the domestic space and spheres of influence of all three are increasing. Comprehensive and considered grand strategic solutions will be needed to break the impasse, beyond Whole-of-Government (WoG), and even Whole-of-Society (WoS) responses.

Divergent “sub-orders” are developing within the International Order. Since the Cold War, international relations among the US, Russia, and China have moved from partnership to competition, with increasing conflict and mutual distrust, fuelled by geostrategic projections. This trajectory, if not disrupted, could devolve into a new Cold War. The influence of the UN, International Law (IL), and International Trade regimes, among other international structures, institutions, and processes, has waned over time. The IL law regime is currently considered to be in crisis (Malksoo, 2017). The international investment and trade regimes have been trending towards a new, politically charged, “gunboat” diplomacy over time, amid widespread dissatisfaction among states with the available dispute resolution mechanisms.

Divergent “sub-orders” are developing within the International Order. Since the Cold War, international relations among the US, Russia, and China have moved from partnership to competition, with increasing conflict and mutual distrust, fuelled by geostrategic projections.

Divergent military and economic strategies and approaches have contributed to sub-orders developing. Russia and China view themselves as both great powers and civilisations. Their long and largely isolated histories have led to unique state trajectories within the International Order, including the development of unique Russian and Chinese military and legal doctrines and interpretations (Malksoo, 2017). Rather than China and

Russia integrating into the West, Russia developed an alternative to the Westphalian system, with greater emphasis on state sovereignty, more so than human rights and self-determination independent of state control (Malksoo, 2017). Russia has emphasised this more over time with “sovereign democracy” and later under President Putin with “immutable sovereignty”, which embraces Russian exceptionalism, or “Russianness”, including in the defence of its near-abroad (Morris, 2019). For example, Russian legal scholars, in advance of the 2014 Crimea invasion, supported this imposition of control within the Russian near-abroad as part of historic Russian land (Malksoo, 2017, p. 134).

The US has continued to focus largely on military projection capabilities (at great expense), and a more organic, laissez-faire development of the tech sector, that left the US on the sidelines of 5G. Russia and China have pursued grand strategies that in addition to investing in military build-up and modernisation focus on more cost-effective, adaptive military and other-than-military means to engage globally, including in the tech and cyber sectors.²

Russia has militarily pursued the Primakov Doctrine, operationalised in the style of Chief of the General Staff, Gen. Valery Gerasimov. The doctrine is aimed at defensively preventing US unipolarity, protecting Russia’s near abroad and sphere of influence, attempting to preserve the international order of equal sovereign states within IL, and Russia’s standing in it (Rumer, 2019). Russia’s foreign policy, by law of 2000, must be informed by IL (Malksoo, 2017). Russia’s 2010 military doctrine and the 2020 national security strategy support Russia’s perceived self-defence within IL and the leveraging of pragmatic and low-cost solutions – consistent with limited military and cyber projection. Russia, in this context, supported the Assad regime in Syria to back-stop state sovereignty and the IL regime against what it viewed as foreign coalition interference in the Syrian state outside of UN Charter sanctioned actions (Malksoo, 2017, p. 149).

² Chinese companies Huawei and ZTE control some 40% of the 5G infrastructure market globally (Benner, 2020).



Russia and China have pursued grand strategies that in addition to investing in military build-up and modernisation focus on more cost-effective, adaptive military and other-than-military means to engage globally, including in the tech and cyber sectors.



Gen. Gerasimov's operationalisation of the Primakov doctrine has been misinterpreted through a Western lens as Western-styled hybrid warfare. Hybrid warfare is not pursued by Russia in its own right as a one-two cyber-kinetic punch; rather, as a cost effective, indirect, and asymmetric military approach for a new ongoing conflict reality in an interconnected world, including in peacetime (Bartles, 2016, pp. 33-34). In doing so, Russia has found a balance in soft and hard power, both "hybrid" (cyber and kinetic) and reflexive (mixing military and non-military means) (Berzins, 2018, p. 19). This operationalisation can be customised to respond to not only NATO actions, but to US hybrid threats (Felgenhauer, 2019), hypersonic weapons, and peacetime threats (Bartles, 2016, p. 37; Felgenhauer, 2019). This cost-effective and indirect approach has allowed for aggressive re-investment in force modernisation (Berzins, 2018, p. 19).³ Russia has carefully risk-assessed and calibrated its defensive posture within an interconnected world, and limited its military projection to avoid escalation to more direct conflict with the West (Galeotti, 2020).

Since Gen. Gerasimov's detailing of the Russian warfare doctrine and its operationalization in 2013 and 2014, Russia's 2016 Conception for Foreign Policy has moved the goal posts further forward from the 2013 notion of "the forming of a new world structure" to "the forming a just and stable world structure" (Butler, 2019, p. 184). This is consistent with Russia having developed both a unique and more autonomous sub-order and commensurate grand strategy within the existing International Order.

China, by contrast, has relied on a strategy of achieving national security through economic power. This includes through achieving technological superiority and through economic expansion and projection, which will add stability and predictability for China in the future⁴ (Spalding, 2019, p. 198).

³ Russia's modernisation target is 70 per cent of Armed Forces arms and equipment by 2021 (Westerlund, 2018, p. 37).

⁴ China has engaged heavily in foreign investment, resource acquisition, supply chains, development of port facilities, and Sea Lines of Communication (SLOCs), including with a view to the long-term – such as with 99-year lease arrangements and expansion into the South China Sea.

This is consistent with the unrestricted warfare doctrine, detailed by People's Liberation Army (PLA) Colonel Qiao Liang and Colonel Wang Xiangsui (Spalding, 2019, p. 12). China has worked hard to lead in 5G development, including through foreign investment. China's efforts in much of the rest of the world are not inconsistent with 5G design, which would be maximised with near full-world coverage, but may also be perceived as geostrategic projection. The US has clearly identified that control of 5G networks and equipment is key to American economic and national security interests, making China's 5G involvement in US and partner state 5G networks a recent source of dispute and push-back by Washington (Benner, 2020).

China, by contrast, has relied on a strategy of achieving national security through economic power. This includes through achieving technological superiority and through economic expansion and projection, which will add stability and predictability for China in the future.

Dissatisfaction with the trade and investment regimes has been a factor for China. While the country has faced push-back for its 5G engagement, it also has concerns about push-back against China's investment and trade more generally, since global investment patterns have bilateralised, with the developing world now increasingly investing into the developed world. China has been growing its domestic brands to go global – Huawei, for example, means “China can achieve” (Hongwen, 2017, p. 31). Beijing has moved away from large multilateral treaties, and has increasingly since 2002 relied on expansive Bilateral Investment Treaties (BITs) with National Treatment clauses, affording China's investors equal footing with domestic investors in other countries, and China more control over these relationships (Wang, 2016, pp. 376-380).

US push-back in relation to Chinese companies' involvement in 5G networks and equipment also represents an investment and trade issue for China, particularly as National Treatment may apply to

telecom/5G investment. Canada signed a BIT with China that includes a National Treatment clause in Article 6 (Global Affairs Canada, 2012). Huawei has invested many millions of dollars into Canadian research, networks, and related areas (Armstrong, 2019). In this context, it is notable that Canada is the last of the Five Eyes countries to not exclude or restrict Huawei from its 5G networks and development.

Sub-order grand strategy and geostrategic projection are supported and amplified by increasing sophistication in, and strategic treatment of, traditional security disciplines. China and Russia are applying these disciplines with more sophistication and at higher strategic levels than typically engaged in by the West, both at the enterprise and state levels. This more strategic treatment of security has bridged, highly effectively, their grand strategies with practitioner expertise from within the traditional security disciplines – linking ways and means across strategic levels and disciplines. This may drive a more strategic security approach in the West, as it responds to these geostrategic projections, and may force a much needed breaking down of silos between national security and traditional security practitioners in the West. This is particularly needed as the traditional security disciplines play an integral role in cybersecurity – now critical within the national security space.⁵

Western National Cyber Security Strategies (NCSSs) have largely relied on infrastructure and network resilience, and have largely avoided escalation to kinetic conflict in response to attacks, through a more defensive and resilience-based approach. This posture may no longer be sufficient, with increasing cyberattacks and influence operations attributed to foreign sources operating at higher strategic levels, and with 5G technology. Organisational Resilience (OR) as a security discipline will be important to develop in this context, as it bridges both multiple security disciplines and multiple strategic levels within enterprises.

⁵ Feaver noted the need for practitioners to be involved in a grand strategy (Feaver, 2009).

Western National Cyber Security Strategies (NCSSs) have largely relied on infrastructure and network resilience, and have largely avoided escalation to kinetic conflict in response to attacks, through a more defensive and resilience-based approach. This posture may no longer be sufficient, with increasing cyberattacks and influence operations attributed to foreign sources operating at higher strategic levels, and with 5G technology.

Risk management (RM) has to date been poorly suited for cybersecurity, resulting in new disciplines and concepts being created, such as cybersecurity economics, cyber-risk, and Return on Security Investment (ROSI) – which is focused on preventing losses rather than security investment returns, as with traditional Return on Investment (ROI) (Bragetto & Kert-Saint Aubyn, 2015, p. 12-14). With prevented losses increasingly being attributed to foreign state or affiliated actors engaged in geostrategic projections, a more comprehensive, and higher strategic-level treatment of cyber risk management may be required. Within organisations, Enterprise Risk Management (ERM) may need to be further strategically developed.

IT security and cybersecurity have historically been applied from lower strategic levels within organisations. These security disciplines are also being driven, including by Russia and China's engagement, increasingly towards strategic-level practice within organisations, albeit from their lower levels. For example, Moving Target Defences (MTDs) and federated security among organisations/providers (DHS, n.d.) are strategically more sophisticated, even though they often operate from further down within organisations.

China and Russia, whether by intention or in effect, have leveraged a more matured and strategic-level use of traditional security disciplines in practice, and are driving these disciplines and practices to higher strategic levels within a grand strategy context. Russia, with its 2014 strategic planning law, Federal Law No. 127, has attempted to take strategic

planning, across multiple levels of government, to an impressive level of sophistication (Monaghan, 2018, p. 14; Uskova & Chekavinskii, 2014).

Security convergence (which considers both IT and physical security together) is typically conducted at the operational level. In tandem, China's geostrategic projection of 5G networks and National Intelligence Law of 2017 (which may in certain conditions require Chinese persons globally to cooperate in China's intelligence activities) may represent a strategic-level, and even grand strategic-level, security convergence risk, requiring a response well above the operational level, and pushing the boundaries of the security convergence discipline.⁶

Business Continuity Management (BCM), an operational-level security discipline, was taken to an impressive strategic level by Huawei and its subsidiary, HiSilicon, created in 2004. The company had persisted in developing mobile CPUs without profitability until 2013, "toiling on 'spare tires' kept in reserve". It was a long-run investment and higher strategic level treatment of business continuity that "safeguarded the *strategic security* and uninterrupted supply of a large share of Huawei's products" (emphasis added). Following US restrictions in 2019 that blocked Huawei smartphones from using Qualcomm chips, HiSilicon unveiled its Kirin 990 chip. Not limited to being a strategic-level security success, the release of the Kirin chip – thought to be too risky, too expensive, and unlikely to perform to market expectations – launched with a "strategic surprise" effect quickly after Huawei was blocked. Business operations continued even despite international- and foreign state-level induced disruption, well beyond the organisation itself (Dou, 2020).

⁶ The UK's 2020 Intelligence and Security Committee of Parliament Report, "Russia", recommended that the UK also require social media companies to cooperate with the UK's MI5 intelligence service, and that the UK expand the powers of other intelligence and related laws (Intelligence and Security Committee of Parliament, 2020). This may match any security convergence risk with counter-projection, rather than address the original projection risk directly.

In tandem, China's geostrategic projection of 5G networks and National Intelligence Law of 2017 (which may in certain conditions require Chinese persons globally to cooperate in China's intelligence activities) may represent a strategic-level, and even grand strategic-level, security convergence risk, requiring a response well above the operational level, and pushing the boundaries of the security convergence discipline.

The development of unique Russian and Chinese legal doctrines and practices has contributed to the development of unique sub-orders. Russia currently follows the Chernichenko school of legal thought, with a sovereign state focus and division between international and domestic legal domains. Since 2000, Russia has required by law that its foreign policy be informed by International Law – which is interpreted along Russian legal doctrine lines (Malksoo, 2017).

China has also informed its Foreign Policy (and its disputes) with IL. In the absence of international cyber law, China has innovatively applied other law by proxy to disputes, such as International Investment Law (IIL). This is a divergence from most states, which have applied by proxy International Law (IL), International Humanitarian Law (IHL), or International Human Rights Law (IHRL) regimes as the closest proxies for the international cyber law void – not IIL.

For example, after the CFO of Huawei was detained in Canada regarding a US extradition matter, China effectively shifted the larger 5G-related matter to a Public International Investment Law and trade dispute with Canada by restricting agricultural exports from Canada to China. This effectively served as an asymmetric retorsion⁷ in response to the Canadian detainment of the Huawei CFO, with linked but dissimilar treatment. This further complicated management of the dispute, by playing up

⁷ Retorsion is defined as “a retaliation; reprisal; esp., in international law, mistreatment by one country of the citizens or subjects of another in retaliation for similar mistreatment received” (Webster, n.d.).

the gaps and seams between the various regimes within Public International Law (IL, IHL, IHRL, and IIL). China similarly responded to growing momentum against Huawei involvement in 5G network development in the West with warnings of investment and trade retorsion, or asymmetric retorsion.⁸

Australia identified the displacement of cyber-related disputes to the non-cyber Public International Law space (specifically IHRL, IHL, and IL – but not IIL), and highlighted the need for clarification on how states are interpreting international law in relation to cyber-related matters (Australian Government, 2019). This recognition of differences in interpretation is not inconsistent with divergent legal doctrine and interpretations within the developing sub-orders.

Recent domestic laws in Russia and China are also reflective of their developing sub-orders and expanded global geostrategic projection and reach. In July 2006, Russia passed a law authorising extrajudicial killings provided they are authorised by the President and the Federal Council is notified within five days (Cuddy, 2018). Since then, Alexander Litvinenko was killed in the UK in November 2006, Sergei and Yulia Skripal were poisoned there in 2018, and Zelimkhan Khangoshvili was shot dead in a public park in Berlin, Germany in 2019. All cases were attributed to Russia, which Russia has rejected. Meanwhile, China's new domestic laws, including the Intelligence Law (2017), Internet Security Law (2017), and the 2020 security law, have implications beyond China and for non-Chinese citizens; this may potentially be a legal geostrategic projection of China's domestic laws, including for grand strategic purpose.⁹

⁸ For example, China reportedly responded with pressure against the auto industry in Germany, a free-trade agreement with Denmark, European company development in China with France, and unnamed “repercussions” against Federal Government of Canada (McCuaig-Johnston, 2020).

⁹ The proposed 2019 extradition legislation is also of concern, as China is already suspected of conducting extraordinary renditions (Li, 2019). The 2020 security law may increase control over Hong Kong in advance of 2047. The Internet Security Law may drive personal data storage geographically to China, potentially increasing China's control and furthering its objective of technological dominance (Spalding, 2019, p. 198).

These domestic laws and conflicting doctrines and interpretations of IL are entrenching the diverging sub-orders within the International Order. Like many laws, they will be difficult to reverse. The increasing incompatibility of laws and legal interpretations within the International Order and sub-orders cannot be ignored by the US, particularly with projection of these laws (both international and domestic) and in some cases their applicability globally (Wallace, 2020). Russia and China not only view their sub-order interpretations and engagement as compatible within the International Order, but as both adding stability to it and necessary to their national interests.

The increasing incompatibility of laws and legal interpretations within the International Order and sub-orders cannot be ignored by the US, particularly with projection of these laws (both international and domestic) and in some cases their applicability globally.

China and Russia appear to have developed “counter-projection” strategies and conditions that isolate and insulate themselves against push-back or consequences of geostrategic projections and interconnectivity. While Washington relies heavily on military projection, alliances and coalitions, and the resilience of critical and cyber infrastructure and systems, Moscow and Beijing appear prepared for external risks and threats to their domestic infrastructure and systems.

Russia’s “strategic solitude” strategy reflects its self-reliance posture in military and international affairs (Westerlund, 2018, p. 37). Russia has developed the capability to effectively disconnect its internet from the outside world under the Internet Isolation Law which was successfully tested in 2019 (Doffman, 2019; Wakefield, 2019). China, in addition to its Great Firewall, has also moved toward renewed self-sufficiency and assured continuity with the Belt and Road Initiative (BRI), Plan 2025 for manufacturing, and the Thousand Talents initiative (Spalding, 2019). Article 37 of China’s Internet Security Law (2017) requires that

the personal information of Chinese citizens must be kept on servers in China, which may prompt companies to operate in or cooperate with companies in China, likely affording more control over data and digital supply chains to this country (KPMG, 2017, p. 12).

China has made significant efforts toward restricting capital flight from China (Spalding, 2019). While there remains significant personal foreign investment by Russian citizens and expatriates, Russia – unlike China – does not have a Global Systemically Important Bank (G-SIB). This may buffer Russia from cascading effects within the international banking system, and potentially also shield Russia from serious effects of attacks on banking infrastructure and systems.

There has been a noted increase in what some believe to be the conduct of “hostage diplomacy” by states, to influence state actions or buffer against state responses and consequences, short of military conflict. This may include potential asymmetric retorsion linked to the larger 5G-related dispute playing out in Canada, and as the US attempts to isolate its sphere of influence and interests from tech/5G geostrategic projections, including from China or affiliated entities.¹⁰

Resorting to such tactics is likely to escalate over time, particularly given the effect on the individuals and families affected. They are likely to cause further damage to international relations, which are already at a low with the expulsions of numerous Russian diplomats from the West following the Salisbury, UK targeted attack in 2018, and closing of consulates in both China and the US in July 2020.

¹⁰ Huawei CFO, Meng Wanzhou, was detained in Canada on 1 December 2018, followed by the detentions of Canadians Michael Spavor and Michael Kovrig in China on 10 December 2018 for alleged spying activity. All remain in detention. Given the impasse, a Canadian petitioner submitted information to the UN Office of the High Commissioner for Human Rights, under Special Procedures, regarding alleged violations of the human rights of Spavor and Kovrig, including arbitrary detention and torture. The list of facts notes: “...the linkage the Government of China itself has made between the continued detention of the two Canadians and the extradition proceedings in Canada against Meng Wanzhou” (Canadian petitioner, 2020).

These new “gunboat diplomacy” tactics may be symptomatic of the development of sub-orders within the fracturing International Order, in part due to the dissatisfaction among many states with International resolution mechanisms, and of dispute displacement. This has left fewer good options, as states engage over matters of critical national interest and national security importance.

These new “gunboat diplomacy” tactics may be symptomatic of the development of sub-orders within the fracturing International Order, in part due to the dissatisfaction among many states with International resolution mechanisms, and of dispute displacement.

While Russia, China, and the US can all both geostrategically project and take measures to isolate and insulate themselves to varying degrees from perceived projections and their effects, other states must navigate carefully in between these competing powers, often with fewer resources and less influence. This has put some states under considerable stress, reminiscent of Cold War shatterbelt effects. The concerns over 5G networks and cybersecurity may be creating new tech/5G shatterbelts and effects for countries caught in between in deciding which 5G providers to go with, and what effects 5G decisions will have for them in other areas and for relationships. This is also affecting tech sector markets, enterprises, and investors, who face more uncertainty and greater risk amid the grand strategic engagement of great powers.

Canada is, for example, caught between US warnings that further engagement on 5G with Huawei could jeopardise Canada’s intelligence-sharing relationship with the US, and apparent asymmetric retorsions from China – which may also explain Canada being last among the Five Eyes alliance to make a decision regarding excluding or restricting Huawei from its 5G networks and development. Similarly, the UK recently reversed its earlier position on allowing limited Huawei involvement in UK 5G networks, under pressure from the US and while the UK is seeking a trade deal with

the US (McCuaig-Johnston, 2020). On a larger scale, the D-10 initiative aims to create a trusted partnership and trusted zone among the G-7 states and Australia, India, and South Korea in relation to 5G and supply chains (McCuaig-Johnston, 2020). This is prompting states to choose among 5G providers, and effectively, between great powers. China appears to have moved to impose greater certainty and predictability in the context of new 5G/tech shatterbelts, having negotiated an unprecedented 25-year comprehensive partnership with Iran that would resist third country pressures, including in relation to 5G development (Davar, 2020). Such longer-run arrangements could harden divisions and reduce options further for states in between.

Even with isolation and insulation strategies, the new geostrategic projections and the push-back against them are nonetheless causing escalation and challenging the traditional meaning and stability that borders previously provided, especially in peacetime. The result is not inconsistent with Gen. Gerasimov’s detailing of a persistent conflict environment, even while at peace.

This has resulted in a defensive stand-off posture among the three great powers. There is a limited window of opportunity in which to address this escalatory stand-off, as the International Order, and its multiple sub-orders, transition toward multipolarity. The stand-off is tilted against the United States, in that it must address separate grand strategies by its strategic competitors, Russia and China, which are themselves currently acting as strategic partners (Westerlund, 2018, p. 39). The US and its partners have a military and alliance strategic advantage, while Russia and China have strategic advantages in asymmetry and innovation, which have been systematically and methodically developed, and leveraged through geostrategic projection short of direct conflict. These advantages are now facing push-back and risk escalating distrust and friction.

Hard power is increasingly gaining importance for credibility and deterrence in achieving objectives; however, even when limited, it risks escalation,

particularly when involving geostrategic projections. Russia's protection of its near-abroad (e.g. Crimea and Donbas) did not escalate to full-scale conflict, in part due to proximity to Russia and Russian forces. Russia's limited military intervention in Syria, further from its near-abroad, was intended to support the International Order focused on the primacy of state sovereignty, but may have pulled Russia further into Middle East politics beyond the original objective of stabilising the International Order (Galeotti, 2019, p. 86-88; Rumer, 2019). China has built out its interests in the South China Sea; however, the US recently rejected the legality of most of China's claims (Hansler, 2020). This legal dispute also escalated from legal interpretations to hard power, with two American aircraft carriers deployed simultaneously to the South China Sea, on two separate occasions in July 2020 (Pearson, 2020).

Hard power is increasingly gaining importance for credibility and deterrence in achieving objectives; however, even when limited, it risks escalation, particularly when involving geostrategic projections.

Russia and China appear to have attempted to impose greater stability and predictability upon the international system, further cementing these developing sub-orders. China has engaged in very long-term investment and development agreements globally – some lasting 99 years, for example. Russia and China have also both extended their leadership term limits – with President Putin potentially being able to serve until 2036 as of 2020, and President Xi Jinping being able to serve potentially indefinitely since constitutional amendments in 2018 (Hodge & Ilyushina, 2020).

There is also a notable trend toward a more aggressive and uncompromising approach among new actors in China, as with its more aggressive “wolf warrior diplomacy” (Westcott & Jiang, 2020). Huawei senior personnel were also noted as less willing to consider a merger or partnership with American counterparts after a failed attempted

deal with Motorola, favouring a more self-driven path forward since then (Dou, 2020).

Without de-escalation, this defensive stand-off may continue to fracture the overall International Order toward a new Cold War, with hardened lines between powers with entrenched sub-orders. De-escalation will require convincing the great powers that they are not under threat from each other: Russia must be convinced that NATO expansion is not a threat to Russia's near abroad and sphere of influence; China that its economic ambitions and engagement, and thereby national security, are not being impeded by the US; and the US that its great power and economic position (closely linked to 5G), and its values, are not being excessively eroded by ascending strategic competitors with new entrenching sub-orders and understandings within the International Order.

If de-escalation and trust-building cannot be achieved among them, then adjustments to the International Order and its structures, institutions, and processes may need to be considered, particularly in the investment/trade and public international law spaces. This may add sufficient flexibility, stability, and predictability.

Stabilising the International Order may ease geostrategic projections and reactions to them, while addressing new geostrategic projections (like 5G or the targeting of individuals), may not suffice in stabilising the International Order over the long run. Geostrategic projections are symptoms of and catalysts for greater turbulence within the International Order, while great powers are at an impasse in the transition to multipolarity within an interconnected landscape.. Without de-escalation and management, the situation may slide into a new Cold War with hardened lines and Balkanised global networks.

Without de-escalation and management, the situation may slide into a new Cold War with hardened lines and Balkanised global networks.

Possible ways forward in a more complex and interconnected geostrategic space

In the short-run: urgently address the detention and targeting of individuals, including that resulting from globalised applicability of domestic laws, extended even to non-citizens; avoid dispute displacement to other sectors and asymmetric retorsions, which add complexity; strengthen diplomatic relations and other communication channels (such as military-to-military) to prevent misunderstandings and unintended escalations; limit geostrategic projection provocations; and provide increased flexibility and options for states in the middle.

In the medium-run: further the collaborative technical and regional initiatives to increase trust in new technologies and prevent network

Balkanisation; develop the traditional security disciplines to strategically bridge practitioner expertise with grand strategy; augment capacity and competition within the tech sector, particularly in 5G (Benner, 2020); and develop new diplomatic tools – in between those with waning effect (sanctions, condemnation) and those with escalatory effect (asymmetric retorsion, hostage diplomacy).

In the long run: identify and manage the entrenchment of divergent sub-orders and strategies within the existing International Order; redouble efforts to fill the international cyber-law void; and avoid a new human intelligence and espionage race that could negatively impact the privacy, rights, and freedoms of individuals. ■

About the author:



Bonnie Butlin, also known around the world as “Canada’s First Lady of Security” is the co-founder and executive director of the Security Partners’ Forum (SPF), a first-of-its-kind agile international network of security professionals, bridging all domains and disciplines of security. Under the SPF banner, she created the Women in Security and Resilience Alliance (WISECRA), which engages a growing network of women in security and resilience associations and groups globally.

Since 2013, Bonnie Butlin has received some 21 international and national-level awards and accolades related to security, resilience, and leadership, including being named as a “Fellow of (ISC)2 in August 2020. In 2017, she was appointed to the World Economic Forum’s Expert Network in Cybersecurity, and in 2018 was appointed to the Global Advisory Council of the Institute of Strategic Risk Management (ISRM).

References

- Armstrong, P. (2019, November 29). Huawei funds \$56M in academic research in Canada. That has some experts concerned. *CBC*. Retrieved from <https://www.cbc.ca/news/business/huawei-academic-funding-in-canada-1.5372310>
- Australian Government. (2019). *2019 International Law Supplement: Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace*. Australia's International Cyber Engagement Strategy. Retrieved from https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html
- Bartles, C.K. (2016, January). Getting Gerasimov Right. *Military Review*. 96(1), 30-38. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf
- Benner, K. (2020, February 06). China's Dominance of 5G Networks Puts U.S. Economic Future at Stake, Barr Warns. *The New York Times*. Retrieved from <https://www.nytimes.com/2020/02/06/us/politics/barr-5g.html>
- Berzins, J. (2018). *The Russian Way of Warfare*. In J. R. Deni (Ed.). *Current Russia Military Affairs: Assessing and Countering Russian Strategy, Operational Planning, and Modernization*. Strategic Studies Institute, United States Army War College. Carlisle, PA. (pp. 18-20).
- Butler, W.E. (2019). *Foreign Policy Discourses as Part of Understanding Russia and International Law*. In P. S. Morris (Ed.), *Russian Discourses on International Law: Sociological and philosophical phenomenon*. *Routledge Research in International Law*, New York, NY: Routledge (pp. 177-196).
- Brangetto, P., & Kert-Saint Aubyn, M. (2015). *Economic aspects of national cyber security strategies: Project Report*. CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. Retrieved from <https://ccdcoe.org/uploads/2018/10/Economics-of-cybersecurity.pdf>
- Canadian petitioner. (2020) *Submission of information to the Special Procedures*, to the United National Human Rights Office of the High Commissioner, filed on 2020, July 22. Retrieved 29 July 2020.
- Cuddy, A. (2018, March 08). What authority does Putin have to order extrajudicial killings abroad? *Euronews*. Retrieved from <https://www.euronews.com/2018/03/08/what-authority-does-putin-have-to-order-extrajudicial-killings-abroad->
- Davar, F. (2020, July 08). Exclusive: Iran Agrees to Be China's Client State for the Next 25 Years. *Iranwire*. Retrieved from <https://iranwire.com/en/features/7275>
- Department of Homeland Security (DHS). (n.d.). *Federated Security*. Retrieved from <https://www.dhs.gov/science-and-technology/federated-security>
- Doffman, Z. (2019, May 01). Putin Signs 'Russian Internet Law' To Disconnect Russia from the World Wide Web. *Forbes*. Retrieved from <https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#72012a251bf1>
- Dou, E. (2020, June 18). Huawei chip unit short-circuited Trump's sanctions. Then it got burned. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/asia_pacific/huawei-china-trump-sanctions-hisilicon-chips-technology/2020/06/17/732aed58-a936-11ea-a43b-be9f6494a87d_story.html
- Feaver, P. (2009, April 08). What is grand strategy and why do we need it? *Foreign Policy*. Retrieved from <https://foreignpolicy.com/2009/04/08/what-is-grand-strategy-and-why-do-we-need-it/>
- Felgenhauer, P. (2019, March 07). A New Version of the 'Gerasimov Doctrine'? *Eurasia Daily Monitor*. *The Jamestown Foundation*. 6(32). Retrieved from <https://jamestown.org/program/a-new-version-of-the-gerasimov-doctrine/>
- Galeotti, M. (2019). *We Need to Talk About Putin: How the West gets him wrong*, London, England: Penguin Random House UK.
- Galeotti, Mark. (2020, April 28). The Gerasimov Doctrine. *Berlin Policy Journal*. Retrieved from <https://berlinpolicyjournal.com/the-gerasimov-doctrine/>
- Global Affairs Canada. (2012). *Agreement Between the Government of Canada and the Government of the People's Republic of China for the Promotion and Reciprocal Protection of Investments*. Retrieved from <https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/china-chine/fipa-apie/index.aspx?lang=eng&ga=2.13253684.2087700122.1595780686-229343471.1595780686>
- Hansler, J. (2020, July 14). US declares 'most' of China's maritime claims in South China Sea illegal. *CNN*. Retrieved from <https://www.cnn.com/2020/07/13/politics/south-china-sea-pompeo-announcement/index.html>

- Hodge, N., & Ilyushina, M. (2020, July 02). Russian voters overwhelmingly back a ploy by President Vladimir Putin to rule until 2036. CNN. Retrieved from <https://www.cnn.com/2020/07/01/europe/russia-referendum-putin-power-2036-intl/index.html>
- Hongwei, L. (2017). *Ren Zhengfei & Huawei: A business and life biography*, New York, NY: LID Publishing Ltd.
- Intelligence and Security Committee of Parliament (2020). *Russia*. Presented to Parliament pursuant to section 3 of the Justice and Security Act 2013. Ordered by the House of Commons to be printed on 21 July 2020. Retrieved from [https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXtBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEy-N2Y3NjM0OWFIKPMG, IT Advisory KPMG China \(2017\). Overview of China's Cybersecurity Law. Retrieved from https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf](https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXtBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEy-N2Y3NjM0OWFIKPMG, IT Advisory KPMG China (2017). Overview of China's Cybersecurity Law. Retrieved from https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf)
- Li, J. (2019, June 16). China's history of extraordinary rendition. *BBC News Chinese*. Retrieved from <https://www.bbc.com/news/world-asia-china-48634136>
- Malksoo, L. (2017). *Russian Approaches to International Law*, Oxford, United Kingdom: Oxford University Press.
- McCuaig-Johnston, M. (2020, July 04). China's threats on behalf of Huawei are becoming desperate. *The Globe and Mail*. Retrieved from <https://www.theglobeandmail.com/opinion/article-chinas-threats-on-behalf-of-huawei-are-becoming-desperate/>
- Monaghan, A. (2018). *From Plans to Strategy: Mobilization as Russian Grand Strategy*. In J. R. Deni (Ed.). *Current Russia Military Affairs: Assessing and Countering Russian Strategy, Operational Planning, and Modernization*. Strategic Studies Institute, United States Army War College. Carlisle, PA (pp. 14-17).
- Morris, P.S., (2019). "Sovereign Democracy" and International Law: Legitimation and Legal Ideology. In P. S. Morris (Ed.), *Russian Discourses on International Law: Sociological and philosophical phenomenon*. Routledge Research in International Law, New York, NY: Routledge. (pp. 100-130).
- Pearson, J. (2020, July 17). U.S. aircraft carriers return to South China Sea amid rising tensions. *Reuters*. Retrieved from <https://www.reuters.com/article/us-southchinasea-usa-carriers/u-s-aircraft-carriers-return-to-south-china-sea-amid-rising-tensions-idUSKCN24119W>
- Rumer, E. (2019, June 05). The Primakov (Not Gerasimov) Doctrine in Action. *Carnegie Endowment for International Peace*. Retrieved from <https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254>
- Spalding, R. (2019). *Stealth War: How China took over while America's elite slept*, United States of America: Penguin Random House.
- Swaine, M. (2015). Xi Jinping's Address to the Central Conference on Work Relating to Foreign Affairs. *Carnegie Endowment for International Peace*. Retrieved from <https://carnegieendowment.org/2015/03/02/xi-jinping-s-address-to-central-conference-on-work-relating-to-foreign-affairs-pub-59220>
- Uskova, T., & Chekavinskii, A. (2014). Law on Strategic Planning in the Russian Federation: Advantages and unresolved issues (expert evaluation). *Economic and social changes: facts, trends, forecast*. 4(34), 63-67. Retrieved from https://www.researchgate.net/publication/280746370_Law_on_strategic_planning_in_the_Russian_Federation_advantages_and_unresolved_issues_expert_evaluation
- Wakefield, J. (2019, December 24). Russia 'successfully tests' its unplugged internet. *BBC*. Retrieved from <https://www.bbc.com/news/technology-50902496>
- Wallace, A. (2020, June 30). Hong Kong security law: What is it and is it worrying? *BBC*. Retrieved from <https://www.bbc.com/news/world-asia-china-52765838>
- Wang, G. (2016). *International Investment Law: A Chinese Perspective*. Routledge Research in International Economic Law, New York, NY: Routledge.
- Webster. (n.d.). Retorsion. In Webster's New World College Dictionary, 4th Edition, Houghton Mifflin Harcourt. Retrieved from <https://www.collinsdictionary.com/dictionary/english/retorsion>
- Westcott, B., & Jiang, S. (2020, May 29). China is embracing a new brand of foreign policy. Here's what wolf warrior diplomacy means. *CNN*. Retrieved from <https://www.cnn.com/2020/05/28/asia/china-wolf-warrior-diplomacy-intl-hnk/index.html>
- Westerlund, F. (2018). In J. R. Deni (Ed.). *Current Russia Military Affairs: Assessing and Countering Russian Strategy, Operational Planning, and Modernization*. Strategic Studies Institute, United States Army War College. Carlisle, PA (pp. 35-39).

