VOLUME 9 (2023) ISSUE 1

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

European Cyber Security Cooperation: Overview and Challenges

Heli Tiirmaa-Klaar

Cybersecurity is a Global Public Good

Interview with Francesca Bosco

ANALYSES • POLICY REVIEWS • OPINIONS

The Kosciuszko Institute

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

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

ISSN: 2450-21113

Citations: This journal should be cited as follows:
"European Cybersecurity Journal"
Volume 9 (2023) Issue 1, page reference

THE KOSCIUSZKO INSTITUTE

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

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

Contents

Editorial

Ewelina Kasprzyk

Chief Editor of the European Cybersecuirty Journal

Dear Readers,

Technology remains one of the greatest drivers of change in nearly all areas of life. Human rights are also immensely affected by it, both positively and negatively.

On one side, technology has given us numerous improvements in access to information, education and healthcare services, empowered freedom of expression, activism and independent journalism, allowed for a more secure communication, and also created a platform for the more marginalized communities to share their stories and advocate for their rights.

On the other, darker side, we have to deal with censorship, surveillance, manipulation of information, hate speech, digital divide, online harassment and cyberbullying, unrestrained mass data collection, job displacement, AI bias, and so on – all of which are enabled by uncontrolled development and abuse of technology.

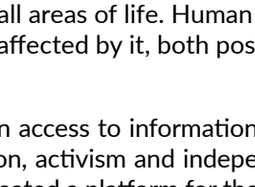
Striking the right balance between tech advancements and protecting human rights is an ongoing global challenge. With this issue of the European Cybersecurity Journal, we would like to add a few perspectives to this debate.

We gathered a variety of experts and scholars, to share their insights into the issues like challenges in EU cybersecurity cooperation, ethical concerns stemming from AI, the potential 'Cyber Article 5', connectivity and digital transformation in Africa, and tech-enabled human trafficking.

We sincerely hope you will find this issue informative, inspiring, and worth sharing with your colleagues. Thank you for reading the ECJ!

Signed,

Ewelina Kasprzyk



EXPERT'S COMMENTARY

European Cyber Security Cooperation: Overview and Challenges

HELI TIIRMAA-KLAAR
DIRECTOR OF DIGITAL SOCIETY INSTITUTE AT THE EUROPEAN SCHOOL OF MANAGEMENT AND TECHNOLOGY

Keywords: European cybersecurity cooperation, policy coordination, information sharing, incident response, diplomacy

The European cyber security landscape is a complex and multi-layered web, with a myriad of national, public, private, civilian, and military policies, initiatives, and operational cooperation mechanisms in play. Within this intricate web, there exist several interconnected bubbles of cooperation and information sharing at different levels. These levels encompass institutional and policy coordination at the European Union (EU) and NATO levels, operational-technical collaboration through the efforts of Cyber Incident Response Teams (CERTs), and bilateral intelligence sharing agreements between countries. Furthermore, many European governments have turned to private companies to bolster their cyber intelligence capabilities, adding an extra layer of intricacy to this already convoluted picture. This article will delve deeper into the various dimensions of cyber resilience cooperation across Europe, examining the challenges, opportunities, and recommendations for strengthening this aspect of the continent's digital security landscape.

Among the public sector entities there are four distinct functional cyber communities that exist in all European countries and belong also to the respective EU or NATO cooperation frameworks. First, there is a quite large cyber incident response and resilience community, which consists of both technical and policy experts, and engages in incident response, information sharing, early warning and related coordination activities in order to protect critical information infrastructure. The second community is dedicated to the fight against cybercrime, and consists of law enforcement representatives, prosecutors, judges and other experts in European criminal justice systems. The third community is cyber intelligence and diplomatic community, which addresses the state-sponsored (or organised) cyber operations,and has their own distinctive cooperation and information exchange structures. And finally, there is a defence community with a primary mission to protect cyber networks of defence forces. This community also engages in defence cooperation bilaterally, multilaterally or within larger NATO frameworks. All these communities work closely with the private sector that owns and runs ca. 85% of critical cyber assets in European countries.

Governments, defence and other public sector entities own and control a relatively small portion of cyberspace in democratic nations. Hence, achieving cyber resilience requires a major coordination and cooperation effort on behalf of all stakeholders.

The Role of EU Institutions and Its Agencies

In order to understand the EU's role in strengthening the European cyber posture, one should start with citing the EU foundational documents, explaining what EU is mandated to do according to its legal foundation. Under one principle, the EU may only act within the limits of the competences conferred upon it by the EU Member States in the treaties[1]. In practice, it means that European Commission has the right for initiative primarily in customs union, monetary policy, internal market, economic policy as well as in civil protection and some internal affairs competence area as all EU Member States have decided to give the European Commission and Parliament an upper hand in those policy fields. The Common Foreign and Security Policy remains inter-governmental – meaning that the EU High Representative for Foreign Affairs and Security Policy, and its External Action Service can mostly coordinate and represent the Union in foreign policy matters if they have mandate from the member states. Foreign policy, national security and defence matters remain the exclusive competence of the 27 EU Member States.

The paradox is that cyber security relates to all these competence areas simultaneously. The EU has built up an impressive cyber regulation and policy track record since the adoption of its first Cybersecurity Strategy in 2013.

The majority of the existing EU cyber policies and legislative initiatives intend to increase overall cyber resilience and strengthen the Union's cyber ecosystem by fostering cooperation, advancing technological capacities and creating higher degree of cyber readiness in the EU Member States. The two editions of the NIS directives aim to set higher cyber standards for key economic players and public administration across the Union. The EU Cyber Certification Framework and Cyber Resilience Act seek to provide more trustworthy technology, whereas the European Cyber Competence Centre and Network of National Coordination Centres intend to channel additional resources to cyber innovation and research. Another set of EU mechanisms includes legislative acts fostering the fight with cybercrime, law enforcement cooperation

1 https://eur-lex.europa.eu/EN/legal-content/summary/division-of-competences-within-the-european-union.html

and the collection of e-evidence. A myriad of related EU agencies and cooperation working groups are involved in implementing all these numerous initiatives on a daily basis.

On the national security, diplomacy and intelligence field, the EU relies on the Member States lead and input. The EU has adopted several council conclusions on cyber diplomacy as well as cyber sanctions regime, and a joint framework to respond to malicious cyber activities, also known as Cyber Diplomacy Toolbox. It has applied horizontal sanctions on entities and individuals organising cyber operations against EU interests, and has issued several joint statements attributing and condemning cyber attacks. A nascent EU Intelligence and Situation Centre under the EEAS has been coordinating the information exchange between MSs that is necessary for the common decision-making on cyber attribution and applying sanctions.

On the cyber defence side, the EU's mandate has been to concentrate on its CSDP missions and operations, as well as on capability development projects under the European Defence Agency mandate. A recent EU Cyber Defence Policy intends to strengthen European cybersecurity capacity, boost military and civilian cooperation, close potential security loopholes, reduce strategic dependencies and develop cyber skills. Most of these efforts will be implemented by the EU Member States.

National Cyber Competences: Incident Response, Defence, Intelligence, Attribution

What it all means in terms of cyber resilience and defence? First of all, all intelligence and national security related cyber activities are the prerogative of national governments. Most of serious cyber incidents, their mitigation and response as well as attribution decisions remain national. In case of large scale incidents with extensive global impact, such as NotPetya in 2017, they become public due to their extent and media exposure. At the same time, many isolated but equally serious incidents often remain confidential. Sometimes, nations have made malicious cyber operations public unilaterally[2], and in few instances they have sought solidarity with other European nations to attribute the attacks, such as coordinated German and EU statement condemning Russian cyber attack against the KS-SAT satellite network at the beginning of the war in February 2022.[3]

Often, malicious cyber operations remain within the closed confinements of national incident response and intelligence circles or few private sector actors involved, and the general public will rarely learn about actual cyber incidents that have taken place. There are smaller trust-based circles and cooperation arrangements between European countries to share more sensitive information, both within the intelligence and incident response community.

The large and fragmented cyber incident response community in Europe remains the major forum for information exchange on cyber threats.

There are many formations inside this community. First, there is an official EU Member States' CERT cooperation group (CSIRTs Network) supported by the European Commission, ENISA[4], and some sectoral cyber response groups in pan-European sectors such as European Centre for Cybersecurity in Aviation. Each EU Member State has their national and governmental CERTs, and a number of private sector CERTs. All of them belong also to a global CERTs organisation called FIRST. In each European country, there is also a special military CERT that protects military and defence networks – most of these are separate networks built and owned by the military for efficient command and control functions in wartime. Ideally, military and civilian CERTs in each nation exchange information and coordinate their activities regularly. Military CERTs of NATO nations also share information with NATO HQ in Brussels, and its operational NCIRC Technical Centre in Mons, Belgium[5].

There are also sectoral CERTs in larger countries, and sometimes large private sector companies have their own cyber teams. The companies falling under the scope of the EU NIS 1.0 and 2.0 directives are under the obligation to report cyber incidents to national CERTs. Large consultancy companies also offer cyber services to the industry and have their own dedicated incident response teams. Finally, global tech companies are well established in the European market, and they also hold significant information on routine cyber incidents happening on the continent.

Quite a large portion of cyber threat information is available from the open-source domain, posted by cyber researchers, white hats, and technical expert community. With some effort, 90% of information on recent cyber incidents and hacks can be found on specific websites. Cyberspace is a dual use domain, where secrets tend to come out quickly. Government cyber experts and intel officers will frequently use dedicated hacker websites to update their information.

International Organisations are Well Advised to Maintain Policy Lead, but Stay out of Operations

International organisations with a focus on European security – EU, NATO, CoE and OSCE, have set up useful cyber policies in their respective competence areas, and have contributed to overall European cyber resilience. As discussed above, the EU has been setting up a comprehensive posture of cyber policies in many fields since 2013. NATO has issued three editions of cyber defence policies, and included cyber aspects into its crisis management and collective defence mechanisms. The OSCE has adopted two sets of cyber confidence building measures in 2013 and 2016, and is implementing these now.[6] The Council of Europe champions its Budapest Convention to address cybercrime globally.

However, operational cyber cooperation still takes place between different incident response and other actors in European capitals. Due to the complexity of cyber domain, it would be very difficult to create a cooperation structure at the European level that has operational functions. Currently, the CERT-EU has the mandate to coordinate cyber threat information among the EU institutions, and ENISA provides a meeting venue for the European CSIRTs network.

All these elements might not be known to many external observers who call for stronger European cooperation in cyber resilience and defence.

Even if the EU was grabbing a more operational role, it should start with a huge new investment to build a separate network that connects all capitals securely with the Commission structures.

Currently, the European Commission does not have trustworthy information sharing infrastructure to exchange classified information directly with Member States. However, this infrastructure exists to some extent within the Council of the EU, and in the EEAS.

Smaller groups of EU Member States cooperate more closely and have been coalescing around the topics of cyber stability, coordinated attribution and sharing threat information both on policy and operational levels. Roughly the same number of states are also closely cooperating with the US/

2 Finnish Parliament hack in 2021 was publicly attributed to Chinese actors. https://therecord.media/finland-pins-parliament-hack-on-chinese-hacking-group-apt31/

3 https://www.auswaertiges-amt.de/en/newsroom/news/cyber-attack-russia/2525918

4 https://www.enisa.europa.eu/topics/incident-response/csirts-in-europe/csirts-network

5 https://www.nato.int/cps/en/natohq/topics_78170.htm

6 https://www.osce.org/secretariat/cyber-ict-security

UK led Five Eyes intelligence partnership, which has been instrumental in leading the international ad hoc cyber coalition defending Ukraine from Russian cyber attacks during the war.

Recommendations

When contemplating about European cyber cooperation, a simple analogy should be kept in mind – fighting cyber operations and incidents resembles firefighting.

Each city and town should have its own effective fire-brigade. In many ways, cyber incident responders are like firefighters – they have to locally protect the IT architecture that they know best.

It would be difficult to protect IT systems from outside, although some outside help is certainly welcome in specific functions, e.g. moving critical data to a global company's cloud, or calling in the right technical team to find a fix for a zero-day vulnerability in short timeframe. These are the examples of successful outside cyber assistance during the current war in Ukraine.

1. **Increase cyber expertise and education opportunities.** The first requirement in bolstering European cyber resilience is to grow the local expertise in all countries and help to develop efficient cyber risk management mechanisms and response teams. The EU currently lacks ca. 500 000 cyber experts, and this number is even bigger if to add unfilled IT experts' positions in the public and private sector. Countries should invest in cybersecurity awareness campaigns and educational initiatives aimed at raising awareness among citizens, businesses, and government officials.

2. **Support the Member States in implementing the NIS 2.0.** NIS 2.0 has set a unified cybersecurity framework with common standards for protecting critical infrastructure and vital services across Member States. This framework should be urgently implemented in order to raise cyber resilience in critical infrastructure sectors, and to ensure consistent cybersecurity measures. Many Member States lack experts and funding to reach the targets set by the NIS 2.0, and need Commission support to do it.

3. **Foster public-private partnerships.** Governments could encourage businesses to adopt cybersecurity best practices and standards, and provide incentives for investments in cybersecurity. Public-private partnerships can enable the sharing of resources, expertise, and technology to better defend against cyber threats collectively.

4. **Advance Cyber Crisis Management and Incident Response.** The cyber crisis management mechanisms should be advanced, and tested both at the EU and national levels. Incident response and recovery plans should be in place to outline clear procedures for responding to cyber incidents, mitigating damage, and recovering from attacks.

5. **EU-NATO and international cyber cooperation.** Any cyber crisis in Europe will involve both EU and NATO, as well as other international partners, and organizations. Alliances to enhance cybersecurity cooperation and share best practices should be developed further. EU and NATO respective crisis management mechanisms should be better coordinated, as the EU covers civilian and NATO military cyber crisis elements.

6. **Lessons learned on cyber defence in Ukraine.** It would be useful to analyse cyber incident mitigation examples by the international ad hoc coalition activities to defend Ukraine, and draw lessons on key factors defining the success. The lessons should be integrated to the EU countries' defence planning, especially the role of the private sector, strategic decision-making elements as well as operational coordination of cyber activities during the war, and the correlation between cyber hostilities and battlefield activities. ■

About the author:

Heli Tiirmaa-Klaar is Director of Digital Society Institute at the European School of Management and Technology in Berlin since January 2022. She was serving as Ambassador for Cyber Diplomacy and Director General for the Cyber Diplomacy Department at the Estonian Ministry of Foreign Affairs in 2018-2021, where she led the Estonian efforts to promote norms of responsible state behavior in cyberspace at the United Nations Security Council. Up to Fall 2018, she was working as a Head of Cyber Policy Coordination at the European External Action Service where she steered and coordinated EU external relations on cyber issues and co-led preparations of European Cyber Security Strategies since 2012. She set up EU strategic cyber dialogues with the US, India, Brazil, Japan, South Korea as well as other international organisations. She also kicked off EU global cyber capacity building programs and steered the development of the EU Cyber Diplomacy Toolbox to bolster EU response to malicious cyber activities. In 2011, she was assigned to the NATO International Staff to prepare the NATO Cyber Defence Policy.

She has been working on cyber security since 2007 when she led the development of the Estonian Cyber Security Strategy. In 2008-2010 she coordinated the implementation of the Estonian strategy, managed the National Cyber Security Council and led the establishment of Estonia's national cyber resilience structures as well as building public-private partnerships for cyber security. In her earlier career, she held various managerial positions at the Estonian Ministry of Defence and the Tallinn University since 1995. She was a Fulbright Scholar at the George Washington University and has published in several academic journals throughout her career.

INTERVIEW

Cybersecurity is a Global Public Good

FRANCESCA BOSCO
CHIEF STRATEGY AND PARTNERSHIPS OFFICER, CYBERPEACE INSTITUTE

Cybersecurity is a Global Public Good

Interview with Francesca Bosco – Chief Strategy and Partnerships Officer, CyberPeace Institute

The CyberPeace Institute has been observing the war in Ukraine and publishing in-depth analyses concerning specific attacks and campaigns. And your reports, Cyber Dimensions of the Armed Conflict in Ukraine, present very detailed data about the threat actors, the type of attacks they have carried out so far and some key trends in their malicious activity. Based on your findings, what should we expect from the future cybersecurity crisis and challenges?

Our work relates to the very essence of why the Institute was created. The Institute was launched at the end of 2019 and became operational at the beginning of 2020 during the pandemic. Our mission is pretty ambitious, but very clear – cybersecurity has been historically an area of work where mostly governments and private sector companies were leading actions and the discourse, whilst cyber-attacks were increasingly having an impact on humans, citizens, and users. There was a need of having a civil society organisation representing the interest of people and having a different look at cybersecurity. This is why the Ukraine-related work is very much rooted into the backbone of the Institute.

In February 2022, we started collecting information and then published the first timeline of cyber-attacks to explain the role cyber was playing in the war in Ukraine. For the first couple of months, we used the timeline to show the progression, but we soon understood the need to move from a simple visualisation to an analysis of the data we were collecting.

We realised that by analysing the cyberwarfare through the lens of cyber threats, their harm and impact on the population, and the legal landscape regulating these cyber operations, we could serve the wider audience with much more comprehensive information.

And that is why we created the #Ukraine platform, a user friendly tool for different types of stakeholders ranging from academia to policymakers. Considering the wealth of information that we are acquiring, also in partnership with different stakeholders, we decided to release the outcomes of our analyses as quarterly, publicly available reports.

Concerning the analysis we are continuously making on the war in Ukraine, it's interesting to note that many experts expected cyber to play a much more prominent role in the war. However, the data we have collected shows that attacks are indeed numerous and constant, and while cyber operations are not playing a major role in the tactical advances of either side, cyberattacks that have been targeting vital civilian infrastructure including energy grids, telecommunications networks, and public transportation have caused serious harm to the civilian population and destabilised daily life. Overall, since the start of the war, we have reported over 2,100 cyber-attacks. What is more, we have seen a steady increase in attacks per month, which has reached a peak in May this year at a total of 261 attacks in 31 days.

At the very beginning, we focused on the conflict between Ukraine and Russia, but then we started observing the potential spill-over effect as activities in cyberspace are not bound by national borders and any cyber operation aimed at Ukrainian or Russian targets can reverberate globally by destabilising cyberspace and spreading malware or disinformation. As the war continued, cyber operations started targeting third countries such as Poland, Germany, or France. According to our data, since January this year there was a 99% increase in attacks against those countries. There appears to be a clear connection between countries pledging their support to Ukraine or imposing sanctions on Russia, and being targeted by cyber operations. Especially the ongoing delivery of weapons from several non-belligerent states is highly likely the cause for the malicious cyber activities conducted by pro-Russian hacktivist collectives against entities residing in those countries. For example, after Switzerland's Council of States decided to permit arms re-exports to Ukraine in early June this year, we have seen a significant increase of cyberattacks against Switzerland in the subsequent weeks.