ANALYSIS

Digitalisation – Opportunities for Development

FAUSTINE FELICI

CYBERSEC PROJECT MANAGER, THE KOSCIUSZKO INSTITUTE

The rapid rise of the cross-border digital realm has been an incredible enabler for countries and citizens worldwide – be it in the economic, political, or social sphere. Nowadays, digital technologies already provide billions of people with access to basic services such as healthcare, education, banking, or even government-related services, thus contributing to raising the development level of the countries they are deployed in. Indeed, development in its larger conception encompasses multiple indicators such as life expectancy, education, and per capita income – all of which have the potential to be largely impacted by the spread of new digital applications. However, the impact

of technological progress on a country's level of development is hard to quantify. Considering the most pressing issues when it comes to securing digital transformation and their geographical distribution, four regions are facing the biggest challenges, but also have a great potential in terms of innovation and are therefore likely to benefit from the greatest positive outcomes of digitalisation. These regions are Eastern and Southern Europe, Central Asia, Sub-Saharan Africa, and Central and South America. Varied examples of successful implementation of digital solutions can help illustrate the positive effects of a country's or region's digitalisation.

- **Sub-Saharan Africa.** Sub-Saharan Africa has long been a region with the highest levels of financial exclusion. Because of a lack of financial infrastructure allowing the people in this region to securely save and transfer money or to have access to credit and insurance, in 2013 less than 25% of the population had access to formal financial services (International Finance Corporation, 2013). The introduction of mobile money accounts, eliminating the need for physical infrastructure and lowering the costs of financial services, has drastically changed the situation. In 2017, 21% of adults in the region had a mobile money account, which is nearly twice as much as in 2014 (The World Bank, 2017).
- **Eastern and Southern Europe.** Combatting corruption is an important issue for the region in its effort to achieve a higher level of economic development as well as to get closer to the European Union standards. Greater transparency and lower corruption levels lead to better government services and a larger openness to international trade. To support this effort, digital tools have been deployed throughout the region. In North Macedonia for instance, a website along with a mobile application allow citizens to instantly report cases of corruption. In Ukraine, an online public procurement platform – ProZorro – has ensured an open access to tenders since 2016, thus helping reduce the risk of malpractice. In addition, a risk indicators system has been implemented and, backed by artificial intelligence (AI) algorithms, it helps to detect suspicious tenders and potential corruption cases in the country.
- **Central Asia.** With about 30% of its workforce employed in the agricultural sector, the welfare of Central Asian population is highly dependent on natural conditions. For several decades – and this trend tends to be worsened by climate change – the region has been plagued by the desert locust, a migratory pest species, able to reproduce rapidly and devastate crops. The development and

introduction of an e-agriculture solution – in the form of a mobile application¹ that records and transmits field data via satellite in real time – considerably improved the forecasting and a timely issuance of early warning, leading, in turn, to a decline in the duration and severity of locust plagues in the region.

- **Central and South America.** Particularly marked by its authoritarian past, this region of America has recently proved highly innovative when it comes to the experience of participation and democracy. Increasing levels of ICT ownership and use enabled various e-participation initiatives to flourish. These initiatives engage citizens to contribute to policy processes, suggest new legislation, report on important issues, or even track institutional performance, therefore giving them more weight in the policy-making process. From 2000 to 2016 for instance, Brazil, Colombia, Mexico, and Peru have created 206 initiatives for e-participation, 141 of which were still active in 2017 (Pogrebinschi, 2017).

But with emerging new technologies such as AI, the Internet of Things (IoT), or quantum computing, the potential that digital transformation entails lies far beyond what currently exists. Due to their cross-sectoral character, digital tools can transform economy and society more deeply and more quickly than ever before. This attribute makes them therefore particularly suited for contributing to the fulfilment of United Nations' Sustainable Development Goals (SDGs). Adopted by all UN members in 2015, the SDGs are a call for cooperation to jointly advance towards a sustainable future. The potential benefits that digital technologies can bring to different goals are already well-recognised and emphasised. In a ministerial declaration in 2018, signatories stated that they “will embrace innovation-driven development, digitalization and new technologies, especially information and communications technologies,

¹ The eLocust3 app developed by the FAO. More information on: <http://www.fao.org/3/CA2588EN/ca2588en.pdf>, p. 7.

in managing cities more effectively and holistically, including intelligent and resource-efficient transport systems and new efficiencies in energy consumption and waste management” (United Nations Economic and Social Council, 2018, p. 7).

Cyberspace is therefore a necessary platform for spreading innovation, fostering economic growth, and empowering citizens. The development of ICTs and the fast-increasing Internet access all over the world can facilitate the creation of a global sustainable digital society. All the solutions deployed in the digital world harness the power of transforming digital tools into global public goods. But the increasing number and variety of security challenges linked with the development of digital technologies is threatening this endeavour and the prosperity of the digital ecosystem. Because we are only as strong as the weakest link in our digital global chain, joint effort to maintain and safeguard the security of digital economies and societies should prevail. We must ensure that digital is not used to hinder development and the achievement of sustainable goals. Cyberspace knows no borders between more and less developed countries in terms of cybersecurity; therefore, digital security is a shared responsibility. Cooperation in building cybersecurity capacities and capabilities in all regions of the world is key to enhancing global cyber-resilience.

The increasing number and variety of security challenges linked with the development of digital technologies is threatening this endeavour and the prosperity of the digital ecosystem.

Mapping Digital Threats to Development

If the emergence of ICTs and digital tools can bring many advantages to the development of a country or a region, it can also potentially harm them. Digital tools in the hands of malicious actors pose a very real danger indeed.

Economic damage

It is estimated that the world economy loses over USD 600 billion every year due to cyberattacks (Lewis, 2018). What is even more striking,

cybercrime cost has been estimated to reach USD 2.1 trillion by the end of 2019 (Morgan, 2016). Security is the cornerstone of any digital activity, including telecommunications, and should be considered a priority. So far, however, not all ICT solutions – which are vital to economic and societal welfare – have the features that are both necessary and sufficient to ensure the security of their use. Integrating the security-by-design principle and providing effective security safeguards within the whole life-cycle of a product is therefore essential to mitigate the risks posed to people’s daily lives and development by unsecured ICT solutions.

For many years, cyberattacks have been used as a weapon, not only by malicious individuals but also by state-sponsored groups, and can have extremely grave consequences. A single ransomware campaign of NotPetya, which was first launched against Ukraine in 2016 and went global in 2017, had worldwide repercussions and caused an estimated USD 10 billion in losses. The devastating global impact of this event alone warrants a stronger international cooperation in building cyber-resilience.

Furthermore, Zurich Insurance forecasts indicate that in 2030, losses incurred because of cyberattacks will equal 0.9% of the world’s GDP (2017). Motivations behind cyberattacks vary (OECD, 2012) from money to “hacktivism” (Anonymous), destabilisation (Estonia in 2007), cyberespionage (e.g. Operation Titan Rain), sabotage (e.g. Stuxnet), and the support of a military operation (Russian invasion of Georgia in 2008). Cybercriminals are getting better organised and better at covering their tracks. The degree of sophistication of the attacks has also significantly increased. Therefore, it is important to admit that globalisation and the transformation of societies into digital societies are realities that must be accepted and understood. Additionally, the risks associated with it have to be addressed efficiently.

Political intrusion

Apart from severe economic losses, the risks and vulnerabilities that accompany the digitalisation of a country can touch the political sphere. Intervening in domestic affairs of a foreign country

and trying to influence it has long been an under-cover, but nevertheless existing diplomatic practice. In today's digital era, the interference has gained in strength and shifted to target the very core of the democratic process. In 2016, during the U.S. presidential elections, internet platforms and social media were harnessed to wage information warfare by conducting disinformation and manipulation campaigns as well as spreading hostile propaganda, creating confusion and spreading distrust in voters' minds. More dramatically, in developing countries such as Myanmar, the military used misinformation tactics in social media to escalate ethnic and religious tensions. Members of the Myanmar army were the prime operatives behind a systematic campaign on social platforms that targeted the country's Muslim Rohingya minority (Mozur, 2018). Developed and developing countries alike are often victims of interference in their domestic affairs taking the form of information warfare or misinformation campaigns, and they have to systematically fight these malign trends in order to protect the integrity of their political systems.

Rebalancing of responsibilities

The emergence of a global information society, enabled by the integration of ICTs, increased the dependence of individuals, organisations, and countries on digital products and infrastructures. Therefore, it is evident that both the private and the public sector have been forced to take on new responsibilities. Private companies shape and develop new technologies that have the potential to impact the security of countries and individuals. Globalisation has permitted these technologies to spread across the world, thus increasing the responsibility of private companies in security and policy-making mechanisms. On the other side, the role of states and governing bodies has also changed substantially. Providing systematic guidance to the private sector in order to ensure national security has now become one of their greatest tasks and challenges.

The least cybermature countries are often – in spite of themselves – the patient zero of cyberattacks

which, unreported or undetected, spread rapidly and on a large scale. The lack of one or several essential features like an up-to-date cybersecurity strategy, an effective system of crisis management and cyber incident response, a legal and judicial framework on cybercrime and e-evidence, and well-embedded cyberhygiene can significantly hinder the development of countries and prevent them from taking full advantage of the digital revolution. Bolstering the debate on reinforcing cybercapacities in all regions of the world and strengthening the cooperation in this domain is, therefore, in the common interest.

The lack of one or several essential features like an up-to-date cybersecurity strategy, an effective system of crisis management and cyber incident response, a legal and judicial framework on cybercrime and e-evidence, and well-embedded cyberhygiene can significantly hinder the development of countries and prevent them from taking full advantage of the digital revolution.

Cyberspace is not an Even Playground

Last come, worst served

Nowadays, many countries face an exponential increase in the number of their ICTs users. This trend – in addition to a lack of awareness, shortage of human capabilities or dedicated entities – often prevents them from securing their infrastructure commensurately to the risks. It is therefore unsurprising to find some of the world's fastest growing internet markets among the top regions hosting compromised computers and initiating malicious activities. Cybercriminals have long considered countries with a lower level of cybersecurity as opportune places to commit their criminal acts. Africa, for instance, is extremely exposed to cyber-related threats. A report shows that estimated losses to African business caused by cybercrime amounted to USD 3.5 billion in 2017, compared to USD 2 billion in 2016 (Serianu, 2017). In addition, a staggering 96% of cybersecurity incidents in Africa seemingly go unreported or unresolved (Serianu, 2017, p. 11).

The absence of cooperation between countries with a high level of cybersecurity and cyber-developing countries can generate “safe havens”, where cybercriminals make use of the legal loopholes, including the lack of measures to counteract cybercrime. The ability to ensure security of information, processes, systems, and infrastructure is critical to the successful development of any country.

The level of cybersecurity advancement varies from country to country and from region to region, being often correlated with the level of economic development, but not exclusively. What is even more important than the level of cyber-readiness, however, is the commitment of countries to their cybersecurity. The digital world is indeed evolving at a fast pace, necessitating a constant adaptation of laws, technical and organisational measures, or preventive structures. An overview of the current situation of cybersecurity commitment can be found for instance in the International Telecommunication Union Global Cybersecurity Index (ITU, 2018). Regions with an already high level of cybersecurity such as Europe or North America remain highly committed to maintain their protection. However, it is also essential to note that among the regions with a lower level of cybersecurity, some show a fair level of commitment, given their infrastructure development. These regions are Eastern and Southern Europe, Central Asia, Sub-Saharan Africa, and Central and Southern America.

Cooperation – be it domestic, in the form of in-country public-private partnerships or international, involving the exchange of best practices – facilitates the adaptation and helps secure the digital transformation of a country or a region. Commitment coupled with international cooperation is the key to equalise the level of cybersecurity around the world upwards.

Commitment coupled with international cooperation is the key to equalise the level of cybersecurity around the world upwards.

CEE cyberexperience as a compass through digital transformation

Due to different political, economic, and social contexts, each country must find and forge its own path through digitalisation. However, inspiration and experience from outside can greatly help them successfully navigate through this process.

The states of Central and Eastern Europe embarked on their digital transformation only a few decades ago and are now fully involved in digitalising their economies and societies in a secure manner. According to ITU’s Global Cybersecurity Index (GCI) 2018, 10 out of 12 CEE countries are in the highest category when it comes to their level of commitment to cybersecurity. In 2017, only one – Estonia – was in this category, showing a spectacular change in a brief period of time. The EU membership of these countries is obviously a great catalyst in strengthening cybersecurity. The directive on Security of Network and Information Systems (NIS), the General Data Protection regulation (GDPR), and the recent Cybersecurity Act – just to mention the most well-known of them – are the Union’s wide policies that improve cybersecurity in all countries at once. However, these countries also act by deploying their own policies and programmes that aim to develop their digital tools and improve their cyber-resilience domestically. The Lithuanian government, for instance, is developing a “Secure Network”, a system that will remain separated from public communication networks in order to stay functional in the case of a crisis or a war and allow for responding to cyber-incidents more quickly and effectively (Ministry of National Defence of the Republic of Latvia, 2019).

The eventful world history of the last century witnessed the birth of new countries and some countries regaining their independence. Young countries have equally young and immature institutions and therefore other, more pressing issues to solve than the ones related to digital transformation. However, the level of their commitment is remarkable, which is a positive and encouraging sign. Furthermore, as many of these countries are still at the beginning of the road towards

digital transformation, they may greatly benefit from the experience of CEE, which started its journey just a few years earlier. The initiation of the process is indeed a critical decision that requires deep reflection – sharing experience and advice about it can only be beneficial.

Last but not least, the geographical and geopolitical position of the CEE region – on the eastern border of the EU and NATO – puts it at the forefront of many digital challenges, such as hybrid warfare. The region is also under high threat of being the target of cyberattacks and hostile actions from foreign actors, just like other cyberdeveloping countries. As mentioned earlier, the latter indeed provide an ideal testbed for new and potentially most dangerous types of cyberattacks because they are likely stay undetected in an environment which is not yet secured. The creation and establishment of a cybersecure infrastructure and the reinforcement of cyber-resilience in these countries is both a necessity and a priority in order to ensure their sustainable development as well as global cyberstability.

Sharing a similar context with other cyberdeveloping regions of Europe, Asia, America, and Africa on some aspects, the experience of the CEE region is therefore fully relevant policy-wise. In the same way, success stories from abroad can benefit and nurture digital change in CEE. Establishing cooperation between public administrations, private companies, and NGOs from the CEE and all four regions included in this brief has the potential to lead to a significant improvement that drives digitalisation on all sides.

Digital Transformation – Challenges Ahead

As digitalisation is profoundly transforming societies, the reflection on how to conduct it properly should involve a wide range of sectors that might be impacted by it or have an impact on it.

Sustainable infrastructure

The concern related to the sustainable use of resources, energy in particular, is crucial to address.

As the digital is tightly connected to the energy sector, its effects on society can be double-edged. Digital technologies already allow energy systems around the world to be more connected, intelligent, efficient, and sustainable. Digitalised energy systems and their applications can, for instance, determine the energy needs of a building and deliver energy at the right time, and at an advantageous cost. On the other hand, the demand induced by the growing use of IoT systems and digital technologies may be harmful. According to the International Energy Agency (2017), the energy consumption of data networks and centres is around 185 and 194 terawatt hours (TWh) respectively. This amount represents approximately 2% of the total demand for electricity and is highly likely to increase in the coming years. New schemes improving the energy efficiency of servers, storage devices, networks, and data centre infrastructure are starting to appear in host countries which are and mostly developed countries. The International Energy Agency (2017) estimates that, depending on future trends in energy efficiency, electricity consumption of data networks could either increase by as much as 70% or fall by up to 15% by 2021, highlighting the high potential for change of a better energy management. Because energy is crucial, it has to be at the core of the considerations when it comes to the construction of new digital infrastructure. The use of clean energy sources should become a priority. This transition is not only an opportunity for businesses and citizens but also a necessity from an environmental, economic, and social perspective. Making sure that digitalisation brings beneficial outcomes along with anticipating and limiting the negative ones is an essential part of developing a digital society.

Because energy is crucial, it has to be at the core of the considerations when it comes to the construction of new digital infrastructure. The use of clean energy sources should become a priority. This transition is not only an opportunity for businesses and citizens but also a necessity from an environmental, economic, and social perspective.

International cooperation

Cybersecurity needs a common language in order to be effectively enforced. One of the main dilemmas being faced in cyberspace is the lack of universal definitions, norms, values, rules, regulations, and laws pertaining to the use of digital devices and the prosecution of cybercriminals. Many international forums have been established to discuss these crucial issues. For example, the Global Tech Panel, launched by the European External Action Service of the European Union, fosters new types of cooperation between diplomacy and technology to address new digital challenges and make innovation a true force for good. The EU-AU Digital Economy Task Force, on the other hand, established a working plan to build a partnership and draw mutual benefits from the digital transformation of economy and society in African countries (European Commission, 2017). But cooperation should also be built on the ground. The aim of cybersecurity capability building activities is to bring together skilled actors to exchange ideas, learn from mutual experiences, and support each other through best practices sharing and know-how transfer. Cybersecurity capacity building is a way through which the creation of a safer global cyberspace will be made possible. Dealing with the new digital reality requires understanding that the development objectives and risks related to ICT networks are two sides of the same coin and thus need to be addressed in a more comprehensive and coordinated manner.

The cooperation should also be fair, place all actors on an equal footing, and not be reduced to a pure business activity of technology transfer against money. A looming danger for developing countries is that they may, in exchange for a rapid technological development, become overly dependent on their ICT providers. Growing concerns are surrounding major continent- or world-wide projects such as the Digital Silk Road. As it aims to build communications networks across the developing world, it is also a strategic instrument – a soft power one – putting its initiators at the forefront of a new global rule- and norm-setting. In the context of the current global technology competition, the struggle to contain technological dependency risks will remain central (ITU, 2009).

Dealing with the new digital reality requires understanding that the development objectives and risks related to ICT networks are two sides of the same coin and thus need to be addressed in a more comprehensive and coordinated manner.

The Principles of Cybersecurity Capacity Building

Capacity-building activities rely on a fair cooperation that brings mutual benefits to all actors taking part in it. Working together to achieve the common goal of securing the digital transformation of a country or a region, the participants will also contribute to a more global goal of advancing towards sustainable development worldwide. As underlined many times, cyberspace does not differentiate between more or less developed regions of the world and cyberthreats transcend national borders. Therefore, digital security is a shared responsibility. The level of cooperation to address cyber issues should be as global as possible in order to adequately enhance cyber-resilience. The benefits of such activities are mutual and have the potential to affect a wide array of domains such as economy, governance, social welfare, ecology, migration, and many others.

The ten takeaway points proposed by the European Union Institute for Security Studies presented below, perfectly outline the critical role of capacity building in addressing current cyber challenges across the world. Governments, international organisations, and the private sector acknowledge the importance of secure cyberspace encompassing developing countries.

Discussing how to build awareness, providing a full picture of the current cybersecurity situation in one country or region, identifying the challenges as well as their impact on development, designing a range of best practices and emerging initiatives around the world to build a culture of cybersecurity, or exploring different options for a global response to rising cybercrime – all these are activities that underlie cybersecurity capacity building.

Cybersecurity Capacity Building – 10 Takeaways

1. Cybercapacity building is not a sprint. It is a marathon.
2. Cybercapacity building needs a common language.
3. Cybercapacity building is not only about security.
4. It impacts social and economic development worldwide.
5. Cybercapacity building challenges are not the same for everyone.
6. Cybercapacity building priorities are not the same for everyone.
7. One size does not fit all. But it fits most.
8. Cybercapacity building requires international coordination.
9. Cybercapacity building requires stakeholders' cooperation.
10. Cybercapacity building is not a priority. But it should be.
11. It is time to move from needs to delivery.

Source: Pawlak, 2014

Identifying and debating potential threats and challenges is a stride towards cooperation and mutual generation of solutions among states, civil society organisations, and private stakeholders. The next step is to jump from theoretical discussions on solutions to their implementation.

Capacity Building: From Theory to Action

To maintain global trust in technology – and a secure cyberspace in the face of new and emerging threats – public strategies, policies, and instruments must continue to evolve. To make this a reality, states have to craft their own personalised strategies, laws, procedures, and institutions to reach the desired digital development and cybersecurity level. Although a one-size-fits-all approach is not the answer, there are several key domains that governments should take into account in their frameworks in order to lay the groundwork for strong and effective state-level cybersecurity:

PEOPLE

It is necessary to build information society that respects values, rights, and freedoms and guarantees equal access to information, while encouraging the creation of skills that builds confidence and trust in the use of ICTs. At the end of the day, technical competence and awareness are thought to be the most pressing issues to achieve cybersecurity in developing nations.

Governments should engage with young people with advanced computer skills who might otherwise be tempted to use them for illegal purposes. The educational system is the key component for that endeavour, followed by cybersecurity training designed for the current workforce. It is a well-known cybersecurity principle that the end user is the weakest component of the system. It is essential to develop a knowledgeable, cyber-literate workforce to reduce cyber-risks.

POLICY

To tackle the behaviour of hostile actors, states need to adopt coherent cybersecurity strategies and policies. A successful cybersecurity strategy ensures that a country will perform in-depth risk management, involving risk assessment, and take appropriate steps to ensure the protection of cyberspace. Sectoral and topic-specific policies will create a necessary framework enabling public institutions, companies, and citizens to channel their efforts and investments towards the most important areas of improvements.

In many states, most cybersecurity expertise lies within industry sectors and academic fields, with experts likely to be eager to contribute to cybersecurity policy. Bringing together industry experts, academics, and public sector leaders to develop cybersecurity strategies for the state and help respond to threats is essential.

LAWS AND REGULATIONS

Official regulation for cyberspace is perhaps one of the most important aspects of capacity building, as it serves as vehicle to adequately enforce law in cyberspace and to raise attention to operational capacity. Legal frameworks are essential for nations and organisations to deal with cyber-related risk and crime effectively. This capacity includes trained law enforcement officers, cyber-forensics, prosecutors, and judges who have a good understanding of such crimes and their ramifications. Legal frameworks also enable and provide new opportunities for economic development.

Authorities should identify assets and services critical to the proper functioning of the society and economy, and map existing national laws, regulations, policies, programmes, and capacities to cybersecurity (NIST, 2014). It is also necessary for the public stakeholders to identify existing soft regulatory mechanisms, for example in private-public partnerships. Laws are also important to create a common understanding between relevant authorities in defining potential threats and vulnerabilities in cyberspace. They establish the boundaries between the legal and illegal

actions committed by state and non-state actors, bringing law and order to a chaotic realm. Thus, any strategy developed to counter threats in the cyberspace of a country should promote the development of a domestic legal framework that clearly defines prohibited cyberactivity and measures it can deploy to reduce online crime. Regulations also enable better cooperation between stakeholders within and beyond national borders, enabling the exchange of information and response to security risks in real time.

INSTITUTIONS AND PROCEDURES

The rapid development of digital society and the digitisation of some governmental responsibilities and organisational tasks put national institutions at the forefront of new cyberchallenges. Qualified IT professionals responsible for monitoring and flagging suspicious activities in the networks, providing early warnings as well as coordinating incident responses are of great help when it comes to countering cyberthreats or attacks.

The establishment of what is commonly known as a CERT (Computer Emergency Response Team) or a CIRT (Computer Incident Response Team) does not follow standard rules. Instead, it is important that it is adapted to the environment in which it will operate. A thorough study of the political, economic, social, and technological context is an indispensable prerequisite. As the process of creating such entities is time and resource consuming, establishing a regional cooperation framework and a culture of information exchange can prove beneficial to avoid the duplication of effort. The creation of standardised procedures, both for the internal workflow within the aforementioned institutions and for the cooperation schemes between them, must be an intrinsic part of that endeavour.

TECHNOLOGY

To be able to secure its own cyberspace and to make impactful policy decisions, a country needs to have a competitive national ICT sector at its disposal or benefit from a favourable and cooperative regional context. It has to be based on both educated workforce and available secure-by-design technologies.

Developing countries have to integrate into their systems many well-designed solutions for such tasks as identity management, access control, the use of secure hardware and software platforms, back-up infrastructures, or encryption protocols. Development and implementation of those technologies will vary depending on country-specific factors. Some might include building dedicated domestic R&D infrastructure or supporting local technological companies and start-ups. Others might integrate multiple state-of-the-art commercial technologies from international markets. Again, the one-size-fits-all principle is not the answer to cybersecurity technology transfer.

The Way towards a Bright Cyberfuture

Digitalisation has a unique potential. Numerous examples show how digital tools and solutions bring change in a wide range of sectors from banking to health, to government and education around the world. Therefore, digitalisation is a remarkable opportunity that developing countries have in front of them and leveraging it can help them boost their development level and reach UN SDGs for a better and more sustainable future. But many challenges are sure to come along.

Supporting a secure economic and digital development around the world is a global mission. In this regard, providing region- and country-specific recommendations as well as assistance in the process of developing and introducing appropriate policies, laws, regulations, and strategic solutions in the digital field is pivotal. This process should include the largest range of actors on an international level: private companies, public administration, third sector, and academia. As each of them has different experience and expertise, it is only by bringing them all together that we can achieve the goal of building a resilient global cybersecurity ecosystem. This must be done in a thoughtful and sustainable manner, taking into account growing issues such as the impact of new technologies on the environment and energy consumption. It is indeed crucial that digital transition does not take place at the expense of other sectors.

If we want to see sustainable digital initiatives flourish, cybersecurity and digital capacity building activities must be given priority. Only by sharing experiences, both success and failure stories, will we have a lasting impact on the design of future infrastructure and initiate a true global movement to ensure a higher level of cybersecurity and cyber-resilience. ■



About the author:

Faustine Felici is Project Manager at the Kosciuszko Institute and Executive Editor of the European Cybersecurity Journal. She holds a MA in European Interdisciplinary Studies from the College of Europe (Poland) as well as a MA in European Governance and a Bachelor in Political Studies from Sciences Po Grenoble (France). Faustine spent one academic semester studying European Societies at Saint-Petersburg State University and later on completed a Schuman traineeship at the European Parliament, where she worked mainly on migration and energy related topics in European Neighbourhood countries (Ukraine, Moldova, Georgia, Belarus). She wrote several policy briefs on digitalisation in developing countries and on the topic of strengthening EU-NATO cooperation in cyber defence.

References

- European Commission. (2019). *New Africa-Europe Digital Economy Partnership - report of the EU-AU Digital Economy Task Force*. Retrieved from: <https://ec.europa.eu/digital-single-market/en/news/new-africa-europe-digital-economy-partnership-report-eu-au-digital-economy-task-force>
- International Energy Agency. (2017). *Digitalization & Energy*. Retrieved from: www.iea.org/digital/
- International Finance Corporation. (2013). *Access to Finance, Sub-Saharan Africa*. Retrieved from: <http://documents.worldbank.org/curated/en/599611468202144127/pdf/948820WP0Box380e0Sub0Saharan0Africa.pdf>
- ITU. (2009). *Cybersecurity Guide for Developing Countries*. Retrieved from: <https://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf>
- ITU. (2018). Global Cybersecurity Index. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf
- Lewis, J. A. (2018). *Economic Impact of Cybercrime: At \$600 Billion and Counting - No Slowing Down*. Center for Strategic and International Studies and McAfee. Retrieved from: <https://www.csis.org/analysis/economic-impact-cybercrime>
- Ministry of National Defence of the Republic of Latvia. (2019). *Cyber Security Council discussed EU and Lithuanian cyber security initiatives*. Retrieved from: http://kam.lt/en/news_1098/current_issues/cyber_security_council_discussed_eu_and_lithuanian_cyber_security_initiatives.html
- Morgan, S. (2016). Cyber Crime Costs Projected To Reach \$2 Trillion by 2019. *Forbes*. Retrieved from: <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#391b503f3a91>
- Mozur, P. (2018). A genocide incited on Facebook. *The New York Times*. Retrieved from: <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>
- NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from: <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- OECD. (2012). *Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy*. Retrieved from: <https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>
- Pawlak, P. (2014). *Cyber Capacity Building in Ten Points*. European Union Institute for Security Studies. Retrieved from: <http://www.combattingcybercrime.org/files/virtual-library/capacity-building/cyber-capacity-building-in-ten-points.pdf>
- Pogrebinschi, T. (2017). *Digital Innovation in Latin America: How Brazil, Colombia, Mexico and Peru have been experimenting with E-participation*. OpenDemocracy. Retrieved from: <https://www.opendemocracy.net/en/democraciaabierta/digital-innovation-in-latin-america-how-brazil-colombia-mexico-/>
- Serianu. (2017). *Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line*. Retrieved from: <https://digital4africa.com/wp-content/uploads/2018/04/Africa-Cyber-Security-Report-2017.pdf>
- The World Bank. (2017). The Global Findex Database 2017. Retrieved from: <https://globalfindex.worldbank.org>
- United Nations Economic and Social Council. (2018). *Ministerial declaration of the 2018 high-level political forum on sustainable development convened under the auspices of the Economic and Social Council, on the theme "Transformation towards sustainable and resilient societies"*. Retrieved from: https://www.un.org/ga/search/view_doc.asp?symbol=E/HLS/2018/1&Lang=E
- Zurich. (2017). *Cyber risks scenario for business: Counting the cost of growing societal threats*. Retrieved from: <https://www.zurich.com/-/media/project/zurich/dotcom/industry-knowledge/cyber-risk/docs/global-risks-2017-cyber-risks-business-scenario.pdf>



OPINION

Six Goals for the Digital Services Act

DANIEL CASTRO

DIRECTOR, CENTER FOR DATA INNOVATION; VICE PRESIDENT, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

ELINE CHIVOT

SENIOR POLICY ANALYST, CENTER FOR DATA INNOVATION

The European Commission plans to propose a new Digital Services Act – the legislation that could revise or repeal the e-Commerce Directive and create a new set of regulations for Internet intermediaries. The goal of the legislation is to create clearer and more harmonised rules for digital services and address concerns about illegal and harmful online content, while protecting digital innovation and free expression.

This article highlights six key goals the Commission should prioritise in the forthcoming Digital Services Act. In particular, the Digital Services Act should clarify the types of platforms and content that fall under its scope; set proportionate responsibilities and obligations for platforms; increase legal certainty for platforms; protect freedom of expression; harmonise rules across the EU; and minimise the impact of its rules outside its borders.

1. The Digital Services Act Should Clarify the Rules for Online Platforms and the Definition of Illegal Content, Extend Liability Protections, and Harmonise the Scope of Digital Services Covered

The online ecosystem has evolved significantly since the EU adopted the e-Commerce Directive in 2000, so it is necessary to update at least three aspects of this law: clarify the definitions of illegal information and illegal activity; extend liability protections beyond passive services; and extend liability protections to all online intermediaries to create a level playing field.

First, the Commission should clarify the definitions of illegal information and illegal activity. The current framework requires Internet companies to take down “illegal information” and “illegal activity”, but does not describe precisely what those include. EU policy-makers should clarify these terms so there is no ambiguity and so that online services know to take proactive steps to remove illegal content.

Second, the Commission should extend liability protections beyond “passive” services. The e-Commerce Directive makes a distinction between “passive” and “active” online services, and only extends liability protections to service providers whose activity “is of a mere technical, automatic and passive nature” toward hosted content.¹ In practice, this means hosting providers are the primary beneficiaries of this liability protection. Policy-makers should abolish this distinction for two reasons. First, the difference between passive and active service providers is vague, making unclear to many service providers whether they receive this liability protection. Second, in order to create a level playing field between different types of online services, service providers should receive this liability protection for content they neither produced nor had actual knowledge of being illegal. The new framework should extend to more than just hosting providers, and account for the diversity of online services.

Third, the Commission should extend liability protections to all online intermediaries to create a level playing field. The current framework does not make clear which intermediaries receive liability protections. For example, the e-Commerce Directive only applies to intermediaries that qualify as “information society services” – and individual member states have been free to exclude search engines and other sites that provide indexes or directories of links. Moreover, the online services ecosystem has significantly evolved over the past two decades. The EU should update and harmonise the scope of covered online services to include a broad range of online intermediaries, including Internet service providers, cloud services, content delivery networks, domain name service providers, social media services, search engines, directories, collaborative economy platforms, online marketplaces, online advertising services, discussion boards, digital services built on electronic contracts, and distributed ledgers (i.e., blockchain).

¹ Directive 2000/31/EC, Official Journal, L 178, 17/07/2000, 1–16, recital 42, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>.

The new framework should extend to more than just hosting providers, and account for the diversity of online services.

2. The Digital Services Act Should Preserve the Main Principles of the e-Commerce Directive, Incentivise Voluntary Measures to Take Down Illegal Content, and Hold Companies Responsible for Timely Removal of Illegal Content

The Digital Services Act should preserve the main principles of the e-Commerce Directive, while also removing disincentives for platforms to take down illegal content and introducing penalties for consistent failure to respond to illegal content notifications.

First, the Digital Services Act should preserve the main principles of the e-Commerce directive. Not only does the current law limit the liability of online platforms for the content posted by their users, but it also does not obligate them to actively monitor their systems for illegal content. This is an important provision because many online platforms do not have the resources or capabilities to actively monitor all user content. Such a requirement could force online platforms – driven by fear of sanctions for unintentionally allowing offending content to slip through their moderation process – to err on the side of more restrictive content-moderation policies, or even eliminate user-generated content altogether. Given the popularity of these features today, this type of change would almost certainly reduce the value of online platforms for consumers. Therefore, any new framework should maintain the prohibition of active-monitoring obligations.

Second, to remove disincentives for platforms to take down illegal content proactively and voluntarily, the Digital Services Act should incentivise the adoption of standard technical measures, such as automated filtering systems, to mitigate illegal content. Policy-makers should ensure service providers that use voluntary measures to detect and remove illegal content online do not face additional liability risk. And online platforms exercising editorial control over user content should not be considered evidence they have actual knowledge of illegal content uploaded by users. To do

otherwise would discourage companies from actively self-policing their own services for fear of losing their liability protection. The likely result of preventing services from actively moderating online speech would either be service providers restricting user-generated content entirely or refraining from all content moderation and giving free rein to users, thereby allowing social media sites to grow larger and more toxic, and streaming sites to include more pirated and terrorist content.

Third, the new framework should introduce proportionate sanctions for systematic failure. While companies should not be liable for user content, they should always be responsible for removing or disabling access to illegal content once they learn about such material on their services. The new framework should create penalties for service providers that consistently fail to respond appropriately to illegal content notifications, whether from government, companies, or individuals. While companies should always block or remove content courts or other legitimate government authorities determine to be illegal, they deserve some latitude when making subjective decisions about whether content reported by users violates the law or their own policies.

3. The Digital Services Act Should Improve Online Platform Transparency

The Digital Services Act should require online services to provide more transparency about their policies and processes for responding to illegal content and the appeal processes available to users. Companies should release regular reports on their actions, such as the number of takedown requests received, the results of those requests, the number of appeals, and the time it took to respond to those requests. More transparency can help service providers dealing with specific problems, such as counterfeit products for online retailers, and identify best practices.

More transparency can help service providers dealing with specific problems, but requirements should be proportionate to the level of risk.

However, transparency requirements should be proportionate to the level of risk. The Commission should consider the feasibility of transparency obligations noting that not all companies have the same resources and capabilities. The Digital Services Act should also impose no additional transparency obligations on platforms that use automated processing and filtering technologies to moderate their content because this could force them to expose proprietary details about their algorithms or discourage the use of artificial intelligence (AI). Likewise, the Digital Services Act should not mandate that companies use explainable algorithms, as there are typically trade-offs between accuracy and explainability in AI, and such a requirement could result in platforms using less effective automated content moderation tools.

4. The Digital Services Act Should Cover Illegal, Not Harmful, Content

The Digital Services Act should focus on illegal content and behavior, and not attempt to regulate certain forms of disinformation, harassment, and hate speech that may be undesirable but are not typically illegal in Western democracies. Doing so would increase fragmentation of the Internet in Europe, lead to greater legal complexity for companies operating across member states, and impact freedom of expression. Moreover, it would be inappropriate for the government to require companies to remove online content that would be lawful offline.

5. The Digital Services Act Should Balance Roles and Responsibilities

One critical aspect of any updates to the EU's liability framework lies in the division of the roles and responsibilities between the public and private sectors. The primary responsibility of online service providers should be to remove or disable access to content determined to be unlawful by the authorities, and to moderate all other content according to their own terms of service. Online service providers should not be tasked by the government with deciding whether user-generated content is legal. That should remain the responsibility of the government. This does not mean companies

should ignore problematic content on their platforms. On the contrary, online services can and should make interim decisions about whether user content meets their internal content guidelines – and respond promptly and appropriately, especially when trusted partners report prohibited activity on their platforms. But regulators should not hold companies responsible for correctly predicting whether government authorities will agree or disagree with their determinations. If companies were held liable for incorrectly predicting whether government authorities would find certain content to be unlawful, they would likely err on the side of caution and take down lawful content. Government should also not take on the role of setting guidelines for online content that would otherwise be legal if published offline, as this would unnecessarily suppress free speech online. Nor should governments dictate the technology the private sector should use to moderate content, and instead allow companies to use their technical talent and resources to evaluate the best options.

The Digital Services Act should allow both companies and users to appeal a government's decision to order content to be removed, and they should be able to use this mechanism without restriction. The new framework should ensure platforms are not held legally responsible for the content of their users – and individuals are held legally responsible for the content they produce just as they would be in the offline world.

If companies were held liable for incorrectly predicting whether government authorities would find certain content to be unlawful, they would likely err on the side of caution and take down lawful content.

6. The Digital Services Act Should Harmonise Rules at the EU Level to Create Regulatory Consistency

One of the major barriers to a digital single market is the patchwork of national rules for online services. For example, German and French laws differ on online hate speech. Further fragmentation would only introduce more complexity and uncertainty for companies, as policies may conflict with other countries' laws, and interpretations may diverge between national authorities. In addition, fragmentation makes it harder for EU companies to scale, which is a critical success factor for companies operating in the digital economy. EU policy-makers should take the opportunity to use the Digital Service Act to harmonise rules at the EU level to create a consistent regulatory process and avoid increasing policy fragmentation across member states. As illegal online content is a cross-border issue, it should be addressed at the EU level, but EU policy-makers should not allow the goal of a harmonised framework to enable individual member states to enforce their content regulations outside their borders – neither within the EU nor outside the EU. Within the EU itself, some member states criminalise certain types of speech, while others do not. EU policy-makers should keep in mind enforcing one country's restrictions on online content outside of that particular country will infringe on freedom of speech and limit access to information in other nations. Where there are differences across the EU, member states' takedown requests should only apply domestically. Otherwise, this would allow one EU nation to decide the laws of another. A new framework should also be respectful of the global nature of the Internet by avoiding cross-border conflicts between both jurisdictions outside the EU that have tight speech standards and those that operate according to different standards. It should not require one platform to remove content globally based on either a national or EU standard. Going down this path would open other nations to extending their own policies about Internet content regulation to Europe, thereby limiting free speech and access to information to individuals in the EU. ■

The Center for Data Innovation (@datainnovation, www.datainnovation.org) is a think tank studying the intersection of data, technology, and public policy. With staff in Washington, DC, and Brussels, the Center formulates and promotes pragmatic public policies designed to maximise the benefits of data-driven innovation in the public and private sectors. It educates policy-makers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is a non-profit, non-partisan research institute affiliated with the Information Technology and Innovation Foundation (ITIF), the leading think tank for science and technology policy (@ITIFdc, www.itif.org).

About the authors:



Daniel Castro (@CastroTech) is the director of the Center for Data Innovation and vice president of the Information Technology and Innovation Foundation. Mr. Castro writes and speaks on a variety of issues related to information technology and internet policy, including data, privacy, security, intellectual property, internet governance, e-government, and accessibility for people with disabilities. In 2013, Mr. Castro was named to FedScoop's list of "Top 25 most influential people under 40 in government and tech". In 2015, US Secretary of Commerce Penny Pritzker appointed Mr. Castro to the Commerce Data Advisory Council. Mr. Castro previously worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a BSc in Foreign Service from Georgetown University and an MSc in Information Security Technology and Management from Carnegie Mellon University.



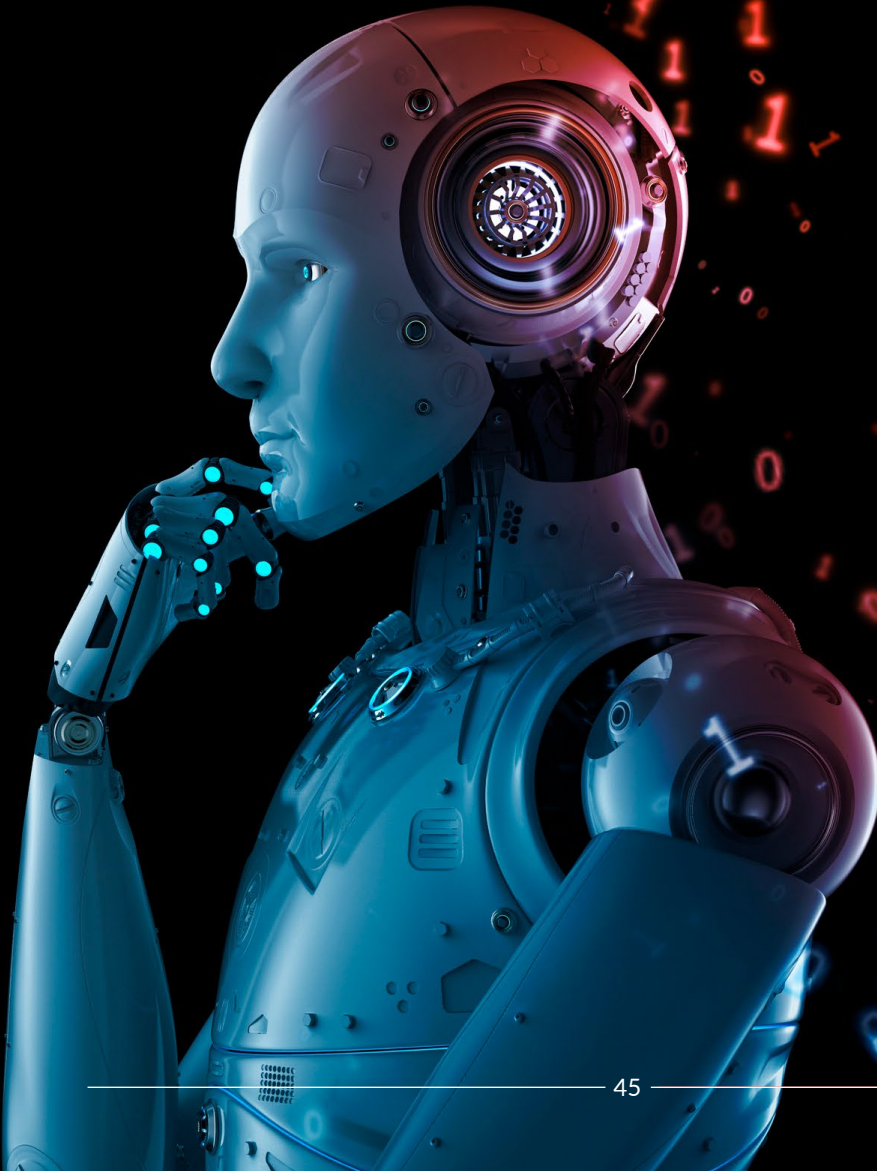
Eline Chivot (@ElineCMC) is a senior policy analyst at the Center for Data Innovation. Based in Brussels, Eline focuses on European technology policy issues and on how policy-makers can promote digital innovation in the EU. Prior to joining the Center for Data Innovation, Eline worked as a policy analyst at the Hague Center for Strategic Studies (HCSS), where her work included research projects on defense, security, and economic policy issues. More recently, Eline worked at one of Brussels' largest trade associations, DigitalEurope, and managed its relations with representatives of the digital tech industry in Europe and beyond. Eline earned master's degrees in political science and economics from Sciences Po Lille, and in strategic management and business administration from the University of Lille.

What Does Resilience-Building to Emerging and Disruptive Technologies Actually Look Like?

A Study Addressing the Public Policy Challenges and Socio-Political Implications of the Development of Artificial Intelligence for European Security and Defence

KULANI ABENDROTH-DIAS

PHD CANDIDATE, GRADUATE INSTITUTE FOR INTERNATIONAL AND DEVELOPMENT STUDIES (IHEID); GRADUATE PROFESSIONAL, UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR)



Introduction

Artificial intelligence, physical security, and political security are inextricably linked in the Digital Age (Bostrom, & Yudkowsky, 2014). Largely due to advances in computing power, machine learning algorithms, deep neural networks, access to datasets, and gains in standard software frameworks that allow for exponential iteration and replication of experiments, artificial intelligence (AI) and machine learning (ML) have progressed rapidly over the past few years (Brundage et al., 2018). At the core of this growth is expanded commercial investment in developing the capacities that feed AI and ML-driven technologies (Chui, 2017; Jordan and Mitchell, 2015).

AI now drives a variety of widely available technologies, such as automatic speech recognition, facial analysis, contact tracing, search engines, spam filters, and self-driving cars (Das, Dey, Pal, & Roy, 2015). In many countries, the COVID-19 pandemic has loosened the regulations on the use of the data that feed AI and ML driven technologies (Dam, 2020, Raskar et al., 2020). For example, in South Korea, immigration databases were used by health officials to increase population surveillance techniques to contract trace those who may have been exposed to COVID-19 (Migration Data Portal, 2020). This increased access to data can fuel the development of the technologies used as digital assistants for nurses and doctors and drones for expedited disaster and pandemic monitoring and relief (Oliver et al., 2020; Raskar et al., 2020; Zwitter & Gstrein, 2020). AI-powered driverless cars and robotic dogs to encourage social distancing (among other social interactions) can be helpful to combat the effects of a pandemic that is fought with behavioural containment and even social isolation (Bavel et al., 2020). It is, however, easy to see how the developments that drive AI and ML-driven technologies can easily be used for malicious purposes, e.g. weaponising consumer drones, hacking public services, create privacy-deficient surveillance states, racial profiling, repression, and targeted disinformation campaigns to name a few (Brundage, 2018; Johnson, 2017; Tucker et al., 2018). Just as doctors, patients, and

the pharmaceutical industry need to understand how a human body works and the symptoms and diseases that can impact our well-being to develop medicines that can protect against ill health, both the regulators and users of AI-driven technologies (i.e. policy-makers, the military, technological developers, and the public) need a better understanding of what constitutes AI and ML-driven technologies and their current and potential uses and misuses to build resilience to their malignant use (Bahnsen, Torroledo, Camacho, & Villegas, 2018).

The need to build resilience to AI and ML-driven technologies is often discussed in policy circles. However, little attention has been paid to operationalising resilience-building to the rapid development of AI- and ML-driven technologies across the continent. At its core, resilience requires inclusive and forward-thinking regulation and research that can build flexibility to respond to evolving security challenges. Developing resilience to AI- and ML-driven attacks is a central tenet to building citizen trust. Cyberattacks that mine citizen data, for example, lead the public to question the robustness of their political and public structures, and work to undermine trust in governments and political participation (Brkan, 2019).

At its core, resilience requires inclusive and forward-thinking regulation and research that can build flexibility to respond to evolving security challenges. Developing resilience to AI- and ML-driven attacks is a central tenet to building citizen trust.

There are several key challenges to developing and regulating AI-driven technologies, including the application of technology developed outside Europe that can threaten its sovereignty, and the legal basis for regulating technology that is re-shaping global political and economic structures (Timmers, 2020). This paper offers insights to address these challenges.

Resilience-building should inform how we design and distribute AI systems, and *who* should design and distribute them. Drawing from a content analysis of 22 interviews, this project presents

an analysis of how resilience building with regard to AI- and ML-driven technologies is currently understood by policy-makers, industrial agents, non-profit actors, and academics who work on understanding, developing, and/or regulating AI- and ML-driven technologies for European security and defence. The goal of this research is to contribute to the technology-security research nexus by presenting the cross-cutting effects of the development of AI and ML-driven technologies for European security and defence along national, supranational, economic, and political levels.

Methodology

Participants

Fifty-three individuals were contacted between February and May 2020 via a standard email message that included an outline of the study with the author's background and credentials. The final sample comprised 22 participants (55% female), i.e. of the 53 participants contacted, 22 responded to and participated in the study. Participants' ages ranged from 28 to 70, and were based in Austria, Belgium, Germany, the Netherlands, Poland, Sweden, Switzerland, and the United Kingdom. Participants came from the academic, policy-making, non-profit, and industrial sectors respectively. The final sample of 22 participants were recruited from the United Nations Institute for Disarmament Research (UNIDIR), the International Panel on the Regulation of Autonomous Weapons (iPRAW), the German Council on Foreign Relations, the German Federal Foreign Office, the German Army (Bundeswehr), the Belgian Royal Military Academy, the University of Namur, the University of Siegen, the Free University of Brussels (VUB), Central European University, ETH Zurich, the Hague Center for Security Studies, Djapo, McKinsey and Company, Compagnie Européenne d'Intelligence Stratégique Sprl (CEIS), the Center for Data Innovation, The Democratic Society, Statewatch, Transparency International, the Stockholm International Peace Research Institute, the European Commission, and the European Parliament. One individual from the European Commission consented to digital

interviews on the basis that their interview would not be audio-recorded. Note-taking was allowed in the instances where participants did not consent to being audio-recorded.

Procedure

Participants were contacted online via cold emails, word-of-mouth, and snowball sampling. Given the onset of the lockdown measures in response to the COVID-19 pandemic, they were interviewed by the author via Skype. The author conducted all interviews in a private room within her home. Participants were either located in a quiet room (alone) within their respective office, or at home. All interviews were conducted in English.

Participants who agreed to take part in the study in response to the emails by the author were sent informed consent forms where they could agree to participate in an exploratory study looking at "The Economics and Sociopolitical Implications of the Development of Artificial Intelligence for European Security and Defence". All but three participants agreed to be audio-recorded during the interview.

The Skype interview began with a brief introduction discussion that was not audio-recorded, where the interviewer explained her background, thanked the participant for being a part of the study, went over the study protocols, and discussed any informal/thematic topics of interest. This was followed by the formal interview, which began with the interviewer requesting consent to begin audio-recording the conversation.

Materials and Design

The semi-structured interview consisted of 13 pre-determined questions in total, asked in chronological order to reduce experimenter bias. The semi-structured interview allowed for follow-up questions between these 13 questions based on participant responses. The interviews on average lasted one hour.

Given the fragmented development of AI and ML-driven technologies for European security and defence across regions and countries, the breadth of

AI as a tool and discipline, as well as the diverse backgrounds of those being contacted and interviewed (from academia, industry, policy, and the non-profit sectors), the questions were wide-ranging and framed in general terms. This was especially important given the technical nature and perception of AI; although everyone who was contacted to participate in the study had published on or worked with AI for European security and defence in some specific capacity, a few of the participants who declined to participate in the study cited the technicality of the subject and their lack of expertise in response to the author's emails requesting their participation in the project. To this end, the wide-ranging and more general framing of the questions was emphasised when reaching out to potential participants. Participants were encouraged to respond to each question based on their own technical expertise and experience. Individuals could skip any question at any time.

The questions comprised mapping the development of AI- and ML-driven technologies for European security and defense in terms of geography and strategic policy/industrial priorities, challenges to policy-makers, cooperation between different actors, and building resilience/mitigating the risks of AI- and ML-driven technologies. Attempts were made to include a discussion of the use of AI in Unmanned Aerial Vehicles (UAVs) and Lethal Autonomous Weapons (LAWS), two key AI-related policy issues emphasised in the literature review.

Participants were informed that the terms "security" and "defence" were meant to be interpreted broadly and include both military and civilian domains. Security therefore included both AI-driven attacks and resilience-building on the battleground, in cyberspace, and civilian life. Therefore, disinformation attacks targeting both civilians and the military as well as cyberattacks and surveillance threats on military personnel, public institutions, and the citizenry were open for discussion.

Eight participants requested the list of questions prior to the Skype call. One participant included in the sample preferred to respond to the questions in writing, and no Skype call was conducted.

Participants did not receive any incentives for participating in the study, and were orally debriefed at the end of the interview.

Results

Analytic Framework

A content analysis of all 22 interviews was carried out by the author to identify the frequency of themes and overall recommendations (Braun & Clark, 2006). The thematic analysis was based on the prevalence of topics mentioned in the literature (deductive approach) and any new challenges identified and recommendations made (inductive approach). This thematic analysis resulted in ten insights for policy-makers. Only those recommendations that were mentioned by at least 50% of participants are presented. Overall content analysis results are presented below.

Overall Findings

All participants discussed the importance of regulating the use of data for privacy protection within the EU. Two participants discussed the role of the General Data Protection Regulation (GDPR) in enforcing this privacy (see Chase, 2019). Interestingly, only three participants identified Berlin as a hub for AI development in Europe. Nineteen participants (86% of the sample) mentioned that it was difficult to identify a "hub" for AI development in Europe per se, stating that AI development is quite diffused across member states. Germany, France, the UK, Sweden, and the Netherlands were mentioned as areas of AI development, with references to London (91%), Berlin (68% of the sample), Amsterdam (50%), and Paris (27%) made. In contrast, all participants mentioned the United States and China as hubs for AI development, with two participants mentioning Israel, one participant discussing India, and two participants noting the role of Russia and South Korea respectively. All participants mentioned the dual-use nature of AI-driven technologies, with their use in offensive and defensive campaigns, and in civilian and military domains. All participants mentioned the increased risk in implementing AI-driven solutions developed outside the EU within member states.

All participants were readily able to recall industrial actors working on AI development within Europe, including Airbus and Palantir. Only four participants mentioned the role of the European Commission and the European Defence Fund by name. All participants emphasised the transnational or international nature of the European defence industry, making references to collaborative projects in the development of AI-driven solutions. Fifty percent of the sample (11 participants) were able to recall the name of an organisation working on responsible AI. Independent references to Statewatch, Transparency International, Algorithm Watch, and the United Nations were made. In response to the role of AI in increased surveillance, 13 participants called on the United Nations or NGOs such as those mentioned above to work with policy-makers to regulate their use. The importance of data protection to combat surveillance was mentioned by all 22 participants.

Nineteen participants emphasised the role of AI in polarising societies via disinformation. Only one was able to recall an organisation working to effectively counter this disinformation. Six participants mentioned the danger of social media platforms such as Facebook in data mining efforts. Ten participants noted the incidence of data mining by the private sector (without explicit references to companies). Four participants noted that sharing one's data was the default of the future, and that an innovative solution would be a centralised space for every citizen to share what types of data they wish to share with, and restrict from, the private sector and public sector respectively. Two participants noted, "There should be an app for that! [To easily grant or restrict access to private data]."

All participants agreed that AI- and ML-driven technologies will contribute to the increase of military budgets and the escalation of arms races. Interestingly, they also noted that this was inevitable. All participants agreed that future wars will not be concluded via the destruction of automated weapons on the field (however developed), but by the death of people, whether civilian or military. They underlined the assistive capacities of AI on the battleground, especially with regard to reconnaissance and carrying out surgical strikes.

Two participants acknowledged the importance of collaboration between the private sector and the military in harnessing AI innovation for defence. Seven participants discussed the role of the North Atlantic Treaty Organization (NATO) in already facilitating discussions between the private sector and the military to build AI-driven resilience in Europe.

All participants noted the importance of collaboration across EU member states in developing and regulating AI-driven solutions. All participants were aware of the risk of coding human biases into ML-driven algorithms, and 50% were able to recall examples of such occurrences. Five participants recalled the now famous case of facial recognition technology implemented at the Berlin-Südkreuz train station resulting in a 20% error rate, mostly misidentifying people of colour at the station. A poignant case of biased data training sets resulting in erroneous outcomes, this was the most cited example used by participants acknowledging the algorithmic bias. Two participants identified women as those at risk of this type of bias, whereas 50% of the sample (11 interviewees) noted that people of colour were most at risk of this type of error. Seventeen participants (77% of the sample) mentioned that white males were explicitly not at risk from algorithmic bias.

All participants noted the importance of collaboration across EU member states in developing and regulating AI-driven solutions.

Insights for Policy-Makers

Recommendations mentioned by at least 50% of participants are presented in this section (i.e. at least eleven participants independently mentioned the policy insights described below during the course of their interviews).

Adapting the Operationalisation and Regulation of AI- and ML-Driven Technologies to Existing International Human Law (IHL) Frameworks

The principles of distinction and proportionality within existing international humanitarian law were signalled by participants as sufficient and

applicable across the implementation of AI-driven solutions in warfare. More than 50% of participants argued that the existing IHL frameworks of proportionality and distinction can be used to govern the use and misuse of AI, as they emphasised the assistive role of AI for military targeting and action versus independent/autonomous action. The framework of distinction was mentioned with regard to providing the best protection possible to civilians in conflict zones, via the analysis of big data to target surgical strikes and avoid civilian casualties in conflict zones.

Moving Beyond “Meaningful Human Control”

In-depth discussions of what constitutes meaningful human control engaging multi-stakeholder perspectives highlighted the need to develop a human-centred regulatory policy. According to one participant, “We need to build on a meaningful discussion of human control instead of polarising the debate between the acceptance or banning of automated systems. The reality is we need to identify where the benefits of automated systems lie, and how harm can be reduced.” The principle of retaining meaningful human control within automated systems has been made clear by the Group of Governmental Experts (GGE) on LAWS, the International Committee of the Red Cross (ICRC), UNIDIR, and a number of actors in the field. More than 50% of participants in this study recommend that the concept meaningful human control is unpacked *along with military, private, and public sector engagement*, with the realistic costs and benefits of these AI solutions in mind.

Critical Thinking Skills Versus Digital Literacy

More than 50% of participants responded to the question of “What does resilience actually look like?” with the need to build more critical thinking skills across the population. These participants emphasised the need to build critical thinking skills to understand what constitutes disinformation versus building digital literacy more specifically. They mentioned that in many European countries critical thinking had been built into school curriculums, which has helped them parse through online and offline disinformation during their lifetimes. Instead

of solely investing in AI skill-building which can result in participant self-selection and gender bias, these participants call for an increased divestment into building critical thinking skills among children and populations vulnerable to AI-driven misinformation.

Increasing AI-Driven Solutions for Military Use

All participants acknowledged that AI is here to stay, and that greater investment and innovation in AI within Europe is required to retain strategic defensive autonomy. More than 50% of them called for clear distinctions to be drawn between military and civilian uses of AI-driven technologies in terms of data protections, surveillance, etc. While acknowledging that these types of distinctions would be difficult to navigate, they called for greater investment in the military uses of AI, from border protection to biometric data processing. This military use of AI did not cover combating disinformation campaigns, which these participants highlighted more as a political issue. Interestingly, the German Army officer interviewed during this project noted the importance of training soldiers in algorithmic bias, and the role of disinformation campaigns in influencing troop morale.

Increasing the Technical Awareness of the Development and Capacities of AI- and ML-Driven Within Policy Solutions

All 22 participants noted that most policy-makers currently building AI-related legislation lack the technical knowledge to do so. The decisions of policy-makers across Europe should be more informed by expert groups, ideally working in tandem with AI innovators in the private and military sectors. Some participants noted the presence of bodies such as iPRAW which are working within this space. However, all noted that more technical capacity development is required in policy circles. In addition, more collaboration between existing AI-focused bodies and policy-makers was iterated.

What Does Retaining Human Responsibility for AI-Driven Attacks Look Like?

Increased human accountability in the perpetration of AI-driven attacks may mediate the incidence of these types of offensive attacks. Several

participants noted that the increased anonymity afforded by AI-driven attacks (from cyberattacks to disinformation) can increase the incidence and size of these attacks. Within the military domain, participants called for the operationalisation of IHL among other laws to develop concrete frameworks to increase human responsibility for potential attacks via UAVs and other automated systems.

Legally Binding Instruments to Regulate the Use of AI in International and EU Versus National Contexts

Ninety-one percent of the sample mentioned the collaborative development of AI-driven technologies across European and international lines. This leads to the question of what legally binding instruments to regulate the use of AI would look like in the EU versus in EU-China relations versus EU-US relations. Participants called for bilateral “rules of the road” to be established along these legally binding frameworks that would govern the development of AI technologies between EU and non-EU states in the future. These frameworks should take into account political, social, and economic concerns while respecting IHL, data protection, and human rights at all times in negotiating the regulation of AI development and application across national and international lines.

Developing AI Competencies and Regulations Within the European Startup Ecosystem

More than half of the participants of this study mentioned the role of startups in Europe in developing AI-driven solutions for European security and defence. While technological giants such as Airbus and SWP were noted, participants called for regulations to develop and limit the competencies of AI startup industries in order to reduce an “arms race to the bottom”. Seventeen participants noted the importance of startup industries in driving European innovation forward, although twelve of these participants noted that these startups have a long way to go to rival the tech and defence giants such as Google and Airbus.