In terms of threat actors, we have seen changes in their number and diversity. Whilst we have observed traditional malicious actors, such as cybercriminal groups and state-sponsored actors –the so-called collectives have been playing a consistently increasing role. Hacktivist collectives are groups of threat actors conducting cyber operations in the name of activism. These collectives have played a significant role in cyberspace during this conflict and have been committing cyberattacks at a rate and scale rarely seen before in allegiance with one or the other belligerent country.

As for threat types, we have identified four main categories that we call "the four D's", depending on the type of consequences they cause: destruction, disruption, data exfiltration, and disinformation. In a way, the main attack vector remains fairly traditional – in 83% of cases it is denial-of-service type of attack.

Considerably, one of the major cyber incidents since the beginning of the conflict took place on the day of Russia's invasion, when a cyber-attack disrupted broadband satellite Internet access and cut off thousands of Ukrainians and Europeans from the Internet for weeks. When we think about the human impact, we can't underestimate the psychological element of cyber operations. This attack did not just disrupt Ukrainian command and control, but also cut off the civilian population from the internet, separating them from both their fellow nationals and the rest of the world. The isolation and lack of access to reliable and timely information can have devastating psychological impacts on a population under attack.

Threat actors are also heavily engaged in influencing the information space and limiting access, for example, to timely, reliable, and official information for the Ukrainian population. This is crucial when we think about the humanitarian context and the risk of humanitarian actions being tricked into diverting the support and help needed as a result of an ongoing disinformation campaign.

This is why we focus our efforts on understanding and highlighting the impact on people. One of the projects that we're also currently doing at the Institute aims to develop is the so-called "harm methodology" which takes into consideration, among others, the psychological, physiological, societal, and political harm caused by cyberattacks. There is a fairly good understanding of what it means for cyber-attacks to impact the financial sector, causing serious financial losses for the population, or to impact the communication sector and isolating citizens from the outside world. But then we also need to be aware of the influence of psychology on people who might start feeling fatigue and losing hope in the resolution of the conflict.

With such a wide array of different opinions, I don't think at this very moment we can be sure what kind of a role cyber is playing in this conflict. I think we have to wait until the end of the conflict to really have a clear view on that. But it's really interesting.

I think that you are mentioning something very important. I spent all my career in cybersecurity, I have also been involved in countering organized crime and terrorism. There is always this sense of urgency in the immediate aftermath of an attack – regardless of the type of attack – to make comments now. With the advent of technology, unfortunately, I would say we need to wait to collect accurate information and see the long-term effects. The interplay of different types of malicious actors means that they might have different aims, not necessarily limited to an immediate impact and disruption, like in the case of data exfiltration and data being used over time. Therefore, the real consequences of attacks, especially in the conflict environment, might be extremely difficult to assess. This is also why the Institute puts all the effort into providing as much reliable data as possible which can later be used as evidence for building convincing arguments or drafting reports to support the work of the expert community, for example. And this is also how we are collaborating with different partners.

Indeed, if I was to describe the CyberPeace Institute's activity over the past years, one word comes to my mind – cooperation. Your projects are mostly based on establishing networks and connecting institutions and individuals from various backgrounds to achieve goals such as better monitoring of cyber threats, advocating for safety in cyberspace, assisting the most vulnerable. My question is – is anything missing here? Is there any sector or a stakeholder you wish was more involved in what you do? How do you engage experts from diverse fields to ensure comprehensive understanding of the issues at hand?

The Institute was created as a multi-stakeholder endeavour and by a diverse group of entities: the MasterCard Center for Inclusive Growth, Microsoft, and the Hewlett Foundation. It was launched after a series of consultations with different partners from various backgrounds and footprints, from think tanks and academia to other civil society organizations, and also private sector partners that agreed to join the initiative since day one. From the very beginning, there was a shared understanding that we need a holistic approach and that nobody can build cyber resilience alone.

Years ago, the understanding of what cybersecurity is and the function it plays were very different. It has gained more prominence, but it's also become a shared responsibility that requires concerted efforts.

The way we work varies depending on the partner. We have partners with whom we share our mission and vision, and we support collaborative initiatives, like NonProfit Cyber or the Coalition against Stalkerware. With the rise of Environmental, Social, and Governance (ESG) principles, private companies are increasingly interested in having measurable social impact – by seeking to align their ESG efforts with the demands of the digital age, they also search for ways to increase their digital responsibility.

It's interesting to note that it's the employees in the private sector that still frequently drive the desire for positive digital effect. A great example of that is our flagship program the CyberPeace Builders, a special network of volunteers from the commercial sector who lend a hand to civil society organisations for no cost. Because of the desire to give back, to move beyond the narrow technical understanding of cybersecurity, and to contribute to something greater, the retention rate has increased. This programme has shown to be a very effective strategy to develop fruitful partnerships with stakeholders from the public and commercial sectors.

We have been able to develop a solid dialogue with several International Organizations and with various states. Our involvement within the UN Open-Ended Working Group and the ad hoc Committee on Cyber Crime has shown the significance of the multi-stakeholder approach, not just on paper, but also in real life. It allowed us to start working with some member states and engage in bilateral collaborations, resulting in, for example, a joint program with the Czech Republic on fostering the cyber resilience of the healthcare sector. In 2021, ahead of the negotiations of the UN Convention on Cybercrime, we joined forces with the Cybersecurity Tech Accord and issued the Multi-stakeholder Manifesto on Cybercrime, which aimed to lay out key human-centric principles we deemed mandatory in any cybercrime legislation.

So, rather than on who is missing, I'd focus on the challenges that we see.

Our goal is to raise awareness about the fact that cybersecurity is a global public good. It's not just a matter of state, tech, or cyber-savvy private sector involvement; it's not just for the so-called "cyber actors".

In fact, all walks of life should consider cybersecurity a priority. I'd like to see the public interest in cybersecurity grow. Since cyber operations have demonstrated how they may obstruct normal life, we must acknowledge cybersecurity as a pillar of society. The difficulty is in increasing public awareness of the effects of cyberattacks, prioritising cybersecurity, and stressing that building cyber resilience requires teamwork.

Historically, cybersecurity had often been treated as a siloed area, disconnected from the variety of economic sectors and communities that form our entire society. This is also one of the reasons why we're currently organizing the Global Conference on Cyber Capacity Building together with the Global Forum on Cyber Expertise (GFCE), the World Bank, and the World Economic Forum. It will take place in Accra, Ghana, at the end of November 2023 and our goal is to connect two communities that historically have been very much separated – the development community and the cybersecurity community. Building cyber competence is crucial for the global digital transition and fosters robust digital economies, and with the help of this conference, nations can invest in their digital future. The human aspect of cybersecurity, however, is frequently disregarded, resulting in unacknowledged human damage and harm, and disregarding the significance of cybersecurity for individuals.

The other challenge that I see from the more organizational point of view, is that collaboration is not that simple. It takes time and resources to build a partnership, to curate it, or to build coalitions; to bring together the private sector, the public sector, and other organizations for more impactful actions. Especially in civil society, there is some sort of pressure to always try to have more collaborations and partnerships. One of the challenges that I see is building them in a sustainable way. Oftentimes the motives are very opportunistic – sure, partners eagerly join an initiative but maintaining cooperation over time is very difficult. This is why we are framing our collaboration to support the mission of the Institute by actively engaging with our partners through our programs and curating the evolving relationships for the long-term perspective.

We have seen first-hand how decisions made by technology corporations can have long-term consequences in the context of the conflict in Ukraine. Are we on the verge of a world order in which the ideas and ideologies of CEOs of big companies hold the same weight as those of policymakers?

I know there has been a lot of hype about the role that tech companies are having and how their tools and services are affecting us, but big tech companies do not have the same level of formal authority and a government mandate with related oversight. I see the growing role of big tech as an opportunity. This is also very much in line with the approach to partnership and collaboration we have adopted at the CyberPeace Institute.

I think the increasing reliance of our society on companies providing the technical infrastructure should be used for greater good by making them more responsible and accountable.

When we think about multi-stakeholder collaborations and public-private partnerships, there is a couple of things worth mentioning. At the CyberPeace Institute, our partnerships are based on the recognition of our principles of independence, neutrality, inclusiveness, and inspired by meaningful contribution. This is why we are progressively evolving in measuring our impact and we make the information publicly available on our website and via our Annual Activity Reports. What I would like to see broadly speaking about collaboration across sectors is an evolution towards a "co-design" attitude, engaging different actors at early stages of a tool or service development, which is still rarely seen these days.

Let's move from technology corporations to technology itself. One buzzword that we keep seeing everywhere is of course, artificial intelligence. And experts are raising questions about possible issues stemming from unregulated use of AI and its impact on ethics, law, even about the full power of AI, which has not been discovered by the scientists yet. Rumman Chowdhury and Sue Hendrickson raised an interesting point that the current development of AI is leading us toward a technocratic world where "the blind pursuit of AI growth and optimization outweighs the imperative for human flourishing". AI is there to save us or destroy us, as if humans had no control over it. Are we doomed? Is the evolution and development of AI already out of control, or is it going to happen soon?

This is a very timely question. My involvement in AI and robotics started when I was working for the UN many years ago, back then AI was exclusively the domain of technology, not regarded as a societal challenge as it is today. But indeed, with the strengths and the capabilities of generative AI, there is a different set of challenges to the security of cyberspace, but also to cyber peace in general. As often said, AI is like a double-edged sword. It brings immediate benefits to us as the users – greater efficiency, speed, and potential, for example in the area of sustainable development. Thinking about the technical community, the ability of generative AI to produce computer code can democratise computer science and coding, and make it easier for cybersecurity newcomers

to enter a field that was previously challenging to enter.

At the same time, AI allows malicious actors to benefit just as much. Researchers have demonstrated the ease with which ChatGPT-generated code can create malware. While recent safeguards attempt to prevent such uses, ChatGPT can still be used to produce encryption software that enables malicious actors with minimal technical knowledge to create ransomware. It lowers entry barriers for newcomers in cybersecurity, but also for cybercriminals. Additionally, its ability to generate text, images, and speech, a key selling point, accelerates spear phishing attacks and the spread of misinformation and disinformation.

That being said, I do not think AI will destroy humanity anytime soon. The biggest danger I do see, like a déjà vu, is again the race to put technologies on the market with no safeguards in place. Historically the potential adverse societal impacts and harms often come as an afterthought, while they need to be assessed at the start.

When we think about security-by-design, it should really mean responsibility-by-design as well. Unfortunately, we are not there yet. This is why there is this flourishing of initiatives that are trying to put a patch on something that indeed can go profoundly wrong.

I feel like we always arrive a little bit too late. Instead, we should learn from our past mistakes and apply the lessons learnt consistently to new technologies.

In the context of vulnerable communities, we need to think about the risks for organizations that are working in the development sector or peacekeeping, and are often a crucial line of defence for the most vulnerable populations. What does the technology uptake, specifically machine learning and AI, mean for them? What are the potential consequences? To what risks can they expose themselves and others?

We have concentrated on using AI appropriately during the past few months. We internalised responsible AI use before advocating for it, some of my coworkers have started using ChatGPT and other AI tools, like many businesses. We acknowledge the potential advantages of AI, but we also stress the need for caution. To ensure responsible adoption, we have mapped our internal use of AI and set responsible AI principles and with such rules in place, we can have intelligent conversation about AI.

Those concerns resulted with quite a few attempts to regulate AI. How should we approach the regulation and governance of technology like AI to strike a balance between fostering innovation and preventing its misuse? What are the key principles or frameworks you would advocate for in this regard?

Firstly, we need a human-centric approach in the development of AI that respects rights, dignity, and equity of people, especially considering the potential harm to vulnerable groups. With the global diversity that we have, technology will not have the same impact on all people. Secondly, do not harm. Sounds very obvious, but it should remain the global guiding principle for developing and implementing AI, as well as establishing regulations that protect data, privacy, and security.

I very much welcome differing opinions on the regulatory side. Regulatory frameworks increase international cooperation and it's good to see a variety of viewpoints on how to regulate. But then there is a risk of having an overproduction of regulation and scarce attention to implementation. The regulatory work should be based on harmonization of core principles, and on keeping the different stakeholders truly involved throughout the process.

When it comes to the production and the implementation of certain technologies, that's something the EU regulatory framework stands for. One of the challenges is to have the private sector involved in the discussion and also to have some kind of checks and balances in place. You need to have oversight and set up accountability mechanisms that are targeting different actors. For the states that means ways to ensure they adhere to commitments they make when they sign international agreements. Similarly, there needs to be a sort of an unwritten contract between the private sector companies and the society in which we all commit to responsible development and use of AI.

The EU and the US are following different approaches to issues like data flows, AI, platforms and digital markets, but we can generally describe their approach to regulation as coming from democratic states – what about the authoritarian states? Can tech regulations on a more global scale, for example, through the UN bring techno-authoritarianism to our doorstep or even into our homes? What should democratic states do to take control of the tech regulation globally?

We have to recognize that currently the approach to regulations is often fragmented, discrepant, and sometimes haphazard. Besides the challenge that you mentioned, there is also another aspect, which is the fact that even "democratic" states are often not regulating technology and allowing it to enter the market in an uncontrolled fashion.

At the most recent UNGA, the UN Secretary-General created a High-Level Advisory Body on AI, giving governments the chance to adopt a responsible AI strategy. Effective execution, not merely having appropriate rules and regulations, is the main concern. Better regulatory safeguards are urgently required, especially for technologies that may be strengthened by offensive cyber capabilities. Currently, accountability assessment is challenging due to an unregulated grey market and hazy actor definitions. ■

About the author:

Francesca has an International Law and Human Rights background and 15+ years' experience in working for international organizations (United Nations and World Economic Forum) on action-oriented research, capacity building and technical assistance in international justice, crime, peace and security. She has developed her expertise on countering and preventing cybercrime (from hackers profiling to protection of critical infrastructure), crime-tech convergence and misuse of technology, focusing on opportunities, systemic risks and threats created by new technologies (e.g. artificial intelligence, robotics, immersive technologies). She has a long standing expertise on leading programs to foster cybersecurity and increase cyber resilience, including cyber capacity building, and diversity and inclusion initiatives. More recently she has been working on securing digital transformation of contextually vulnerable organizations, in developing countries and in fragile contexts, to foster the achievement of the SDGs. At the Institute, she is leading the strategic engagement in programs and initiatives leveraging multistakeholder cooperation with civil society, academia, corporates, philanthropy and public institutions, to reduce the harms from cyberattack and to promote sustainable cyberpeace.

ARTICLE

NATO Article 5 and Its Invocation in Case of Cyber-Attack

GIORGI IASHVILI
CO-FOUNDER & MANAGING PARTNER AT CYBER TRUST LLC;
ASSOCIATE PROFESSOR AT BUSINESS AND TECHNOLOGY UNIVERSITY

Keywords: NATO, article 5, collective defence, collective response, operational domains

1. Introduction

Cyber threats pose significant challenges to NATO. Malicious actors increasingly aim to disrupt the Alliance through the deployment of harmful cyber activities and campaigns. The dynamic and rapidly changing cyber-threat landscape has the potential to reshape the global security environment. Potential adversaries seek to undermine NATO's critical infrastructure, meddle with governmental services, extract sensitive information, and hinder the Alliance's military operations.

Russia's aggression against Ukraine has brought to light the significant role that cyber activities play in modern conflicts. Furthermore, Russia has escalated its hybrid attacks against NATO Allies and partners, incorporating malicious cyber activities. Meanwhile, China's articulated aspirations and coercive strategies pose challenges to NATO's interests, security, and values. In response, Allies are actively countering the growing and relentless cyber threats, even when they are part of broader hybrid campaigns, that jeopardize democratic systems and critical infrastructures. (NATO, 2023) (Maigre, 2022)

2. What is Article 5?

NATO and its Allies depend on robust and resilient cyber defence to effectively carry out the Alliance's fundamental responsibilities, which include collective defence, crisis management, and collaborative security efforts. Article 5 of the North Atlantic Treaty is a cornerstone of the Alliance. It implies the principle of collective defence and "remains a unique and enduring principle that binds its members together, committing them to protect each other and setting a spirit of solidarity within the Alliance." (NATO, 2023)

Article 5 stipulates that in the event of an armed attack against a NATO Ally, all other member nations of the Alliance will interpret this act of aggression as an attack against all members. Consequently, they will respond with the measures they deem necessary to aid the attacked Ally.

Article 5 of the NATO treaty was invoked for the first and only time in its history after the September 11 attacks on the United States in 2001, after NATO confirmed the attacks met the criteria outlined in the North Atlantic Treaty. This led to a collective response by NATO member states to support the United States in its reaction to the attacks.

At the 2016 NATO Summit in Warsaw, Allies acknowledged cyberspace as a new operational domain where the Alliance must ensure its self-defence with the same level of effectiveness demonstrated in the air, on land, and at sea.

In other words, starting from 2016, NATO has been regarding a cyber-attack against any of its Allies as an act of aggression against the entire Alliance. This presents the primary challenge for the Alliance – understanding the issues related to Article 5 is straightforward when it is considered within the classic operational domains – the land, the air, the sea (and the space, acknowledged by NATO as the fifth domain in 2019), but when it comes to the cyberspace, numerous matters become less defined, more ambiguous and need to be re-assessed. These challenging matters are explored and discussed in this article together with the overview and analysis of the evolution of NATO's developments in cyberspace. At the end, sets of recommended actions for the Alliance to address these challenges are provided.

3. NATO and Cyberspace: Evolution

Before delving into the challenges of the Alliance's existing approach to cyber domain, let's start by taking an in-depth look at how NATO's engagement with cyberspace has evolved since 2002. Over the past twenty years, NATO's perspective has transitioned from addressing cyber defence primarily in technical terms to recognizing its significance within the broader strategic context of the Alliance. (Maigre, 2022)

The inclusion of cyber defence on the Alliance's political agenda was initiated during the NATO Summit in Prague in 2002. Four years later in Riga, the leaders of the Alliance once again emphasized the requirement for enhanced protection of the information systems. After the coordinated cyberattacks on Estonia's public and private institutions in 2007 (attributed to Russia, who denied any involvement), Allied Defence Ministers came to a consensus that immediate action was essential in this domain. It resulted in the development and adoption of NATO's first Cyber Defense Policy.