Understanding the Risks of Not Using AI

The risks of an AI-enabled arms race are not only imminent, but ongoing. Participants emphasised the need for Europe to develop more localised solutions for defensive structures to AI-driven attacks. One participant noted, “The best defence is a good offence, right?” Refusing to invest in the development of AI would result in undermining European economic competitiveness and strategic political autonomy. European nations would be forced to apply AI solutions developed by non-European actors deep within their defence and security architecture. This could expose European states to further risks, given potential backdoors and network discrepancies in technology developed by non-European actors who may not see themselves bound to the rules of data integrity, privacy, human rights, or even economic market forces that are inherent within a majority of European processes. Europe needs to innovate and develop AI-driven solutions, to be able to set the rules for how the game is to be played in the future.

Developing the Responsible Democratisation of Data

The open-source culture of most AI research and development within the scientific community has brought the concept of data democratisation to the forefront. Data democratisation refers to allowing free access to data that allows even non-technical personnel to understand it. The data can be used to expedite and inform decision making, understand economic, social, and political trends, and find opportunities for innovation in the workplace etc. Data democratisation calls for the removal of bottlenecks to accessing data, and is disproportionately advocated for by the non-profit actors among the people sampled. It is however at odds with European culturally grounded technical data privacy priorities. Data democratisation has pertinent ramifications on identifying the needs of vulnerable populations across regions. Done responsibly, it would protect privacy while making relevant data accessible to all.

Concluding remarks

This study illustrates the extent to which AI-driven solutions have become inextricable components of the European defence industry over the past few decades. None of the participants interviewed advocated for a ban on AI. They all acknowledged in one way or another that AI is here to stay, and made recommendations for its regulation and innovation to protect and build resilience against future threats (see also: Geist, 2016). None explicitly subscribed to the notion that increased investment in AI-related technologies to build resilience will only result in the development of more sophisticated future threats. All interviewees identified various vulnerabilities that could be exploited by malignant groups, especially in the case of AI solutions developed outside Europe, emphasising the need for more EU investment and innovation. All participants noted the need for more robust regulation and were aware of the shortfalls of AI, e.g. algorithmic bias, in advocating for more assistive versus fully automated AI-driven solutions.

Three participants mentioned the security challenges of 5G technologies developed by non-NATO actors on European security and defence. Future research should include a discussion of the policy challenges of, and recommendations for resilience-building against, 5G technology networks built by non-NATO states and implemented across Europe more generally. These challenges and recommendations should be made as a function of national and regional policy and industrial priorities and bottlenecks.

As illustrated by this project, the hubs for developing AI- and ML-driven technologies tend to be located across Western Europe, with participants mentioning London, Berlin, Amsterdam, and Paris as potential centres for innovation. However, AI-driven threats such as disinformation attacks are often localised to fit contexts when disseminated in southern and eastern European countries, such as Italy, the Baltics, and depending on one's conceptualisation of Europe, Ukraine (La Cour, 2019; Thomas, 2020). The location of the NATO Cooperative Cyber Defence Centre of Excellence

in Tallinn, Estonia, is a step in the right direction of including more European perspectives in building resilience to AI-driven threats. Future research should investigate the involvement of experts, and training of personnel, from Europe's southern and eastern borders in developing more localised solutions to AI-driven security threats.

Future research should investigate the involvement of experts, and training of personnel, from Europe's southern and eastern borders in developing more localised solutions to AI-driven security threats.

This project is a step in the direction of understanding the interwoven political, social, economic, legal, and technical implications of leveraging the development of AI- and ML-driven technologies to build resilience for European security and defence. Building resilience to AI is a phrase often used within policy circles. Yet, much needs to be done to understand what actually constitutes building resilience. This project highlighted ten policy recommendations in building resilience, namely 1) developing the existing frameworks of distinction and proportionality within International Humanitarian Law (IHL), 2) operationalising "meaningful human control" on the basis of the costs and benefits of the assistive use of automated systems, 3) the need to build critical thinking skills to build resilience to disinformation attacks, 4) the need for greater investment in AI within the military and delineation of AI for military and civilian use, 5) the need for technical capacity development among AI policy-makers, 6) increasing human accountability for AI-driven attacks to mitigate the incidence of these offensives, 7) the need to negotiate legally binding bilateral instruments along national and international spaces to regulate the uses of AI keeping European social, legal, political, economic, and technical concerns in mind, 8) regulating the development of AI within the startup ecosystem, 9) understanding the risks of not using or developing AI within Europe and finally, 10) developing the responsible democratisation of data. These AI expert insights should be at the heart of building trust in a human-centred European Strategy on AI. ■

About the author:



Kulani Abendroth-Dias is a PhD candidate at the Graduate Institute for International and Development Studies (IHEID) and a Graduate Professional at the United Nations Institute for Disarmament Research (UNIDIR) in Geneva, Switzerland. She works at the nexus of economics, social psychology, and artificial intelligence. A TEDx speaker on "[Why Good People Do Bad Things - And What We Can Do About It](#)", Kulani formerly worked as a behavioural scientist for the United Nations Development Programme (UNDP) and the United Nations Peacebuilding Secretariat in Sri Lanka. She has an Advanced MSc. in European Integration specialising in Economics and Security, External Relations, and Counter-terrorism from the Institute of European Studies (VUB) in Brussels, Belgium, and an M.A. in Psychology from Princeton University.

References

- Bahnsen, A. C., Torroledo, I., Camacho, L. D., & Villegas, S. (2018, May). DeepPhish: Simulating Malicious AI. In *2018 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-8).
- Bavel, J.J.V., Baicker, K., Boggio, P.S. *et al.* Using social and behavioural science to support COVID-19 pandemic response. *Nature Human Behavior* 4, 460–471 (2020). <https://doi.org/10.1038/s41562-020-0884-z>
- Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. *The Cambridge handbook of artificial intelligence*, 1, 316-334.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101.
- Brkan, M. (2019). Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting. *Delphi*, 2, 66.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeithoff, T., Filar, B., Anderson, H. Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Heigearthaigh, S., Beard, S., Belfield, H. Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.
- Chui, M. (2017). Artificial intelligence the next digital frontier?. *McKinsey and Company Global Institute*, 47, 3-6.
- Dam, P. (2020). *Hungary's Authoritarian Takeover Puts European Union at Risk: COVID-19 Is Not an Opportunity to Shelve Democracy*. Human Rights Watch Dispatches.
- Das, S., Dey, A., Pal, A., & Roy, N. (2015). Applications of artificial intelligence in machine learning: review and prospect. *International Journal of Computer Applications*, 115(9).
- De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). *Artificial Intelligence and the Future of Defense: Strategic Implications for Small- and Medium-Sized Force Providers*. The Hague Centre for Strategic Studies.
- Geist, E. M. (2016). It's already too late to stop the AI arms race—We must manage it instead. *Bulletin of the Atomic Scientists*, 72(5), 318-321.
- Johnson, B. D. (2017). The Weaponization of AI: A Glimpse into Future Threats. *Computer*, (10), 73-73.
- Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Defense & Security Analysis*, 35(2), 147-169.
- Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255-260.
- La Cour, C. (2019). Governments Countering Disinformation: The Case of Italy. Retrieved August 24, 2020, from <https://disinfoportal.org/governments-countering-disinformation-the-case-of-italy/>
- Migration Data Portal. (2020). *Migration data relevant for the COVID-19 pandemic*.

Oliver, N., Letouzé, E., Sterly, H., Delataille, S., De Nadai, M., Lepri, B., Lambiotte, R., Benjamins, R., Cattuto, C., Colizza, V., de Cordes, N., Fraiberger, S. P., Koebe, T., Lehmann, S., Murillo, J., Pentland, A., Pham, P. N., Pivetta, F., Salah, A. A., Saramaki, J., Scarpino, S. V., Tizzoni, M., Verhulst, S., & Vinck, P. (2020). Mobile phone data and COVID-19: Missing an opportunity?. *arXiv preprint arXiv:2003.12347*.

Raskar, R., Schunemann, I., Barbar, R., Vilcans, K., Gray, J., Vepakomma, P., Kapa, S., Nuzzo, A., Gupta, R., Berke, A., Greenwood, D., Keegan, C., Kanaparti, S., Beaudry, R., Stansbury, D., Arcila, B. B., Kanaparti, R., Pamplona, V., Benedetti, F. M., Clough, A., Das, R., Jain, K., Louisy, K., Nadeau, G., Pamplona, V., Penrod, S., Rajae, Y., Singh, A., Storm, G., & Werner, J. (2020). Apps gone rogue: Maintaining personal privacy in an epidemic. *arXiv preprint arXiv:2003.08567*.

Thomas, M. (2020). Defeating Disinformation Threats. Retrieved August 24, 2020, from <https://www.fpri.org/article/2020/02/defeating-disinformation-threats/>

Timmers, P. (2020). There will be no global 6G unless we resolve sovereignty concerns in 5G governance. *Nature Electronics*, 3(1), 10-12.

Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. *Political polarization, and political disinformation: a review of the scientific literature (March 19, 2018)*.

Zwitter, A., & Gstrein, O. J. (2020). Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action* 5 (2020). <https://doi.org/10.1186/s41018-020-00072-6>



ANALYSIS

Training or Technology? The Key to CISO Success Is a Balanced Approach that Focuses First on what Matters Most

ADAM PALMER

CHIEF CYBERSECURITY STRATEGIST, TENABLE

OLIVER HOARE

CEO, DYSART SOLUTIONS

Few organisations managing cybersecurity have sufficient budgets or trained staff to adequately address all risks. In most countries there is a burgeoning cybersecurity skills gap, whilst globally cyberthreats are increasing and diversifying – Operational Technology (OT) and cloud vulnerabilities being the latest cyber-conundrum. So where should the CISO (Chief Information Security Officers) and security teams start? Having a strategy that balances technology, people, and processes is critical. However, the key question for CISOs is: How do you make the best technology choices and where exactly should you focus your limited funds? Answering this question is not simple. The answer is not about how much to spend, or making tough choices about whether to invest in training *or* technology, it is about being *better focused*.

Before CISOs make major strategy decisions, it is fundamental to start by understanding critical vulnerabilities. Technical vulnerabilities – often gauged by CVSS (or common vulnerability scoring system). The average number of vulnerabilities discovered annually since 2017 has roughly doubled compared to any prior year (Tenable Research 2019). However, to really understand how these vulnerabilities may affect your organisation requires a clear understanding of your specific attack surface. In addition to traditional IT assets (servers, internet gateways, apps, websites, desktops, laptops, internet protocol (IP) phones, Bring Your Own Device (BYOD), etc.), CISOs now need to consider vulnerabilities in cloud and OT (Operations Technology) environments as part of their overall attack surface. The problem is that

while adversaries are scanning all of these environments to find the easiest way inside the target organisation, security teams are overworked, understaffed, and stuck with obsolete approaches to security that are limited to scanning only traditional IT environments – so cloud and OT assets remain invisible. This creates an important question for the CISOs – invest in hiring and training more staff or prioritise investing in advanced technology solutions that may both improve security and reduce overall workload.

The Capacity Building Problem

Traditional cyber-risk management approaches typically focus on CVSS¹ to “prioritise” which vulnerabilities to remediate first. Most enterprises will attempt to remediate all of the *high* and *critical* vulnerabilities (those with a CVSS score of seven and above out of possible ten). Some may opt instead to simply concentrate only on the *critical* vulnerabilities (CVSS score of nine and above). In 2019 56% of vulnerabilities were assigned a CVSS score of seven or above – and were therefore considered high or critical. Accordingly, for every 100,000 vulnerabilities an organisation identifies, CVSS dictates that they’d have to remediate 56,000 of them. This workload can quickly spiral out of control.

However, arguably, CVSS is a completely ineffective method for prioritising remediation efforts since most scores are assigned within two weeks of vulnerability discovery. This means the CVSS score only employs a theoretical view of the risk a vulnerability could potentially introduce rather than actual risk. That leads to already overworked security teams wasting the majority of their time chasing after the wrong issues while missing many of the most critical vulnerabilities that pose the greatest risk to their organisation.

Moreover, identifying vulnerabilities is only the first step as you then have to be able to patch them in order to mitigate – an unpatched system

is still the number one cause of security incidents. Patching can have a number of unintended consequences – incompatibility, cost – and may also cause temporary business disruption if systems are taken offline. Patching within the OT environment can be particularly tricky.

All of this leads to the fundamental data problem facing security teams today. CISOs have far more vulnerabilities in their environment than they can possibly handle and they must be able to prioritise. The security team will never be large enough to manage all threats effectively without investment in technology.

Cyber capacity building can be difficult to implement as well as to measure. It should be noted that it is not necessarily about “ticking off” specific risks or vulnerabilities, but rather how you build up your resources, both people and tech, to deal with a myriad of current threats and those coming down the line. It is therefore important to understand what direction you are taking your security staff in, and the organisation as a whole. It’s important to document and communicate how staff are being skilled up, trained, and developed – the retention of essential technical staff is also an indicator of success and cyber-maturity. A happy team leads to good outcomes.

CISOs have far more vulnerabilities in their environment than they can possibly handle and they must be able to prioritise. The security team will never be large enough to manage all threats effectively without investment in technology.

The Expanding OT Threat Landscape Will Increase the Cyber Skills Gap

One of the biggest risks facing organisations today is a lack of basic visibility of their infrastructure. Today’s advanced “smart” OT environments have large attack surfaces with numerous attack vectors. Without complete visibility, the occurrence of an attack is not a matter of “if” but “when”. Because IT & OT are two different worlds that are now connected, an attack that starts in an IT environment

¹ The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. CVSS is a published standard used by organizations worldwide.

can quickly move to an OT environment and vice versa. Lateral movement is an ideal attack methodology for hackers because of the relative ease of finding a weak link in the system, leveraging this as the point of entry, and then quickly moving across the entire network.

Without complete visibility, the likelihood of an attack is not a matter of “if” but “when”.

Recent attacks against OT devices have highlighted the vulnerability of corporate networks. The recent “Lemon Duck” malware campaign is a case in point – it targeted a range of connected devices, including access controls for heavy equipment (Spring 2020).

From smart connected HVAC² to lighting and humidity controls, the workspace can now be centrally managed. Smart technology delivers significant efficiencies, which is driving adoption. However, the network-connected devices that make this possible also greatly expand the potential attack surface. OT-related risks are expected to significantly increase as more cities and work environments continue to “go smart”. While these smart buildings and devices can yield large business benefits, they are also a challenge for security leaders to securely manage them.

Traditionally, IT infrastructure has been the focus for security and control. This approach made sense because the IT environment was the focal point for cyberattacks. For the better part of two decades, this has been the CISOs’ focus, but this reality is changing. Modern industrial operations include complex IT and OT infrastructures. In a standard environment, thousands of devices may be active and connected to the Industrial Internet of Things (IIoT). This creates new challenges in securing industrial environments specifically by making cybersecurity threats even more difficult to detect, investigate, and remediate. With smart cities and smart work environments increasingly interconnected through rapidly converging IT and OT environments, industrial and critical infrastructure

operations have quickly converged. OT has now become a magnet for new attacks and increased security risks.

OT priorities are often safety, reliability, and availability – whereas cybersecurity is concerned with information confidentiality, integrity, and availability. These priorities can coalesce around availability, but much more focus is now required on security. These differences in approach, and the required skills to effectively manage these converged IT & OT devices, will further exacerbate the critical skills gap for security teams now managing security across both types of devices. Understanding the IT threat in an OT environment, and vice versa (OT providing access to enterprise networks), requires new skills and undoubtedly new technology. Monitoring OT traffic should be relatively straightforward via the deployment of sensors, but understanding any anomalies within that traffic requires a different skill set, and one that must appreciate the functions of the operational environment.

With smart cities and smart work environments increasingly interconnected through rapidly converging IT and OT environments, industrial and critical infrastructure operations have quickly converged. OT has now become a magnet for new attacks and increased security risks.

Training Is Still Important, but Striking a Balance Is Key

In the 2017 Harvard Business Review article entitled “The Best Cybersecurity Investment You Can Make Is Better Training”, the authors argued that “to prepare for and prevent the cyberattacks of the future, firms need to balance technological deterrents and tripwires with agile, human-centered defences.” Further, the authors used an analogy of an automobile, noting that “technology is a critical piece of the cybersecurity puzzle, but just as with a car containing all the latest safety technology, the best defence remains a well-trained driver” (Disparte, Furlow 2017).

² Heating, ventilation and air conditioning.

In 2019, journalist Rob Waugh echoed the Harvard journal by writing in the UK *Telegraph*: “Experts recognise that a team trained in cybersecurity could be the strongest weapon in a business’s arsenal when it comes to resilience and protection.” In support of this conclusion, Waugh noted that worldwide spending on cyber defence products and services is forecast to exceed 1 trillion USD in 2021, however there are still cyber data breaches every year – he in fact cited a source stating that “this is a clear sign that all the investment in technology is necessary, but not enough. It is now time to invest in people” (Waugh 2019).

It seems clear that skilled security leaders are critical to an effective defence. Technology has not replaced human beings. However, returning to the automobile analogy, this effectively illustrates the need for a balanced approach. The best automobile is worthless without a good driver, but it is equally true that the best driver will not be successful driving a poor-performing and slow racing car.

A Successful Training Approach: How to Start?

Training complements technology and is essential to successful cyberdefence. But training can also have the benefit of providing a structured career path for security team staff. Certifications and training help staff remain updated on the latest trends in security risk management. This can also improve staff retention which reduces costs and improves organisational stability.

In considering training, it is also important to consider the type of training and its provider. Investing in professional services at the start of a project to train staff to properly use advanced tools can ensure that costly technology is effectively used. Investing in a technology tool is important, but it is equally important to assure that the tool is used effectively. Investing in services that provide a clear roadmap and training in the beginning can save many hours of frustration and failure later. Bespoke training, rather than general courses, may be particularly worthwhile if the service provider can work directly with an organisation’s tools or bring unique expertise on a new and advanced technology. Staff need

good mentors. Bespoke professional services and training provide this critical support function.

Investing in a technology tool is important, but it is equally important to assure that the tool is used effectively.

Properly trained staff will make good decisions about priorities and choosing the right technology tools. After identifying and prioritising critical vulnerabilities, and how they affect the attack surface, it is important to design a training programme that develops the skills that will reduce these risks.

How Can CISOs Balance Technology and Training for Success?

A 2019 study by McKinsey Consulting found that risk-based vulnerability management reduces risk, “by building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats – those that target the business’s most critical areas. [This] approach allows for both strategic and pragmatic activities to reduce cyberrisks... Companies have used the risk-based approach to effectively reduce risk... [up to a] reduction 7.5 times above the original [security] program at no added cost” (McKinsey 2019).

With risk-based vulnerability management, the question isn’t: “How do we protect against and remediate *all* of these vulnerabilities?” The critical question becomes: “Which vulnerabilities pose the *greatest risk*?” Only about 3% of all vulnerabilities pose a significant amount of actual risk and therefore need to be prioritised. This can significantly reduce costs and avoid wasted time, while also providing better security. Security teams should be trained to effectively implement risk-based vulnerability management. But just as importantly, teams should have adequate tools to sift through the thousands of CVSS scores and identify critical vulnerabilities based on intelligence and effective prioritisation.

Only about 3% of all vulnerabilities pose a significant amount of actual risk and therefore need to be prioritised. This can significantly reduce costs and avoid wasted time, while also providing better security.

Navigating cybersecurity risk can be challenging. Without the right tools to understand how and where the business is at risk, there can be security blind spots. New and increasing threats are being identified every day. Staying ahead of cyber-risks can feel like treading water. There is a perception that cyberattacks are executed with a high degree of sophistication. The reality is that, while attacks may appear sophisticated, they are not insurmountable. Most cyberattacks can be overcome, or even prevented, with best practices for risk management. But to be successful, CISOs need to also be strategic. Invest resources in the right places and prioritise critical risks. By understanding where the organisation is exposed, and to what extent, the CISO can get a clearer picture of what's at risk. This enables the CISO to review priorities and understand the overall level of security for the business.

Security teams cannot protect and manage the unknown. CISOs should avoid wasting resources by blindly applying controls. Instead, a better approach is to identify and measure what actually reduces risk. An effective approach to risk management should measure success by risk reduction. With limited resources, it is critical to know what controls are really effective.

A quick look at the history of recent data breaches shows the value of focusing on getting basic risk management right. Advanced attacks only cause a small number of major breaches. It's the known basic vulnerabilities not being addressed that cause problems, not advanced attacks. The best solution, at the least cost, is to focus on aggressively identifying and remediating critical vulnerabilities. Organisations with poor basic vulnerability management are four times more likely to suffer a major data breach. However, a Gartner research study found that by adopting a risk-based vulnerability management programme an organisation is likely to suffer 80% fewer data breaches (Lawson, Schneider, Bhajanka 2019).

Advanced attacks only cause a small number of major breaches. It's the known basic vulnerabilities not being addressed that cause problems, not advanced attacks.

Finding Balance to Achieve Success

C-level leaders should promote the correct cyber risk management approach. Too many security programmes rely on blind capacity building and deploying numerous technical solutions to achieve a random maturity level. They do not effectively prioritise critical risks or provide value based on risk reduction. As an organisation's infrastructure grows and becomes more decentralised, it is even harder to keep track of every component inside and outside the company that might be a risk. Conversely, others hire staff but fail to adequately invest in advanced tools to effectively implement proven approaches such as risk-based vulnerability management. These are racing drivers without an adequate car – and destined to lose.

A strong cyber risk management programme should be based on three critical principles:

1. **Prioritise critical risks.** The CISO should avoid the traditional capability building approach of trying to address every vulnerability. This consumes valuable resources on risks that have a low likelihood of being exploited. Use prioritisation and risk-based analysis to focus aggressively on critical risks that really matter.
2. **Invest in Critical Risk Reduction.** The CISO should present a clear measurable view of cyber-risk exposure. Benchmark internally and externally. Present business leaders with clear quantifiable measurements of risk reduction effectiveness. Invest in training and tools that address critical risks.
3. **Know “how good you need to be”.** Understand “how good you need to be” to reduce cyber-risk. This is a tough question to answer but it should ultimately be linked to critical risks and not generic maturity levels. The CISO must focus on identifying and reducing critical vulnerabilities that pose the greatest likelihood of being exploited by an attacker. Answering “How good do you need to be?” should be based on insights into the critical risks and assets within the business. And remember to start with a cybersecurity baseline, so you have something to measure success against. ■



About the authors:

Adam Palmer, Chief Cybersecurity Strategist, Tenable (apalmer@tenable.com). Adam leads C-level Strategy Outreach for Tenable. Adam has 20 years of global cybersecurity experience including working at both the UN and a Top 20 Global Bank.



Oliver Hoare, CEO, Dysart Solutions (oliver.hoare@cybercapacityunit.org). Prior to becoming an independent consultant Oliver worked for the UK Cabinet Office and was CISO for the London 2012 Olympic Games.

References

Disparte, D., Furlow Ch. (2017). The Best Cybersecurity Investment You Can Make Is Better Training, *Harvard Business Review*.

Lawson, C., Schneider, M., Bhajanka, P. (2019). A Guide to Choosing a Vulnerability Assessment Solution. Gartner.

McKinsey (2019). The risk-based approach to cybersecurity. Retrieved from: <https://www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity>

Spring, T. (2020). New Lemon Duck Malware Campaign Targets IoT, Large Manufacturers, *Threat Post*.

Tenable Research (2019). Vulnerability Intelligence Report.

Waugh, R. (2019). Why cybersecurity training is important for your business, *UK Telegraph*.

ANALYSIS

5G Corridors, a Promising Investment in Europe's Technological Sovereignty

ARSENIO CUENCA-NAVARRETE

MA GRADUATE, FRENCH INSTITUTE OF GEOPOLITICS

The deployment of 5G networks, together with the new technologies fueled by the high-speed Internet it will provide, is set to shift the current paradigm of telecommunications. From the very diverse applications this new-generation network promises, autonomous driving provides one of the best prospects for Europe. Firstly, because it involves the European automotive industry, a domain in which Europe ranks among the champions on a global scale. Secondly, because it presents a major opportunity for the different actors involved in the autonomous-driving value chain to integrate and come together – including both the public and private sectors and academic and research institutions. This joint effort results in 5G corridors, a common initiative between European Member States that makes Europe the biggest experimentation area in 5G technology. 5G corridors connect several European countries through physical and digital infrastructures, representing a superb asset on the path to achieve technological sovereignty, one of the main guidelines of Ursula

von der Leyen's new Commission. Therefore, this European cross-border connectivity will contribute to enhance Europe's strategic autonomy and ensure a secure environment for 5G technology and autonomous driving. This article will discuss in depth the functioning of these corridors and the benefits of this European program, along with other proposals that will ultimately lead to European technological sovereignty.

Innovations from the Past

In 1826, the railroad engineer George Stephenson provided the world with a figure that was going to make transport and trade possible on a European scale: 1,435 millimetres. This unit was the measure of the standard-gauge railway, first used in England to connect the cities of Manchester and Liverpool, and soon adopted by several like-minded European countries. Before that, in 1814, Stephenson had also contributed to European economic development with another major improvement in matters of transportation: the integration of the steam

machine in the locomotive. Together, these two advances were decisive in times of the First Industrial Revolution and changed the course of history; it is extremely tempting to draw a historical analogy between Europe in the early 19th century and Europe today.

Europe is currently heading towards another industrial paradigm shift, the Fourth Industrial Revolution. According to Klaus Schwab, the founder of the World Economic Forum, this revolution will be carried out by the implementation of innovative digital tools and services based on a higher connection speed. It can be argued that the steam machine that exponentially quickened the rhythm of trade exchanges has its digital replica in the present time: the 5G network. The deployment of the fifth generation of mobile network will lead to an immense progress in connectivity, creating a dynamic and flexible telecommunication system based on faster Internet connections and low latency (Andrews et al., 2014).

It can be argued that the steam machine that exponentially multiplied the pace of trade exchanges has its digital replica in the present time: the 5G network.

The third analogy can be established between the application of the steam machine to the locomotive on the one hand, and the incorporation of 5G to automotive vehicles on the other, laying out the basis of autonomous driving. Self-driving vehicles are one of the most remarkable breakthroughs that accompany 5G, a vow for a more secure and decarbonised transportation. At the time of the First Industrial Revolution, the underpinning principle of technological progress was to increase the speed of commercial exchanges and travel. Now, Europe is determined to transition to an ecological and safer transportation system between Member States (MSs). With this in mind, the fourth and last analogy – and the main subject of this article – can be introduced: the standard-gauge railway and 5G corridors. If those 1,435 millimetres allowed countries to connect through railways, the project of 5G corridors will lead to the creation of common 5G networks between States, helping develop cross-border autonomous driving.

R&D and Stakeholder's Integration: The European Approach to Autonomous Driving

The EU seeks to remain a competitive player in the incoming digital revolution. In order to achieve this, the European Commission has shown a strong interest in the mastery of 5G technology since its very first steps. From the outset, the commission has promoted cooperation between public and private actors to carry out innovation in state-of-the-art 5G technologies. In 2013, the Commission made public its 5G Public-Private-Partnership (5G-PPP), a call to 31 leading organisations from the ICT sector, including research centres, leading mobile operators and 5G providers, funded with 700 million euros of public spending (European Commission, 2016c). By then, the Vice-President of the Commission, Neelie Kroes, set the basis of the European policy oriented towards technological sovereignty and its relation to the 5G network: "European 5G is an unmissable opportunity to recapture the global technological lead."¹ Superior-capacity broadband networks are a fundamental part of the existing ecosystem created by emerging technologies and new digital tools such as the Internet of Things (IoT) or cloud and edge computing, which explains why Europe was not willing to miss that train.

At the end of that same year, the regulation that established Horizon 2020 was approved. This program would also provide a solid budget between 2014 and 2020 to fund the Europe 2020 Strategy, a future-oriented investment in innovation and R&D (EU Regulation 2013/1291: Art. 3). The 5G-PPP was soon to be incorporated in Horizon 2020, thus gathering manufacturers and service providers both from the SME domain and the research community.² Later on, in 2016, another cornerstone of European 5G strategy was announced, the 5G for Europe: An Action Plan (5GAP). This document acknowledges the game-changing nature of this

¹ See 5G-PPP History. Development of the 5G Infrastructure PPP in Horizon 2020.

² See Advanced 5G Network Infrastructure for the Future Internet Public-Private Partnership in Horizon 2020. "Creating a Smart Ubiquitous Network for the Future Internet". Ref. Ares(2014)327845 - 10/02/2014.

technology, which deeply alters the dynamics of several business and public services across multiple sectors. Specifically, one of the more liable sectors for innovation is the automotive field, where Europe remains one of the main players in the global industry (OICA, 2019). That is reason why key stakeholders from the telecommunications sector and the vehicle manufacturing industry had already started GEAR 2030, a high-level dialogue about Cooperative Intelligent Transport Systems (C-ITS). For its part, the Commission was working on the regulatory environment for standardisation and resource efficiency (European Commission, 2016a).

Internet of Vehicles (IoV) is possible thanks to the advanced 5G features, mainly under the 5G New Radio (NR) standards prescribed by the 3rd Generation Partnership Project (3GPP): Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC); and Massive Machine-Type Communications (mMTC) (Mallinson, 2016). An enormous improvement of the network performance will allow real-time Vehicle-to-Vehicle communication (V2V), including with their environment, or Vehicle-to-Everything (V2X). C-ITS will benefit from Mobile Edge Computing (MEC), which is already present in several testbeds (Chochliouros, 2019). MEC is fundamental for faster data processing halfway between the sending device and the cloud. Many diverse services are involved in the functioning of self-driving vehicles, namely HD maps with improved positioning systems, infotainment, or predictive Quality of Service (QoS). These differentiated services are able to coexist without any interference as a result of Network Slicing, which increases the separation between different layers on the same network (NIS Cooperation Group, 2019).

C-ITS itself will lead to another form of understanding mobility, the so-called mobility-as-a-service, more efficient and safer (Ferreira, 2019). It stems from the necessity of an enhanced accident prevention, a better traffic management and a reduction in fuel consumption and CO₂ emissions (Pandi et al., 2016). Concerning road accidents, C-ITS offers a major safety improvement that human

drivers or other autonomous-driving-related devices like sensors fail to ensure. According to some studies, intelligent vehicles that eliminate stop-and-go driving and constant idling can contribute to drastic fuel economies, representing a 30% saving of total consumption (Gonder et al., 2012). C-ITS is interrelated with other key advances in transportation too, including platooning: autonomous trucks rolling along as a tightly packed column of vehicles that share information between themselves and their environment, saving energy and highway capacity (Saduki et al., 2016b). Taking into account that truck platooning seems to be one of the first applications of autonomous road vehicles to be spread, and that the EU strongly relies on the trucking sector for the transportation of merchandise, Europe would greatly benefit from this area of the C-ITS.

All these improvements in transportation make autonomous driving a crucial asset for the EU's Digital Single Market strategy. Yet for this technology to operate throughout Europe, MSs have to ensure network continuity. The 5GAP highlights the need for 5G network to be available at a regional level, avoiding fragmentation and the digital divide between MSs. The same philosophy is also present in the EC communication "Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society" (2016b). In fact, interoperability between networks is remarked in both reports as soon as the issue of cross-border corridors for self-driving vehicles arises. Gigabit connectivity furnished by 5G technology will open the way for road corridors, among other types of land and air routes, transited by autonomous transportation (2016b). Thus, service continuity between MSs is presented as a condition *sine qua non* for the correct functioning of European automated transport. The "Declaration of Amsterdam for Cooperation in the field of connected and automated driving", a statement signed in 2016 by EU MSs and the Commission, focusing on cooperative, connected, and automated mobility (CCAM), also echoes the principle of convergence between complementary technologies.

Service continuity between MSs is presented as a condition sine qua non for the correct functioning of European automated transport.

2016 ended with the creation of the European Alliance of Telecoms and Automotive, where both industries, along with several MSs and supra-national entities, joined their efforts to propose solutions for cross-border CCAM.³ The following year in Frankfurt, this willingness was reinforced by the round table on Connected and Automated Driving (CAD).⁴ As a result, and with the aim to make 5G corridors a flagship of European CCAM, today around 11 corridors that involve public and private participation have been set up in Europe, according to the European 5G Observatory. These initiatives make Europe the biggest experiment area in 5G technology. Among these corridors, there are three particular projects that depend on the financial support of the Commission, which are part of the 5G-PPP and the funding of Horizon 2020, particularly with the budget of the 2018–2020 period, oriented towards green vehicles and automated road transport.⁵

The first corridor supported by the Commission is 5G-Carmen. This project connects a 600 km road system through the cities of Bologna (Italy) and Munich (Germany) via the Brenner Pass, covering the regions of Bavaria, Tirol, and Trentino/South-Tyrol. 5G-Carmen is a testbed for cooperative manoeuvring, notably lane changing, with the subsequent data sharing of information about speed, positions, and intended trajectories. An advanced system of situation awareness is put in place which

reflects the traffic situation, weather conditions, and potential dangers. The second project is 5G-CroCo, which triangulates the cities of Metz (France), Merzig (Germany), and Luxembourg (Luxembourg). In this case, the emphasis is placed on tele-operated driving where the remote control is taken by a human, HD maps that provide accurate location of static and dynamic objects, and Anticipated Cooperative Collision Avoidance (ACCA).⁶ Finally, 5G-MOBIX, which connects the Iberian Peninsula across two corridors: Evora (Portugal) – Merida (Spain) and Porto (Portugal) – Vigo (Spain). Another testbed has been deployed in the Greek-Turkish border, enhancing collaboration between European MSs and extra-EU countries. The case of 5G-MOBIX is notable as it involves urban sites in six European cities (Noussan et al., 2020).

There is another project developed in the Horizon 2020 framework that operates on a global scale: 5G-DRIVE, which involves the two main regions invested in 5G technology in the world, Europe and China. The approach of this partnership is three-dimensional, focused on technical development, regulation, and business. Under the supervision of EURESCOM, up to 17 European actors from 11 countries encompassing the whole value chain of CCAM participate in 5G-DRIVE. 5G-DRIVE has been conceived as a twin initiative of the National Science and Technology Major Project (NSTMP) launched in China in 2018, implying an excellent opportunity to test network interoperability. One of the main interests of this project is the optimisation of band usage in scenarios with different coverage and geographic features, looking to implement testbeds in both regions.⁷ Apart from that, 5G-DRIVE aims to conduct trials with the rest of the end-to-end 5G deployment scenarios mentioned above, such as eMBB and V2X.⁸

3 See EU and EEA Member States sign up for cross-border experiments on cooperative, connected, and automated mobility.

4 See Cross-border corridors for Connected and Automated Mobility (CAM).

5 The commission shows a strong commitment to promote strategic technologies belonging to the autonomous vehicle value chain. Also under the umbrella of Horizon 2020 and the European Investment Bank, European loans have recently financed several projects related to the production of lithium-ion batteries, a market with optimistic forecasts (European Commission, 2019a).

6 This system facilitates a more fluid reaction than sensors at the moment of avoiding potential dangers (Hetzler et al. 2019).

7 See ICT-22-2018: EU-China 5G Collaboration.

8 See 5G-DRIVE. About 5G-Drive.

Strategic Autonomy to Overcome Power Rivalries around 5G

Nevertheless, as many will be aware, the EU-China partnership in the realm of 5G is not currently at its best. Their relations are already complicated on account of their idiosyncratic differences (European Commission, 2019b), and the ongoing trade war between the USA and China is pushing Europe to reconfigure its system of alliances. At the centre of this confrontation is Huawei, the Chinese tech giant, world-leader in 5G technology, accused of being the CCP's Trojan horse. Huawei is present in the telecommunications network of the majority of MSs, and in 5G corridors like 5G-Croco. However, the transatlantic alliance is in no better shape. On the one hand, just after the entry of the GDPR into force in 2016, US president Donald Trump approved the CLOUD Act in 2017 requiring American cloud service providers to grant access to any data in their possession regardless of where it is stored (Daskal, 2018). On the other, the American GAFAM⁹ are also a major concern for the EU, as they stand as giant tech corporations with the hidden power of big data, on the margins of any democratic process (Calzada, 2019).

This delicate situation forces Europe to question its technological sovereignty. Although this issue had already been raised at the time of Edward Snowden's revelations (Ilves & Osula, 2020), which claimed that several MSs were victims of an espionage network led by the USA, it has gained force with regards to Europe's current circumstances. Looking eastwards, they see the emergence of a Chinese "technological nationalism", in which government and tech make profit form a reciprocal relation to develop a hyper-vigilant State (Calzada, 2019). Then, westwards, big tech multinationals are colonising an increasing amount of domains in their user's daily lives to make private profit and accumulate even more power. The EU is not willing to depend on any of these technological paradigms, proposing in contrast

a sustainable regionally rooted and inclusive third way-out (Calzada, 2019). In the words of Ursula von der Leyen, president of the Commission: "[...] it is not too late to achieve technological sovereignty in some critical technology areas" (2019).

5G corridors are a promising investment in Europe's technological sovereignty because they enhance many of the principal European assets in the domain of tech. Due to EU's interstate features, the opportunity to develop standard procedures and know-hows between countries that can later be replicated in different geographical contexts is unique. Innovation in domains like cloud computing, supported by initiatives like GAIA-X, is more than pertinent, despite what some skeptics of European techno-sovereign momentum may argue (Laurent, 2019). CCAM will demand a superior data processing capacity, opening a window of opportunity to this kind of projects. Besides, in the spirit of the GDPR, Brussels can stimulate the creation of new regulatory frames to be applied to CCAM like the recent EU Cybersecurity Act that can set an example for the rest of the world (Ilves & Osula, 2020). The logic of this regulation is to create a safe environment for the functioning of C-ITS, an extremely necessary advancement considering its own particularities and its global value chain. Finally, these corridors encourage greater political and economic cohesion between supranational institutions and European tech projects, a positive practice frequently used by the United States and China (Mazzucato, 2013; Boschet et al., 2019).

5G corridors are a promising investment in Europe's technological sovereignty because they reinforce many of the principal European assets in the domain of tech.

In sum, the technological sovereignty approach does not aim towards any kind of technological autarky: instead, it assures Europe's strategic autonomy. The guarantee that a country or region is technologically sovereign does not lie in its capacity to host most of the supply chain of the main strategic technologies within its borders. To secure its sovereignty and cybersecurity,

⁹ Acronym that includes five information technology companies with the largest volume of data storage, based in the United States: Google, Apple, Facebook, Amazon, and Microsoft.

Europe can resort to other means and mechanisms. Concerning 5G corridors, strategic partnerships developed for instance with China can contribute to reducing the uncertainty created by the globalisation of 5G value chains and cybersecurity risks (Timmers, 2019, 2020). However, these partnerships might not be viable in the long term, as an exacerbated interdependence in the area of strategic technologies can be a source of high instability.

In sum, the technological sovereignty approach does not aim towards any kind of technological autarky: instead, it assures Europe's strategic autonomy.

Cybersecurity concerns can consequently be mitigated through a holistic risk management strategy. The three corridors under the scope of Horizon 2020 collaborate with more than two 5G providers, as recommended by the NIS Group toolbox (2020). In parallel, technology certification systems are being developed to accomplish effective checks, like the Common Criteria certification. Other multilateral initiatives like the Paris Call for Trust and Security in Cyberspace help associated key stakeholders to develop international legal frames (Timmers, 2020). These initiatives promote multilateralism and have a positive effect on coexistence and dialogue at the international level.

Yet, they can be challenging to maintain over time, inefficient at times, and expensive. For this reason, all hopes are most fundamentally being placed in new technologies for distributed authentication, like blockchain. These trust technologies configure a new paradigm of automated “security by design” that could ultimately lead to “autonomy by design” whose integrity is shielded against any exterior interference (Ilves & Osula, 2020).

As Ilves and Osula rightly point out, despite a plethora of measures that mitigate cybersecurity issues linked to technological sovereignty, they do not solve the European problem of long-term tech dependency (2020). Nevertheless, “they do give policy-makers more leverage, allowing them to focus on developing domestic technologies and supply chains in a more targeted manner” (Ilves & Osula, 2020). For now, innovation based on 5G technology in the automotive sector, backed by strategic partnerships and adoption of common regulatory frameworks, enables Europe to compensate its technological backwardness, a delay which should by no means stand as a reason to hinder its progress. Ultimately, 5G corridors can contribute to enhancing Europe’s strategic autonomy by creating a proper domestic field of expertise, giving Europe more economic and political leverage in years to come. ■

About the author:



Arsenio Cuenca has just completed his master’s at the French Institute of Geopolitics, based in Paris, with a thesis exploring the geopolitical concerns of the 5G network deployment in Europe, including a case study of France. Currently, he is pursuing another master’s in cyberstrategy, combined with a traineeship at the digital research unit of the French Gendarmerie. Arsenio was granted a scholarship of excellence by the French Ministry of Europe and Foreign Affairs. He is a regular contributor to the Spanish digital media *El Orden Mundial* on geopolitics and international relations. He is committed to European technological sovereignty as well as to the democratic values of the EU.

References

- Andrews, J.G., Buzzi, S., Choi, W., Hanly, S.V., et al. (2014). What will 5G be? IEEE JSAC Spec. Issue 5G Wirel. Commun. Syst. 32(6), 1065–1082.
- Boschet, A., Chimenti, J., Mera Leal, N., & Duval, T. (2019). *Chine Digitale. Dragonhacker de puissance*. V.A. Éditions, Versailles.
- Chochliouros I.P. et al. (2019). Testbeds for the Implementation of 5G in the European Union: The Innovative Case of the 5G-DRIVE Project. In: MacIntyre J., Maglogiannis I., Iliadis L., Pimenidis E. (eds) Artificial Intelligence Applications and Innovations. AIAI 2019. IFIP Advances in Information and Communication Technology, vol 560. (pp. 78–92). Springer, Cham.
- Daskal, J. (2018). "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0". Stan. L. Rev. Online, 71, 9.
- European Commission. (2016a). A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility.
- European Commission. (2016b). Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society.
- European Commission. (2016c). 5G for Europe: An Action Plan.
- European Commission. (2019). Report on the Implementation of the Strategic Action Plan on Batteries: Building a Strategic Battery Value Chain in Europe.
- European Commission and HR/VP contribution to the European Council. (2019b). EU-China. A strategic outlook.
- EU REGULATION 1291/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.
- Ferreira, J. (2019). "Cooperative, Connected and Automated Mobility (CCAM): Technologies and Applications". *Electronics*. 8. 1549. 10.3390/electronics8121549.
- Gonder, J. Earleywine, M., & Sparks W. (2012). "Analyzing vehicle fuel saving opportunities through intelligent driver feedback," SAE International Journal of Passenger Cars - Electronic and Electrical Systems. Vol. 121, no. 7, pp. 450–461.
- Hetzer, D. Muehleisen, M. Kousaridas, A., & Alonso-Zarate, J. (2019) "5G Connected and Automated Driving: Use Cases and Technologies in Cross-border Environments". In 2019 European Conference on Networks and Communications (EuCNC) pp. 78–82. IEEE.
- Ilves, L., & Osula, A. M. (2020). "The Technological Sovereignty Dilemma—and How New Technology Can Offer a Way Out". *European Cybersecurity Journal*. Vol. 6, no 1, pp. 24–35.
- Laurent, L. (2019). "Macron and Merkel Are Caught in a New Cold War". *Bloomberg*. Source: <https://www.bloomberg.com/opinion/articles/2019-11-14/technological-sovereignty-france-and-germany-join-a-new-cold-war>. Date of consultation: 15/07/2020
- Mallinson, K. (2016). "The path to 5G: as much evolution as revolution". 3GPP-The Mobile Broadband Standard.
- Mazzucato, M. (2013). *The Entrepreneurial State. Debunking Public vs. Private Sector Myths*. Penguin Group, Londres.
- NIS Cooperation Group. (2019). "EU coordinated risk assessment of the cybersecurity of 5G networks".
- NIS Cooperation Group. (2020). "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures".
- Noussan, M., Hafner, M., & Tagliapietra, S. (2020). *The Future of Transport Between Digitalization and Decarbonization: Trends, Strategies and Effects on Energy Consumption*. Springer Nature.
- OICA. (2019). WORLD MOTOR VEHICLE PRODUCTION BY COUNTRY AND TYPE 2018-2019. Paris: Organisation Internationale des Constructeurs d'Automobile.
- Pandi, S., Fitzek, F. H., Lehmann, C., Nophut, D., Kiss, D., Kovacs, V., ... Liebhart, R. (2016). "Joint design of communication and control for connected cars in 5G". In 2016 IEEE Globecom Workshops (GC Wkshps) (pp. 1–7). IEEE.
- Timmers, P. (2019). Strategic Autonomy and Cybersecurity. Policy in focus, EU Cyber Direct.
- Timmers, P. (2020). There will be no global 6G unless we resolve sovereignty concerns in 5G governance. *Nature Electronics*, 3(1), 10–12.
- Tsugawa, S., Jeschke, S., & Shladover, S. E. (2016). "A review of truck platooning projects for energy savings". *IEEE Transactions on Intelligent Vehicles*, 1(1), 68–77.
- von der Leyen, U. (2019). A Union that strives for more. My agenda for Europe. POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2019-2024.

From High Tech to High Politics: A Geopolitical Analysis of the European Approach to Secure 5G networks

SÉGOLÈNE MILAIRE

ADVANCED MA IN POLITICAL AND GOVERNANCE STUDIES, COLLEGE OF EUROPE



In the context of growing *geopoliticisation* of technology, rising international pressures and internal risks of fragmentation, the European Union (EU) has been lured into rethinking its attitude towards power politics. A perfect stage for the latest geopolitical drama, the discussion on 5G network security discussion insightfully reveals trends on Europe's positioning in the face of US-China rivalry. This article explores the ways in which the EU can be a geopolitical actor *by other means* through an in-depth analysis of the first common European approach to secure critical infrastructures as 5G networks.

Introduction – Bringing Geopolitics back in

For a long time, the EU “turned a blind eye on geopolitics” (Biscop, 2019, p. 8). Understood as “anything and everything related to power politics, realpolitik, influence, hard power, imperialism or conflict” (Cadier, 2019, p. 77), geopolitics does not seem to be at the core of the EU’s DNA. Rooted in a concept of security based on interdependence and shared sovereignty, the beginnings of the European integration project were in fact conceived in strict opposition to power politics – of which legacy had brought the horrors of war to Europe (Lehne, 2020). Yet, in recent years, there has been a great resurgence of interest among EU policy-makers, national officials,¹ and scholars in embracing the idea of an EU having a more geopolitical and less naïve approach (Nitoiu & Sus, 2019). The latest notable fledgling signs of this are: branding the new European Commission as geopolitical by its President Ursula von der Leyen (2019a) and labelling China as a “systemic rival” in a joint communication of the High Representative and Vice-President (HRVP) and the Juncker Commission (2019). However, despite a similar level of interest from academics in the analysis of the geopolitical turn in EU’s approach (Nitoiu & Sus; Laïdi; Lehne, 2019); few agreed on a common definition and spelt out how a more geopolitical EU would and should translate into practice. This article explores the ways in which the EU – the “[o]ld power who had forgotten what power was” (Biscop, 2020) – can be a geopolitical power in the digital age.

Major technological promise and foundational enabler of the fourth industrial revolution² for some, emblem of the rapid technological shift, ideal

target of COVID-19 conspiracies or new scapegoat for rising global anxiety over climate change for others; the fifth generation (5G) of mobile networks remains a key issue to watch. The debate on 5G network security – less focused on the technology itself than on the profile of its equipment makers (Nocetti, 2019) – constitutes also the first chapter in an increasingly heated trade and technology competition between the United States (US) and China. According to the think tank Eurasia Group (2020), the technological decoupling³ can be considered the most impactful geopolitical development since the collapse of the Soviet Union. Against this background, the global race for 5G network leadership is a faithful mirror reflecting the new geopolitical logics in the digital era, i.e. attempts to expand one’s sphere of influence and achieve flow controls by means of technological dependence by prioritising relative economic and normalising a systemic confrontation (Rühlig and Björk, 2020). Indeed, in response to 2017 Chinese National Intelligence Law,⁴ the US political leadership banned government agencies from using Chinese 5G equipment makers (Huawei or ZTE) on national security grounds.⁵ Throughout a global campaign lobbying against the “*sinification* of 5G networks” (Financial Times, 2020), the US administration encouraged European allies to exclude Huawei and threatened to limit intelligence sharing with countries that by failing to do so “chose autocracy over democracy”⁶ (New York Times, 2020); thus, reflecting the main features of the Cold War *containment strategy* and friend/foe rhetoric. Considering the EU’s high level of

3 Splitting the world into two spheres of technological influence between US and China.

4 In June 2017, the Chinese National People’s Congress adopted national intelligence law obliging Chinese companies under penal sanctions to cooperate in intelligence gathering with Chinese intelligence services.

5 In May 2019, the US President Trump issued an executive order and declared the national emergency to protect US critical ICT infrastructure and supply chains against foreign adversaries (White House, 2019). In addition, the US department of Commerce added the firm’s name to the US Entity list.

6 Nancy Pelosi allocution at the 2020 Munich Security Conference (Financial Times, 2020).

1 Josep Borell (2019) stressed the need for the EU to “relearn the language of power and position itself on the international scene to avoid being squeezed between the US and China”. French President Emmanuel Macron warned against the risk “that in the long run the EU might ‘disappear geopolitically’ if it did not wake up” (Economist, 2019).

2 Game changer for the industries, 5G as a technical infrastructure will enable the development of transformative applications that rely on fast speed and low latency: digitalising the industrial production processes (develop future industry 4.0); transforming the way we drive, the way we farm (European Commission, 2016).

technological dependence on both US (cloud services; software provisions) and China (critical raw materials; imports of high-tech products with €23 billions of EU's trade deficit) and the risks of internal fragmentations⁷, the decision to sidetrack one partner under pressure from the other would have harmful consequences for the Union's technological autonomy and security. The 5G discussion has therefore put the EU under intense pressures at both the economic and political levels and shed light on EU's puzzling situation of strategic dependence vis-a-vis non-EU suppliers. The decision it is facing – to ban or not to ban Huawei and ZTE from the 5G roll-out – can be seen as the “first of many awkward choices for Europe” (Rachman, 2019) that is likely to surface in other strategic sectors⁸ (Kleinhans, 2019). From a different – more optimistic – perspective, the EU's decision on 5G can also be considered a window of opportunity to *enter into power politics* and position itself as a *geopolitical actor*. Assessing the European approach to secure 5G networks will provide us with a better understanding of geopolitical thinking in a non-traditional security field and help us identify the drivers and obstacles in EU's alleged nascent geopolitical positioning.

The global race for leadership on 5G networks is a faithful mirror reflecting the new geopolitical logics in the digital era.

Case selection – A European Approach to Secure 5G Networks

“Historic” is the adjective chosen by the European Commissioner for the Internal Market and Defense, Thierry Breton, to describe the European approach to secure 5G networks. In January 2020, the EU Toolbox⁹ was adopted unanimously by

the European member states and endorsed by the European Commission. This is the first time that the 27 member states, against all the different national interests, managed to coordinate themselves and to take a joint approach in an area of national security: the security of 5G networks. Main focus of this case study analysis, the EU toolbox is a non-binding document that lays out a set of technical, strategic, and supporting measures to implement at both the national and European levels in order to secure 5G networks.

In January 2020, the EU Toolbox was adopted unanimously by the European member states and endorsed by the European Commission. This is the first time that the 27 member states, against all the different national interests, managed to coordinate themselves and to take a joint approach in an area of national security: the security of 5G networks.

This innovative and coordinated approach is the product of a one-year process of extensive institutional cooperation that involved member states' authorities, cybersecurity agencies, the Commission, the European Agency for Cybersecurity (ENISA), and the European External Action Service (EEAS). Following the call of the European Council¹⁰ for a concerted approach to secure 5G networks, the Commission adopted a Recommendation¹¹ in March 2019. Based on national risk assessments, the EU member states then identified the main strategic risks, vulnerabilities, and threat actors in a European coordinated risk assessment.¹² Step by step and building a common definition on who to trust and who to fear, the member states – acting through the NIS Cooperation Group with the support of the Commission and the technical input of ENISA's threat landscape mapping (2019) – adopted the EU toolbox of risk mitigating measures

7 27 member states taking different approaches on Huawei's role in their 5G networks would be detrimental to the Digital Single Market.

8 Other ICT sectors: Alibaba's AI and quantum computers or smart city solutions from Huawei (Kleinhans, 2019).

9 “Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures” (NIS Cooperation Group, 2020).

10 Council Conclusions (2019).

11 European Commission. (2019b). Commission recommends common EU approach to the security of 5G networks.

12 NIS Cooperation Group (2019). EU coordinated risk assessment of the cybersecurity of 5G networks.

at the centre of this study. We based our analysis on semi-structured interviews with cybersecurity experts and officials in charge of network policy or cybersecurity at both the national and the EU levels (member of cabinets and services under Junker and von der Leyen Commission, EEAS), as well as on a review of publicly available information in official documents and position papers. Our field work was carried out between December 2018 and July 2020, that is from the premise of an EU-level action – with the former Commission Vice President Ansip saying that “the EU should be worried about Huawei” (Reuters, 2018) – to the implementation of the European toolbox on Cybersecurity of 5G networks.

Broadening the Definition – The Geopoliticisation of Technology

When used in the academic or public debate, the term “geopolitics” traditionally tends to refer to “any power struggle over a given territory” (Lacoste, 2012, p. 18). In the light of the growing *geopoliticisation of technology*,¹³ the current race for power is no longer characterised solely by the use of military force over a territory but also by the control over the technology and infrastructure that enables connectivity (Rühlig and Björk, 2020). Geopolitics, we argue, is a product of its times (Cohen, 2014) and can take several meanings depending on the context, being what Müller would call a “floating signifier”¹⁴ (2020). Besides, we have witnessed in recent years the emergence of new concepts revisiting the traditional notion of geopolitics such as “digital sovereignty”, “connectivity war”, “virtual Berlin wall” and “technological hegemony” among others (Leonard & Franke, 2016; Carr, 2020). As a “[n]ew frontier of power in the fourth industrial revolution” (Soler i Lecha, 2019), digital technologies – mobile networks, artificial intelligence, cloud, quantum computing – have indeed become strategic leveraging tools to influence economic, societal, and

political outcomes (EPSC, 2019). In recent years, several studies in the field of digital geography have stressed the geopolitical implications of strategic technologies in the cyberspace, the geopolitics of submarine cables (Taillat, Cattaruzza, Danet, 2018; Morel, 2017). The issue of 5G networks, however, still remains unexplored in the European studies literature. As outlined by the CEO of the Swedish telecom company Ericsson, Börje Ekholm, it is only very recently that the issue of 5G has moved from what was, not so long ago, a “non-issue”, a dry and technical subject, to a much-debated topic and crucial issue on top of the geopolitical agenda: “The funny thing is that when we started the journey it had nothing to do with the geopolitics.”¹⁵ Hence, the notion of geopoliticisation (Cadier, 2019; Meunier & Nicolaidis, 2019) allows us to grasp the dynamic nature of the process whereby an issue – here the security of 5G networks – comes to be constructed as a geopolitical problem, and policy instruments – such as digital policies – end up embedded in power rivalries. Having said this, a geopolitical actor is understood in this article from both a static and a dynamic perspective – as a way of being, acting, and thinking. Widening the definition of geopolitics and breaking up the clear-cut neo-realist hierarchy of threats that can be legitimately included in the security agenda – high politics – and those that cannot and remain in the realm of low politics, we revisit Carl von Clausewitz’s contribution and argue that technology has become the continuation of politics by *another means*.

As outlined by the CEO of the Swedish telecom company Ericsson, Börje Ekholm, it is only very recently that the issue of 5G moved from what was, not so long ago, a “non-issue”, a dry and technical subject, to a much-debated topic and crucial issue on top of the geopolitical agenda: “The funny thing is that when we started the journey it had nothing to do with the geopolitics.”

13 Acknowledged by the European Political Strategy Centre on the occasion of a high-level hearing on strategic autonomy in the digital age in 2019.

14 A word still subject to struggle and contestation between different discourses (Müller, 2010).

15 Interviewed with Politico (Cerulus, 2019).

Two-step Analysis – Geopolitical by Other Means

A non-conventional power constrained by a constellation of national interests (Howorth, 2010), “unidentified political object” in the words of Delors (1985), or *sui generis* actor with a unique institutional architecture¹⁶ (Grevi, 2020), the EU cannot and should not, we argue, play power politics like the others. Throughout a case study analysis of the European approach to secure 5G networks, this section explores the drivers and obstacles in the shaping of the EU as a geopolitical actor *by other means*. Breaking with one-size-fits-all definitions of being geopolitical, this tailored approach allows us to demonstrate in what ways the EU can be a geopolitical actor in its own way – without imitating others’ geopolitical logics. Challenging the traditional understanding of geopolitics, we assume that the EU can become an important power by building on its market power, its strong communalised policies (Ghering, 2017), and its administrative capacities. Drawing on Nye’s concept of “one voice strategy” (2011), we acknowledge the relation of causality between the capacity of the EU to act as a collective actor with a single voice and its ability to become an influential actor on the global scene. However, the security of 5G networks remains a very divisive matter at the core of national member states’ competences – thus, complicating the co-construction of a harmonised approach and making impossible any transfer of competences to the EU level. “A few years ago, member states would have said: ‘Back off, the EU does not need to be involved in this.’”¹⁷ Hence, why did the member states agree to push for a coordinated EU-level approach to secure 5G networks? From a dynamic perspective, we first assess the internal and external drivers for collective action in the network security field, with a particular zoom-in on the strategic role played by the Commission in the backstage

16 Peculiarities of the EU polity: multilevel structure, combination of supranational and inter-governmental elements, functional and technocratic style, heterogeneity of the actors involved in policy-making, institutional hybridity (Featherstone & Radaelli, 2003, p. 8).

17 Interview with an EU official, expert in cybersecurity.

coordination of a joint EU-level effort to secure 5G networks (4.1.). This first part shows somehow the extent to which the Commission, by acting in a non-geopolitical way contributed to the shaping of the EU’s geopolitical thinking. From a more static perspective, the second part of our case study analysis then offers a form of snapshot analysis of the main geopolitical features of the EU toolbox on the Cybersecurity of 5G networks (4.2.).

Drivers of collective action on network security

In the face of mounting pressures from strategic partners (US and China), at risk of international splitting tensions over 5G networks and the internal fragmentation of the digital single market, the EU member states agreed to engage in an EU-level action as part of a strategic “double-level game”. Drawing on Putnam’s rational choice assumption¹⁸, we first argue that the multilevel and neutral nature of the EU institutional structure highly benefitted national level actors – protecting them against potential international backlashes over their national decisions. Going further, one can draw a parallel with a similar case, the Foreign Direct Investment (FDI) screening mechanism, where the member states highly valued the possibility of having a supranational actor to speak in the name of Europe to international partners.

Given the interconnected and cross-border nature of mobile networks, the technical disparities, different maturity levels in network security, and the variation in strategic cybersecurity culture played a key role in the push for a consistent and coordinated security approach at the EU level. Although network security is a national prerogative, one breach or incident in country A can affect the national security of country B and the EU as a whole. Following on the transnational implications of the 2018 hacking of Cyprus system – with the hackers getting access to the whole European database of diplomatic notes (New York Times, 2018) – although the “European security” is not legally defined in the EU treaties, one can understand what it means in practice.

18 “The interpenetration between the domestic and the EU level create variety of opportunities for actors to exploit” (Featherstone & Radaelli, 2014, p. 9).

The pre-existing EU-level coordination mechanisms and administrative resources made available to the member states – such as the NIS Cooperation Group¹⁹, institutional legacy of the 2016 Network and Information Security (NIS) Directive – facilitated the emergence of a collective decision-making process (i.e. eased the exchange of information among EU member states and reduced the transaction costs).

Although the “European security” is not legally defined in the EU treaties, one can understand what it means in practice.

Strategic role of the European Commission

Despite its lack of legal competence and mandate in the field of network security, the Commission (aware of its limited scope of action) strategically built on its institutional resources and played a key behind-the-scenes role in its capacity of “secretariat” of the working groups²⁰ according to the cyberexperts interviewed as part of this research. In a nutshell, the Commission adopted a low-profile politics approach – to preserve the member states’ feeling of political ownership all along the process – by using strategically its administrative instruments and technical capacities. Present at most stages of the decision-making process and in charge of the administrative tasks,²¹ the Commission tried not to generate negative reactions from national capitals (i.e. member states are sovereign on cybersecurity-related issues) and engaged in constant efforts of monitoring, recommending, and keeping the pressure at both technical and political levels.²² All the more so as, since the EU

toolbox on the Cybersecurity of 5G networks is a non-binding document, its implementation mainly relies on the political commitment of member states.

NIS Cooperation Group at glance

Commission’s body with an intergovernmental soul, the hybrid nature of the institutional architecture of the NIS Coordination Group contributed to preserve the member states’ feeling of political ownership over the drafting-process of the EU-level approach to secure 5G networks. A strategic platform in the 5G network security debate, the NIS Cooperation Group emerged as the most convenient arena for the cyberagencies, national member states, and EU institutions (Commission, ENISA) to meet, share information, coordinate an EU-level risk assessment, draft and monitor the implementation of a common toolbox of measures.

The Commission also contributed to push for convergence of interests among member states by depoliticising the 5G network security discussion and turning this controversial topic into a technical issue. Through a two-step methodology, the Commission dissociated the threat framing (coordination of the EU-level risk assessment) from the treat management (the drafting of common risk mitigating measures in 2020). By compartmentalising the work of the NIS Coordination Group in this way, the Commission helped move the discussion from a confrontational logic of naming and banning to a cleaner and less sensitive discussion where member states and cybersecurity experts identify potential security risks via objective criteria regardless of the supplier’s country of origin. As part of a “riskification approach”²³ (Corry, 2011), the Commission together with the EU member states successfully depoliticised the 5G-splitting discussion and bypassed the inherent rhetoric of power politics. Put concretely, rather than finger-pointing to a list of specific actors, the EU listed the “objective” criteria and factors to assess

19 Aimed at boosting cybersecurity at the EU level, the 2016 NIS directive established two cooperation groups to “facilitate the cooperation and the exchange of information among EU member states” at a strategic and political level through the NIS Cooperation Group and at a more operational one with EU CSIRT network. (2016/1148).

20 NIS Cooperation Group, Body of European Regulators for Electronic Communications (BEREC).

21 Logistics, meeting agenda, speakers’ invitations.

22 Interview with a former member of the NIS Coordination Group.

23 The idea to “focus on the conditions of possibility for harm rather than direct causes of harm” (Corry, 2011, p. 238).

The Commission helped move the discussion from a confrontational logic of naming and banning to a cleaner and less sensitive discussion where member states and cybersecurity experts identify potential security risks via objective criteria regardless of the supplier's country of origin.

the “risk profile” of third-party suppliers. By using a non-confrontational approach and an expert discourse (with technical assessments of “non-technical vulnerabilities”), the EU managed, step by step, to come to a common definition of who to fear and who to trust without mentioning any specific actors. Though, when reading between the lines of the risk factors listed, one can easily identify²⁴ the profile of Chinese equipment providers (Huawei and ZTE).