In 2008, the NATO Summit in Bucharest prompted the creation of two new entities focused on cyber domain:

- NATO CCDCOE (Cooperative Cyber Defense Centre of Excellence) in Tallinn, with the mission to support the member nations and NATO with unique interdisciplinary expertise in the field of cyber defence research, training, and exercises.

- Cyber Defence Management Authority (later renamed as Cyber Defense Management Board) in Brussels, with the sole responsibility for coordinating cyber defence throughout NATO Headquarters and its associated commands and agencies – on a more operational level.

The Russo-Georgian war in the summer of 2008 showcased the capacity of cyber-attacks to emerge as a significant element within conventional warfare strategies – Russia undertook a coordinated cyber campaign parallel to ongoing military operations. It is considered as the first ever use of cyber capabilities aligned with an armed conflict.

At the NATO Summit in Lisbon in 2010, the Alliance adopted a Strategic Concept that, for the first time, acknowledged the potential for cyber-attacks to reach a threshold that threatens national and Euro-Atlantic security and stability.

NATO Communications and Information Agency was established in 2012, as part of the reform of NATO's existing agencies.

In 2013, five NATO countries Canada, Denmark, the Netherlands, Norway and Romania agreed to collaborate on the "Multinational Cyber Defence Capability Development Project" aimed to develop advanced cyber defence sensors and improve the threat information sharing.

In the same year, the Tallinn Manual on the International Law Applicable to Cyber Warfare was published. This 300-page study was written by a group of researchers at the invitation of NATO CCDCOE in Tallinn.

During the 2014 NATO Summit in Wales, the Allies adopted a new cyber defence policy where cyber defence was acknowledged as a part of NATO's core task of collective defence. This implied a cyber-attack could serve as a basis for invoking Article 5 of the Alliance's founding treaty. Additionally, the Allies acknowledged the applicability of international law in the realm of cyberspace.

The same year, NATO's CCDCOE gathered scholars to explore the potential courses of action available to governments, within the framework of international law, for countering cyberattacks originating from foreign nations. This endeavour, referred to as the Tallinn Manual 2.0, aimed to provide comprehensive insights into the legal considerations surrounding cyber operations.

At the 2016 NATO Summit in Warsaw, Allies reaffirmed NATO's defensive mission and recognized cyberspace as a new operational domain where the Alliance must ensure its self-defence with the same level of effectiveness demonstrated in the air, on land, and at sea.

In 2017, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, the updated and considerably expanded second edition of the academic, non-binding study of 2013 was published. Although it is independent academic research that solely reflects the perspectives of its authors in their individual capacities, and it does not convey the viewpoints of NATO or any other entity or nation – Tallinn Manual is considered as the most comprehensive analysis of how existing international law applies to cyberspace.

The NATO Summit in Brussels in 2018 resulted in setting up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure. Additionally, the member nations for the first time reaffirmed their commitment "to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign." (NATO, 2018)

The NATO Communications and Information Agency, via the NATO Cyber Security Centre established in 2019 and located in Mons, Belgium, is equipped with the mandate of delivering technical cybersecurity services throughout NATO. The Centre plays a crucial role in promptly addressing any cyber incidents that have an impact on NATO's operations. A year after, the Allied Joint Doctrine for Cyberspace Operations was published.

In 2021, NATO issued a warning that it could potentially treat cyber-attacks in a manner equivalent to an armed attack against any of its member nations, thereby potentially initiating a military response against those accountable. The decision to invoke Article 5 would be evaluated on a case-by-case basis. Furthermore, NATO emphasized that its response is not limited solely to the realm of cyberspace and could extend beyond that domain. The same year the North Atlantic Council designated NATO's inaugural CIO (Chief Information Officer) with the objective of streamlining the integration, alignment, and cohesiveness of ICT systems across the entirety of NATO.

During the 2022 NATO Summit in Madrid, the Alliance revealed its intentions to create virtual rapid response capabilities aimed at countering substantial malicious cyber activities. NATO additionally committed to collaborating with the private sector to mitigate threats. It officially acknowledged the cybersecurity threats posed by Russia and China in the realm of cyberspace. Furthermore, NATO committed to revising its command structure to better encompass emerging cyber threats.

This year in Vilnius, NATO announced that VCISC (Virtual Cyber Incident Support Capability) has been launched to aid national mitigation endeavours in response to malicious cyber campaigns.

The Allies reiterated that either a single or a cumulative set of malicious cyber actions could potentially escalate to the threshold of an armed attack. This escalation might prompt the North Atlantic Council to consider invoking Article 5 of the Washington Treaty, with decisions made on a case-by-case basis. (NATO LibGuide, 2018), (NATO, 2023)

4. Limitations of Current Approach

Understanding the issues related to Article 5 is straightforward when examined within the conventional operational realms of land, air, and sea. However, when the context shifts to cyberspace, numerous factors become less distinct, uncertain, and blurry. Let us indicate such issues that need more clear and precise understanding:

4.1 Establishing a Threshold for "Armed Attack"

As according to Article 5, only "armed attack" may invoke the collective defence principle. So, which cyber-attack may qualify as an "armed attack" and trigger Article 5? There isn't a definitive answer as it varies based on the situation. The conventional mindset traditionally holds that a "severe cyber-attack" requires physical destruction, involving loss of life and visible harm to critical infrastructure. However, as our reliance on data and non-physical assets grows, scenarios like the manipulation of health records might trigger the invocation of Article 5. Additionally, could the impact differ between manipulating banking data and healthcare data, with one causing significant economic disruption and the other potentially resulting in fatalities in extreme cases? (Limnell, 2016)

It's important to remember how cyberattacks have moved further away from traditional warfare in pursuit of subtler influences and involving coercive political pressure – the US Congress, for instance, imposed sanctions on Russia for its meddling in the 2016 US presidential election in favour of the then-candidate US President, Donald J. Trump. (Layne, 2018)

Since 2014 we have seen sophisticated Russian state-sponsored cyber campaigns against Ukraine. These campaigns intensified at the beginning of 2022 and accompanied Russia's ongoing military operations. As Russia faces increasing losses in the conventional conflict and feels the effects

of sanctions and Western military assistance to Ukraine, there's a possibility that Russia might intensify cyber intrusions, even targeting NATO member states, in response to their backing of Ukraine. (Banks, 2022)

It's essential to keep in mind that cyber-attacks have presented a persistent challenge to NATO for a few years and adversaries like Russia are consistently being a source of limited cyber activities, thus far avoiding significant escalation.

Accordingly, up until now, none of the cyber incidents encountered by Allies have prompted the activation of Article 5, and the Alliance has not openly specified the threshold of damage or impact that an initiating cyber-attack would need to achieve.

Although this approach faces occasional criticism for being vague, it also holds a logical foundation. As NATO Secretary-General Jens Stoltenberg has expressed, the scale of such an attack and the corresponding Allied response under Article 5 should intentionally remain undefined. NATO refrains from disclosing to potential adversaries the specific demarcation between an ordinary cyber-attack and an armed attack within the cyber realm. This deliberate ambiguity functions as a deterrent, encouraging potential adversaries to exercise caution in their malicious cyber activities and to refrain from initiating a significant attack that could breach the uncertain boundary. This strategic approach of ambiguity is evident in official documents that outline a case-by-case evaluation approach. (Prucková, 2022)

Besides, according to some experts, the existing notion of threshold, even de facto and blurry, is high and leaves all other attacks (which are not qualified as "armed attack") unaddressed. (Roggeveen, 2017)

Next Steps: Defining "Armed Attack"

While the provided argumentation supports NATO's strategic stance of threshold ambiguity, there is a pressing need to establish a precise definition of the term "armed attack" tailored to the cyber domain. In other words, it should describe what constitutes an attack that would qualify for the invocation of Article 5 and what would be an accepted retaliatory action.

The Alliance must find a clear way to deal with a 'Cyber Article 5' event. Reinterpretation of Article 5 and the concept of an armed attack within the context of today's world is needed. What is the most challenging is achieving a collective consensus on the thresholds – both in terms of physical and cyber dimensions – that could prompt a member state to invoke Article 5. Simultaneously, defining the concept of proportionality in response needs to be clearly outlined.

Indeed, the decisions are inherently political and demand a strong understanding of the strategic cyber domain, along with its progression, from the involved political actors. In addition, the "case-by-case" approach of assessing the cyber-attacks should be re-evaluated and some unified threshold for qualifying the cyber-attack as an "armed attack" should be set. In result, it will enable the Alliance to make more determined, "quantitatively" proven and respectively comprehensive decisions when some Ally country suffers from the severe cyber-attack. It's important to note that invocation of Article 5 is not an everyday measure but a major political decision on which all 31 Allies must agree. Bringing in more determination and quantitative parameters would comprehend the decision-making process of the North Atlantic Council.

Next Steps: Addressing the attacks below threshold

Frequently, scenarios arise in which the cyberspace remains unharmed, but multiple unsuccessful attempts take place. These endeavours may not surpass the threshold for action, thus remaining unattended. Besides defending and keeping infrastructure secure and resilient, it's also essential to thoroughly analyse and allocate proper attention to such attempts, leveraging them for preparation purposes. Hence, the Alliance needs an effective approach to address cyber threats that remain below the established threshold.

4.2 Defence-Oriented Approach

The Alliance's existing cybersecurity strategy is primarily focused on defence. The NATO Cyber Security Centre is responsible for safeguarding the Alliance's internal networks and assisting member states in their independent cyber defence efforts. This is achieved through activities such as gathering and sharing intelligence, positioning rapidly deployable cyber defence teams, creating benchmarks for allied nations to enhance their national cyber defence capacities, and making investments in education, training, and simulation exercises.

As James A. Lewis, the director of the Strategic Technologies Program at the Center for Strategic and International Studies, highlighted in the Tallinn Papers – a collection of publications from the NATO CCDCOE:

"a cyber defensive orientation is the equivalent of a static defence, defending fixed positions rather than manoeuvring, and conceding initiative to opponents."

While defensive measures can deter individual cyberattacks, they fail to tackle the underlying threat. Despite the importance of safeguarding the national networks of NATO Allies, the most effective approach to ensuring sustainable and long-term defence against cyberattacks lies in the realm of offensive capabilities. This encompasses actions such as dismantling adversary networks and systems.

While individual member states can take specific actions to move toward this objective, the United States, for instance, has already demonstrated the deployment of potent offensive cyber capabilities (as seen with Stuxnet), a collective NATO doctrine would offer allied nations crucial guidelines concerning the principles of proportionality and subsidiarity in the utilization of offensive cyber capabilities. NATO's cybersecurity policy should establish a comprehensive framework aimed at navigating the relatively unexplored domain of offensive cyber operations. (Roggeveen, 2017)

In 2018, the Allies for the first time stated that NATO would "employ full range of capabilities, including cyber, to deter, defend against, and counter the full spectrum of cyber threats". This is regarded as shifting away from securing cyberspace with defensive measures only. The term "full range" means that NATO can utilize both defensive and offensive capacities in alignment with its defensive mission and in adherence to international law. While NATO will not independently develop offensive capabilities, it will depend on the voluntary contributions of member nations, like in other operational domains. (Maigre, 2022)

Next Steps: Preventive Measures

The Alliance must set a framework that will allow member states to not only act defensively, but also offensively. The evolving landscape of cybersecurity demands a shift towards a more proactive approach. To effectively counter cyber threats, NATO should pursue a broader and more adaptive operational framework than the traditional concept of collective defence. In the face of escalating cyber capabilities displayed by NATO's adversaries, including Russia's recent cyber campaigns in Ukraine and China's coercive strategies in cyberspace, it is essential for the Alliance to adopt a comprehensive cybersecurity strategy that can proficiently counter these emerging threats. (Roggeveen, 2017)

5. Other Challenges

In addition to the strategic challenges, the Alliance must deal with measuring the **magnitude** of each severe cyber-attack and address the following issues: What were the outcomes of the attack? The rapid and concealed nature of cyber-attacks makes it difficult to promptly determine their scale and consequences. Furthermore, do estimates of consequences encompass secondary or tertiary effects? (Limnell, 2016)

Besides, it's essential to have a clear understanding of what constitutes a **proportional response**. Given that cyber capabilities will predominantly remain within national purview, certain member states might opt for symmetrical responses, while others contemplate asymmetric actions. Determining proportionality is a political decision, necessitating a more adaptable and historically contextual assessment than a straightforward IF-THEN statement in code. Moreover, there is also a possibility for Ally to overreact in the event of a cyber-attack. (Limnell, 2016)

One of the biggest challenges in this case remains attribution. It is often difficult to trace cyberattacks back to one specific organization. Here not only the organization, but the attacking state must be detected, that makes the task much harder. So, who is responsible?

Attributing cyber-attacks to their originator continues to be a major problem, particularly when the attribution is intended to be publicly disclosed and certain. There is also a prevailing trend towards governments subcontracting cyber operations to entities that are not officially affiliated with states. (Limnell, 2016)

To invoke Article 5, attribution becomes essential. Based on well-known cases, when dealing with a cyberattack, establishing conclusive evidence and attributing the attack to a specific state might be concluded after an extended period, spanning months or even years. Accordingly, if something is proven years after the cyber campaign, what outcomes can the act of invocation achieve in terms of restoring the security of the state and the Alliance?

NATO needs to ensure they possess up-to-date cyber capabilities and, which is a very important issue – to **maintain credibility**. In order to ensure its standing as a defence alliance, NATO must have a substantial cyber policy in place, encompassing a reliable approach to cyber deterrence. Credibility arises from a set of actions much like those that NATO has undertaken in relation to conventional military operations. However, achieving the same in the cyber domain is currently more challenging. For instance, what would be the equivalent, in practical terms, of establishing permanent battalions within member states in the cyber realm? How can you effectively demonstrate your commitment to defend and counter aggression in the cyber domain through public messaging, striking a balance between seriousness and non-threatening intent? (Limnell, 2016)

Although certain steps are being taken in this direction, with more and more states establishing their national cyber commands, releasing joint statements etc., we're far from a NATO-wide strategy. Addressing these challenges requires the establishment of a well-defined and consecutive policy, which should encompass a transparent declaration of all cyber operations conducted by the Alliance. ■

About the author:

Co-Founder & Managing Partner at Cyber Trust LLC. Associate Professor at Business and Technology University. Cyber Security strategy and governance consultant with over 17 years of leadership experience and with solid expertise in critical infrastructure protection and resilience against advanced threats, including sophisticated and state-sponsored cyber-attacks. Giorgi is a former Director of IT Infrastructure and Cyber Security at Central Election Commission of Georgia and Chief Information Security Officer (CISO) at National Bank of Georgia. Cardiff University graduate and BSI certified ISO/IEC 27001 Lead Implementer and Lead Auditor. Largely engaged in international development projects in Europe & Eurasia (including the Western Balkans, Wider Black Sea region, Central Asia), where he provides expert advice on cyber security governance to the lead national institutions. Co-Founder & Board Member of Georgian Information Security Association (GISA), Information Sharing and Analysis Center (ISAC Georgia) initiative.

References

Banks, W. (2022, August 8). Cyberattacks and the Russian War in Ukraine: The Role of NATO and Risks of Escalation. From Georgetown Journal of International Affairs: https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%EF%BF%BC/

Ducaru, S. (2018). NATO advances in its new operational domain: cyberspace. Retrieved September, 2018 from https://www.fifthdomain.com/opinion/2018/07/05/nato-advances-in-its-new-operational-domain-cyberspace/

Goodman, R. (2018). Cyber Operations and the U.S. Definition of "Armed Attack". Retrieved September, 2018 from https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/

Layne, N. (2018, December 19). U.S. imposes fresh Russia sanctions for election meddling. From https://www.reuters.com: https://www.reuters.com/article/us-usa-russia-sanctions-treasury-idUSKCN1OI27F

Limnell, J. (2016). Challenge for NATO - Cyber Article 5. Stockholm: Center for Asymmetric Threat Studies (CATS), Swedish Defence University.

Maigre, M. (2022, April 6). NATO's Role in Global Cyber Security. From https://www.gmfus.org: https://www.gmfus.org/news/natos-role-global-cyber-security

NATO. (2018, July 11). Brussels Summit Declaration. From NATO: https://www.nato.int/cps/en/natohq/official_texts_156624.htm

NATO. (2023, July 4). Collective defence and Article 5. From https://www.nato.int: https://www.nato.int/cps/en/natohq/topics_110496.htm

NATO. (2023, August 3). Cyber Defense. From https://www.nato.int: https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en

NATO LibGuide. (2018). NATO Multimedia Library. Retrieved September, 2018 from http://www.natolibguides.info/cybersecurity

Prucková, M. (2022). Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO. From https://ccdcoe.org: https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

Roggeveen, B. (2017). NATO Needs an Offensive Cybersecurity Policy. Retrieved 2018 from http://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-an-offensive-cybersecurity-policy

ARTICLE

Protecting Responsible Cybersecurity Vulnerability Research

Lessons from the evolution of ethical hacking, and ensuring we can fix security holes before the bad guys get there

JOHN MORGAN SALOMON
CYBERSECURITY ADVISORS NETWORK

NICK KELLY
SECUREFLAG / CYBERSECURITY ADVISORS NETWORK

ABSTRACT:

The Ethical hackers identify, and help vendors and consumers fix, security bugs before malicious actors can abuse them. Current laws related to "hacking" are often unclear and inconsistent, placing responsible researchers in legal jeopardy for their work, creating unnecessary risk to industry and society. This paper provides a history of responsible vulnerability disclosure, and argues for stronger and clearer legal protections for good-faith researchers.

Keywords: cybersecurity, cybersecurity vulnerability, ethical hackers, vulnerability researchers, legislative reform, bug bounty

Introduction

There is no 100% guarantee of security for any software in existence. Whatever the reason for them, cybersecurity vulnerabilities are a fact of life. If malicious actors find vulnerabilities, they will exploit them to advance their objectives: digital vandalism, theft, sabotage, espionage and other forms of sensitive data and systems abuse.

The best way to remove this risk is for the good guys to find and quickly fix bugs first. The more experts can inspect a piece of software, whether through manual review or using automated tools, the more likely they are to detect flaws, which can then be fixed.

Unfortunately, many countries' laws do not distinguish between badly-intentioned persons and groups, and researchers working in good faith to uncover bugs. At the same time, many software and services providers and operators are not inclined to find and fix security holes for myriad reasons, and may want to prevent others from doing so when they can.

This means that well-intentioned, "ethical" hackers risk criminal prosecution and civil lawsuits when publishing their findings. Whether due to an explicit fear of legal consequences or insecurity about what is legal and what is not, researchers are thus discouraged from reporting and publishing their findings.