Finally, the strategic choice of “toolbox” as non-legislative vehicle and innovative policy instrument paves the way for more flexibility, transactionality, and horizontal coherence across policy areas. Alongside technical and security recommendations, the toolbox puts forwards a wide range of strategic and supporting measures that embrace the issue of network security in its broader sense (i.e. consider its international, political, technological, industrial, and cybersecurity dimensions). Indeed, the EU toolbox comprises a wide range of policies such as trade defense instruments, FDI screening mechanism, EU funding and R&D programme and EU's state aid regime (IPCEI). Therefore, by designing a policy toolkit that mentions a wide range of measures (economic and trade policy ones), the Commission puts all its instruments of (market) power – “EU's most important power” (Gros, 2019) – to the benefit of one strategy – here: reducing technological dependence and strengthening network security. As a telling example of the transactional feature of the EU strategy towards 5G security, the EU toolbox was endorsed simultaneously by three EU Commissioners in charge of distinct portfolios.²⁵ Also, such a non-binding policy

24 Informants interviewed in this research argued that it is possible to recognise Chinese equipment makers behind a certain number of criteria such as: the link between the supplier and a government of a given country, lack of democratic checks and balances and data protection in a third country's legislation, offensive cyber policy, the supplier's corporate ownership, ability for the third country to exercise any form of pressure (see NIS Coordination Group, 2019).

25 Margrethe Vestager (Executive Vice-President for a Europe Fit for the Digital Age), Margaritis Schinas (Vice-President for Promoting our European Way of Life), and Thierry Breton (Commissioner for the Internal Market).

toolkit enables the Commission to put bold ideas on the agenda, allows for new concepts – that are not legally defined – to germinate and provide input for a debate on the geopolitical positioning of the EU to emerge (i.e. European sovereignty, strategic autonomy, or technological sovereignty).

Towards a European Way on 5G security?

Given the peculiarity of the EU polity and the changing geopolitical configuration, it was assumed earlier that the concept of being geopolitical needed to be refined and nuanced in order to be applied to the EU context. The European approach to secure 5G networks remains country-neutral and partner-neutral (i.e. does not acknowledge “rivals” nor does it draw a clear friend/foe enemy line), it cannot therefore be considered as geopolitical in the traditional sense

Table 1. Drivers of convergence in the field of network security

<p style="text-align: center;">VERTICAL <i>Between member states</i> <i>Between member states and the Commission</i></p>	<p style="text-align: center;">HORIZONTAL <i>Within EU institutions</i></p>
<p>Differentiated level of preparedness, capability, and maturity among member states, i.e. member states push for a minimum level of security to avoid fragmentation and build common resilience.</p> <p>Political will and peer pressure phenomenon among member states: first time member states in such sensitive area agree to set up a coordinated approach that will be touching their national security.</p> <p>Crucial role of NIS Cooperation Group Workstream (introduced under NIS Directive) as a coordination mechanism that identified effective common methodologies and tools to mitigate risks related to 5G networks. NIS Cooperation Group as a Commission body likely to see its mandate expanded to monitor implementation of the Toolbox.</p> <p>The same understanding of threats shared by member states with EU institutions because they used a similar methodology to assess security risks: coordinated risk assessment and common methodology likely to foster “natural convergence” in the behaviors of member states</p> <p>Whole security approach is the same for the 27 member states, but in practice implementation varies depending on national specificities and market characteristics since the penetration of suppliers in 5G networks varies considerably depending on member states.</p>	<p>Growing culture of co-ordination between EU institutions visible through complementarity of expertise between the Commission and ENISA: ENISA threat landscape mapping as a “further input for the toolbox”.</p> <p>Effective internal coordination within the Commission and between Directorate Generals: Well-coordinated efforts between cabinets, and EU toolbox announced by three Commissioners</p> <p>The same understanding of the security risks shared by European institutions since they worked jointly at all stages of the process, i.e. building on the conclusions of EU coordinated risk assessment, the EU toolbox recommends a set of mitigating measures</p> <p>Smooth coordination among EU institutions: – Commission launched the process right after the European Council called for a concerted approach, and consulted the member states at every stage of the process; – coordinated risk assessment was carried out at multiple levels with the technical support of ENISA’s threat landscape.</p>

Source: Own work, 2020.

of the term. Hence, the European way towards 5G network security is not built on an antagonism with a model or through the reifying of an “otherness” but rather through the positive assertiveness of its model and principles: pragmatism, territoriality, neutrality, and proactiveness.

Pragmatic – Looking at this issue from a more nuanced perspective, we see that the EU approach towards 5G security is based on the rationale that zero risk is impossible and one can learn how to manage it by knowing the factors that increase/decrease the risk. The EU toolbox lists the factors identifying “risk-suppliers” and sets out a common methodology to distinguish trustworthy from untrustworthy partners. One could argue that, by developing such comprehensive screening and joint risk-based approach, the member states together with the EU-level institutions “look at the world

as it is and not as they would like to see it” – in line with the concept of principled pragmatism developed by the former HR/VP Federica Mogherini.

Territorial – Although the EU approach to secure 5G networks can be described as country-neutral (i.e. no mention of country or company), it is still designed in relation to territoriality, in two different ways. First, the toolbox distinguishes European from non-European countries and somehow reifies EU borders by acknowledging the likelihood of a supplier being subject to interference from a non-EU country. Second, the main rationale at the core of the EU’s mode of reasoning is to decrease the vulnerability of the EU to external pressure and strengthen the European sovereignty. Such approach, aimed at reducing the level of dependence of the EU to foreign actors, can be characterised as territorial.

Neutral – The underlying logic of the European approach towards 5G network security remains faithful to the non-discriminatory, rule-based and market-first approach of the EU. The fulfilment of objective criteria and updated security requirements is a prerequisite to access the European market. You follow our rules, you can join the club. Once you violate them, then we kick you out. Good bye. Applicable to everybody regardless of their country of origin and the technology at stake (6G, XG), the European approach is less confrontational than that of other players and aims to retain its openness to trade and its support for a multilateral rule-based order. However, in line with Gstöhl’s transposition of the “weaponisation of trade” concept to the European context (2020), we notice that the EU model is more strategic and understands market instruments as part of a wider comprehensive strategy (here reducing technological dependence and enhancing network security) rather than viewing them in their own logic.

Proactive – By making EU funding conditional on compliance with 5G network security requirements, the EU intends to project internationally and spread its regulatory standards. In line with the concept of “Brussels Effect” (Bradford, 2020), the Commission attempts to externalise its European 5G model by circulating this toolbox to other regions in the world. By doing so, the EU

adopts a proactive approach in order to preserve and project its influence on regulation and standard setting at the global stage.

Main Conclusions

First and foremost, a geopolitical EU takes its roots in the member states’ common awareness and political willingness to act in a collective manner at the European level. In other words, a geopolitical approach is a “whole-EU” approach that embraces the hybridity of the EU polity and is grounded in both intergovernmental and supranational dynamics. Benefiting from the multi-level and neutral nature of a more geopolitical EU, the member states, as part of a “two-level game”, delegated the coordination of a very politically sensitive discussion to a supranational arena that acts in the name of Europe with demanding partners.

Second, being geopolitical does not necessarily mean acting in a geopolitical way. The micro-politics analysis of the European Commission showed that this institution, constrained by national interests with a limited mandate, emerged as a strategic actor by: building on its administrative capacities, depoliticising a national security issue, keeping a hands-off approach, and developing innovative non-binding policy instruments. As a result, it played a key role in the building of the EU-coordinated approach by pushing for convergence and coordination at both the horizontal level (within EU institutions) and the vertical one (between EU institutions and EU members and between member states). In addition, the Commission, through the use of strategic policy tools, managed to put new bold ideas and concepts on the EU agenda while preserving the member states’ feeling of ownership throughout the process.

Third, we demonstrate that the EU can be a geopolitical actor by *putting its own means* to a common end. The assessment of the first common European approach to the security of critical infrastructures shows that the EU, while addressing a new security threat and positioning itself in a context of intensifying power rivalries, remains faithful to its neutrality and openness. The European way on 5G is therefore not shaped in the antagonisation of rivals but through a more pragmatic and territorialised

approach that positively asserts its model and principles. This study indicates the emergence of a geopolitical thinking in the EU strategy and proposes an analytical framework to assess it. In the light of growing *geopoliticisation* of technology and trade, with power rivalries becoming more embedded in low-politics issues, the EU is more likely to gain influence by leveraging its regulatory and market powers.

As for next steps, further in-depth analysis would be needed on the new tools developed at the EU level in other potential strategic sectors where international tensions are likely to arise, especially in what was not so long ago a *dirty word*: the European industrial policy. ■



About the author:

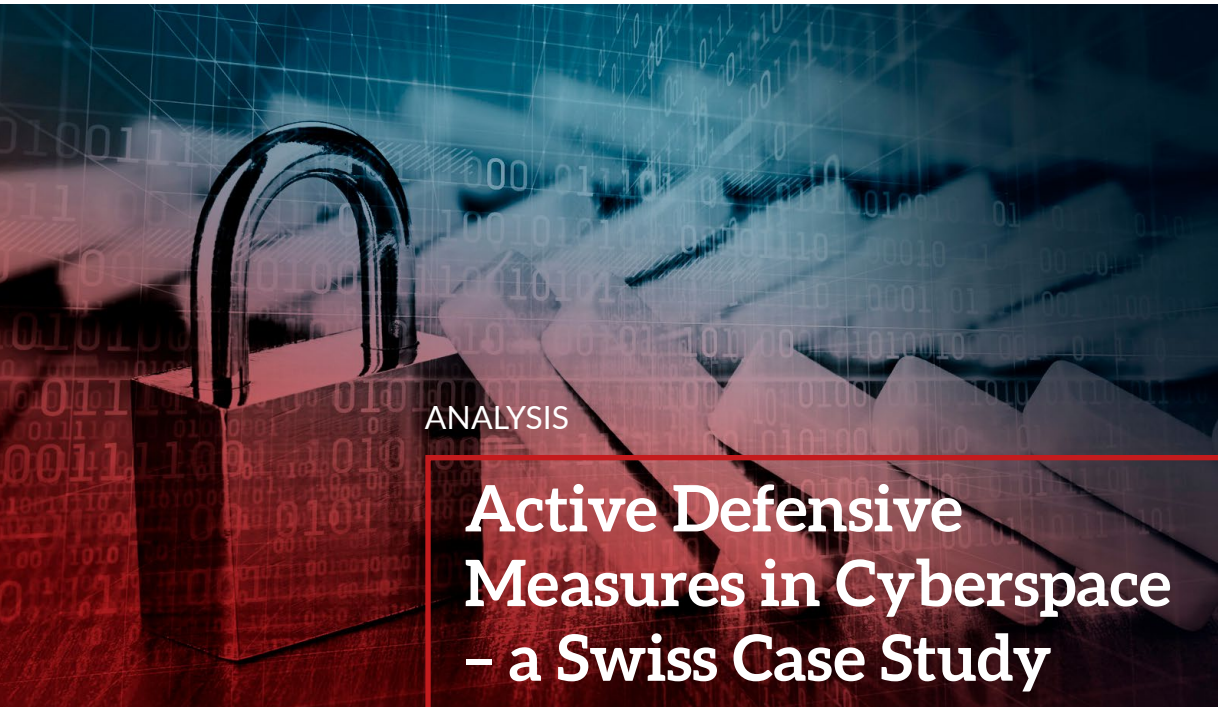
Ségolène Milaire – Postgraduate Student at College of Europe Bruges, Political and Governance Studies Department. She is a graduate of European Studies at Sciences Po Grenoble in France and also studied Political Sciences in Stockholm University. She has a professional experience in public policy at both the national and European levels, supporting ICT companies in their policy activities. Her interests encompass the transformations of security in the digital age and European digital policies.

Research field: Political sciences, Geopolitics, International Relations.

References

- Biscop, S. (2019). *European Strategy in the 21st Century: New Future for Old Powers*, Oxon (Abingdon): Routledge.
- Borell, J. (2019, October 7). A Stronger Europe in the World. *Parliamentary Hearing by the Committee on Foreign Affairs (AFET) of the European Parliament in Brussels*.
- Bremmer, I., & Kupchan, C. (2020). *Top Risks 2020*. Eurasia Group, Retrieved on 24 April 2020 from https://www.eurasiagroup.net/files/upload/Top_Risks_2020_Report_1.pdf.
- Bradford, A. (2020). *The Brussels Effect. How the European Union rules the world*, Oxford UP.
- Cadier, D. (2019). The Geopoliticisation of the EU's Eastern Partnership. *Geopolitics*, 24 (1), 71-99.
- Cattaruzza, A. La construction politique de l'espace numérique. In S. Taillat, A. Cattaruzza, D. Danet. *La Cyberdéfense, Politique de l'espace numérique*. (2018). Armand Colin.
- Carr, B. (2019). Deep dive: How the U.S. is Addressing 5G and Security. *US Department of State*, Retrieved on 28 April 2020 from <https://www.state.gov/deep-dive-how-the-u-s-is-addressing-5g-and-security/>.
- Cerulus, L. (2019, July 25). Q and A with Ericsson boss on 5G security. *Politico*. Retrieved on 23 April 2020 from <https://www.politico.eu/pro/pro-transcript-q-and-a-with-ericsson-boss-on-5g-security/>.
- Cohen, S. B. (2014). *Geopolitics*. 3rd edn. London: The geography of International Relations, Rowman & Littlefield.
- Corry, O. (2011). Securitisation and 'Riskification': Second-order security and the politics of climate change. *Journal of International Studies*, 40(2), 235-258.
- Council. (2019). Council Conclusion on the significance of 5G to the European economy and the need to mitigate security risks linked to 5G, 2019/C 414/03, 2019.
- 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 L 194/1. 2016.
- European Union Agency for Cybersecurity (ENISA). (2019). Threat landscape for 5G networks. Retrieved on 3 May 2020 from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>.
- European Commission. (2019a). Political Guidelines for the next European Commission 2019-2024: A Union that strives for more.
- European Commission. (2019b). Commission recommends common EU approach to the security of 5G networks. *Question and Answers*. Retrieved on 25 April 2020 from https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_1833.

- Featherstone, K., & Radaelli, C. (2003). *Politics of Europeanization*. Oxford: OUP.
- Ghering, T., Urbanski, K., & Oberthür, S. (2017). The European Union as an Inadvertent Great Power: EU Actorness and the Ukraine Crisis. *Journal of Common Market Studies*, 55(4), 727-743
- Grevi, G. (2020, February 3). EU Foreign Policy: Context and Priorities. *Lecture College of Europe*.
- Gros, D. (2019, December 6). What EU Geopolitical Power Will Cost. *Project Syndicate*. Retrieved on 7 May 2020 from <https://www.project-syndicate.org/commentary/eu-geopolitical-commission-economic-power-by-daniel-gros-2019-12?barrier=accesspaylog>.
- Gstöhl, S. (2020). The Geopolitical Commission: Learning the 'Language of Power'?. *College of Europe Policy Brief Series (CEPOB)*. Retrieved on 04 May 2020 from <https://www.coleurope.eu/fr/research-paper/geopolitical-commission-learning-language-power>
- Guarascio, F., Yun Chee, F. (2018, December 7). Europe should be wary of Huawei, EU tech official says. *Reuters*. Retrieved on 4 May 2020 from <https://www.reuters.com/article/us-eu-china-huawei/europe-should-be-afraid-of-huawei-eu-tech-official-says-idUSKBN1O611X>.
- Howorth, J. (2010). The EU as a Global Actor. *Journal of Common Market Studies*, 48(3), 455-474.
- Interview with Emmanuel Macron. (2018). *The Economist*. Retrieved on 6 May 2020 from <https://www.economist.com/europe/2019/11/07/emmanuel-macron-in-his-own-words-english>.
- Kleinhans, J. (2019, February). 5G vs. National Security, A European Perspective. *Stiftung Neue Verantwortung*. Retrieved on 24 April 2020 from https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf.
- Laïdi, Z. (November 2019). Can Europe learn to play power politics? *Centre for European Reform*.
- Lehne, S. (2020). How the EU can survive in a geopolitical age. *Carnegie Europe*. Retrieved on 4 May 2020 from <https://carnegieeurope.eu/2020/02/25/how-eu-can-survive-in-geopolitical-age-pub-81132>
- Mamadou, V., Dujkink, G. (2016). Geopolitics, International Relations and Political Geography: The Politics of Geopolitical Discourse. *Geopolitics*, 11(3).
- Nitoiu, C., & Sus, M. (2019). Introduction: The Rise of Geopolitics in the EU's Approach in its Eastern Neighbourhood. *Geopolitics*, 24(1), 1-19.
- NIS Cooperation Group (2020). EU Toolbox of risk mitigating measures - Cybersecurity of 5G networks.
- NIS Cooperation Group (2019). EU coordinated risk assessment of the cybersecurity of 5G networks.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy (HR/VP). 2019. "EU-China – A Strategic Outlook". JOIN(2019) 5, Brussels, 12 March 2019.
- European Commission. (2016). 5G empowering vertical industries. Retrieved on 3 April 2020 from https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BA_T2_PL.pdf
- European Political Strategy Centre (EPSC). (2019, June 30). Rethinking Strategic Autonomy in the Digital Age (30). Retrieved on 28 April 2020 from https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf.
- Leonard, M., & Esther Franke, U. (2016). *Connectivity Wars: Why Migration, Finance and Trade are the Geo-economic Battlegrounds of the Future*. London: European Council on Foreign Relations.
- Lacoste, Y. (2012). La géographie, la géopolitique et le raisonnement géographique. *Hérodote*, 3(146-147), 14-44.
- Morel, C. (2017, Mars). Les câbles sous-marins: un bien commun mondial ?. *Études*, 3, 19-28.
- Nocetti, J. (2020). *Intervention dans Emission France Culture*. La guerre de la 5G. Retrieved on 12 May 2020 from <https://www.franceculture.fr/emissions/affaires-etrangeres/la-guerre-de-la-5g>.
- Nye, J.S. (2011). *The Future of Power*. New York: Public Affairs.
- Meunier, S., & Nicolaidis, K. (2019). The Geopoliticization of European Trade and Investment Policy. *Journal of Common Market Studies*, 57(51).
- Müller, M. (2010). Doing Discourse Analysis in Critical Geopolitics. *Les théories de la Géopolitique*, 12(3).
- Rühlig, T., & Björk, M. (2020). What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe. *Swedish Institute of International Affairs*. Retrieved on 2 May 2020 from <https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2020/ui-paper-no.-1-2020.pdf>.
- Peel, M., & Warrell, H. (2020, February 14). Nancy Pelosi warns Europe over 5G dangers. *Financial Times*.
- Sanger, D. (2020, February 17). Huawei Is Winning the Argument in Europe, as the U.S. Fumbles to Develop Alternatives. *The New York Times*.
- Sanger, D., & Erlanger, S. (2018, December 18). Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran. *The New York Times*.
- Soler i Lecha, Eduard. (2019). The World in 2020: Ten issues that will shape the global agenda. *Barcelona Centre for International Affairs (CIBOD)*, Notes internacionales.
- von Clausewitz, C. (1918). *On War*. London: Kegan Paul, Trench, Trubner & C.
- White House. (2019, May 15). Executive Order on Securing the Information and Communications Technology and Services Supply Chain.



ANALYSIS

Active Defensive Measures in Cyberspace – a Swiss Case Study

BASTIEN WANNER

RESEARCHER, UNIVERSITY OF LAUSANNE

SOLANGE GHERNAOUTI

PROFESSOR, UNIVERSITY OF LAUSANNE

Introduction

Every four years, Switzerland organises large-scale integrated security exercises (ISE) to test its crisis prevention position and improve the command and control capacities of its national crisis management bodies. In November 2019, the main theme of the 52-hour exercise (ISE19) was the response to a terrorist threat involving a nuclear malfunction and blackmail (Keystone, 2019). Involving around 2,000 people in total, its main objective was to foster and test cooperation and coordination among the various federal departments, cantons, and cities. Under the leadership of the Federal Department of Justice and Police (FDJP) the exercise involved all relevant

federal and local authorities, their emergency task forces,¹ the intelligence services, the armed forces, the national early warning units, and those responsible for strategic communication. While the overall drill focused on terrorism and its implications, this article mainly focuses its analysis on its cyber component. During the exercise, many events occurred through cyberspace. Four critical infrastructures sectors were subject to cyberattacks. Three of these – energy, finance, and transport infrastructures – were private and civilian; the fourth was the Swiss military. Given the scope of the cyberattacks during the exercise, the Swiss policy-makers recognised the need to implement a set of active cyberdefence (ACD) measures, using the ISE19 as an opportunity to test the existing political and legal framework.

¹ The Swiss Security Network (SSN) is a security policy organisation which comprises all federal, cantonal, and communal security policy instruments aimed at coordinating decision-making (SSN, 2020).

This article aims at describing the political structures and legal norms surrounding ACD in Switzerland. With this in mind, we outline the relevant roles, responsibilities, and decision-making processes. Our primary focus is on two legal provisions strengthening Switzerland's overall cybersecurity position: The Intelligence Service Act (IntelSA) and the Armed Forces Act (ArmA). As both provisions were designed to improve Switzerland's capacity to defend against cyberattacks that reach the threshold of national security, their applications have common and distinctive features that demand consideration. First, for both, the scope of application is peacetime. In an armed conflict, the Armed Forces will be on "active service", in which case other legal norms will apply that are beyond the scope of this analysis. Second, both distinguish between types of targets. Is it purely military or civilian? Or were the attacks directed at both types of objectives? Third, each Act determines the political oversight, the agencies responsible, and the conditions necessary for deploying ACD.

Against this background, the paper is structured as follows. After the introduction, the concept and definition of ACD are set out and the relevant legal provisions described. Then, the significant events leading to the current cybersecurity-governing structures in Switzerland are summarised. Alongside the roles and responsibilities of the involved units, their inter-agency collaboration mechanisms will be presented. The core of the article is the case study of the cyber aspects during the ISE19 exercise. In relation to this, various policy options as well as their advantages and limitations are discussed. Finally, we provide recommendations designed to improve the existing Swiss ACD framework.

Given the scope of the cyberattacks during the exercise, the Swiss policy-makers recognised the need to implement a set of active cyberdefence (ACD) measures, using the ISE19 as an opportunity to test the existing political and legal framework.

Swiss Framework for Active Cyberdefence

Before analysing the case study, it is necessary to first define and conceptualise ACD, the pertinent legal framework, and the Swiss cybersecurity governance apparatus.

Definition of Active Cyberdefence

States have come to realise that complementing their cyber defensive positions with active measures improves not only their overall cybersecurity but also and ultimately their national security. Consequently, the last decade has seen the emergence of "active cyberdefence" (ACD) as a cyberdefence concept. Lacking a commonly accepted definition, a number of states (e.g., the USA, the UK), international organisations, such as the Cooperative Cyber Defence Centre of Excellence, and scholars have provided explanations that help qualify ACD. Rosenzweig (2013) describes ACD as the capacity to detect, analyse, and mitigate threats pertaining to cyber. Ducheine and van Haaster (2014) add that it includes "proactive measures launched to defend against malicious cyber activities or attacks". While the related research is still in an inchoate stage, it is gaining traction. At its core, the academic work involves analyses of common ACD features. For example, Denning and Strawser's (2014) *effect-based approach* provides a categorisation of actions based on their intended impacts. One comparative analysis (Wanner and Ghernaouti, 2019) posits that some of the most characteristic features are, inter alia, out-of-own-perimeter activities as well as reactive, direct, and real-time response in the aftermath of an attack. Also common to many definitions are actions that impair, destroy, nullify, or reduce attackers' capacities.

Legal framework of Active Cyberdefence in Switzerland

In Switzerland two legal provisions provide the basis to conduct active cyberdefence: the Intelligence Services Act (IntelSA) (IntelSA, 2020) and the Armed Forces Act (ArmA) (ArmA, 2020). First, Article 37 of IntelSA allows the Federal Intelligence Service (FIS) to infiltrate systems and networks located abroad

if they are used to attack critical infrastructures located in Switzerland. Two cumulative conditions regulate the FIS's mandate to infiltrate systems and networks. First, these systems and networks have to be located abroad. Second, the targeted systems and networks have to be used to attack critical infrastructures located in Switzerland. If these conditions are met and if the Federal Council approves the measure, the FIS has the right to disrupt, impede, and slow the attacker's access to information. According to Article 24 of the Intelligence Service Ordinance (IntelSOrd, 2017), the basis for the Federal Council's decision is a formal request specifying six essential points: the legal field of activity, the type of information sought, the potential third parties, the period in which the measure will be used, the concerned computer systems and networks, and finally, the proposed measure's necessity, proportionality, and risks.

Second, in the event that computer systems and networks of the armed forces are attacked, Article 100 of ArmA authorises the Swiss armed forces to take the necessary measures. These measures may include breaking into any computer systems and networks used to carry out the cyberattacks and disrupting, impeding, or slowing their access to information. Except in the case of active service during a conflict, the Federal Council must decide on the implementation of these measures. The ArmA has recently been reinforced through the Ordinance on Military Cyberdefence (OrdMilCy, 2020), which governs measures to be taken in cyberspace for purposes of self-protection or self-defence in the event of an attack against the Swiss armed forces' computer systems. Like the IntelSOrd, the OrdMilCy lists the conditions under which active cyberdefence actions are to be authorised, namely the purpose of the action, the period during which the action will be conducted, the systems and networks concerned, the maximal number of penetration, the proof of legality (notably its proportionality), and the risks' assessment related to the action in cyberspace.

The Swiss Path toward Cybersecurity

Since the Swiss Federal Council defined cybersecurity as an integral part of its national security position, a series of important milestones in promoting Swiss cybersecurity have been achieved: in 2010 the Swiss government's declaration of its political will to protect Switzerland from cyberrisks marked the inception of a Swiss cybergovernance. In 2012, when the Swiss government adopted its first national cybersecurity strategy (NCS) (FITSU, 2012), it expressed, for the first time, a vision regarding Swiss cybersecurity. Furthermore, the NCS defined roles and responsibilities of governmental agencies and established a set of measures to improve cybersecurity both nationally and internationally. At the core of the NCS was a decentralised approach, according to which each Federal Department would lead the implementation of particular measures. In 2018, the second cybersecurity strategy (FITSU, 2018) followed suit. Based on a whole-of-government approach, it defines, for the first time, three areas of governmental work: cybersecurity, cyberdefence, and law enforcement. In response to increasing political demands to adopt a stronger, more centralised approach to deal with cyberrisks, the Federal Council appointed a Federal Cybersecurity Delegate on 14 June 2019.

Federal Governance

In addition to representing the Swiss Confederation in other governmental agencies, the Federal Cybersecurity Delegate is in charge both of strategic management of cybersecurity and of IT security guideline development for the Federal Administration. He is also the head of the National Cybersecurity Center (NCSC) launched on 1 July 2020 with the Ordinance on Protecting against Cyberrisks in the Federal Administration (OrdPCy, 2020). The NCSC serves, inter alia, as the national point of contact for questions related to cyberrisks and cyberincidents. It integrates the national Computer Emergency Response Team (GovCERT) and takes over operational incident management in the event of severe cyberincidents (GovCERT, 2020).

Roles and responsibilities within the Federal Department of Defence pertaining to cyberdefence

The General Secretariat of the Federal Department of Defence, Civil Protection and Sport (DDPS) supports the Head of the Department both in managing the Department and as a member of the Federal Council. It includes two units that deal with cybersecurity related matters: the division Cyber, Information Technology and Information Security (CII) and the Security Policy Division (DDPS, 2020). The CII entrusted the Cyberdefence unit with managing and coordinating cyber related activities and strategic cyber development in the Department. The Security Policy Division heads the development of security policy in the Department and supports the Head of the DDPS in all national and international matters relating to security and defense policy and in the development, formulation, and management of initiatives implemented by the DDPS's administrative units.

The Federal Intelligence Service (FIS) is a Swiss security policy instrument. Its mission² is to prevent threats that could derive from terrorism, violent extremism, espionage, the proliferation of weapons of mass destruction and their delivery systems as well as cyberattacks against Swiss targets such as critical infrastructures. Furthermore, the FIS is in charge of assessing the situation on behalf of the decision-makers. Its *raison d'être* lies in prevention and early detection. According to the NCS and its implementation plan, the FIS has two units designed to prevent cyberattacks from undermining Swiss interests and critical infrastructures (FITSU, 2019). First, the cyber FIS is responsible for identifying and attributing state-sponsored cyberattacks (measure 22, NCS). Second, the FIS manages the Operation and Information Centre (OIC) – the intelligence part of the Reporting and Analysis Centre for Information Assurance (MELANI). It provides situational awareness in cyberspace and assesses the overall cyber-threat landscape (measure 4, NCS).

² Defined in Art. 6 of the Federal Act on the Intelligence Service (IntelSA).

The Swiss armed forces (SAF) offer the last line of cyberdefence. In compliance with their constitutional responsibilities,³ the SAF should ensure their operational readiness across all situations in cyberspace (measure 24 NCS). They should have sufficient means, resources, and capabilities to face any extraordinary situation in cyberspace. In addition, as a strategic reserve, they can support, on a subsidiary basis, the civilian authorities (FITSU, 2018). They are led by the Chief of the Armed Forces (CAF). The Armed Forces Staff (AFS) support the CAF in military-strategic work. This constitutes the interface between the armed forces and the strategic political level (SAF, 2020). As the Military-Strategic Staff (MSS) translate political will into military-strategic directives, they control the operational level. Following their directives, the Joint Operations Command (JOC) is responsible for planning and leading all SAF missions and operations at the operational level (SAF, 2020). JOC staff also ensure operational readiness and overall military situational awareness, triggering and coordinating the necessary measures to react to a specific security event. The Command Support Organisation (AFCSO) provide the essential Information and Communications Technologies (ICT) and electronic operations services for the SAF. With the Centre for Electronic Operations (CEO), the AFCSO provide permanent services in electromagnetic, cyber, and cryptology matters (SAF, 2020).

Concerning the capability to deploy ACD and according to the legal provisions (IntelSA and ArMA), measure 23 of the NCS requires the DDPS (FIS and Armed Forces) to have sufficient qualitative and quantitative competencies and capacities to disrupt, impede, or slow down attacks on critical infrastructures.

Inter-agency collaboration

The Security Core Group is responsible for the coordination of national security issues. It is composed of the FIS Director, the State Secretary of the FDFA,

³ Art. 58 of the Federal Constitution of the Swiss Confederation: The armed forces serve to prevent war and to maintain peace; they defend the country and its population. They shall support the civilian authorities in safeguarding the country against serious threats to internal security and in dealing with exceptional situations.

the Director of the Federal Office of Police (fedpol) and a representative of the Security Policy Division (DDPS).

In July of 2020, the Federal Council established three overarching interdepartmental units to coordinate cyber related decisions (OrdPCy, 2020). The *Federal Council Cyber Committee* consists of the heads of three Federal Departments: Finance (FDF), Justice and Police (FDJP), and Defence, Civil Protection and Sport (DDPS). The *Cyber Core Group* helps coordinate matters of cybersecurity, cyberdefense, and cybercrime. It is composed of the Federal Delegate for Cybersecurity, the fedpol Director, a member of the DDPS, and a representative of the cantons. It provides cyberthreat assessments and supervises the handling of severe and interdepartmental incidents. And the *NCS Steering Committee* – consisting of representatives of the Confederation, cantons, business community, and universities – guides the ongoing development of the NCS.

Case Study

Setting the scene – Scenario ISE19

A fictitious terrorist group, the “Global Liberation Front” (GLF), mounted a set of attacks on Swiss interests in Geneva in 2017. In addition to threatening to bomb the airport, it bombed a train station, resulting in heavy casualties, and assaulted the headquarters of the United Nations, taking numerous hostages. Three members of the GLF were arrested and are awaiting trial in the Federal Criminal Court in Bellinzona in November of 2019. In the run-up to the lawsuit, the situation escalated following the GLF’s attempts to disrupt and ultimately to subvert the trial: spreading propaganda, political blackmail, manipulation of media, acts of sabotage, and cyberattacks against critical infrastructures. In a video, the GLF claimed responsibility for these actions and threatened to continue to terrorise Swiss society unless the prisoners were immediately released. Against this backdrop, the armed forces were called to provide subsidiary support to the cantons and the confederation with military personnel.

According to this scenario, the main event occurred on 8 November 2019, when the GLF attacked the Zurich station, with its members indiscriminately opening fire and detonating a bomb in the main hall. This course of action led to more than numerous casualties. As a result, the Swiss national crisis management apparatus was triggered. In parallel to the assault on Zurich station, cyberattacks were carried out, presumably from abroad, by entities of a foreign power known to sympathise with the terrorist organisation. In fact, the cyberattacks targeted various critical infrastructures across multiple sectors. Three major financial companies were hit by ransomware, along with one national and two important local cantonal banks. Within the transport sector, the federal railway and the air navigation service provider were also hit. A critical tipping point was reached when two energy providers were impaired due to cyberattacks. As one of the potential outcomes could have been an overall nationwide power outage, the risk of massive loss of lives became real. Moreover, the armed forces reported problems with their command and control systems, particularly affecting the air force.

Policy Options

The situation rapidly deteriorated. Domestic security was critically threatened, as both the Cantonal and the Federal levels were impaired: critical infrastructures failed to provide vital services; there was civil disarray and furthermore the armed forces were on the brink of being unable to fulfil their mission. As the crisis unfolded and escalated to the level of a national security concern, the head of the DDPS asked the federal authorities to formulate both civil and military policy options – the ultimate goal being to regain control of the situation by stopping the ongoing attack and preventing further casualties. At the core of all policy options was the FIS’s identification of the attacker and its attack vectors. The FIS had verified reports that the cyberattacks against Swiss interests were being launched through a technical university located abroad, namely in the terrorist group’s country of origin.

Three separate response options were developed and presented in such a way that they ranged from the least invasive to the most offensive. The first proposed penetrating foreign computer systems and networks with the sole objective of retrieving further information on the ongoing terrorist threat. Based on Art. 37 para. 2 of IntelSA, the head of the DDPS could, having consulted the heads of the FDFA and FDJP, authorise the FIS to conduct such a measure. The second option entailed the penetration of the foreign computer systems and network in order to disrupt, impede, or slow down their access to information. Since this response would constitute a more invasive action, it would necessitate the approval of the Federal Council (Art. 37 para. 1 IntelSA). The third option would require the armed forces to take action. Pursuant to Art. 100 para. 1 let. c of ArmA, the SAF would be authorised to penetrate foreign computer systems and computer networks, aiming to disrupt, impede, or slow down their access to information. The fourth option would have combined option 2 and 3. As this would have envisaged a joint action of the FIS and the SAF, it would have created an additional layer of coordination. Because of this added complication, this possibility was immediately discarded.

Advantages and Limitations of the Policy Options

The advantage of applying Art. 37 para. 2 of IntelSA is that this measure can be implemented very swiftly and bears manageable risks. Furthermore, this active cyberdefence action would only require the consultation of two heads of departments (FDFA and FDJP). Their official approval is, however, not necessary in order to conduct computer network exploitation (CNE). As a matter of fact, the political oversight for Art. 37 para. 2 of IntelSA is dependent upon the authorisation by the head of one department and thus in the hands of one decision-maker only, namely the head of DDPS, leaving this minister a greater leeway. On the downside this policy option is by far the least effective and can be characterised as a toothless tiger. In fact, CNE would not be enough to regain control of the situation as its primary purpose is to collect further information on the cyberattack rather than

making the malicious cyberoperation cease. Quite on the contrary, it is highly likely that if this policy response had been opted for, the cyberattacks targeting Switzerland would have continued.

Building upon the first policy option, Art. 37 para. 1 of IntelSA allows for an additional level of activeness and envisages a further degree of invasiveness. Clearly, this option could have the highest impact on the ongoing attack as slowing down, impeding, or disrupting the adversary's computer systems and networks could have the potential to cease the attack at its source. The added value of applying Art. 37 para. 1 lies in its civilian nature. Given that the majority of the Swiss targets are privately owned and civilian critical infrastructures, it is proportionate to respond through a civilian authority, namely the FIS. One of the disadvantages of this second policy option is its potential for escalation since it constitutes a breach of integrity of a foreign computer system. It is important to underscore that this option necessitates the approval of the Federal Council; it has to be green-lighted by seven heads of departments. While this procedure is an important check and balance and constitutes a crucial political oversight, it is time consuming, which in turn could stall the triggering of the countermeasure.

The third policy option, carried out by the SAF, is based on Art. 100 ArmA. It shares a common advantage with the second policy option, namely the potential of cessation of the attack. One could also argue as advantageous that the SAF, a military organisation, would have the highest deterrent effect. However, one important drawback is the high potential for inadvertent escalation: Responding by a military unit could lead to considerable detrimental political implications and provoke retorsion, retaliation, and even a military reaction. In addition, authorising the SAF to penetrate a foreign computer system and network could be considered disproportionate compared to the harm caused by the cyberattack against Switzerland itself. According to the scenario, the SAF was one among many targets. Therefore, it is reasonable to believe that the SAF was not the primary objective of the campaign. By

comparing the second and the third option, the choice between those two is, after all, primarily a choice of leadership for the implementation of the action. Delegating the leadership to a civilian authority undoubtedly corresponds to the nature of the threat itself, thereby limiting the response to the national level. If the SAF is chosen to be the executor of this measure, the decision-makers need to bear in mind that they would automatically turn the internal threat into one of external security, thereby externalising the problem and making it an international issue.

Taking everything into consideration, the advantages of the second policy option outweigh the limitations and disadvantages of the first and the third policy. The second policy option has the highest potential to reach the goal, which is for the ongoing cyberoperations to cease while at the same time managing the political risks. Thereby, the Federal Council was recommended to pursue with the ACD measures based on Art. 37 para. 1 IntelSA. Consequently, the Federal Council was advised to authorise the FIS to conduct the countermeasure against the technical university located abroad, drawing on military resources if necessary.

Discussion

The national cybersecurity strategies adopted in 2012 and 2018 have laid the foundation for an active cyberdefence framework. Active cyberdefence has become one important element of larger strategic considerations for Swiss cybersecurity and ultimately national security. Based on the political will conveyed therein, the Swiss Federal Council complemented the political framework by two legal provisions, the IntelSA and the ArmA. Both Acts define the rights and obligations of governmental authorities as well as their restrictions and their political oversight.

Furthermore, for the deployment of ACD, a number of principles as set out in the respective Ordinances are defined, that is the principles of necessity and proportionality. Moreover, the risks of the measure itself need to be described and analysed.

The principle of necessity is crucial, as ACD should be considered the last resort, when all other measures have been exhausted. Also, ACD should pursue the purpose of mitigating a specific threat rather than an act of retaliation. Consequently, and given the situation as presented during the exercise, the intrusion into the computer systems and networks of the technical university is considered the only course of action that will lead to a halt of these cyberattacks within a reasonable period of time. Since Switzerland was in a state of emergency, it seemed unlikely that criminal law was enough to counter this threat. In addition, the diplomatic channels had also been unsuccessful in preventing further malicious activities targeted against Switzerland. Therefore, the criterion of necessity by exhausting all other means was met.

The second criterion, proportionality, guides the course of actions. Proportionality means that the effect and harm caused are proportionate to the benefits gained. With respect to proportionality, the technical university located abroad which will be the target of ACD, does not constitute a comparable critical infrastructure to the targets attacked in Switzerland which are vital to the functioning of Swiss society.

By applying ACD there is in particular one risk to be taken care of. Switzerland could run the risk that the country – that has been subject to its ACD – could also respond with countermeasures, thereby increasing tensions between the two countries.

The Federal Council has adopted a series of structural and organisational decisions to render cybersecurity and cyberdefence more effective. The nomination of the Federal Delegate for Cybersecurity, the establishment of the Cyber Core Group and the NCSC are milestones to improve the overall Swiss capacities to mitigate cyber risks. Inter-agency coordination and national collaboration are at the core of these decisions aimed at promoting a coherent and consistent cybersecurity and cyberdefence policy.

However, the ISE 19 exercise illustrated one thing in particular: while the structures and agencies were established and do exist, the processes and

the inter-agency collaboration for decision-making still need to mature. During the exercise and as the crisis unfolded, it remained unclear for a while which collaboration platform to use to formulate the policy options: either the Security Core Group or the newly established Cyber Core Group.

After a while of hesitation, the choice was made to coordinate a response through the Security Core Group. The main argument being that cyber is an integral part of a wider and much broader national security matter. Interestingly enough, the Federal Delegate for Cybersecurity was invited to the meetings of the Security Core Group in order to put forth the situational awareness pertaining to cyber. Another interesting fact is that the Security Policy Division within the Secretariat General of the DDPS was involved in the formulation and development of the policy options. The newly established Cyber, Information Technology and Information Security (CII), however, had no say during the decision-making process. One could ask the question whether the newly established units (CII) and structural platforms (Cyber Core Group) are ideal to handle cyberoperations of such a scale. It remains to be seen whether their initial purpose, which is to deal with cybersecurity in a dedicated manner, will prevail or whether the decision-makers will take a step back and integrate cyber into overall national security structures.

Another complexity in coordinating a response was the experts' involvement. While the experts representing the civil governmental units (FIS, fedpol and FDFA, and the Federal Delegate for Cybersecurity) had a crucial say in the decision-making process, the experts from military agencies were not implicated. In fact, there was not only a lack of involvement but also of information sharing between the strategic and the operational levels. The strategic level, the Security Policy Division (DDPS) directly collaborated with the Military Strategic Staff. Unfortunately, the MSS never reached out to the operational level even though the operational level was directly impacted by the cyberattacks. The irony of the exercise is that the Joint Operations Command (JOC) developed with the Armed Forces Command Support

Organization (AFCSO) a formal request for support in order to counter the attacks impacting the operational readiness of the Armed Forces. While this request was finalised, the official policy options had already been formulated without informing, let alone implicating these units.

ISE 19 illustrated one thing in particular: while the structures and agencies were established and do exist, the processes and the inter-agency collaboration for decision-making still need to mature.

Recommendations

Exercises are ideal playgrounds to test existing structures, procedures, and inter-agency collaboration. ISE 19 has allowed Switzerland to scrutinise the established framework for ACD and to consider political norms, legal provisions, and their implementation. The exercise served as a case study enlightening the advantages and limitations of the existing framework. Furthermore, the ISE19 highlighted the gaps that need to be addressed. The first recommendation is thus to continue using exercises as a tool to improve cybersecurity.

The second recommendation refers to the policy options. In our view, CNE as outlined in the first policy option does not constitute a real option. It was clear from the outset that CNE is insufficient to handle the cyberattacks at this stage of the crisis as an immediate impact is needed to regain control of the situation. However, information collection on the target is an integral aspect of ACD. As such, it is the first step to be able to conduct an active cyber defensive measure. As a matter of fact, CNE needs to be authorised as soon as possible once the state of emergency has been declared.

The third recommendation addresses the need for the early involvement of expert level. The collaboration between the strategic and operational level both within the civilian and military units is a *conditio sine qua non*. From the very beginning, cyber-experts have to advise the decision-makers. This is all the more important given the recent emergence of cyber as a security policy issue and due

to the fast-evolving domain. Senior level decision-makers rarely have the specific in-depth knowledge that cyberthreats require.

The fourth recommendation relates to the risk identified that the ACD could provoke an even harsher response of the state from which the initial attack was launched. It is recommendable to consider ACD only if the state is at the disposal of a robust and strong defensive posture – both politically and technically speaking – in order to be ready to absorb a reaction. Otherwise, the ACD could backfire. This in turn underscores the necessity to implicate experts from various disciplines as soon as possible.

Fifth, time is of the essence! Given that time is a critical factor, the decision-making process needs to be designed in such a way that it allows for a swift and adequate response. While the checks and balances through political oversight are crucial, they can slow down an effective response. This is a real challenge because of the decentralised approach to cybersecurity. As many actors and units deal with cybersecurity, coordination of all involved agencies needs to be well established in order to not lose time.

Sixth, the service provider necessary to deploy ACD remains the same independently of whether Art. 37 IntelSA or Art. 100 ArmA is applied. However, it is important to understand that this service provider is institutionally part of the Swiss Armed Forces. Therefore, another recommendation would be to have two separate units, one integrated in the civilian and the other in the military organisations.

The seventh and last recommendation is designed to avoid duplications. Cyber is not a distinct security threat. As such, cyber should be integrated in existing structures and processes rather than being dealt with in parallel units, such as the Cyber Core Group. Consequently, it would be advisable to invite the Federal Delegate for Cybersecurity to the Security Core Group as a permanent member.

Conclusion

For the first time, the 2019 Integrated Security Exercise (ISE19) tested Switzerland's legal and political instruments' combined capacity to introduce active cyberdefence measures against ongoing sophisticated cyberattacks targeting critical Swiss infrastructures. The ISE19 served as a case study, allowing governmental, civilian, and military actors to juxtapose two legal Acts: the IntelSA and the ArmA. It also both underscored ACD's utility and demonstrated its validity and value to decision-makers who manage a crisis entailing cyberaspects.

At the same time, it exposed areas in need of improvement. Among these is the involvement of experts as rapidly as possible to advise policy-makers on highly complex and fast-evolving matters. Given Switzerland's federal political system and its decentralised approach to cybergovernance, inter-agency coordination is key.

Therefore, it is vitally important for decision-makers at all levels to become acquainted and familiarised with the roles and responsibilities of each cyber related unit. As cybersecurity has recently emerged as a domain of national security and international relations, states have created new procedures and new structures to govern cyber. From our standpoint, the exercise raised one particularly important question: to what extent, if any, has the development of additional dedicated cyberstructures – currently sitting alongside the national security apparatus – brought about real added value? The ISE19's most striking outcome was its illustration of how integral cyber is to wider national security understanding and thus of how it needs to be managed within existing national security governance structures.

In a crisis, speed is a critical factor for success. This is all the truer in cyber, where reaction time crystallised as a determinant element for an effective response to cyberattacks. The exercise also underscored the importance of short communication lines, and simple, efficient decision-making process involving the right experts.

In a crisis, speed is a critical factor for success. This is all the truer in cyber, where reaction time crystallised as a determinant element for an effective response to cyberattacks.

Concerning the two new legal provisions, the exercise highlighted that they are basically identical regarding their intended impact. Their main difference is whether leadership is civil or military. In fact, it is highly likely that policy-makers will,

during peacetime, consider Art. 37 of the IntelISA the only manageable option. The underlying rationale is that a sophisticated cyberattack will most likely never impact the SAF alone, i.e., without also affecting diverse other national security interests. Therefore, the SAF could hypothetically be considered a critical infrastructure and thus, concerning ACD decision-making, fall under the auspices of the Intelligence Service Act. If this perception prevails, the provisions of the Armed Forces Act and the Ordinance on Military Cyberdefence for ACD would be solely aimed at deterrence. ■

About the authors:



Bastien Wanner is completing his doctoral research in information systems at the University of Lausanne. His research focuses on cyberdefence, competitive intelligence, and IT security. With more than 10 years' experience working in cybersecurity and cyberdefence, he has, inter alia, participated in a range of multilateral European and NATO exercises and workshops on cyberoperations. He worked as an IT auditor, cyber security & operational risks consultant in the financial sector in Geneva and Zurich. He holds a BSc in Business Administration and a LLM in Legal Issues, Crime and Security of Information Technologies. He is a cyberdefence practitioner within the Federal Department of Defence, Civil Protection and Sport (DDPS). In 2015, he was a member of the first Swiss winning team which participated in the international cyberpolicy competition Cyber 9/12 Student Challenge in Geneva. He is reservist general staff officer of the Swiss Armed Forces.



Dr. Solange Ghernaouti, director of the Swiss Cybersecurity Advisory and Research Group, professor of the University of Lausanne, is an independent cybersecurity advisor, an influential analyst, and a regular media commentator. She has authored more than 300 publications and thirty books including *Cyber Power: Crime, Conflict and Security in Cyberspace* (translated into Mandarin). She is Chevalier de la Légion d'honneur, Member of the Swiss Academy of Sciences and has been recognised by the Swiss press as one of the outstanding women in professional and academic circles.

References

- Bonetti, U. (2019, June). „Global Liberation Front“ – oder lieber doch nicht... Retrieved from: <https://www.ogb.ch/aktuelles/13-blog/57-global-liberation-front-oder-lieber-doch-nicht.html>
- Carrel, L. F. (2005). "Epidemic in Switzerland": Description of a strategic leadership exercise by the Swiss Government. *Journal of contingencies and crisis management*, 13(4), 170-175.
- Denning, D. E., & Strawser, B. J. (2014). Active cyber defense: Applying air defense to the cyber domain. *Cyber Analogies. Calhoun: The National Postgraduate School (NPS) Institutional Archive*.
- Ducheine, P., & Van Haaster, J. (2014, June). Fighting power, targeting and cyber operations. In *2014 6th International Conference On Cyber Conflict (CyCon 2014)* (pp. 303-327). IEEE.
- Federal Constitution of the Swiss Confederation. (2020). Retrieved from <https://www.admin.ch/opc/en/classified-compilation/19995395/index.html>
- Forster, C. (2019, 31 October). Angriff auf AKW Beznau, erschossener Berner Regierungsrat: Die Schweiz probt eine Terror-Notlage. *Neue Zürcher Zeitung (NZZ)*. Retrieved from: <https://www.nzz.ch/schweiz/schweizer-behoerden-ueben-fuer-eine-terroristische-bedrohung-ld.1518945?reduced=true>
- Keystone. (2019, 31 October). Can Swiss authorities deal with terrorist attacks? Retrieve from https://www.swissinfo.ch/eng/be-prepared_can-swiss-authorities-deal-with-terrorist-attacks-/45338452
- Laubacher-Kupat, E. (2018). Erfahrungen und Lehren der Strategischen Führungsübung 2017 (SFU 17). *Military Power Revue der Schweizer Armee*. Bern, Switzerland. Retrieved from: https://www.vtg.admin.ch/content/vtg-internet/de/media/publikationen/military-power-revue.download/vtg-internet/de/publications/military-power-revue/_80_024_MPR_2-18_KOMPLETT.pdf
- Rosenzweig, P. (2014). International law and private actor active cyber defensive measures. *Stan. J. Int'l L.*, 50, 103.
- Rosenzweig, P., Bucci, S. P., & Insera, D. (2017). Next Steps for US Cybersecurity in the Trump Administration: Active Cyber Defense. *Backgrounders*, (3188), 11.
- Swiss Armed Forces (SAF). (2020). Armed Forces Command Support Organisation. Retrieved from <https://www.vtg.admin.ch/en/organisation/afcs.html>
- Swiss Armed Forces (SAF). (2020). Armed Forces Staff (AFS). Retrieved from <https://www.vtg.admin.ch/en/organisation/armed-forces-staff.html>
- Swiss Armed Forces (SAF). (2020). Joint Operations Command. Retrieved from <https://www.vtg.admin.ch/en/organisation/kdo-op.html>
- Swiss Armed Forces (SAF). (2020). Principes relatifs aux engagements subsidiaires de sûreté de l'armée. Retrieved from <https://www.vtg.admin.ch/fr/actualite/engagements-et-operations/sse.html>
- Swiss Cyber Experts (SCE). (2020). Retrieved from <https://www.swiss-cyber-experts.ch/en-gb>
- Swiss Federal Council. (2018). Auswertungsbericht Strategische Führungsübung 2017 (SFU 17). Bern, Switzerland. Retrieved from: https://www.bk.admin.ch/dam/bk/de/dokumente/strategische-fuehrungsunterstuetzung/strategische_fuehrungsuebung/Auswertungsbericht%20SFU%2017%20-%20DE%20-%20definitiv.pdf.download.pdf/Auswertungsbericht%20SFU%2017%20-%20DE%20-%20definitiv.pdf
- Swiss Federal Department of Defence, Civil Protection and Sport (DDPS). (2020). Administrative units. Retrieved from <https://www.vbs.admin.ch/en/ddps/organisation/administrative-units.html>
- Swiss Federal Department of Defence, Civil Protection and Sport (DDPS). (2020). General Secretariat. Retrieved from <https://www.vbs.admin.ch/fr/ddps/organisation/unites-administratives/secretariat-general.html>
- Swiss Federal Department of Defence, Civil Protection and Sport (DDPS). (2020). Federal Intelligence Service. Retrieved from <https://www.vbs.admin.ch/en/ddps/organisation/administrative-units/intelligence-service.html>
- Swiss Federal Department of Defence, Civil Protection and Sport (DDPS). (2020). Exercice du Réseau national de sécurité 2019 (ERNS 19). Retrieved from <https://www.vbs.admin.ch/fr/themes/politique-securite/exercice-reseau-national-securite-2019.html#documents>
- Swiss Government Computer Emergency Response Team (GovCERT). (2020). Retrieved from <https://www.govcert.admin.ch/>
- Swiss Security Network (SSN). (2020). The Swiss Security Network. Retrieved from <https://www.svs.admin.ch/en/home.html>
- Switzerland Federal Assembly. (2020). *Federal Act on the Armed Forces (ArmA)*. Bern, Switzerland. Retrieved from <https://www.admin.ch/opc/fr/classified-compilation/19950010/index.html>

Switzerland Federal Assembly. (2020). Federal Act on the Intelligence Service (IntelSA). Bern, Switzerland. Retrieved from <https://www.admin.ch/opc/en/classified-compilation/20120872/index.html>

Switzerland Federal Council. (2017). *Intelligence Service Ordinance (IntelSOrd)*. Bern, Switzerland. Retrieved from <https://www.admin.ch/opc/fr/classified-compilation/20162430/index.html>

Switzerland Federal Council. (2020). *Ordinance on Military Cyberdefence (OrdMilCy)*. Bern, Switzerland. Retrieved from <https://www.admin.ch/opc/fr/classified-compilation/20182319/index.html>

Switzerland Federal Council. (2020). *Ordinance on Protecting against Cyberrisks (OrdPCy)*. Bern, Switzerland. Retrieved from <https://www.admin.ch/opc/fr/classified-compilation/20200291/index.html>

Switzerland Federal IT Steering Unit (FITSU). (2012). *National Strategy for the Protection of Switzerland against Cyber Risks 2012-2017*. Bern Switzerland. Retrieved from https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie-2012.html

Switzerland Federal IT Steering Unit (FITSU). (2013). *National Strategy for the Protection of Switzerland against Cyber Risks 2012-2017 – NCS implementation plan*. Bern Switzerland. Retrieved from https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie-2012/umsetzungsplan-ncs-2012.html

Switzerland Federal IT Steering Unit (FITSU). (2018). *National strategy for Switzerland's protection against cyber risks (NCS) 2018-2020*. Bern, Switzerland. Retrieved from https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie.html

Switzerland Federal IT Steering Unit (FITSU). (2019) *Implementation plan for the 2018-2022 national strategy for the protection of Switzerland against cyber risks (NCS)*. Retrieved from https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/umsetzungsplan.html

Switzerland National Cyber Security Center (NCSC). (2020). The National Cyber Security Centre. Retrieved from https://www.melani.admin.ch/melani/en/home/ueber_ncsc/das_ncsc.html

Wanner, B., & Ghernaouti, S. (2019). Conceptualizing Active Cyber Defence in Cyber Operations: Quo Vadis, Switzerland?. *St Antony's International Review*, 15(1), 58-82.





ANALYSIS

Social Media at War. The Case of Kurdish Fighters and Their Impact on the Perception of the On-Going Anti-ISIS Conflict in Western Countries

GINEVRA FONTANA

PROJECT ASSISTANT, ITALIAN MILITARY CENTRE FOR STRATEGIC STUDIES

Introduction

In this paper, I aim to analyse the situation of fighters joining Kurdish anti-ISIS forces (hereby called foreign as they come from Europe) through their social media narrative. By following the social media presence and actions of three Europeans, I explore the current jurisprudence in connection with the Kurdish struggle. Proceeding from an analysis of the three possible cases stemming from real case studies, I carry out a theoretical exercise of possible prosecution outcomes if national authorities were to bring their “careers” to the attention of national courts. Since the outburst of the anti-ISIS conflict in the majority-Kurdish areas of Iraq and Syria in 2014, foreign pro-Kurdish fighters’ self-representation on their personal social media

accounts has had an astonishing impact on the portrayal and perception of the conflict in Western countries. Therefore, the use of social media by the fighters proves to be a source of not only information, but also polarisation – and a primary source for future conflict studies. The use of technology has never been so pervasive as in our times; social media are therefore not only part of our daily lives, but actively contributing to our perception of the world – including conflicts located thousands of kilometres away.

The use of social media by the fighters proves to be a source of not only information, but also polarisation – and a primary source for future conflict studies.

Research Gap

“Terrorism” has begun to be considered more and more as an international issue after the 9/11 attacks (Saul, 2015) – a wake-up call for many in the international community, bringing to the forefront of the discussion the question of a now-internationalised, trans-national terrorist threat. Yet, international terrorism is no novelty (Goldie, 1987; Krähenmann, 2015). There also happens to be another skewed perception concerning the terrorist threat post-2001: that it is inherently intertwined with Islamic extremism (Marone & Vidino, 2018; Scheinin, 2015). This is clearly reflected in the research carried out in the past 19 years, the majority of which has focused on Islamic extremist groups. Although this may be explained in more utilitarian terms – research is carried out in fields where funds are supplied, and the interest spike in Islamic extremist terrorism has channelled spending towards analyses on the topic – this still does not exhaustively explain why certain acts are perceived as clearly criminal if carried out by Islamic extremists, and not if executed by people linked to different ideologies (Bech Gjørsv et al., 2012; Marone & Vidino, 2018). The same notion appears in the context of *foreign fighters* (Bakker & Singleton, 2016): even though the research is muddled by the hard-to-discern circumstances in which the phenomenon develops, it is undeniable that in the past six years it has specifically focused, nearly exclusively, on foreigners – especially from Western countries – joining ISIS in Iraq and Syria. Some studies (Higgins, 2004; Kraehenmann et al., 2014; Marone & Vidino, 2018; Zelin, 2013) have incidentally touched upon the foreign fighters that have joined Al-Nusra and other Islamic extremist groups in the area, but only a few mentioned the fact that there were foreign nationals joining the Kurdish resistance and even less has been written on the topic (Ahmad, 2014; Marone & Vidino, 2018; Tuck et al., 2016). Without the presumption of being able to compile an extensive or final research on the subject – which is extremely wide and should be the focus of in-depth studies by more experienced authors – I would like to anyway add this personal

contribution to the question of foreign nationals joining the Kurdish forces fighting in Northern Syria and Iraq.

Contextual Background: the situation in Syria and Iraq – a brief outline

An attempt at explaining the full extent of the conflict(s) in Syria and Iraq would far exceed the objective of this paper, if only by length. The current situation in the area is rendered particularly complicated by the intertwining of a myriad of different factions at play, both local and international. Before the Syrian Civil War, the autonomous and oil-rich region of Iraqi Kurdistan (populated mostly by Kurds) was heading towards a referendum on the status of the city of Kirkuk (Frantzman, 2015; Romano, 2007) that, according to the post-US invasion Iraqi constitution, was supposed to be held no later than 31 December 2007. The population was composed of Kurds, as well as Turkmen, Yazidis and Christians – alongside other ethnic and/or religious minorities – and had suffered different Arabisation policies, most recently under Saddam Hussein’s regime. In Syria, most Kurds lived in the Al-Hasakah governorate, in the north-eastern tip of the country, an oil-rich area which did not enjoy any special status based on its ethnic composition; in early 2011, protests against Bashar al-Assad’s regime broke out as the Arab Spring revolutions surged. A rebellion ensued, and in 2012 the independence of Western Kurdistan was announced. Meanwhile, in the same areas, ISIS expanded its territorial influence – and in 2014, Abu Bakr al-Baghdadi proclaimed the Caliphate in Mosul’s Al-Nuri mosque (Callimachi et al., 2018). For the next five years, NATO and Kurdish forces fought strenuously to regain control over the territory that ISIS had captured since the Arab Spring (Peçanha & Watkins, 2015) – with the last stronghold, the city of Baghouz in Syria, capitulating in March 2019 (Wu et al., 2019). Although this latest victory compelled US President Donald Trump to declare ISIS “defeated”, the group still exists, with sleeper cells still being sought out in the area by forces of the International Coalition for Operation Inherent Resolve and its local allies (Lister, 2019). It is clear that the fight against ISIS

has blurred the borders between northern Iraq and northern Syria, therefore dissolving those between the Kurdish groups' areas of involvement: these are the areas that have been most involved in the struggle against ISIS, with Mosul, Raqqa, Kirkuk, Afrin, Baghouz, and Sinjar becoming sadly symbolic.

Methodology

This contribution presents a summary of the findings stemming from an individual research project that has been continuously carried out since 2017. The author has monitored, copied, and catalogued the social media entries by three Europeans of Kurdish origin who travelled back to Kurdish areas of Syria and Iraq to fight alongside Kurdish forces to free the region from ISIS control. These individuals have been selected on the basis of multiple reliable sources pointing to the fact that both their identities and statements were truthful, including – but not limited to – personal ties with reliable sources of the author.¹ Their multiple social media accounts on Instagram, Twitter, and Facebook (the latter now fallen into disuse) have been monitored from December 2017 onwards on a daily basis; in the first months of 2018, all entries preceding said date – up until early 2015 – were also catalogued. Since 2019, accounts from the fighters' friends, journalists who have come in contact with them, and military personnel gravitating around the three Europeans were monitored on a bi-weekly basis. Over three years, a database of more than 10,000 entries was built. All findings and conclusions here presented therefore stem from said data collection work. The results are hereby presented on an anonymised basis, using the input from this research as groundwork for all inferences.²

Possible prosecution outcomes

Understanding the position of foreign pro-Kurdish fighters in the conflict against ISIS is extremely difficult. First, it is important to underline that, although there are UNSC Resolutions condemning

the “crime of terrorism” (UNSC, 2001a; UNSC, 2001b), an internationally agreed-upon definition of *terrorism* is yet to be found. Many scholars have tried to solve the problem by suggesting solutions and definitions – for the purpose of this paper, I will rely on Antonio Cassese's definition:

[...] broadly speaking, terrorism consists of (i) acts normally criminalized under any national penal system, or assistance in the commission of such acts whenever they are performed in time of peace; those acts must be (ii) intended to provoke a state of terror in the population or to coerce a state or an international organization to take some sort of action, and finally (iii) are politically or ideologically motivated, i.e. are not based on the pursuit of private ends. (Cassese 2006, p. 937)

At the same time, although the crime of terrorism does not exist *per se* in international law, crimes conducted by terrorist groups are prosecutable under international criminal law, international humanitarian law, and domestic law. There does not seem to be any reason to believe that terrorists could not be brought to justice under charges of already-existing crimes (e.g. civilian targeting).

Nevertheless, the problem of foreign fighters has risen to prominence under the umbrella of Islamic extremist terrorism. Therefore, in UNSC Resolution 2178 (2014), the reference is made to “foreign terrorist fighters”, and the Security Council asks States to take action in order to criminalise activities which it considers to be terror-related, such as “providing or receiving terrorist training”, “recruitment”, “travel”, and “preventing foreign terrorist fighters from crossing their borders” (*ibidem*). Still, with a non-existing definition of what *terrorism* actually is, States have been very free in applying this resolution in their domestic law – as commentators noted, this has also brought along excuses to trump human rights in certain cases (Cassese, 2006).

The situation of foreign Peshmerga fighters appears in all its complexity if the cases are analysed in depth. The theoretical exercise of evaluating their stance is a good starting point to underscore the difficulty of classifying the position of foreigners joining Kurdish forces in the current international law framework.

1 The author can provide further information on the methodology used to select these individuals via email.

2 The author can provide further information on data collection techniques, categorisation system, and the database itself via email.

In Option A, men born in Iraqi Kurdistan or Syrian Kurdistan, raised in the West, who willingly chose to return to their region of origin to join Kurdish forces in the fight against ISIS. In this case, having proven they were not mercenaries and had been in compliance with IHL norms, they would not be prosecutable under most Western domestic law. Moreover, fighting alongside local security forces on the basis of their Kurdish background would raise the question of whether they could actually be considered *foreign* fighters.