Malicious actors don't care about laws or lawsuits. They can find and use these flaws, resulting in economic cost and loss of confidence in digital services – the same digital services built by those unmotivated to find and fix them in the first place. Unfortunately, this doesn't just hurt the software maker – it hurts everyone.

Bug bounty platforms and coordinated vulnerability disclosure resources and practices have gone some way to improving the flow of vulnerability information in a responsible manner, but this is not enough – universal legal reform is needed.

The Organization for Economic Cooperation and Development (OECD) has issued a set of policy recommendations encouraging governments to create safe harbors that would legally protect cybersecurity vulnerability researchers working in good faith, and to promote the adoption of responsible disclosure policies and processes by organizations. It is now up to member countries to implement these in law, thus mitigating risks from lack of access to cybersecurity vulnerability information hampers our ability to protect our systems, our economy, and our society.

A Note About Terminology

Several of the topics discussed in this paper have significant personal, political, economic, and philosophical implications, and can involve a wide range of fundamentally divergent viewpoints. This can result in emotionally charged exchanges, not least due to inconsistent use of terminology. For the purposes of this paper, we conflate the terms "ethical hacker", "white hat", and "responsible researcher" to mean anyone who investigates cybersecurity vulnerabilities with the aim of getting them fixed, whether driven by profit, altruism, or simple curiosity, as long as this does not include knowingly deriving any illicit benefit from the process.

Background

The original definition of "hacker" or "hacking" was introduced in the 1950s by the MIT Model Railroad Club[1], and continues to describe some variation of a person using technology to solve a problem in a creative manner not originally intended by that technology. A few years earlier, the world's first computer bug[2] disrupted

1 The club mentions this claim to history at http://tmrc.mit.edu/hackers-ref.html

2 Sep 9, 1947 CE: World's First Computer Bug. National Geographic

the operations of a Harvard University computer. Works like Steven Levy's book *Hackers: Heroes of the Computer Revolution* have helped popularize a generally positive perception of the term.

While unauthorized uses of computer systems go back a long way, these were historically limited to serious academics and other professional enthusiasts playing with machines in harmless ways.

Similarly, early "breaches", such as hacker Captain Crunch's development of public telephone network "phreaking" to obtain free phone calls, and the creation of "phreaking boxes" of various colors to automate this process, were victimless[3] crimes, albeit technically illegal. Only in the late 1970s and early 1980s, did breaches and other forms of abuse arise – for example, Karl Koch/"Hagbard" and colleagues' intrusions into various networked systems on behalf of the Soviet KGB, and graduate student Robert Morris' first "worm" in 1988, which took down a significant portion of networked computers around the world.

At the tail end of this era, helped along by popular movies such as 1983's *War Games*, the worldwide evolution of the Internet, growing dependence on computer technology, and the expansion of online criminal abuse led to the term "hacker" having ever more negative connotations. It was increasingly used to describe a person who gained unauthorized access to systems and information through illicit means, despite the efforts of technology enthusiasts to maintain the original spirit of the word.

3 We assert that, like illicit software or content duplication, the unauthorized use of almost infinitely scalable digital services does not constitute material loss, and thus differs from classical "theft". This is a contentious topic, and we respect your right to disagree with us.

The Legislative Good Idea Fairy Comes to Visit

In response to concerns about spreading cybercrime, in 1984 the US legislature passed the Comprehensive Crime Control Act[4], one of the world's first laws criminalizing misuse of electronic systems. Updated in 1986 in the form of the Computer Fraud and Abuse Act[5] (CFAA), this ushered in a series of no doubt well-meaning "anti-hacking" rules in many countries around the world. Even countries which, according to UNCTAD[6] have "no cybercrime legislation", frequently implemented some form of legal restrictions on unauthorized access to systems.

For example, Belgium's Act of 28 November 2000 on IT-related crime introduced article 550bis(1), which provided punishments for "a person who, knowing that he is not entitled to do so, accesses or maintains access to an IT system"[7]. The 2001 Council of Europe's Budapest Convention on Cybercrime similarly criminalized a broad set of hacking-related activities and provided for international cooperation in suppressing these, under the guise of fighting child pornography, terrorism, and a number of other dangers to societal stability, both perceived and real[8].

These prohibitions did not prevent breaches and other incidents, nor did they stop research into system and software vulnerabilities – whether stemming from programming flaws in source code, configuration mistakes, or problems resulting from unforeseen combinations of software components. While reliable historical cybercrime

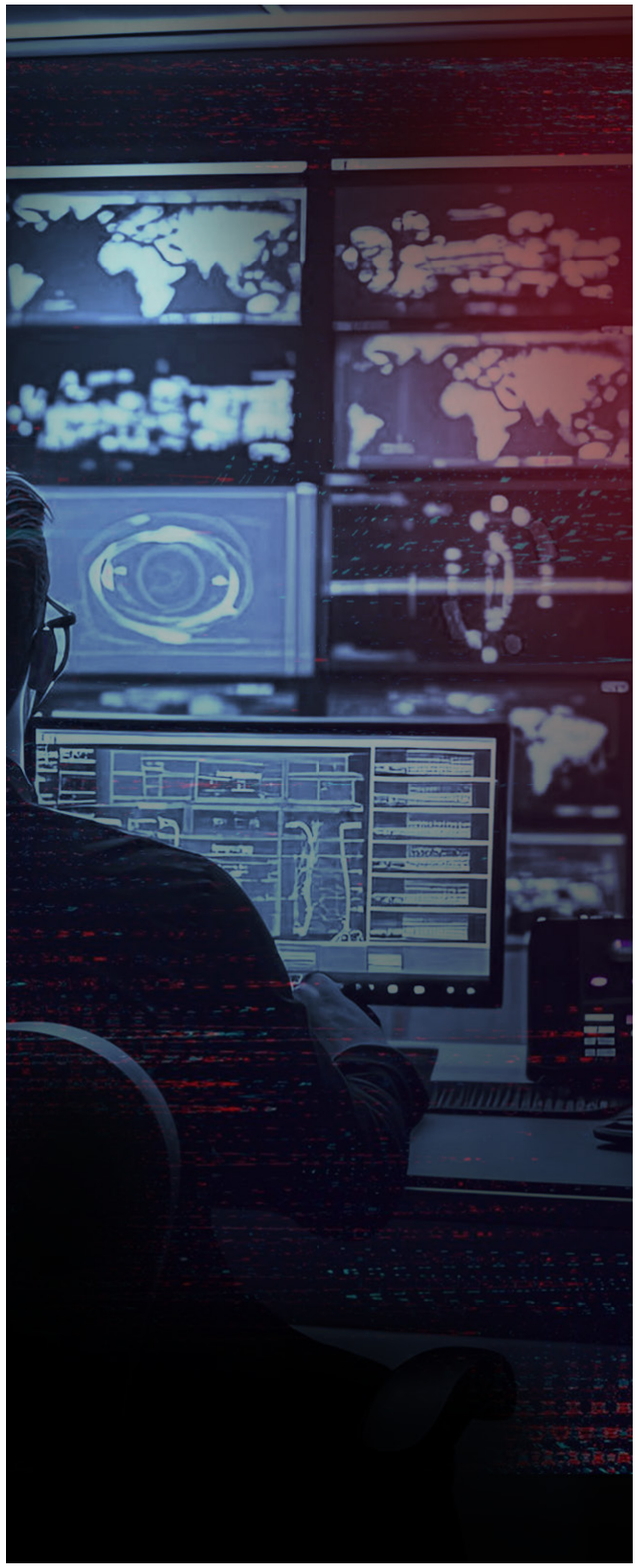
4 S. 1762, Comprehensive Crime Control Act of 1984

5 18 U.S. Code § 1030, Fraud and related activity in connection with computers

6 Cybercrime Legislation Worldwide, United Nations Conference on Trade and Development

7 Center for Cybersecurity Belgium, Guide to Coordinated Vulnerability Disclosure Policies Part II: Legal Aspects

8 The Electronic Privacy Information Center (EPIC) position on the Budapest Convention is worth reading – https://archive.epic.org/privacy/intl/ccc.html



figures are difficult to come by[9], the late 1990s nonetheless saw an explosion of, for example, website defacements[10].

Let's Get Patchin'

In 2003, Microsoft instituted "Patch Tuesday", a weekly event when (mostly security-related) software updates are released. These scheduled occurrences were largely a response to industry pressure, arguably because of the ever-escalating severity of major incidents. These included major outages stemming from the 2001 Code Red and 2003 SQL Slammer worms. The discipline of organized software security vulnerability management was in its infancy, and even though several major vendors had already started providing bug fixes to security flaws in the 1990s, large international firms had pushed for a more predictable cycle of security patch issuance for years, allowing for better planning of testing and deployment of patches.

Several vendors, including Adobe and Oracle, soon signed on to the Patch Tuesday schedule, ushering in a much more proactive attitude by many software makers towards communicating bug fixes. This contributed to an overall greater level of communication between consumers and providers of software – important, because not only is consumer pressure a major driver of bug remediation, the more consistent availability of "actionable" fixes motivates users to deploy patches. This was, and often still is, a very manual process.

9 This is due to several reasons. In the 1990s, law enforcement attention on cybercrime was still in its relative infancy, and major regular reports such as the Europol IOCTA had not yet been launched. Notification mechanisms were still highly immature, and victims frequently did not know how to report incidents. Furthermore, the term "cybercrime" is extremely broad (part of the underlying issue addressed by this article). Lastly, many historical statistics are provided by security vendors – leading to questions about reliability and impartiality.

10 White, Kelly. The Rise of Cybercrime 1970s–2010. Self-published

While some vendors began making genuine efforts to remediate bugs and communicate fixes, and pressure from industry and consumers, security vulnerability research was frequently only performed in-house. This meant little transparency for consumers and other stakeholders. Mechanisms allowing external vulnerability researchers to reliably and safely communicate their findings to providers were still highly inconsistent and ad hoc.

The Law Still Doesn't Quite Get It…

Legislation also often continued to fail to differentiate between researchers acting in good ("white-hat") or bad ("black-hat") faith, not to mention not providing consistent definitions of the bounds of "good" and "bad" in this context. Throughout the 2000s and 2010s, this culminated in several high-profile cases of legitimate researchers being arrested or legally harassed for disclosing their findings. For example, in 2016, David Levin was arrested[11] and charged by the Florida Department of Law Enforcement with violating Florida Statute 815.06(2), criminalizing unauthorized access to computer systems[12]. Disclose.io maintains an extensive list of legal threats against security researchers available via GitHub[13] and several other channels, comprising both criminal and civil actions.

Germany's controversial 2007 "hacker paragraph", StGB §202c[14] and its accompanying sections §202a and b, are another major example of an overly draconian, overly broad, unclear regulation. An implementation of the Council of Europe's 2001 Convention on Cybercrime[15], the paragraph provides for imprisonment of up to 2–3 years for any person who (paraphrased) gains access, without permission, to any non-public data set not intended for them.

Not only does the law criminalize the act of research itself, it fails to provide for any form of responsible vulnerability disclosure.

The Chaos Computer Club's 2008 position on this law[16] points out that, rather than increasing the security of German software and online services, it would have the opposite effect; an illustration of how such rules have a chilling effect on the identification, disclosure, and remediation of vulnerabilities can be found in the 2021 legal proceedings against a German programmer as a result of his attempts to motivate an online marketplace to fix a serious privacy leak[17]. This, despite Germany's highest constitutional court supposedly creating "clarity"[18] with regards to the law in 2009, in response to a 2007 lawsuit.

Enter Responsible, Coordinated Disclosure and Bug Bounties

The concept of "responsible disclosure" dates back to at least 1999, when the Nomad Mobile Research Center published its policy[19] of "first [working] to verify the basics surrounding said problem", then giving the vendor either a week or a month to respond (depending on the criticality of the problem) before publishing details. Cisco's Duo Labs maintains a comprehensive overview, up to 2015, of significant events and actors contributing to the evolution of many current approaches to vulnerability disclosure[20].

This has remained, more or less, the core of current widely accepted responsible disclosure practice. Deadlines for responding to a request for comment by researchers vary, and many policies have adopted elements such as "do no harm". It clashes fundamentally and philosophically with the "full disclosure" approach taken primarily by earlier security researchers, as well as arguments against providing free vulnerability information to vendors without compensation. A variant of this is "coordinated disclosure" or "coordinated vulnerability disclosure", formalized by Microsoft in 2013[21], which involves communication of a vulnerability to a "coordinating entity" – such as a CERT, national cybersecurity agency, even a security vendor, who then manages both countermeasures and communication of vulnerability details.

"Bug bounty" programs, offering financial rewards as incentives for researchers to report their findings in private rather than in public (at least, for a given grace period), are also nothing new. As Cybercrime magazine notes, the first such program was created in 1983[22], with Netscape being the first to offer cash for bugs in 1995.

The 2000s and 2010s saw the rise of commercial, dedicated bug bounty platforms and communities, such as Bugcrowd and HackerOne. Even as the legal situation of vulnerability disclosure is still murky in many jurisdictions, these organizations have seen vast numbers of bugs reported, and in many cases, remediated.

It's Not All Smooth Sailing

Bug bounty programs are not without their detractors, though. Whether because of perceived lack of scalability, insufficient rewards for ethical hackers, claimed perverse incentives for malicious bug hunters, or other argued flaws, a quick web search for "bug bounty controversy" yields a large number of arguments as to why they are not a panacea. Some groups even take a fundamental philosophical stance against bug bounties in principle, such as the Chaos Computer Club, whose position[23] is that they constitute a "dangerous black market", encourage monopolization of vulnerabilities by malicious-yet-legal (i.e. state) actors, and are not ethically justifiable. And yet, bug bounties appear to work, at least to some degree.

These are not the only objections to coordinated vulnerability disclosure and bug bounty platforms, though. A reviewer for this article who is a member of a mid-sized commercial firm's information security leadership recounted having encountered:

- exaggerated sense of criticality and value of bugs reported, whether due to cognitive bias from having spent significant time on finding a bug, or from a desire for greater financial gain;
- lack of understanding of company-internal vulnerability management and remediation processes.

In our reviewer's experience, this occasionally resulted in outright aggressive harassment of their organization, as researchers badgered information security staff to recognize (and pay for) information about vulnerabilities that were actually low-priority or even already patched. In extreme cases, this could conceivably take the role of outright fraud, as in the case of Tiversa[24], who outright invented leaks and vulnerabilities.

11 Goodin, Dan. How a security pro's ill-advised hack of a Florida elections site backfired. Ars Technica, 10 May 2016

12 The Circuit Court of the 20th Judicial Circuit's arrest warrant against David Levin: https://s3.documentcloud.org/documents/2823587/David-Levin-Arrest-Warrant.pdf

13 https://github.com/disclose/research-threats

14 (German language) Strafgesetzbuch (StGB). § 202c Vorbereiten des Ausspähens und Abfangens von Daten

15 Convention on Cybercrime (ETS No. 185), Council of Europe

16 (German language) frankro. § 202c StGB gefährdet den IT-Standort Deutschland. Chaos Computer Club, 21 Jul. 2008

17 (German language) Tremmel, Moritz. Hausdurchsuchung Statt Dankeschoen. Golem.de, 14 Oct. 2021

18 (German language) Schmitz, Peter. Dank Verfassungsgericht endlich Klarheit zum Hackerparagraph §202c StGB. Security-Insider.de, 08 Jul. 2009

19 The Nomad Mobile Research Centre announcement: https://www.nmrc.org/pub/advise/policy.txt

20 Thu T. and Meer, Haroon. History of Vulnerability Disclosure. Cisco Duo Labs, 03 Aug. 2015

21 Goodin, Dan. Microsoft imposes security disclosure policy on all workers. The Register, 19 Apr. 2011

22 Zurkus, Kacy. State of Bug Bounty Programs in 2017. Cybercrime Magazine, 17 Aug. 2017

23 Erdgeist. How to dry up the market for IT security vulnerabilities. Chaos Computer Club, 26 Nov. 2022

24 Khatchadourian, Raffy. A Cybersecurity Firm's Sharp Rise and Stunning Collapse. The New Yorker, 28 Oct. 2019

Also, what constitutes an "ethical", "legitimate" researcher? We are aware of several parties involved in vulnerability disclosure policy development who go so far as to call for the establishment of databases of such researchers. Civil liberties and privacy concerns aside, this raises all sorts of questions about certification, governance, cultural differences, and more.

Despite these concerns, the availability of both legitimate vulnerability reporting channels, and informational resources for vulnerability researchers has grown massively in scope.

There is no longer any excuse for a researcher to claim full ignorance (notwithstanding the experience many of us had as callow secondary school or university students, playing around with security vulnerabilities).

Digital rights-focused entities, such as the Electronic Frontier Foundation, as well as online information clearinghouses like the disclose.io project, provide volumes of easily accessible guidance, links, organizations, and help for researchers seeking to work constructively and ethically.

Perverse Incentives for the CxO

Even when mechanisms are in place to allow organizations to learn about and fix vulnerabilities, they are not always motivated to make use of them. On purely short term economically rational grounds, a software vendor or digital services provider (for example, an operator of a website, managed service providers etc.) should not be inclined to search for and fix software security bugs. The reason for this is simple – if a security vulnerability is fixed, and a patch is shared, this creates a) inconvenience for users (albeit less so given the rise of automated security patching mechanisms supplied by vendors and third parties), and b) the implication that where there is one vulnerability, there may be others. They may even believe in "security through obscurity" – the idea that not publishing source code means nobody will find bugs – a thoroughly disproven idea. There is also the fear of competitors claiming that their own product is more secure, because no vulnerabilities have been published.

All this can have an impact on sales, share price, and other results of reputational damage. Managers and engineers involved in the creation of code with security holes may also be held accountable by company leadership unfamiliar with the nature of information technology products, specifically the widely accepted idea that it is impossible to design a 100% secure system. Similarly, security holes in online services such as banking, retail, and even voting, are often viewed as hypothetical and low-probability, especially in cost-driven organizations.

Even though security through obscurity is patent nonsense, the likelihood of a particular security hole being found and exploited is comparatively low, while investigation and remediation can be difficult and expensive – or at least, the maintenance of staff and technology that is capable of doing so costs a lot of money. Managers may thus prefer to take a very short term "out of sight, out of mind" approach and count on moving to another job before an incident occurs. If ethical hackers can be legally dissuaded from poking at a system and publishing any findings, whether via threat of prosecution or civil suits, then obviously no bugs will be found, thus they do not exist.

While understandable, this attitude is nonsensical and irresponsible. To create a real-world analogy, one of the authors lives in a very rural area with a thankfully low crime rate. Leaving a door unlocked and relying on laws prohibiting passers-by from jiggling door handles does not prevent burglary. Rather, it prevents neighbors from stopping by, trying the door, and calling in to say hello, and if nobody is home, letting the resident know that their door is open. Whether or not it is appropriate to open another person's door without being invited is irrelevant – we want to know if a well-intentioned person finds such an obvious gap in our home security so that we can remember to lock it in the future.

More concerning is the (again, understandable) poor reaction many software publishers have had to being contacted about security holes by external parties. Absent a proven, reputable disclosure framework, how could they know that the person reporting the bug is genuinely acting in good faith? Could such a bug report even be an implied blackmail attempt?

Many companies nowadays either respond positively to reported vulnerabilities[25], or, at the very least, do not respond at all. However, legal threats are still commonplace in many jurisdictions. Ed Farrell, an Australian security researcher whom we recently interviewed for a podcast[26], asserts that he was menaced with a lawsuit by a maker of high-value physical infrastructure control software, in whose product he had discovered a critical vulnerability. Despite the researcher following proper accepted procedure and privately communicating his findings to the company in question, the firm was at the time engaged in legal proceedings and feared that reputational damage from publication of a security hole could harm their chances of success – thus, they resorted to the threat of legal action.

The thought process behind this approach, although wrong-headed, is fathomable. It is not reasonable to expect an entity to not defend itself against a perceived threat through legal means. It is worrisome that current legislation permits such a threat in the first place.

It should also be noted that this particular vulnerability remained unpatched, widespread, and readily exploitable for two years, compared to a similar vulnerability in a competitor's product, also reported by Mr. Farrell, which was patched in all of its Internet-facing systems within 48 hours as a result of constructive cooperation with the researcher.

Thankfully, as we will show below, this attitude is changing – albeit slowly in many areas. Data breaches of critical organizations due to software vulnerabilities or poor security practices, continue to grow in scale and impact. It is telling that the 2012 Saudi Aramco breach, the 2014 Sony Pictures hack, or even the 2017 Equifax compromise, were considered unprecedented in their extent at the time, and yet today only figure far down lists of major breaches in terms of severity. Cyber risk insurance and cybersecurity risk management frameworks have become mainstream, even expected. Chief Information Security Officers are increasingly viewed as a business function. Cyber risk quantification and linkage of cyber-risk to other more financial and fundamental business risk structures helps justify spending on both preventative, detective, and remediative security controls. Cybersecurity has thus long ceased to be just an expensive hobby to protect against an attack that may never come.

Seeing the Light at the End of the Policy Tunnel

In 2022, the US Department of Justice announced[27] that it would no longer prosecute white-hat hackers under the CFAA. While a welcome step, this does not go nearly far enough. First, it does not abrogate the CFAA's provisions that allow prosecution of security researchers. Future administrations may decide to backtrack on the DoJ's policy; considering the instability of US national politics in recent years, having to rely on the good will of a given administration is not a comforting thought, especially given the receptiveness of many voters

25 This is one of the findings of the OECD report on Encouraging Vulnerability Treatment

26 What to Consider When Reporting Vulnerabilities – Edward Farrell. CyAN Secure-in-Mind Conversation series, 14 Apr. 2023. Video at https://youtu.be/w-Mr53Xe_Vc

27 Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act. Office of Public Affairs, Department of Justice, 19 May 2022

to tough-on-crime policies and many politicians' ignorance of how software technology works.

Second, and more importantly, it does not consider the vast array of jurisdictions and legal structures in a country the size of the US, many of whom are free to make and enforce their own rules (insofar as they are not subordinated to national jurisdiction under the US constitution's supremacy clause). David Levin, the security consultant who reported a flaw in a Florida electoral website, was arrested and prosecuted under state law – which may still apply even if a given action is permissible at national level. The whole model obviously breaks down completely across multiple sovereign states when each has different laws, but all claim jurisdiction over an entity or action.

A few countries have historically taken a pragmatic approach to vulnerability disclosure. In the Netherlands, for example, the national cybersecurity center (NCSC-NL) has promoted CVD for several years, leading to its adoption by a large number of firms across several industries. While Dutch criminal law makes no distinction between "good" and "bad" hacking[28], the strong Dutch culture of public-private cooperation and the highly mature and sensible nature of the NCSC have made legal jeopardy for researchers much less of an issue than in more prosecution- or lawsuit-happy jurisdictions. However, like the US DoJ announcement, this depends on the good graces of current government policy rather than being enshrined into law.

In 2022, Belgium took the important step of reforming[29] its vulnerability disclosure law. Belgium thus became the first major economy to explicitly, legally permit ethical hacking – albeit still within strict parameters. Significantly, vulnerability researchers must inform the Belgian national CERT (CCB), and are subject to several restrictions, including "proportionality", and the need to demonstrate "good intentions". One of the concerns of the Belgian law is the inclusion of such subjective terminology.

Maybe most significantly, in 2021 the OECD Working Party on Security in the Digital Economy (SDE) developed several papers[30] through a multi-stakeholder process, calling for legal reform by governments and legislatures, to create "safe harbors" protecting ethical hackers.

Building on these papers, the OECD Council in 2022 adopted its *Recommendation on the Treatment of Digital Security Vulnerabilities*[31]. As an OECD standard, this international legal instrument reflects the consensus among OECD countries' to adopt public policies that reflect its content. It includes the creation of safe harbors, and several other measures to promote the coordinated disclosure of vulnerabilities. Not only is it highly encouraging to see both the problem and the concept of coordinated disclosure so explicitly recognized by an influential inter-governmental organization like the OECD, the recommendations for reform are concrete, principles-based, and actionable.

Now that OECD member countries have agreed upon this position, it is up to their governments to implement the policy recommendations into law. Such legislation must:

- define responsible disclosure policies and processes,
- list clear criteria for what constitutes a responsible, ethical, good faith researcher,

28 Berndsen, Michael. Ethical Hacking and Criminal Law. Meijers Canatan Advocaten, 24 Apr. 2019

29 Vulnerability reporting to the CCB. Centre for Cybersecurity Belgium (CCB)

30 Encouraging Vulnerability Treatment papers:
- Overview for Policy Makers
- Responsible management, handling and disclosure of vulnerabilities
- How policy makers can help address digital security vulnerabilities
OECD.int, various dates

31 Recommendation of the Council on the Treatment of Digital Security Vulnerabilities. OECD.int, 26 Sep. 2022

- encourage ways for researchers to benefit financially from their findings, if they are determined to be relevant,
- give software and service providers and operators enough time to fix systems and products, and
- ensure that digital services can continue to grow and flourish with minimal fear of abuse.

This evolution comes in an era where governments have repeatedly learned that they no longer have a monopoly on backdoors and security vulnerabilities. Edward Snowden's revelations about US domestic and foreign cyber-espionage activities in 2013 brought such government capabilities to the public's attention. I Since then, incidents such as the breach of Italian spyware provider Hacking Team in 2015, and revelations about the activities and technologies of such vendors as NSO Group, DarkMatter, Quadream, and others who provide exploit tools to governments, have created further awareness of government research and use of security backdoors, whether these are intentional or accidental. As a result, both legitimate and criminal actors have upped their level of scrutiny of known but unpublished security holes.

State entities can thus no longer rely on secrecy and national security to keep vulnerabilities out of the hands of unauthorized persons.

The growing realization of this fact seems to be driving an expanding level of awareness and introspection among lawmakers, not least supported by newer, more technologically literate generations coming into elected office and helping to drive positive policy change.

It is conceivable that this shift is in large part also due to a growing understanding by governments of the importance of "critical industry" or "critical national infrastructure". Security breaches of key economic actors – whether in the areas of energy, finance, transportation, or manufacturing – have the potential to impact society far beyond the perimeter of the affected organization.

As a result, regulatory guidance, such as the Monetary Authority of Singapore's *Guidelines on (Technology) Risk Management*[32], the New York State Department of Financial Services' 23 NYCRR 500[33], the US Securities and Exchange Commission (SEC) *Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*[34] or the European Network and Information Security Directive (NIS2)[35] increasingly specifies either rules or strong recommendations for cybersecurity risk management. In the case of NIS2 and the parallel financial sector-specific DORA (Digital Operational Resilience Act)[36], supply chain security is called out explicitly as an area for attention.

Many regulators have understood that private industry, often due to the factors pointed out in the previous section, will not "do the right thing" unless forced to do so by regulatory pressure. Cybersecurity regulation disempowers significant firms' from deciding whether or not to invest in protections against threats that might cause damage above and beyond the company's own business actions. This, however, requires that both software vendors and digital services providers have access to up-to-date cybersecurity vulnerability information so that they can protect themselves and their stakeholders – and that they do not have the ability

32 Guidelines on Risk Management Practices – Technology Risk. Monetary Authority of Singapore, 18 Jan. 2021

33 Proposed Second Amendment to 23 NYCRR Part 500. New York State DFS, 09 Nov. 2022

34 SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. US Securities and Exchange Commission, 26 Jul. 2023

35 The NIS2 Directive: A high common level of cybersecurity in the EU. EU Parliament Think Tank, 08 Feb. 2022

36 Digital finance: Council adopts Digital Operational Resilience Act. Council of the EU, 28 Nov. 2022

to muzzle ethical vulnerability researchers who are trying to do the right thing and help them protect their customers. Several of the above-mentioned regulations recognize this need and explicitly address it, albeit without creating corresponding legal protections for researchers.

None of the laws and frameworks listed in this section are perfect – far from it. However, they are all important parts of an evolutionary process, and a positive sign that some governments are increasingly paying attention.

The "Real World" Starts Responding

While legislation is starting to adapt, a cultural shift in how vulnerability disclosure is viewed is thankfully also under way. The period between 2020 and 2022 saw a dramatic rise in the number of supply chain vulnerabilities – including the identification of serious weaknesses in key software components such as Excellion, SolarWinds, Log4Shell, and Microsoft Exchange. Many of these were very rapidly exploited by threat actors.

Nonetheless, in all cases, alerts and patches were very rapidly made available. Regardless of whether the vulnerability was abused before (e.g. SolarWinds/Orion) or directly after (e.g. Log4Shell) public disclosure, users were quickly informed, details of the vulnerabilities rapidly shared by the original software vendors, security firms, CERTs and similar bodies, and industry sharing initiatives such as ISACs, and patches made available. We are not aware of any criminal or civil legal threats being made against those external researchers who discovered and published these vulnerabilities.

In another positive step, in response to the aforementioned OECD recommendations, several key industry players, together with the nonprofit Cybersecurity Advisors Network, formed the Good Faith Cybersecurity Researchers Coalition (GFCRC)[37] in 2022. This organization mobilizes voices from industry, academia, and international non-governmental organizations, and complements the work of the OECD – which focuses primarily on informing legislatures and other government actors. Other initiatives, such as the Charter of Trust, the Hacking Policy Council, and the Paris Call, all pursue similar goals – namely the mobilization of all stakeholders to help drive positive policy change.

We strongly believe that the pragmatic and fast approach to reporting initial findings, and provision of patches, without any known attempts to suppress details or pursue researchers responsible for identifying the security holes, is largely attributable to an increasing understanding that transparency is key to avoiding very serious systemic cyber-incidents.

The Trouble With TETRA

There is dramatic room for improvement, in both disclosure culture and mechanisms, and reform of legal obstacles to researchers and responsible disclosure. The case of the TETRA radio communications encryption vulnerabilities is a good example of both negative legacy approaches to security holes, and positive developments in attitudes to responsible disclosure.

In 2021, a team of Dutch researchers[38] identified a series of major encryption vulnerabilities in the highly critical, widespread TETRA (TErrestrial Trunked RAdio) communications standard. The flaws, some of which were intentional and known to vendors of the TETRA radio technology for about 25 years of its existence as a core part of many important radio communications services, provide an object lesson about the importance of peer review of security mechanisms, particularly encryption technology. Proprietary encryption algorithms and cryptosystems are far more difficult to test for weaknesses – however, the fact that the Dutch team was able to identify the serious holes applying zero-day exploits to commonly available off-the-shelf radio technology means that a skilled threat actor could do the same.

That at least one of the vulnerabilities was an intentional backdoor, included by design, makes this even more disturbing – it implies that certain actors already had access to sensitive radio communications for years. We leave it as an exercise to the reader to decide whether they consider certain government agencies using known backdoors against critical components to be "malicious actors", and whether the existence of such access means that truly criminal elements may also have been covertly abusing this flaw for years.

Better mechanisms (e.g. bug bounty and responsible disclosure programs, when they work as designed), clearer laws, and a stronger culture of cooperation amongst vendors, consumers, government agencies, and ethical hackers make it more likely that such a major problem would have been detected and fixed long ago. At the same time, the research team agreed to not publicly disclose the vulnerabilities until they had been fixed. This is a good example of how both responsible disclosure attitudes, and willingness by vendors to take action on reported bugs, have been shifting positively.

Conclusion

This article is not an argument in favor of any particular security vulnerability reporting and remediation mechanism. There are many differing attitudes to what degree of transparency is correct, how long a company should be given to fix a bug, what amount of compensation a researcher deserves, how to keep vulnerabilities out of the hands of bad

37 The Good Faith Cybersecurity Researchers Coalition – https://gfcrc.org

38 Zetter, Kim. Code Kept Secret for Years Reveals Its Flaw – a Backdoor. Wired Magazine, 24 Jul. 2023

guys, the role of government, the role of academia, the list goes on.

What is clear is that, even though positive change in how bugs are communicated and how researchers are treated is well in progress, there is a long way to go in terms of clear consistent, principles-based rules around the world. Laws must take into account not only the security of organizations creating and running software – their primary purpose is to provide security and stability for all.

Dullness and predictability are healthy for a society; we can only grow and prosper in a digital ecosystem when we know that there are no hurdles to securing the systems that we rely on as individuals and economic actors.

Similarly, we cannot simply hand-wave the bad guys away through legal mandates; we have to acknowledge that bad actors will always seek to find and abuse loopholes, including in the digital world. The best way to ensure that we are not only prepared but also resilient, is to transparently and critically think like them – and to confront flaws in all aspects of society heads-on and pragmatically so we can fix them, or at least realistically evaluate the risk that they bear.

It is vital that all stakeholders in society with an interest in secure software and digital services (in short, everybody) are at the very least informed about challenges, opportunities, and ongoing activities surrounding cybersecurity vulnerability and their detection and remediation.

Our world is digital, and runs on software – it's our elected officials' job to ensure that anyone can contribute easily and without risk to themselves to making that software as secure as possible. We already have many of the tools and norms to do so; now we need protection under the law for the white hats doing the heavy lifting in the world of vulnerability disclosure. ■

About the authors:

John Salomon has spent over 25 working in cybersecurity, risk management, operational resilience, technology, and strategy around the world. He has extensive experience in financial services and numerous other critical sectors, from keyboard jockey to senior leadership. A member of the Cybersecurity Advisors Network (CyAN), John is currently a board advisor, independent consultant, conference speaker, and investor with a focus on information security and fintech. He is based in Spain, together with his elite team of 8 feral cats.

Nick Kelly is a co-founder and member of the Secretariat of the non-profit GFCRC, a Coalition created to help advance legislation protecting researchers conducting Coordinated Vulnerability Disclosure. Nick is also VP for non-profit CyAN, a closed member network that serves as an incubator for globally impactful cyber-oriented initiatives. Nick's day job is as Business Development Director for SecureFlag, a secure coding training platform.

ARTICLE

EU Cyber Capacity Building: a Progressive Journey

LIINA ARENG
PROJECT DIRECTOR, EU CYBERNET

SILJA-MADLI OSSIP
COMMUNITY LEAD, EU CYBERNET

LAURI AASMANN
TRAINING AND SERVICES LEAD, EU CYBERNET

ABSTRACT:
The European Union (EU) and its Member States are dedicated to enhancing global cybersecurity through the EU Cyber Capacity Building Network (EU CyberNet). Established in 2019, EU CyberNet coordinates cyber expertise to support partner countries, align regulations with EU standards, and advise on national cybersecurity strategies. In 2022, the Latin America and Caribbean Cyber Competence Centre (LAC4) was inaugurated to promote international collaboration in cybersecurity. These efforts highlight the EU's commitment to a secure global cyberspace in the face of borderless cyber threats.

Keywords: cyber capacity building, international cooperation, financing, digital transformation

The European Union and its Member States have gained significant experience in working with cyber issues and are one of the leading providers of cyber capacity building (CCB) to partner countries.

The EU's formal commitment to cyber capacity building can be traced back to the first Cybersecurity Strategy of the European Union, which was adopted in 2013. This strategy marked the beginning of a more coordinated and comprehensive approach to addressing cyber threats and vulnerabilities. It outlined the EU's priorities in the field of cybersecurity, including enhancing cyber capabilities, promoting cooperation, and supporting Member States' efforts to develop robust cybersecurity policies and legislation.

The global CCB ecosystem has been evolving and there is a steady growth in the number and financing of relevant projects and involved actors, coupled with an evolving scope of CCB interventions and their interplay with other relevant fields of activity (e.g. digitalisation and digital infrastructure, disinformation, hybrid threats etc.) that create an additional layer of complexity and demand in the required expertise for the design and implementation of such actions. Different communities of practice (notably criminal justice, ICT security, foreign policy, digital development, human rights, defence etc.) continue working in interconnected dimensions of cyber issues and CCB in silos, often not connecting and even less so cooperating or drawing lessons from one another. This highlights the need for better cooperation across cyber communities of practice engaging in CCB activities, while the coordination mechanisms and practices amongst donors, implementors, partner countries and regional organisations, private sector, and civil society have yet to mature.

EU CyberNet – the Bridge to Cybersecurity Expertise in the European Union

The EU Cyber Capacity Building Network **EU CyberNet was launched in 2019** to improve the EU's ability to mobilise its collective expertise to support partner countries in building their capacity to defend against cyber threats and promote EU's good practices and standards in cybersecurity. EU CyberNet contributes to the global delivery of the EU's external cyber initiatives through running a 300+ member pan-European Expert Pool, carrying out training activities and providing a forum for exchanges of experiences and mutual learning among the large European Stakeholder Community of capacity building.

EU CyberNet is implemented by the Estonian Information System Authority (RIA) with the support from the Advisory Board partners – the Federal Foreign Office of Germany and the National Cybersecurity Competence Centre of Luxembourg. It is funded by the European Union and managed by the European Commission's Service for Foreign Policy Instruments.

The European Union is intensifying its focus on cyber capacity building due to the interconnected nature of cyberspace.