In Option B, keeping each premise as in Option A, if the men crossed the border from their region of origin (for the sake of the theoretical exercise, it will hereby further be assumed as Iraqi Kurdistan, but the statement holds even when the other way around is considered) into the other Kurdish area (Syrian Kurdistan), this would change their status: their ethnic background would be no safe escape for them now. The fact that they are of Kurdish descent will not play a significant role in their acquittal – on the contrary, the fact that they have fought for a free Kurdistan in Syria, whilst born in Iraq, makes them fully fledged foreign fighters. Although it could be argued that some Kurdish units in Northern Syria could actually be considered, under International Humanitarian Law (IHL), civilians taking up arms against a foreign invasion (art. 4, par. 6, III Geneva Convention, 1949), legally speaking these fighters' position shifts once they cross the border to that of a prosecutable *foreign* fighter.

In Option C, another subtype of foreigners joining Kurdish forces can be examined: veterans of the wars in Afghanistan and Iraq, whose years of service were spent in an attempt to bring democracy to the area, chose to return to the region to fight against ISIS alongside Kurdish forces. The fact that most Kurdish militias have been allied with Western countries participating in the Global Coalition to Defeat Daesh, as well as Operation Inherent Resolve, has actually allowed the first returnees with this background to be acquitted of terror charges (Abbit, 2020).

The online narrative

Incidentally, Option C introduces us to the public perception of the conflict. Firstly, public opinion in Europe and North America has viewed “the Middle East” as a cluster of countries at war, in which Western countries would intervene in an effort to bring democracy and eradicate terrorism. The invasion of Afghanistan in 2001 followed the 9/11 attacks; the US invaded Iraq in 2003 on the same – albeit contested – grounds, and toppled Saddam Hussein's regime on this basis. American opinion was especially fed the narrative that the US were bringing a democratic regime to the country – an achievement still far from being reached to date. American and European veterans from the wars of the 2000s and 2010s declared similar reasons for joining Kurdish forces to fight ISIS.

Similarly, Kurdish fighters framed their fight online within an anti-ISIS, pro-Kurdish independence, and pro-democracy narrative. Calls were made to destroy ISIS's territorial capacity, to retake Mosul (the city where the Caliphate had established its slave market), and to protect the local minorities (first and foremost, the Yezidis, whose men were slaughtered, and whose women were sold into sexual slavery). Their online presence brought them popularity and support from public opinion in the West, with fighters being featured in documentaries and magazines to recount their experience.

In 2018 and 2019, while Coalition forces grew closer to take away all territorial control from ISIS, Kurdish fighters saw their calls legitimised and expected them to be recognised. Once Baghouz fell, though, US President Donald Trump declared ISIS defeated and began the withdrawal of US troops from the area. Clashes therefore began with Turkish forces near the border, as well as Russian troops – but still, Kurdish forces maintain their positive associations in the eyes of Western public opinion. Grassroots conflict journalism sides with their cause, and their increased following gathered on social media platforms is a testament to their “reliability”. Kurdish fighters are young men who engage with their followers, post pictures and videos of fights and downtimes in the war zone,

remember their fallen comrades, repost memes, and publish stories in which they listen to the latest music releases. They are the embodiment of moral fighters, choosing to take arms against bigger and better-equipped forces for their ideals.

Kurdish fighters are young men who engage with their followers, post pictures and videos of fights and downtimes in the war zone, remember their fallen comrades, repost memes, and publish stories in which they listen to the latest music releases.

Conclusion

Kurdish fighters have now been portraying their battles, first against ISIS and now against Turkey, for at least the past six years. Their social media accounts, as well as the constellation of satellite accounts run by sympathisers, friends, former colleagues, journalists, etc. have more followers and provide more content than all official social media accounts (e.g. Operation Inherent Resolve's official Twitter account, established in 2014, has roughly the same amount of followers as grassroots conflict journalism platform Popular Front, which was established in 2018, and has significantly less engagement – around a tenth of the latter). This has caught the attention of Western youth throughout the whole political

spectrum, who side with the Kurdish cause regardless of their political ideas – to the extent that often-times quarrels break out in the comment section over diametrically opposed political stances.

Indeed, their use of social media in the past six years has allowed them to build a solid base of supporters, irrespective of most political stances, ethnic or religious backgrounds, who are willing to financially help them – this was seen especially between 2017 and 2019, when fighters would make appeals online for supplies they lacked on the field, and their followers would respond by sending them money and/or equipment. There appears to be at least a couple of cases of fighters returning home, not being prosecuted, and establishing entrepreneurial careers post-war on the basis of their already well-established social media following.

In future conflicts, it is more and more probable that other groups will take a page out of the Kurdish fighters' book, so as to sway the international public opinion in their favour. Similarities have indeed appeared with the clashes in Hong Kong in 2019 – unfortunately, the success of the attempt died down, as the world's attention turned to the coronavirus pandemic in early 2020. Once the dust settles, it will be interesting to see if the Kurdish fighters, the Hong Kong protesters, or other politically-charged groups will be able to (re)utilise this blueprint to gather international recognition and support. ■



About the author:

Ginevra Fontana holds a BA in International Studies (University of Trento) and a MSc in International Security Studies (Sant'Anna School of Advanced Studies & University of Trento). In 2018, she won the first edition of the European Cybersecurity Forum's "Young Cybersecurity Leader" Award. Ginevra currently works as a project assistant at the Italian Military Centre for Strategic Studies. She is a permanent member of the standing group at #ReaCT – Osservatorio sul Radicalismo e il Contrasto al Terrorismo (National Observatory on Radicalisation and Counter-Terrorism). Thus far, her research has mainly focused on the intersection between terrorism, new technologies, and military practices.

References

- Abbit, B. (2020). I'm a former paratrooper who fought Islamic State after the Manchester bomb – so why was I charged with terror offences?. *Manchester Evening News*. Retrieved from <https://www.manchestereveningnews.co.uk/news/greater-manchester-news/im-former-paratrooper-who-fought-18579381>.
- Ahmad, R. (2014). *Western “comrades” join Kurds, Arabs, secularists, Yezidis, and Syriac Christians against Islamic State*, Your Middle East. Retrieved from <https://yourmiddleeast.com/2014/10/29/western-comrades-join-kurds-arabs-secularists-yezidis-and-syriac-christians-against-islamic-state/>.
- Bakker, E., & Singleton, M. (2016). Foreign Fighters in the Syria and Iraq Conflict: Statistics and Characteristics of a Rapidly Growing Phenomenon. In de Guttery, A. et al. (Eds.), *Foreign Fighters Under International Law and Beyond* (pp. 9–25). The Hague: T.M.C. Asser Press.
- Bech Gjør, A. et al. (2012). *Rapport fra 22. Juli-kommisjonen*. NOU 2012:14, Kapittel 16, PSTs arbeid med å avdekke og avverge terrorisme.
- Callimachi, R. et al. (2018). Chapter 6: Paper Trail. *The New York Times*. Retrieved from <https://nyti.ms/2Wc50FL>.
- Cassese, A. (2006). The Multifaceted Criminal Notion of Terrorism in International Law. *Journal of International Criminal Justice*, 4(5), 933–958.
- Frantzman, S.J. (2015). ‘Long live Kurdistan’. *The Jerusalem Post Magazine*.
- Goldie, L.F.E. (1987). Profile of a Terrorist: Distinguishing Freedom Fighters from Terrorists. *Syracuse Journal of International Law and Commerce*, 14(2), 125–139. Retrieved from <https://surface.syr.edu/jilc/vol14/iss2/3/>.
- Higgins, N. (2004). *The Approach of International Law to Wars of National Liberation*. Monograph 3, Martin Monograph Series, The Martin Institute, University of Idaho.
- Krähenmann, S. (2015). Foreign Fighters under International Law and National Law. *Militair Rechtelijk Tijdschrift*, 108(6). Retrieved from https://puc.overheid.nl/mrt/doc/PUC_21650_11/1/.
- Krähenmann, S. et al. (2014). Foreign Fighters under International Law, Academy Briefing No. 7., Geneva Academy of International Humanitarian Law and Human Rights.
- Lister, C. (2019). Trump Says ISIS Is Defeated. Reality Says Otherwise. *Politico*. Retrieved from <https://politi.co/3erBamJ>.
- Marone, F., & Vidino, L. (2018). *Destinazione Jihad. I foreign fighters d'Italia*, ISPI: Milano. Retrieved from <https://www.ispionline.it/sites/default/files/pubblicazioni/foreignfighter.pdf>.
- Peçanha, S., & Watkins, D. (2015). ISIS' Territory Shrank in Syria and Iraq This Year. *The New York Times*. Retrieved from <https://nyti.ms/3gT3L66>.
- Romano, D. (2007). The Future of Kirkuk. *Ethnopolitics*, 6(2), 265–283.
- Saul, B. (2015). Defining Terrorism: A Conceptual Minefield [PDF file]. Legal Studies Research Paper No. 15/84, Sydney Law School. Retrieved from <http://ssrn.com/abstract=2664402>.
- Scheinin, M. (2015). The Council of Europe's Draft Protocol on Foreign Terrorist Fighters is Fundamentally Flawed. *Just Security*. Retrieved from <https://www.justsecurity.org/21207/council-europe-draft-protocol-foreign-terrorist-fighters-fundamentally-flawed/>.
- III Geneva Convention Relative to the Treatment of Prisoners of War of 12 August 1949. Retrieved from https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.32_GC-III-EN.pdf.
- Tuck, H. et al. (2016). “Shooting in the right direction”: *Anti-ISIS Foreign Fighters in Syria & Iraq*. Horizons Series No. 1, The Institute for Strategic Dialogue.
- United Nations Security Council. (2001a). *Resolution 1373*. Retrieved from https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf.
- United Nations Security Council. (2011b). *Resolution 1377*. Retrieved from <http://unscr.com/en/resolutions/doc/1377>.
- United Nations Security Council. (2014). *Resolution 2178*. Retrieved from <http://unscr.com/en/resolutions/doc/2178>.
- Wu, J. et al. (2019). ISIS Lost Its Last Territory in Syria. But the Attacks Continue. *The New York Times*. Retrieved from <https://nyti.ms/3fqVlXk>.
- Zelin, A.Y. (2013). European Foreign Fighters in Syria. Retrieved from <https://icsr.info/2013/04/02/european-foreign-fighters-in-syria-2/>.

ANALYSIS

Cybersecurity of 5G Networks. EU Toolbox of Risk Mitigating Measures – Practical Consequences of the Approach Taken

PAWEŁ GRUSZECKI

ATTORNEY-AT-LAW, COUNSEL IN IP & TMT PRACTICE,
DOMAŃSKI ZAKRZEWSKI PALINKA SP.K.

Introduction

Subject of analysis

The subject of this analysis is to examine how, from legal perspective, strategic issues have been addressed in a document entitled *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures (ETRM)* which was adopted and published by the NIS Cooperation Group (NCG) in January 2020. In the context of this publication, strategic issues should be understood as risks of this nature as well as measures to mitigate them. The analysis of the above document in this respect is necessary for four reasons.

First, it helps assess the scope of permitted actions in the selection and application of the strategic mitigation measures identified in the ETRM (see points 2.1. – 2.3. below), which EU Member States will take when managing two strategic risk scenarios (i.e. state interference through 5G supply chain and dependency on any single supplier within individual networks or lack of diversity on a nation-wide basis), which are also referred to in the ETRM. Second, the need to present this issue also results from the fact that during the public discussion on a number of decisions of individual EU Member States regarding the management of these strategic risk scenarios there has been no mention that these decisions had their source precisely in the ETRM. Third, it is very rarely emphasised that the adoption of the ETRM document, and thus each risk management-related decision it contains, was preceded by the adoption of a number of political but also analytical EU documents and statements including:

- support expressed by the European Council on 22 March 2019 for a common approach to the security of 5G networks;
- the European Commission's Recommendation on the cybersecurity of 5G networks published on 26 March 2019;
- the NCG's report on the EU Coordinated Risk Assessment on Cybersecurity in 5G Networks from 9 October 2019, and
- the European Council Conclusions of 3 December 2019.

Consequently, particular attention should be paid to the fact that **the provisions of the ETRM were adopted with the political support of such EU bodies as the European Council, which defines the European Union's overall political direction and priorities and comprises the heads of state or government of the EU Member States. This means that all actions currently taken by individual Member States to manage the strategic risk scenarios described above are very often only a consequence of the findings made jointly – within the EU – in the ETRM.** Fourth, the analysis in this area also aims to show that the vast majority of EU Member States' actions that are currently being taken do not apply to risk scenarios of a technical nature, but a strategic one. For this reason, the arguments of a technical nature presented by suppliers cannot be the only ones raised (e.g. **arguments regarding the cybersecurity of certain products will not solve the problem of their producer's dependence on the government of a given country**). Fifth and finally, the purpose of this analysis is also to indicate the difficulties that individual EU Member States may encounter while implementing the ETRM provisions and the weakness of some proposals resulting from the ETRM.

All actions currently taken by individual Member States to manage the strategic risk scenarios described above are very often only a consequence of the findings made jointly – within the EU – in the ETRM.

NIS Cooperation Group

In order to analyse the ETRM in this respect, the first thing to do is to explain the nature of the activities of the strategic cooperation group that adopted the above document, i.e. NIS Cooperation Group. The NCG was established on the basis of art. 11 paragraph 1 of the NIS Directive (Directive (EU) 2016/1148) in order to:

- support and facilitate strategic cooperation and
- the exchange of information among EU Member States and
- to develop trust and confidence, and

- with a view to achieving a high common level of security of network and information systems in the EU.

Moreover, the NCG works according to the EC Implementing Decision of 1 February 2017 and follows its own rules of procedure. According to these two documents, the decisions of the Group shall be taken by consensus, unless otherwise provided for in the EC Implementing Decision of 1 February 2017. What is important, the NCG is composed of representatives of the EU Member States, the European Commission (EC) and EU Agency for Cybersecurity (ENISA). The NCG's tasks have been precisely indicated in art. 11 paragraph 3 of the NIS Directives, among them *“exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems”* (Article 11, paragraph 3(c) of the NIS Directive). NCG has published over eight working documents such as: Reference document on security measures for Operators of Essential Services (CG Publication 01/2018); Reference document on Incident Notification for Operators of Essential Services (CG Publication 02/2018); EU coordinated risk assessment of the cybersecurity of 5G networks (Report, 9 October 2019) and CG Publication 02/2020 – Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity.

Technological sovereignty

The first section of the ETRM, “Introduction” (p. 3), states that the cybersecurity of 5G networks is *“[...] also crucial for ensuring the technological sovereignty of the Union”*. Which seems important, because the phrase *“technological sovereignty of the Union”* is not commonly used if we consider the harmonisation measures (e.g. directives or regulations) that are adopted by the EC and the European Council on the basis of Art. 114 of the TFEU (Treaty on the Functioning of the European Union, 2007). In particular, the above phrase has not been used in any way (e.g. as the purpose of issuing a given regulation) in the NIS Directive, the Cybersecurity Act (Regulation (EU) 2019/881), the whole EU

telecommunications framework or even the foreign direct investment (FDI) Screening Regulation 2019/452. What is important, the term *“technological sovereignty”* was used in the ETRM in the same context as it has already been in the past, although in extra-legal circumstances, when it comes to *“digital sovereignty”* or *“strategic autonomy”*, the need for which was cited by individual politicians of some EU Member States (in particular Germany and France) and EU officials (e.g. European Commissioner for Internal Market Mr. Thierry Breton or the President of the EC Mrs. Ursula von der Leyen) in the context of e.g. the Quaero and Galileo initiatives or the Gaia-x initiative (Barker, 2020). At the same time, it is notable that this concept refers to technological sovereignty at the level of the European Union, not individual EU Member States. In addition, it is worth noting that the term *“digital sovereignty”* is used also – in other circumstances – in the context of providing data subject with the right to dispose of their personal data, which is not the subject of this publication. **Consequently, according to the NCG, one of the objectives of adopting the risk mitigation measures described in the ETRM is to ensure the technological sovereignty in the European Union's 5G networks. Therefore, particular attention should be paid to two risk scenarios which will be discussed below.**

One of the objectives of adopting the risk mitigation measures described in the ETRM is to ensure the technological sovereignty in the European Union's 5G networks.

ETRM Objectives

Strategic risk scenarios and mitigating measures

As stated in the ETRM, the objectives of the document are to *“identify a possible common set of measures which are able to mitigate the main cybersecurity risks of 5G networks, as they have been identified in the EU coordinated risk assessment report, and to provide guidance for the selection of measures which should be prioritised in mitigation plans at national and at Union level”*. What is important, the mitigating measures are grouped into

two general categories: strategic and technical. The above means that the measures described in ETRM are to mitigate the technical, organisational, and strategic risks indicated in the nine scenarios referred to in the NCG's report *EU Coordinated Risk Assessment on Cybersecurity in 5G Networks from 9 October 2019*. In addition, the common goals of the above measures should involve minimising the exposure to risks stemming from the risk profile of individual suppliers, avoiding or limiting major dependencies on any single supplier in 5G networks, and promoting a diverse, competitive, and sustainable market for 5G equipment, including by maintaining EU capacities in the 5G value chain. **From the nine risk scenarios, the following two scenarios of strictly strategic risks should be distinguished: state interference through 5G supply chain and dependency on any single supplier within individual networks or lack of diversity on nation-wide basis.**

State interference through 5G supply chain

According to the ETRM, the risk scenario of state interference through the 5G supply chain takes place when a hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities. **Unfortunately, the ETRM does not indicate how to identify that we are dealing with a hostile actor and that there is a situation where it exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets.** The above should be considered one of the greatest weaknesses of the analysed document. The lack of clear guidelines on the issue made it possible for individual EU Member States to not use the ETRM in this particular regard. There is some clarity, however, that both conditions mentioned above (i.e. a hostile actor and a situation where it exercises pressure over a supplier under its jurisdiction) should occur simultaneously. Therefore, the above would suggest that the analysed risk scenario does not cover the situation in which, although there is pressure on the supplier, it is not performed by the hostile actor. At the same time, it should be noted that it

is also possible to adopt an interpretation according to which the mere fact of exerting the above pressure means that we are dealing with a hostile actor. In conclusion, it should be considered that the EU Member States that intend to comply with the ETRM indications should fill the described legal gaps (by adopting appropriate regulations) in order to gain a legal basis to decide whether a given risk scenario exists in their case.

Mitigating measures

Instead of the above clarification and despite its lack, the ETRM goes further and states that such risk should be limited by restricting the use of high risk suppliers (**HRS**) and strengthened access controls, network monitoring, and patch management processes, which means taking, in the short term (within two years), the following measures:

Strategic and technical measures to mitigate the risk of state interference through 5G supply chain	
1.	Strengthening the role of national authorities.
2.	Performing audits on operators and requiring information.
3.	Assessing the risk profile of suppliers and for suppliers considered to be high risk, applying restrictions, including necessary exclusions, for key assets.
4.	Controlling the use of Managed Service Providers (MSPs) and vendor third line support.
5.	Ensuring strict access controls.
6.	Ensuring secure 5G network management, operation, and monitoring.
7.	Reinforcing software integrity, update, and patch management.

Table 1. Strategic and technical measures to mitigate the risk of state interference through 5G supply chain.

Strengthening the role of national authorities

The above-mentioned mitigating risks have been clarified in the ETRM. For the purposes of this publication, mitigation measures number 1, 3, and 4 will be described. Strengthening the role of national authorities (mitigating measure no. 1) means that national authorities (without specifying whether it is any national authority or only those responsible for the regulation of the telecommunications market) should be able to use ex-ante powers to restrict, prohibit, or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment, and operation of the 5G network equipment, taking into account such risks as interference by a third country in the 5G supply chain and threats to national security. Therefore, it should be emphasised that in the legal orders of EU Member States, imposing any ex-ante obligations or restrictions is associated with the need to conduct an appropriate administrative procedure, and then granting a given entity the status justifying the introduction of the said obligations or restrictions. By way of example, if it is determined there is an entity with SMP (special market power) in a market, President of UKE (Office of Electronic Communications – the Polish regulatory authority) shall issue a decision in which (i) determines the relevant market, (ii) designates SMP, and (iii) imposes regulatory obligations, taking into account the adequacy and proportionality of the obligation in question to market problems, and whether the solution serves the purposes of achieving the objectives specified in the Polish 2004 Telecommunications Law.

In view of the above, this mitigating measure appears to be one of the most complicated in terms of its possible implementation. However, it should be noted that under the provisions of the 2018 Act on the National Cybersecurity System, which implement the NIS Directive, it is possible to issue recommendations regarding the use of IT devices or software, in particular in terms of its impact on public security or an important state security interest. Pursuant to the regulations currently in force in Poland, the obligation to comply with the above recommendations would, in turn,

result from the administrative regulation that will be issued on the basis of the Telecommunications Act. The entities bound by the provisions of the above regulation may be providers of publicly available telecommunications networks. Such legislative solutions would significantly simplify the procedures related to the considered implementation of the discussed mitigating measure. At the same time, however, it should be emphasized that the solution presented above does not extend the powers of the national telecommunications authority, as the recommendations will be issued by a specially appointed person within the government structure, and the administrative regulation will be issued by the competent minister. Consequently, there will be no national telecommunications authority at any stage of the discussed scheme, which makes it difficult to classify this course of action within the scope of the mitigating measure under analysis.

Assessing the risk profile of suppliers and for suppliers considered to be high risk, applying restrictions, including necessary exclusions, for key assets

Mitigating measure no. 3 above includes performing rigorous assessments of the risk profile of all relevant suppliers at the **national level or EU level (for example jointly with another Member State or Mobile Network Operator – MNO)** and applying restrictions – including necessary exclusions to effectively mitigate risks – for key assets defined as critical or sensitive in the EU coordinated risk assessment report (e.g. core network functions, network management and orchestration functions, and access network functions). When discussing the risk scenario and mitigating measure no. 3, it should also be noted that in Annex 2 to ETRM the main vulnerabilities, in particular supplier-specific vulnerabilities, are listed. The above is due to the fact that the EU coordinated risk assessment followed the approach set out in the ISO/IEC: 27005 risk assessment methodology which reflects the assessment of a set of parameters, including the main vulnerabilities. According to this Annex, **the risk profiles of individual suppliers can be assessed on the basis of several factors**, among them the likelihood of the supplier being subject to interference from a non-EU country that may manifest through i.a.:

- a strong link between the supplier and a government of a given third country;
- the third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country;
- the characteristics of the supplier's corporate ownership, and
- the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.

Unfortunately, in this respect as well, it is necessary to point out the lack of guidance on the basis of which EU Member States should present identification according to which e.g. there is a strong link between the supplier and a government of a given third country or the characteristics of the supplier's corporate ownership means the likelihood of the supplier being subject to interference from a non-EU country. Therefore, it should be pointed out again that the EU Member States that intend to comply with the ETRM recommendations should fill the indicated gaps (by adopting appropriate regulations) to gain a legal basis for deciding whether a given risk scenario occurs in their case.

It is necessary to point out the lack of guidance on the basis of which EU Member States should present identification according to which e.g. there is a strong link between the supplier and a government of a given third country.

Controlling the use of Managed Service Providers (MSPs) and vendor third line support

Mitigating measure no. 4 above means controlling the use of Managed Service Providers (MSPs) and vendor third line support. According to the ETRM, the above would follow through establishing a legal/regulatory framework which limits the types of activity and conditions under which MNOs are able to outsource particular functions to Managed Service Providers (MSPs) for both physical and virtual infrastructure. In other words, there would be a specific restriction of the principle

of freedom to conclude contracts, referred to e.g. in the Polish Civil Code, which would apply only to a specific group of entrepreneurs, i.e. MNOs. This would also mean giving priority to the need to manage the identified risk scenarios over the principle of freedom of contract. At the same time, it should be noted that the above would obviously not be a completely new limitation if we look at entrepreneurs in general. Some of these limitations occur – to a lesser extent – e.g. in the case of outsourcing banking activities (banking law) or cybersecurity services (the Act on the National Cybersecurity System). According to the ETRM, such limitations shall include:

- applying restrictions in particular in sensitive parts of the 5G networks, such as the security and network operations functions and where MSPs are considered to be **high risk suppliers** within the meaning of description to mitigation measure no. 3 above, and
- (for functions outsourced to MSPs) imposing enhanced security provisions around the access that MSPs are given to perform those functions.

In addition, in the case of equipment manufacturers' third line support (in particular suppliers considered to be high risk within the meaning of description to mitigating measure no. 3 above) the ETRM proposes to consider imposing strict access controls, especially on critical sensitive components and sensitive network parts. The above would apply to the design, implementation, and operation of the network.

Political impacts

Particular attention should be paid to the fact that mitigating measures indicated in points 3 and 4 above are related – according to the ETRM – to (potentially) broader economic or political impacts. According to author of this analysis the above means that those states whose suppliers were the subject of actions described in items 3 and 4 above can take a specific type of political action that may take the form of, for example, economic pressure. **The above proves how unique – in terms of content and taking into account strategic aspects – the ETRM is.**

Dependency on any single supplier within individual networks or lack of diversity on a nation-wide basis

According to the ETRM, the risk scenario of dependency on any single supplier within individual networks or lack of diversity on a nation-wide basis takes place when a mobile network operator sources a large amount of its sensitive network components or services from a single supplier. As stated in ETRM, the above is intended to constitute a risk because the availability of equipment or updates from this supplier might be subsequently drastically reduced, due to a failure by the supplier to supply (e.g. due to trade sanctions by a third State or other commercial circumstances). In consequence, the quality of a supplier's equipment decreases due to priority given to guaranteeing supply over improvements in product security.

Mitigating measures

In consequence, the ETRM states that the risk should be limited by implementing measures listed below. For the purposes of this publication, mitigation measures number 5 and 6 will be described:

Strategic and technical measures to mitigate the risk of dependency on any single supplier within individual networks or lack of diversity on a nation-wide basis

1.	Strengthening the role of national authorities.
2.	Performing audits on operators and requiring information.
3.	Ensuring the diversity of suppliers for individual MNOs, through appropriate multi-vendor strategies.
4.	Strengthening the resilience at national level.
5.	Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU.
6.	Maintaining and building diversity and EU capacities in future network technologies.

Table 2. Strategic measures to mitigate the risk of dependency on any single supplier within individual networks or lack of diversity on nation-wide basis.

Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU

Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU (mitigating measure no. 5) means building on the EU's Foreign Direct Investment screening mechanism to improve the monitoring of FDIs across the 5G value chain (e.g. through a mapping of key 5G assets, the use of monitoring tools, and exploring specific guidelines), in order to better detect foreign investments in the 5G value chain that may pose a threat to the security or public order of more than one EU MS. Critical infrastructure, public security, access to and control of information, and cybersecurity are well embedded in the scope of the FDI Regulation, allowing for investment evaluation that takes into account such factors as the risk profile of buyers/companies.

Maintaining and building diversity and EU capacities in future network technologies

According to the ETRM, maintaining and building diversity and EU capacities in future network technologies (mitigating measure no. 6) means developing policies which create optimal conditions for European technological firms and foster innovation in key technology areas to promote a diverse, sustainable, and secure European 5G eco-system, including by:

- developing the proposed EU institutionalised partnership in the field of NGI/6G ("Smart Networks and Services") to ensure there is a sufficient degree of diversity of suppliers and sufficient knowledge and supply capacity in the EU across the telecoms value chain;
- developing EU capacities and therefore also avoiding dependencies by supporting disruptive and ambitious research & innovation, which relates to the implementation of the various EU funding programmes, in particular Horizon Europe, the Digital Europe Programme, and the Connecting Europe Facility (CEF) (e.g. through initiatives such as 5G Corridors for Connected and Automated Mobility);

- bringing together knowledge, expertise, financial resources, and economic actors throughout the Union, so as to overcome potential important market or systemic failures along the value chain (IPCEI), and further specific industry initiatives.

The above-mentioned activities are of a framework nature and relate primarily to pan-European strategies. As a consequence, and unlike the other mitigation measures discussed above, they do not fall within the exclusive competence of individual EU Member States. However, it is important that the representatives of individual countries gathered under the NCG decided that the objectives of the ETRM would not be achieved without taking actions of this nature. The above confirms the statement already contained in this publication that the management of the analysed strategic risk scenarios has been coordinated at the EU level.

Implementation of the strategic mitigating measures

In summary, the ETRM suggests that the European Union's 5G network technological sovereignty will be achieved by implementing – both at the EU level and in individual EU Member States – a whole set of mitigating measures, such as strategic mitigating measures. The above implementation will take place according to the steps indicated in the ETRM, i.e.

- risk prioritisation according to the national / EU Coordinated Risk Assessment;
- review of the effectiveness of existing mitigations in addressing the risks in the Risk Assessment and identifies gaps;
- identification of prioritised risks to address the gaps described above;
- studying the corresponding recommended measures and mitigation plans and the selection of the measure(s) that will have the most effect and considers potential implementation factors, **alone or with aligned EU Member State(s);**
- implementation of **all or parts of measure(s)** accordingly, **individually or with aligned Member State(s).**

Particular attention should be paid to the fact that the process proposed in the ETRM and set out above shall be implemented by the EU Member States to the extent they consider appropriate, and with or without the participation of other countries. As a consequence, we are dealing with a **hybrid model**, which, on the one hand, indicates to the Member States a course of action, including risk scenarios that should be addressed as well as measures to mitigate them, and on the other hand, it gives the EU Member State the opportunity to implement this scheme in proportion to the identified risk. The most important thing is that by the decision of the collegiate body comprising EU Member States' representatives, i.e. NCG, a specific goal has been set, i.e. **the sovereignty of the 5G network at the EU level**. It is also not without significance that the above scheme has not been introduced under any legal measure in the form of a directive or regulation. **In consequence, the above approach is characterised by flexibility but also a potential ambiguity as to what actions are to be taken.**

The author of this publication sees the above as beneficial due to the **dynamism of the situation with which we deal, as well as its complexity and sensitivity**. At the same time, taking into account the flexible form of introducing the analysed scheme, it should be noted that this means the **necessity to actively monitor the situation and frequently supplement the proposals for strategic mitigating measures**. In terms of this last postulate, it should be noted that the strategic mitigating measures are neither being further specified nor developed. The above should be considered a serious obstacle in achieving the set goals, which is important because we are dealing with the risks of a strategic nature. Consequently, it should be considered necessary to clarify the method of implementing the strategic mitigating measures and to introduce new ones. ■



About the author:

Paweł Gruszecki specialises in providing legal services for projects requiring knowledge of cybersecurity law, IT law, personal data protection, copyright, media law, and telecommunications law. He is in charge of legal services for projects to adapt operators of essential services, particularly those operating on the energy market, to the requirements of the Act on the National Cybersecurity System. He has extensive experience in providing services to international internet service providers, operators of the largest internet platforms and telecommunications operators. He has headed more than 40 projects to adapt business organisations to the requirements of the General Data Protection Regulation, which involved entities from the e-commerce, media, manufacturing, automotive, energy, construction, and other sectors.

References

Barker, T. (January 2020). Europe Can't Win the Tech War It Just Started. *Foreign Policy*. Retrieved from: <https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/>.

COMMISSION IMPLEMENTING DECISION (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive; (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on the Functioning of the European Union - Protocols - Annexes - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 - Tables of equivalences, Official Journal C 326 , 26/10/2012 P. 0001 – 0390.

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, L 194/1.

Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, PE/72/2018/REV/1, OJ L 79I, 21.3.2019.

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.

Telecommunications legislation: Consolidated text: Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive); Consolidated text: Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive); Consolidated text: Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive); Consolidated text: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office (Text with EEA relevance).

The Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws 2018.1560, as amended).

The Telecommunications Act of 16 July 2004 (consolidated version: Journal of Laws 2019. 2460, as amended).

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**