Recognizing that the well-being and economic stability of the European Union are interdependent with global developments, the EU is actively sharing knowledge, fostering international collaborations, and contributing to the enhancement of global cyber capabilities. Through this approach, EU is establishing a safer environment and increasing its own level of protection.

Enhancing EU Cyber Capacity Building: the Imperative for Effective Implementation

EU practitioners are called to design and implement CCB interventions against this complex backdrop and ensure coherence between CCB programming and the needs of partner countries with the EU's strategic vision and policies for cyberspace. This is essential given the increased available financing for CCB under geographic envelopes, but also due to the links with digital transformation and infrastructure, which are priorities for the EU's international cooperation. Before the conceptualisation of the "policy-first" and "value-driven" approach for the EU's overall external action as defined in the NDICI-Global Europe, the 2018 Council Conclusions on the EU External Cyber Capacity Building Guidelines had underlined that external cyber capacity building efforts should:

- support cyber resilience building in partner countries that contributes to an improved global digital ecosystem;
- foster strategic alliances aimed at promoting the notion of a global, open, free, stable and secure cyberspace in line with the EU's core values and principles, the rule of law, human rights, fundamental freedoms and democratic values;
- encourage the creation of formal and informal cooperation frameworks between partner countries and regions and the EU and its Member States;
- promote the EU's development commitments and the implementation of the 2030 Agenda for Sustainable Development.

To do so, EU staff need knowledge, tools and resources, such as the Operational Guidance for the EU's international cooperation on cyber capacity building that combines the different dimensions of cyber policy with international/development cooperation principles. Following a decade of increasing efforts in CCB, the 2020 EU Cybersecurity Strategy recognised that "EU capacity building efforts in the field of digitalisation should include cybersecurity as a standard feature" and that "to this end, the EU should develop a training programme dedicated to EU staff in charge of the implementation of EU digital and cyber external capacity building efforts".

A 3-Day Cyber Capacity Building Programme

In 2021, EU CyberNet developed an EU External Cyber Capacity Building training programme. This 3-day course is addressed to programme managers and policy officers in EU Delegations and headquarters who are not cyber specialists, but who are currently, or may in the future, be involved in the programming, identification, formulation and implementation of international cooperation actions with a cyber-specific or cyber-relevant focus.

The overall objective of the course is to convene a region-specific training workshop that will increase the EU practitioners' understanding of cyber concepts and provide them with methods, tools and approaches to design and implement CCB programming, i.e. with a distinct operational focus. The course aims to result in practical, user-friendly guidelines and constructive ideas for EU practitioners in addressing programming and implementation issues on how to cooperate with partner countries and support them in their efforts to strengthen their cyber resilience, their ability to address cybercrime and their capacity to engage in cyber diplomacy in a way that is coherent with EU values and policies.

The CCB trainings are designed and delivered with the specificities of a region in mind. Among the most recent CCB trainings organised by EU CyberNet, the following could be highlighted: in May for the EU Delegations in Asia-Pacific, in February for Sub-Saharan Africa, and in November last year for the EU Delegations in Latin America and the Caribbean.

Diverse Cyber Capacity Building Initiatives and Their Impact

In a team of EU CyberNet experts, an assessment was conducted on cyber regulations and draft legislation across multiple countries, with the aim

of aligning them with EU NIS Directive compliance objectives. This work facilitated discussions between the Commission and respective authorities to harmonize legislation with EU standards.

As another example, the project team provided expert support to the Critical Maritime Routes Monitoring, Support and Evaluation Mechanism (CRIMSON III) project in designing an action on cyber and maritime security.

Experts conceptualised, drafted and delivered a study on Cybersecurity in Maritime Critical Infrastructure. This desk research provides an assessment of the available maritime security (safety and cybersecurity) concepts for ports as well as security management standards, methodologies, best practices, tools, and frameworks, and analyses the existing legal and regulatory regimes. Furthermore, the report presents cyber threats and attacks that the maritime ecosystem (ports, ships, maritime companies, authorities, maritime supply chains) face due to rapid digitalisation.

In response to the request from the EU Delegation in Nairobi, EU CyberNet made recommendations to design and identify a new CCB project in Kenya, supporting the implementation of Kenya's cybersecurity strategy that was adopted in the autumn of 2022. Based on the feedback from the EU Delegation and Kenyan authorities, EU CyberNet has developed a primary concept of a possible study visit to Europe by Kenyan authorities (NC4) directly related to the implementation of the strategy.

In December 2022, EU CyberNet conducted an online seminar for Malaysian National Cybersecurity Agency at the request of the EU Delegation in Kuala Lumpur. Malaysia is drafting its new cybersecurity legislation (to be presented to the parliament in the end of 2023) and accordingly reached out to learn from the EU experience. Our team cooperated in the support activities with the Enhancing Security Cooperation in and with Asia (ESIWA) Project. EU CyberNet prepared and delivered a seminar on EU cybersecurity legislation, providing insights from key stakeholders in the EU, including aspects of the legal framework and implementation of legal acts from both the EU (ENISA) and Member States' perspectives.

A few months ago, EU CyberNet team got a request to give our opinion and thoughts on the Future Digital Program for Ecuador. The team found that the action document has great objectives, and it is properly linked with Ecuador's Digital Transformation Agenda. Our experts made suggestions to further elaborate on the impact of digitalisation in addressing the challenges the country is facing.

CCB Projects Mapping on External Cyber Capacity Building Actions

EU CyberNet has compiled a cyber capacity building mapping, which gives an overview of all EU funded external cyber capacity building projects (actions) around the world, as well as a variety of EU Member States activities. The mapping is an initiative of the Service for Foreign Policy Instruments (FPI) of the European Commission, conducted in cooperation with the European External Action Service (EEAS) and the Directorates-General for International Partnerships (INTPA) and Neighbourhood and Enlargement Negotiations (NEAR).

The main purpose of the mapping is to increase **operational awareness**, enhance **coordination**, **reduce fragmentation** and support various target groups (e.g. European Commission services, EU-funded projects & initiatives, EU Member State's actions etc.).

The mapping is not meant to be a comprehensive and final overview of all the actions in cyber domain but to provide a general overview of EU's and EU Member States' engagements in the cyber field around the world.

As of 1 January 2023, a total of 33 ongoing EU funded cyber capacity building actions were mapped with an estimated overall funding of almost 179 MEUR. The majority of the actions focus on cybersecurity (12), while 11 actions address cybercrime and 2 deal with cyber diplomacy. Geographically, the most funds have been directed to the EU's Neighbourhood (11 actions operate in the East, 7 in the Western Balkans and 4 in the South), followed by Sub-Saharan Africa (9 actions), Asia-Pacific (7 actions) and Latin America & the Caribbean region (5 separate actions).

There are also many external cyber projects and activities funded by the EU Member States and the mapping relies on their voluntary contributions. 15 EU Member States have provided information to EU CyberNet so far of about 40 projects with mostly regional and bilateral scopes.

The external cyber capacity building projects mapping has already **proven useful** for many counterparts of EU CyberNet and continues to be a good source of information. The online mapping with up-to-date information can be found at www.eucybernet.eu/ccb-table.

LAC4 – Latin America and Caribbean Cyber Competence Centre

LAC4, officially inaugurated in May 2022 with headquarters in Santo Domingo, the Dominican Republic, serves as a training and knowledge hub for sharing expertise in cybersecurity and cybercrime, facilitating practical collaboration between the Latin America and Caribbean region and the EU as well as other like-minded partners, and promoting the benefits of an open, free and inclusive cyberspace.

The LAC4 virtual hubs in Brazil, Ecuador, Costa Rica and Uruguay allow to promote subregional collaboration and enhance cyber capacities in the whole LAC region, delivered by the EU CyberNet though its Expert Pool and in collaboration with other EU-funded capacity building projects and international partners.

Cybersecurity requires an internationally coordinated approach and agile collaboration models. LAC4 aims to become an international, cross-sector effort, serving as a nexus for cooperation between national and international, public and private stakeholders. As an EU-founded Centre, LAC4 is optimally positioned in sharing know-how accumulated in the EU, and considers further alignment of policy goals and experience with like-minded partners indispensable to reach the overarching objectives of secure and sustainable digital transformation.

LAC4 has carried out around 50 training events since its establishment. The main focus has been facilitating cross-border collaboration in cyber crisis preparedness and response.

LAC4 has successfully organised 4 subregional table-top exercising, testing the countries' ability to nationally and regionally deal with large scale cyber incidents. EU CyberNet experts have also contributed to helping organisations across public and private sectors to deal with information security issues, organised hands-on trainings for CSIRTs and helped to train diplomats on the aspects of cybersecurity and cyberdiplomacy.

LAC4 is a practical example of a joint international commitment, forward-looking ambition and pooling of multicultural interdisciplinary knowledge for the common benefit of secure and trustworthy cyberspace.

Measuring Impact: The Transformative Power of EU CyberNet

In the light of the above information, the reader may wonder how one can measure the results and effects of capacity building projects and assess whether EU funds have been well spent.

In a study carried out this year, the EUCN sought evidence of the impact of project activities in its target countries. As the host country of our LAC4 training centre is the Dominican Republic and the project has an overview of the cybersecurity situation there, we carried out the impact analysis using the Dominican Republic as a case study. We analysed thirty activities that the project delivered for the Dominican cyber community aimed at improving cybersecurity in the Dominican Republic for the period 2021–2023. A series of exercises, trainings and awareness-raising events have created a whole new quality and added value to the Dominican cyber community. From a project perspective, the most impactful activities have been:

- Cyber Crisis Management tabletop exercises. The exercises are the most effective events to focus the attention of operational level leaders and have a tangible impact in terms of developmental leaps. Already after the first exercise in 2021, there was a significant improvement in communication between national leadership on cyber issues. Exercises are time-consuming but a valuable investment in terms of results;

- developing the concept of the Executive Cybersecurity and Digital Society Seminar (CIDI) and conducting training courses based on it. The training curriculum was handed over to the National Cyber Security Centre, which will continue to train Dominican officials based on it;

- training on designing and conducting cyber exercises. This unique cyber exercise training developed by EU CyberNet provided the Dominican Republic with a tool to test its preparedness for future cyber crises;

- training on cyber security for information security managers; crisis communication specialists; legal advisors, including judges, prosecutors and investigators; operators of critical services. The sectoral training courses will be tailored to the needs and input of local authorities and will thus address specific problem areas;

- events dedicated to the design of cyber security strategies which allow to share the experience of leading European countries and learn from the mistakes of others. The greatest value of these events is not only the advice on strategy design, but also the insight into the development of the strategy implementation plans, giving the strategy a practical dimension and value;

- technical training for CERTs. Organised in partnership with FIRST, the CERTs umbrella organisation, and relying on global best practices, these events will provide guidance on how to improve the organisational and technical capacity of CSERT-RD in responding to incidents;

- conducting a national cyber risk assessment and mapping of critical infrastructure, resulting in a whole new quality of crisis management in the country. In the Dominican Republic, the CII mapping had been done but needed to be revised in the light of new practices. Together with the national risk assessment, the country and operators are aware of their role and responsibilities in responding to cyber incidents.

According to the Dominican cyber security leadership, through various exercises, trainings and awareness-raising activities carried out under the EU CyberNet/LAC4 initiative, there has been an improved awareness of cyber threats among the public and private sectors, increased inter-agency interoperability, a more effective cyber crisis management capability, and a stronger incident management capability.

One widely accepted indicator of cyber security is a country's position in an international cyber security ranking or index. To assess the EUCN's performance in the Dominican Republic, we used the National Cyber Security Index (NCSI), a global index that measures countries' preparedness to prevent cyber threats, combat cybercrime and manage large-scale cyber incidents. The NCSI was developed by the Estonian e-Governance Academy in 2016 and is being developed in cooperation with the Estonian Ministry of Foreign Affairs. The index includes data from five assessments of the Dominican Republic, the earliest of which was conducted in 2018 and the most recent in January 2023. For the purposes of our analysis, we looked at Dominican's ranking in the index just before the EUCN project started in 2020 and the country's rise in the rankings in the following years.

It is interesting for the reader to know that the project team analysed each category of the index separately and went to the bottom of what caused the positive change in each case. The results confirm that EU CyberNet has played a decisive role in the improvement of the Dominican Republic's performance in the NCSI Index. Among the reasons for the improvement of the 2021 ranking, EU CyberNet activities were associated with four out of five improvements. In 2022, the improvement in performance was directly caused by the opening of the EU CyberNet LAC4 centre, and in 2023, EU CyberNet was involved in four out of six developments. From that we can unmistakeably conclude that the increase in the Dominican Republic's ranking in the e-Governance Academy's NCSI National Cybersecurity Index in 2021, 2022 and 2023 is directly attributable to EU CyberNet's activities in the Dominican Republic.

In addition to objective figures, we sought confirmation of our hypothesis from people working in the field of cybersecurity and interviewed Dominican officials and management. The interviews confirmed that the project has had a significant impact on the cyber resilience of the Dominican Republic. The Dominican officials in charge of the project rated the Dominican Republic's emergence as a serious cybersecurity implementer in the LAC region as a major achievement of the project.

A Safer Digital Future: The EU's Unwavering Commitment

In conclusion, the European Union and its Member States have exhibited enduring commitment to cyber capacity building, culminating in the establishment of the EU Cyber Capacity Building Network (EU CyberNet) in 2019. This journey has seen them evolve into prominent global contributors, emphasizing values like the rule of law, human rights, and democratic principles in the realm of cybersecurity. EU CyberNet, exemplifying this commitment, has become a beacon of knowledge exchange and support for partner countries. In an era where cyber threats transcend borders, the EU's steadfast commitment to empowering partners and securing a global, open, and stable cyberspace is a beacon of resilience. Together, we can continue building a safer digital future for all. ■

	Position in the overall ranking of the countries and score on the Index's rating scale			
e-GA National Cyber Security Index NCSI	**2019**	**2021**	**2022**	**2023**
Dominican Republic	63rd (42%)	52nd (53%)	51st (57%)	28th (71%)

About the authors:

Liina Areng – EU CyberNet Project Director. Liina has been leading the creation of the Latin America and Caribbean Cyber Competence Centre (LAC4) in the Dominican Republic since 2021.

Silja-Madli Ossip – EU CyberNet Community Lead. Silja has been involved in the EU CyberNet project since its inception and manages partnerships with stakeholders, EU institutions and other projects. Silja is also leading the initative ofMapping of the EU Cyber Capacity Building actions.

Lauri Aasmann – EU CyberNet Training and Services Lead. Lauri is coordinating the training and consultation missions and upholding the CyberNet's training and services catalogue since 2022. He organises the EU External CCB trainings for the EU Delegations and is the main point of contact for new service requests.

ARTICLE

European HR Community: a New Vision for Human Resources in Cybersecurity

ARNAUD DE VIBRAYE
JUNIOR MANAGER FOR SKILLS AND HUMAN FACTORS,
EUROPEAN CYBER SECURITY ORGANISATION (ECSO)

Keywords: human resources, cybersecurity skills, expert gap, cybersecurity personnel

Emerging Potential: The Increasing Role of Human Resources in Cybersecurity

Cybersecurity is a domain where everyone has a role to play. The multiplication and sophistication of cyber threats in all aspects of the economy and life have revealed the need to take into account human factors, and, consequently, human resources. Indeed, although HR practitioners are not the primary owners of cybersecurity risk management, their role in cybersecurity is considerably **evolving**, due to a **convergence** of factors.

The first factor is an **active regulatory environment** at the EU level with, for example, the NIS2 Directive, the Cyber Solidarity Act, and the Cyber Skills Academy. This will inevitably create an increasing demand for different kinds of experts, namely in the field of Governance, Risk, and Compliance (GRC), but also engineers, managers, and people that can communicate with both technical and non-technical experts.

The second factor is the pervasive use of **technology** and devices in employees' work has increased the cyber risks in companies and the recognition of the importance of a strong **cybersecurity culture**

at the office is now at the heart of the strategies of companies.

The third factor is that the cybersecurity sector is under great strain when it comes to human resources: the **expert gap** is estimated between 260 000 and 560 000 professionals. It is therefore essential to support HR in equipping Europe with the diversity of talent needed to respond to cyber threats and ensuring the cyber resilience of our society, economy, and infrastructure.

To deal with this challenge, the European Cyber Security Organisation, contributing to Europe's cyber resilience and digital autonomy, has created the European HR Community for Cyber, the cornerstone of ECSO's HR initiatives. Based on a community driven approach, this network of HR professionals fosters a **collective effort** with industry to develop a **solid HR ecosystem** to help reduce the workforce gap and speed up the hiring process in cybersecurity in Europe.

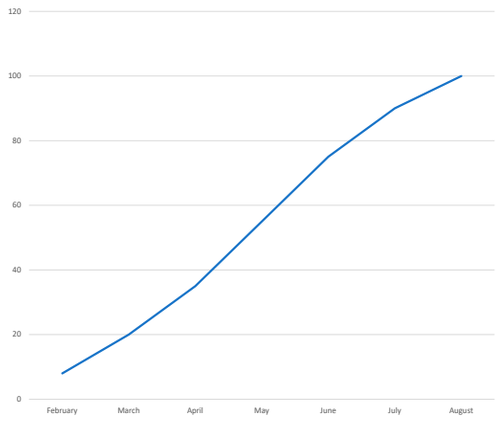


Figure 1 – Growth of the European Community in terms of members

Combining Forces: The European Community of HR Professionals in Cyber

With its European HR Community, ECSO aims at empowering HR practitioners with the skills, knowledge and tools necessary to better understand cybersecurity needs and equip Europe with the needed cyber talent. ECSO's approach is based on a combination of competencies between technical and non-technical experts. Therefore, we put great emphasis on the creation of communities of peers and to an effective collaboration mechanism between them.

Indeed, at ECSO, we encourage **dialogue** between peers and between HR and cyber experts (e.g. C-level experts) through **webinars**, **workshops**, and informal **meetings** to improve **communication**, exchange experiences and best practices. The aim of this community is to shape solutions to better address the current **needs** for experts in cybersecurity and to support the creation of an effective **talent pool**.

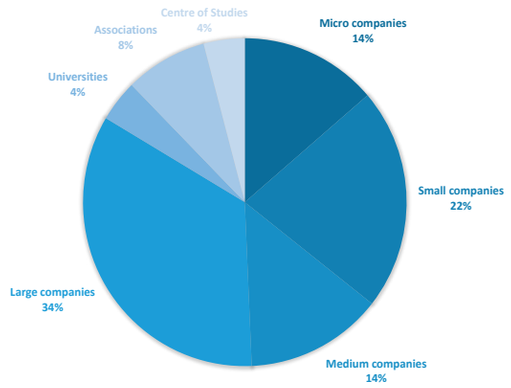


Figure 2 – Origins of the members of the European HR Community

To achieve this, ECSO is collaborating with Women4Cyber on the launch of a job platform and a talent pool for its HR community and members in general: **"Road2Cyber"**. This platform will be a fundamental tool for the European HR Community as it will help our members find the profiles they need, facilitate the posting of job offers and accelerate the recruitment process.

Focus on Talent Retention, Cybersecurity Awareness and Diversity

At ECSO, we think that the main challenge in human resources is the pedagogy and clarifying the role of HR in cybersecurity, at a time where threats are becoming more widespread, particularly for businesses. In other words, the HR has to gain skills in cyber to better **define** the **needs** of companies for cybersecurity personnel. HR managers will also benefit from this community of peers by gaining skills to address talent recruitment, retention, and the fostering of a sound cybersecurity culture within companies, as a result of collaboration with C-level experts.

Another challenge is that the IT sector suffers from a lack of diversity (gender balance etc.), and the cyber sub-sector is no exception to this. The European HR Community, an ECSO initiative supported by Women4Cyber, intends to bring up new ideas and solutions on how companies can support women's professional development in cybersecurity to make the sector more diverse.

Building the Road to Cyber: What Next for the European HR Community?

Towards the end of 2023, we expect to launch the platform Road2Cyber. This platform, linked to Women4Cyber, will include a training portal (emanating from the Women4Cyber Academy) and a job portal. The latter will allow a better visibility of the job offers while supporting HR in posting job descriptions and job seekers in getting access to an extensive and complete database of opportunities across Europe. This will provide a comprehensive approach to building the European cybersecurity workforce (from education to hiring).

In the long term, the European HR Community for Cyber is expected to strengthen its national presence, based on the involvement of points of contact in European countries, selected among the HR community members. Said points of contact will be the main references at the national level to contact companies, reach out to HR practitioners and organise events. Eventually, ECSO aims to support the European HR Community for Cyber with knowledge about the current state of the cyber workforce in Europe. To do so, ECSO is mobilising national cyber actors to gather information, studies and data on the current state of affairs in their respective countries.

Figure 3 – Representation of each HR Community members

The road to cyber is not a long and quiet river but will contribute to mobilise the needed resources to deliver tangible results for the future European cyber workforce.

While the European HR Community is open to both ECSO members and non-ECSO members, ECSO members will get priority and free access to activities and tools as well as the opportunity to take part in the future direction of the community, in line with ECSO's wider strategic objectives. To become a member of ECSO and get immediate access to the European HR Community as well as a range of other activities and services, check out our website.

About ECSO

The European Cyber Security Organisation (ECSO) is a non-for-profit organisation, established in 2016. ECSO unites more than 270 European cybersecurity stakeholders, including large companies, SMEs and start-ups, research centers, universities, end-users, operators, associations, national and regional administrations. ECSO works with its Members and Partners to develop a competitive European cybersecurity ecosystem providing trusted cybersecurity solutions and advancing Europe's cybersecurity posture and its technological independence. ■

About the author:

Arnaud de Vibraye is Junior Manager for Skills and Human Factors at the European Cyber Security Organisation (ECSO). He holds a MA in European Security and International Stability from Science Po Strasbourg (France) and a MA in European Interdisciplinary Studies from the College of Europe in Natolin (Poland), where he wrote his Master Thesis to analyse the action of the European Union as a cyber security provider. In 2023, he joined ECSO to further contribute to the development of a European cyber security ecosystem for the strengthening of the digital autonomy of Europe. He is contributing to ECSO initiatives to mobilise cyber actors to develop education, awareness, and to empower HR practitioners and fill the workforce shortage in Europe. He is also involved in the launch of an ECSO European research project on the current state of the cyber workforce in EU and associated countries.

References

Greenlee, M. (2023). The Role of Human Resources in Cybersecurity. Security Intelligence. https://securityintelligence.com/articles/role-human-resources-cybersecurity/

Marinelli, I. (2023). Closing the cybersecurity talent gap: the Commission launches the Cybersecurity Skills Academy. Digital-Skills-Jobs.europa.eu. Retrieved September 8, 2023, from https://digital-skills-jobs.europa.eu/en/latest/news/closing-cybersecurity-talent-gap-commission-launches-cybersecurity-skills-academy

Olesen, N. (2022). Unlocking our potential: Cybersecurity education and workforce needs in Europe. ECSO. https://ecs-org.eu/unlocking-our-potential-cybersecurity-education-and-workforce-needs-in-europe-2/

Riddle, J. (2019). What's the Role of HR in Cybersecurity and Why Is It Important? Blog.devolutions.net. https://blog.devolutions.net/2019/07/whats-the-role-of-hr-in-cybersecurity-and-why-is-it-important/

ARTICLE

Cybersecurity Governance in Indonesia and the Netherlands: Towards More Cooperation

OSKAR J. GSTREIN
ASSISTANT PROFESSOR, DEPARTMENT OF GOVERNANCE AND INNOVATION AT CAMPUS FRYSLÂN OF THE UNIVERSITYOF GRONINGEN

TAIS FERNANDA BLAUTH
PHD RESEARCHER, DEPARTMENT OF GOVERNANCE AND INNOVATION AT CAMPUS FRYSLÂN OF THE UNIVERSITY OF GRONINGEN

FAIZ RAHMAN
ADJUNCT RESEARCHER, CENTER FOR DIGITAL SOCIETY (CFDS); LECTURER, FACULTY OF LAW, UNIVERSITAS GADJAH MADA, INDONESIA, PHD RESEARCHER, LEIDEN LAW SCHOOL, UNIVERSITEIT LEIDEN

ANISA PRATITA KIRANA MANTOVANI
ADJUNCT RESEARCHER, CENTER FOR DIGITAL SOCIETY (CFDS), UNIVERSITAS GADJAH MADA, INDONESIA; HEAD OF PUBLIC POLICY AND GOVERNMENT RELATIONS, INDONESIAN E-COMMERCE ASSOCIATION (IDEA)

ANNISA PARAMITA WIHARANI
ADJUNCT RESEARCHER, CENTER FOR DIGITAL SOCIETY (CFDS), UNIVERSITAS GADJAH MADA; PHD RESEARCHER, DEPARTMENT OF INTERNATIONAL RELATIONS AND INTERNATIONAL ORGANIZATION, UNIVERSITY OF GRONINGEN

ABSTRACT:
This article analyses cybersecurity frameworks which address cybercrime, safeguarding critical infrastructure, approaches to cyberwar and cyberespionage in Indonesia and the Netherlands. We compare approaches addressing cybersecurity-related challenges in an international context. While Indonesia and the Netherlands share some common history, significant differences in geographical location, population size, socio-economic status, and other factors remain. Despite substantial differences, both nations face comparable challenges, which present opportunities for closer cooperation. This paper underscores the need for making a concerted effort to foster dialogue and collaboration.

Keywords: cybersecurity, Indonesia, Netherlands, governance, cooperation, regulation

Funding notice: Research on this paper was funded through a Nuffic/Orange Knowledge Programme grant (OKP-TMT+.20/0011) aiming at 'Enhancing Higher Education Capacity for An Interdisciplinary Cybersecurity Study Program'. This project was implemented in collaboration between researchers of the Center for Digital Society (CfDS), located at the Faculty of Political Sciences, Gadjah Mada University, Yogyakarta/Indonesia and the Data Research Centre (DRC) at Campus Fryslân, University of Groningen/The Netherlands.

1. Introduction

The number of cyberattacks has grown in recent years (Europol, 2021, pp. 10–16), especially during the COVID-19 pandemic (Chigada & Madzinga, 2021). Increasing geopolitical tensions and the use of emerging technologies such as machine learning to enhance cyberattacks reinforce this development (Brooks, 2023). This illustrates the need for national governments to deal with cybersecurity-related issues. Studies considering such efforts frequently focus on the comparison of policies of a few very large and powerful actors – such as the United States or the People's Republic of China (see e.g. Jisi & Ran, 2019; Goel, 2020). In this article, we compare Indonesia and the Netherlands.

While the two countries have some shared (colonial) history, they face similar cybersecurity-related challenges emerging in the 21st century. Nevertheless, the different socio-economic and geopolitical context remains relevant and provides fertile ground for analysis and discussion from an unconventional angle.

Indonesia has the fourth-largest population among countries globally and the 10th largest purchasing power parity economy, making it the largest economy in Southeast Asia (World Bank, 2022). Moreover, Indonesia is ranked 9th for average daily internet use, with 204.7 million internet users – 73.7% of the total Indonesian population (social & KEPIOS, 2022a). As a developing

country and emerging economy in the world, these statistics illustrate considerable economic potential, especially when considering its innovative use of data and e-commerce. The Netherlands, in contrast, has one of the highest Internet penetration rates in the world. A report shows that Internet users in the Netherlands have reached 16.5 million, which is 96% of the of the country's total population (social & KEPIOS, 2022b). Thus, the threat of cyberattacks increasingly affects the lives of the Dutch population and the Dutch economy. With this article, we aim to raise awareness of the differences and commonalities between the two countries to identify themes for enhanced cooperation. This study might also be relevant for European states with comparable historical relationships with countries outside the continent.

1.1 Context of the study

Indonesia and the Netherlands are key partners in many different areas. As proposed by Robert Keohane and Joseph Nye (1998, pp. 77, 81), the interconnectedness of states through numerous channels emphasizes the importance of cooperation when addressing shared challenges. Indonesia and the Netherlands share a complex web of interdependencies through channels such as trade, diplomacy, and technological networks. Specifically, Indonesia and the Netherlands collaborate, for instance, in the economic (Kingdom of the Netherlands, 2020), educational (Nuffic, 2023), and cultural sectors (Vermeulen, 2020). In addition, the countries have been strengthening their cooperation in cybersecurity. As Indonesia and the Netherlands have established bilateral trade and investment relations in various sectors, enhancing cybersecurity collaboration is crucial to safeguard the thriving trade and investment partnership in various industries. Cyber threats have the potential to severely affect business operations, confidential information, intellectual property, and innovative creations. Collaborative cybersecurity governance efforts can ensure the continuity and secure the bilateral economic activities and trade flow. Among the initiatives, we highlight those presented in Table 1.

Year	Agreement/Initiative	Remarks
2018	Letter of Intent expressing the commitment of the governments to enhancing bilateral cooperation in cyberspace, signed on 3 July of 2018.	This letter was signed by the Foreign Minister of the Netherlands, Stef Blok, and the Head of the Indonesian National Cyber and Crypto Agency in Jakarta.
2019	ASEAN-EU Statement on Cybersecurity Cooperation	This document emphasized the commitment of ASEAN and the EU, in which Indonesia and the Netherlands are part of the respective organizations, to promote an open, secure, stable, accessible, and peaceful ICT environment through strengthening cooperation on cyber issues.
2019	EU-Indonesia's 4th Security Policy Dialogue, 12 November 2019	The dialogue aimed at strengthening EU-Indonesia cooperation on security issues, including cybersecurity. The commitment for cooperation further emphasized in the 5th and 6th Security Policy Dialogue in 2020 and 2021.
2017-2022	Orange Knowledge Programme (OKP) - Nuffic	The Dutch OKP aims at contributing to "societies' social and economic development by strengthening knowledge and skills of professionals and organisations". Indonesia has been one of the participating countries and cybersecurity one of the priorities of the programme.
2021	Indonesia-Netherlands Cyber Policy Dialogue, held on the 21stof January of 2021.	The dialogue reinforced "the two countries' ongoing commitment to enhance bilateral engagement on, and mutual understanding of, cyber issues".
2021-2022	OKP Tailor-Made Training Plus – 'Enhancing Higher Education Capacity for an Inter-Disciplinary Cybersecurity Study Program'	The Ministry of Foreign Affairs of the Netherlands provided funding for grants within the OKP, managed by the agency Nuffic (OKP-TMT+.20/00119). One of the projects was focused on capacity building in the field of cybersecurity, promoting collaboration between higher education institutions in Indonesia and the Netherlands. This article was written as part of this initiative, by an independent and international team of researchers, both from Indonesia and the Netherlands.

Table 1. Selected Indonesia-Netherlands Cooperation Initiatives Related to Cybersecurity. Source: Compiled by Authors, 2023.

As Indonesia's digital population continues to grow rapidly, the need for effective cybersecurity measures becomes increasingly crucial. The country has faced numerous challenges securing its diverse and expansive digital ecosystem as the accelerated growth of internet users and mobile internet connections increase the number of cyber threats and cyber-attacks to a level which has not been seen before. From 2019 to 2021, Indonesia experienced a 5-fold increase in cyberattacks (Kiswondari, 2021). The National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN) noted that throughout 2021, there were 1,637,973,022 traffic anomalies detected, which is a significant increase from the 2020 figure of 495,337,202 (Rahman et al., 2021). The number of cyberattacks has surged with various types of attacks emerging, such as malware deployment, capturing websites, data breaches, data manipulation, as well as illegal content distribution (National Information and Communication Technology Council, 2018). The vulnerabilities are further exacerbated by infrastructure with poor cyber-resilience and generally low digital literacy rates. Moreover, Indonesia does not have a comprehensive Cybersecurity Act to provide a legal basis for cybersecurity. Hence, cybersecurity is currently regulated through various sectoral acts and implementing legislation.

Ultimately, collaboration with the Netherlands could provide valuable insights and guidance as Indonesia continues to develop and enhance its cybersecurity governance mechanisms. Such a partnership could benefit both countries, especially as cybersecurity threats multiply.

As for the Netherlands, the country is in a unique position to capitalise on the opportunities brought about by digitalisation. Nevertheless, cyber-attacks and threats are on the rise as cybercriminals continuously develop new ways to commit various

types of attacks and exploit system vulnerabilities (National Cyber Security Centre, 2019). In particular, the deployment of ransomware and Distributed Denial of Service (DDoS) attacks pose a considerable threat to national security and may have disruptive consequences for society. Therefore, the country needs to strengthen its defences against cybercrime, in particular through enhanced cooperation between the public and private sectors (National Coordinator for Counterterrorism and Security, 2022, pp. 15–18). This includes improving the country's digital resilience and ensuring that laws and regulations stay up to date, which is also mandated by emerging strict regulation of the European Union.

Collaboration can help both countries to benefit from each other's advancements and contribute to developing cutting-edge cybersecurity solutions. In addition to that, the historical ties between Indonesia and the Netherlands may serve as a foundation for closer collaboration in various areas, including cybersecurity governance. Building upon these historical connections can foster trust, mutual understanding, and shared objectives, which in turn can facilitate more effective joint efforts in addressing cybersecurity challenges. It is essential to recognize the potential benefits of such collaboration and work towards leveraging these historical ties for the greater good.

1.2 Methodology

The examples in Table 1 demonstrate a wide range of collaborative initiatives between the Netherlands and Indonesia, including, but not limited to, raising awareness, increasing cyber resilience, and capacity building. This article aims to investigate how Indonesia and the Netherlands compare in terms of cybersecurity regulation and governance. To this end, we evaluate the international and regional contexts of the countries, analyse national frameworks, and discuss recent challenges. Moreover, we seek to answer the following sub-questions:

- Which issues are being identified by both countries relating to cybersecurity?
- Which common characteristics can be identified by comparing the different national governance models in an international context?
- How do Indonesia and the Netherlands contrast in their cybersecurity national governance models?
- What are the main possibilities for further cooperation between the countries in cybersecurity on a bilateral and multilateral level?

This methodology is based on an analysis of government documents and websites, reports, and academic literature. We have only reviewed papers/documents/reports/web pages available in English, Dutch, German and Indonesian, due to the composition of the research team, with researchers from Europe and Indonesia.

2. Indonesian Cybersecurity Governance Framework in a Nutshell

The Indonesian government has paid increasing attention to cybersecurity issues in response to the rise in cyberattacks and cybercrime over the past decade. Cybercrime was explicitly mentioned as a top priority in the previous Indonesian National Medium-Term Development Plan.[1] The RPJMN 2020-2024[2] states that the development of the current national cybersecurity governance framework is based on indicators of the Global Cybersecurity Index (GCI), which consists of five pillars. The pillars cover legal, technical, and organisational aspects, as well as capacity development and cooperation (International Telecommunication Union, 2020, p. vii.). See Table 2 for more detailed information compiled by the authors.

1 RPJMN – see e.g. Appendix of Presidential Regulation No. 5 of 2010 on National Mid-Term Development Plan Year 2010-2014 2, Book II Strengthening Inter-Sectoral Development Synergy, II.5-13, 5-42-43, 6-49; Appendix of Presidential Regulation No. 2 of 2015 on National Mid-Term Development Plan Year 2015-2019, Book II Sectoral Development Agenda, 5-35, 9-24-25).

2 See Appendix IV of Presidential Regulation No. 18 of 2020 on National Mid-Term Development Plan Year 2020-2024, A.7.44-A.7.46

Stakeholders & Governmental Actors	
National Cyber and Crypto Agency (BSSN)	An executive agency with primary responsibilities in the field of cybersecurity. It focuses on the formulation, establishment, and implementation of technical policies in the field of cybersecurity. The BSSN also coordinates the formulation of the National Cyber Security Strategy. The ID-SIRTII/CC is currently coordinated by the National Cyber Security Operations Centre at the BSSN.
Ministry of Communication and Informatics	The primary institution dealing with content violations in cyberspace. It has the power to remove illegal content. In recent years, the MCI has also been concerned with raising cyber security awareness, improving the quality of human resources, and improving cyber security technology.
Ministry of Defence	One of the leading institutions in developing cyber security and resilience in Indonesia's defence sector, including through the development of a cyber defence strategy.
Indonesian National Armed Force (TNI)	The National Armed Forces are implementing cyber defence measures. They are at the forefront of cyber warfare. In recent years, cyber defence has become a regular discussion among three branches – Army, Navy and Air Force. The National Armed Forces also carry out a routine cyber defence exercise and promote several initiatives to improve the cyber-related skills of soldiers.
Indonesian National Police (POLRI)	The National Police has a Cybercrime Directorate, which is part of the Criminal Investigation Unit.
National Intelligence Agency (BIN)	The National Intelligence Agency's focus is on strengthening cyber intelligence as a means of early detection of threats, challenges, and disturbances from domestic and abroad.
Personal data protection authority (*Lembaga Pelindungan Data Pribadi*, to be established)*	The Personal Data Protection (PDP) Authority is a new institution introduced to implement the recently enacted PDP Act. This authority is designed as an executive agency. The PDP Authority is yet to be formally established. The establishment will be regulated through a Presidential Regulation.
Legislation	
Electronic Information and Transactions Act (EIT Act)	This is currently the main act regulating cyberspace in general. The act regulates 'prohibited acts', including illegal access, interception, data and systems interferences, misuse of devices, computer-related forgery, computer-related fraud, and speech-related violations.

Electronic Information and Transactions Act (EIT Act)	This is currently the main act regulating cyberspace in general. The act regulates 'prohibited acts', including illegal access, interception, data and systems interferences, misuse of devices, computer-related forgery, computer-related fraud, and speech-related violations.
Personal Data Protection Act (PDP Act)	On 20 September 2022, the House of Representatives passed the PDP Bill. The new PDP Act effectively came into force on 17 October 2022. The PDP Act defines personal data, establishes rights of data subjects, regulates the processing of personal data, the obligations of the data controller and data processor, as well as inward and outward transfer of personal data. It establishes sanctions (administrative and criminal), a data protection authority, international cooperation, community participation, dispute resolution, as well as individual remedies.
Telecommunication Act	The Act imposes obligations on public and private telecommunications operators to protect telecommunications equipment and networks from any interference and to maintain the confidentiality of information in telecommunications networks. This Act also serves as the legal basis for the establishment of the ID-SIRTII/CC, which is currently being coordinated by the BSSN.
Government Regulation on Implementation of Electronic Systems and Transactions (GR EST)	This is the implementing regulation of the EIT Act. The GR EST further regulates the obligations of electronic system providers in the public and private sectors to secure their electronic systems by fulfilling various requirements provided. Moreover, the GR EST also provides several articles related to personal data protection, including principles and obligations for Electronic System Provider to protect their users' data.
Presidential Regulation on Electronic-Based Government System	This Presidential Regulation emphasises the importance of security as a central aspect of developing an Electronic-Based Government System (SPBE). The National SPBE Master Plan also highlights that strengthening security is one of the priority agendas in the first phase of the SPBE strategic plan.
Presidential Regulation on National Cyber and Crypto Agency	The Regulation serves as the legal basis for the establishment of National Cyber and Crypto Agency (BSSN).
Presidential Regulation on Vital Information Infrastructure Protection	The purpose of this Regulation is to protect the public interest against any disruption of vital information infrastructure caused by the misuse of electronic information and transactions that disrupt public order.
Minister of Defence Regulation on Cyber Defence Guidelines	This regulation serves as guidance for the Ministry of Defence and National Armed Forces to implement cyber defence. The guideline covers four essential aspects to be developed—policy, organisation, technology, and human resource.
Indonesian Criminal Code	This act is frequently being used by the National Police for tackling issues concerning cybercrime, especially fake news in the digital space. On 2 January 2023, the new Indonesian Criminal Code was enacted, which repealed the previous Criminal Code. The new Criminal Code also revoked several articles related to cybercrime offences previously regulated in the EIT Act.
Initiatives and Tools	
Technical	• ID-SIRTII/CC – currently under BSSN coordination. • Gov-CSIRT – sectoral CSIRT. • Organisational Standards such as Indonesia's National Standard (Standar Nasional Indonesia - SNI) IEC/ISO 27001:2013, SNI ISO/IEC 27018:2016, Trust+Positive, and KAMI (*Information Security Index*). • Standard for Professional from National Standard of Work Competency.
Capacity Building	• BSSN's National Polytechnic of Crypto and Cyber (*Politeknik Sandi dan Siber Nasional*, *Poltekssn*). • Cyberhub.id, a digital hub that brings various government and non-government stakeholders to form a cybersecurity ecosystem in Indonesia. • Cybersecurity Hub by Ministry of Education and Culture. • Born to Control – Cybersecurity Talent Pool. • National Digital Literacy Movement (GNLD). • Digital Intelligence Course (*Kelas Kecerdasan Digital*) – MCI, UGM, and various industries and associations.
Cooperation	• Indonesia - KOICA- ITB in cyber investigation. • Plans to develop cooperation with Singapore to Defence Industry and Cyber Defence. • MIKTA interregional cooperation. • Cooperation with Industries, such as Huawei, Cisco, EC-Council.

Cooperation	• Bilateral cooperation in cybersecurity with e.g., Australia, South Korea, Romania, the Netherlands, and the UK. • Triple helix collaboration between the MCI with association, academic community, and also industries.

Table 2. Indonesia Cybersecurity Governance. Source: Compiled by Authors, 2023.

Indonesia is still developing a comprehensive Cybersecurity Act. Currently, legislation related to cybersecurity is scattered over various sectoral laws. Accompanying regulations are being used to implement them (Indonesia, 2019). The main acts and implementing regulations include the Electronic Information and Transactions Act (EIT Act), the Telecommunications Act, the Government Regulation on the Implementation of Electronic Systems and Transactions (GR EST), the Presidential Regulation on the Protection of Vital Information Infrastructure (PR VIIP), and the Minister of Communications and Informatics Regulation on the Protection of Personal Data on Electronic System. Although other sectoral laws and implementing regulations with provisions related to cybersecurity exist, most of them only regulate cybersecurity-related aspects in general (Hidayat & Juaningsih, 2022).

Regarding stakeholders and government actors, the main actor specifically assigned to implementing cybersecurity promoting measures is the National Cyber and Crypto Agency (BSSN). The main tasks of this executive agency concerning cybersecurity are to formulate, establish, and implement technical policies in the field of cybersecurity (Indonesia, 2021). Given the broad scope of cybersecurity, other government institutions also have a role in implementing cybersecurity, including the Ministry of Communications and Informatics (MCI), the Ministry of Defence, the State Intelligence Service, the National Police, and the National Armed Forces.

Apart from legislation and stakeholders, the Indonesian government has also implemented several initiatives and tools through various institutions. The intent is to leverage the potential of cyber-resilient infrastructure, foster technical readiness, and promote digital literacy. These initiatives result from cooperation between the government and stakeholders on the national and international levels.

3. The Dutch Cybersecurity Governance System

This section provides a high-level overview of cybersecurity governance in the Netherlands. It first turns to institutions and frameworks existing at the national level, before briefly elaborating on the European and International context – which is rapidly changing in the aftermath of the invasion of the Russian Federation in Ukraine.

3.1 National level

The main stakeholders that can be identified are governmental actors such as the National Cyber Security Centre (NCSC), the Cyber Security Council (CSR), the Radiocommunications Agency, as well as the General Intelligence and Security Service of the Ministry of the Interior and Kingdom Relations (AIVD). While cooperating, these institutions have different roles in enhancing the Dutch cybersecurity level. An overview of relevant legislation is provided in Table 3.

Stakeholders & Governmental Actors	
National Cyber Security Centre (NCSC)	Key organization within the cybersecurity framework. As part of the Ministry of Justice and Security, the NCSC is responsible for "making the Netherlands more resilient to cybercrime".
Cyber Security Council (CSR)	This independent advisory body of the Dutch government is focused on working at the strategic level to strengthen cybersecurity in the country. In this capacity, the CSR provides advice, expert reports, organizes meetings and symposiums, among other activities.
Radiocommunications Agency	The Radiocommunications Agency (in Dutch, *Agentschap Telecom*) is designated as the National Cybersecurity Certification Authority (NCCA) in the Netherlands. The responsibilities and powers of the NCCA are detailed in the Cybersecurity Act.
General Intelligence and Security Service of the Ministry of the Interior and Kingdom Relations (AIVD)	The AIVD safeguards national security by identifying risks and threats before they become apparent through the gathering of intelligence and risk analysis. Its tasks and areas of interest are detailed in the 2017 Intelligence and Security Services Act (Wiv 2017).
Legislation	
Security of Network and Information Systems Act (Wbni Act)	In effect since 9 November 2018. According to the Wbni Act, suppliers of critical services, digital services providers, and the central government must take measures to prevent cybercrime, protecting their network and information systems. In addition, these organisations must report cybersecurity incidents to the NCSC. The main aim of the Wbni is to mitigate the consequences of cyber-attacks while increasing the country's digital resilience.
Ministerial Decision on Network and Information Systems Security (Bbni)	Created to clarify some aspects of the Wbni. For example, it details what the essential service providers are and how an incident should be reported.
Dutch Telecommunications Act	According to the Dutch Telecommunications Act (in Dutch, *Telecommunicatiewet*), providers should "minimize the risk of threats to their safety and security, ensure continuity and notify the competent authority of any cyberthreats or incidents".
Selected Dutch criminal laws	Police Data Act, Criminal Data Act, Dutch Criminal Code (Wvsr), and Computercrime I, II, III Acts.

Initiatives and Tools	
Netherlands Fraud Help Desk	Offers information and shares cybersecurity-related trends in the country. It also provides warnings against frauds and scams, sharing relevant and updated information and alerts on the website and social media. Without any investigative capacity, the Help Desk focuses on raising awareness and protecting people against cybercrime.
Digital Trust Center (EZK)	The Digital Trust Center helps enterprises to have their digital security in order and ensures that they are digitally resilient.
Information Sharing and Analysis Centers (ISACs)	ISACs are non-profit organizations gathering information on cyber threats and allowing two-way sharing of information between the private and public sector.

Table 3. The Netherlands Cybersecurity Governance. Source: Compiled by Authors, 2023.

The Netherlands has imposed various types of regulations, standards, and protocols for organisations to follow in data handling and in information security. Furthermore, the Netherlands has also passed various criminal provisions detailing many digital crimes – the most important ones are mentioned in Table 3 as well. Lastly, the Netherlands has rolled out various initiatives and tools that help the country not to fall victim to cybercrime. An important initiative of this kind is, for instance, the Fraud Help Desk, administrating all recent reports of country-wide frauds (Fraudehelpdesk.nl, 2023). Finally, enterprises and organisations are being engaged through various initiatives whose aim is to help ensure compliance with all cybersecurity requirements.

3.2 European and international level

Considering the political and geographical position of the Netherlands, it is also important to take into account initiatives at the international level – particularly the Council of Europe and the European Union. While it goes beyond the scope of this article to mention all relevant frameworks in detail, it is appropriate to name the most important ones. It should also be stressed that in this section, we focus on frameworks directly addressing cybersecurity, whereas related frameworks, such as the 2016 EU General Data Protection Regulation, might also have a considerable impact on the cybersecurity landscape (Wicki-Birchler, 2020). Some of them might also create pathways towards more cooperation – or at least indirect harmonisation of laws – with Indonesia.

As the only internationally binding treaty on the subject, the Budapest Convention on Cybercrime – also known as the 2001 Convention on Cybercrime – is of central importance (Wicki-Birchler, 2020, p. 65). The Convention aims to regulate cybercrime and create a standardised policy to protect society against cyber threats. As of July 2023, 68 states have ratified the convention, with additional 2 states having provided signatures in the absence of ratification (Council of Europe, 2023). The Netherlands ratified the convention in 2006. According to the Budapest Convention, ratifying states should align their national laws and procedures with its provisions, either by creating new laws or amending existing ones. It remains the most significant international instrument addressing cybercrime and is open to ratification by states that are not members of the Council of Europe. The Convention has gained recognition worldwide, with countries like the United States, Argentina, Australia, Canada, and Japan, as well as many others across Africa, Asia, Latin America, and the Pacific Ocean, signing and ratifying it (Council of Europe, 2023).

The convention has been extended through two additional protocols. The first protocol, focusing on xenophobia and racism, aimed to penalise acts of a racist and xenophobic nature committed through computer systems (Council of Europe, 2006). In 2021, a second protocol was added, addressing enhanced cooperation and disclosure of electronic evidence across borders (Council of Europe, 2022; Spiezia, 2022). This protocol aims to facilitate cross-border investigations and overcome challenges posed by shifting or unknown jurisdictions in the digital age.

At the level of the European Union, the Network and Information Security (NIS) Directive from 2016 was the first EU-wide legislation on cybersecurity. It is aimed at achieving a high common level of cybersecurity across Member States (Markopoulou et al., 2019). However, its implementation faced challenges, leading to fragmentation in the European Union and differences between the Member States. In response, the European Union worked on the NIS2 Directive, which aims to strengthen security requirements, address supply chain security, streamline reporting obligations, and introduce stricter supervisory measures and enforcement requirements, including harmonised sanctions across the EU. NIS2 was adopted by the European Parliament and the Council in November 2022, entering into force on 16 January 2023. Member States have until 17 October 2024 to transpose their measures into national law (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive), 2022; Schmitz-Berndt, 2021; Schmitz-Berndt & Chiara, 2022).

However, in Member States such as the Netherlands, questions remain on how to concretely transpose the enhanced lists of cybersecurity requirements in public and private sector organisations (e.g. which institutions count as essential services providers, which as digital service providers, how to implement heightened technical and organisation cybersecurity requirements, etc.).

These developments must be considered together with establishing the 2019 EU Cybersecurity Act, a framework that strengthens the mandate of the European Union Agency for Cybersecurity (ENISA). The Cybersecurity Act contains provisions to establish certification schemes enhancing the security of information and communications technology products, services, and processes (European Union, 2023b). Considering the most recent events in Ukraine, the European Commission has further proposed to work on a Cyber Resilience Act (European Union, 2022) and a Cyber Solidarity Act (European Union, 2023a). The former should result in a comprehensive and enhanced cybersecurity framework to guarantee cybersecurity over the entire product lifecycle on the European single market, whereas the latter establishes emergency funding to tackle big cyber-incidents with the support of ENISA and the European Cybersecurity Competence Centre established in 2021.

4. Comparison and Pathways Towards Enhanced Cooperation

In this section, we compare the analysis presented above and summarise it along guiding themes such as legislation and international cooperation, technology and infrastructure, human capacity, and digital literacy.

4.1 Legislation & international cooperation

As outlined in Table 1, several bilateral and multilateral efforts have been made to pave the way towards more cooperation between Indonesia

and the Netherlands. However, such initiatives remain limited to political statements of intent or cooperation among research institutions. This raises the question of whether overarching international frameworks have indirectly affected harmonisation. Although Indonesia has not formally ratified or accessed the Council of Europe's Budapest Convention, it has been highly influential in shaping the country's approach to national cybersecurity governance. The Indonesian EIT Act of 2008, particularly Chapter VII, lists similar offenses to those outlined in the Convention on Cybercrime, although several articles were revoked by the newly enacted Indonesian Criminal Code.

Additionally, content-related offences in Indonesia are regulated per the Convention's provisions. Thus, the Convention has played a significant role in framing Indonesia's cybersecurity governance framework. Whether the recent EU efforts mentioned above will have a similar effect seems too early to conclude at this point.

4.2 Technology & infrastructure

Both countries recognise the need for improved infrastructure to mitigate cyberattacks risks. In Indonesia, cyberattacks through malware, website defacement, data breaches, and data manipulation have increased significantly in recent years. Moreover, Internet users are becoming increasingly suspicious of the practices in the IT/technology industry (UGM, 2022b), while there are questions from the government regarding reliance on foreign data platforms. Such issues are also well known in the Netherlands, as the country experiences an increasing amount of cyberattacks but also faces questions relating to international data transfers (e.g. to the United States; see e.g. Gstrein & Zwitter, 2021). In the past years, DDoS and ransomware attacks have targeted educational institutions, the financial sector, public organisations, and Internet Service Providers. Furthermore, the reported number and duration of DDoS attacks have been significant, putting the Dutch National Internet Providers Management Organisation in a difficult position to defend against those incidents in 2021 (National Coordinator for Counterterrorism and Security, 2022, p. 35, 36, 39). This highlights the need to enhance the cybersecurity of technology and (critical) infrastructure in both countries.

4.3 Human capacity & digital literacy

Indonesia must enhance human capacity to effectively mitigate the effects of cyberattacks and increase digital literacy to prevent them. It requires more than a sophisticated infrastructure and legislation to create a secure cyberspace, as some types of cyberattacks happen using social engineering methods. Social engineering takes advantage of the negligence of tech users in securing their personal information. A recent survey by the MCI showed that the Digital Literacy Index of Indonesians scored at 3.49 (average) in 2021 (Center, 2022). In collaboration with an independent consultant, Katadata, the Ministry assessed citizens with four pillars of Indonesia's digital literacy curriculum: Digital Ethics, Digital Culture, Digital Skills, and Digital Safety. The finding of the survey shows that Digital Safety scores the lowest. Therefore, low awareness of cybersecurity issues among the public and government officials is also a concern that must be addressed to improve cybersecurity in Indonesia (Ashari, 2020).

In comparison, the Netherlands is in top position in Europe regarding digital literacy and digital skills. In 2021, it was reported that 80% of its population had at least 'basic' or 'above basic' digital skills (Dutch Statistics Institute – CBS, 2022). Furthermore, the Netherlands recognises the need to develop high-quality cybersecurity knowledge. For this reason, in the past years, the government has encouraged and invested in developing higher education courses and research on cybersecurity, e.g. the National Cybersecurity Research Agenda (National Cyber Security Centre, 2019). However, the Dutch government also recognises that there is a shortage of highly trained cybersecurity professionals. This shortage leads to insufficient cybersecurity knowledge in organisations, often causing them to be not sufficiently resilient.

5. Conclusion

In this article, we presented an unusual comparison of cybersecurity governance in two different countries and analysed their respective policies. Despite those differences, Indonesia and the Netherlands face similar cybersecurity-related challenges and have initiated cooperative efforts to address them. With its large population and developing economy, Indonesia is vulnerable to cyber threats due to rapid spread of the Internet, especially through mobile connections. The country has experienced a significant increase in cyberattacks, facilitated by an infrastructure that lacks resilience, and a low digital literacy rate of the population. In contrast, the Netherlands has a high Internet penetration rate and higher digital literacy rates. Nevertheless, challenges remain as the enhanced connectivity results in more potential for attacks and require more maintenance through qualified personnel.

Both countries need to develop their governance frameworks and infrastructure to address these challenges.

Indonesia needs to develop comprehensive cybersecurity legislation. This will provide a legal basis for cybersecurity, lend more legitimacy to the topic, and enable better coordination among various government institutions. The Netherlands should continue to enhance digital resilience and ensure that laws and regulations keep pace with evolving cyber threats, in collaboration with European and international partners. Furthermore, both countries should prioritise awareness programs to educate the public, organisations, and government agencies about cybersecurity risks and best practices. Capacity-building initiatives, such as training programs and partnerships among higher education institutions, can facilitate developing a skilled workforce (see e.g. the online course on 'digital intelligence', UGM, 2022a). Finally, despite increasing geopolitical tensions, international cooperation remains instrumental in improving cybersecurity.

It is evident that Indonesia and the Netherlands face distinct cybersecurity challenges due to their geographic locations. By collaborating, these two countries can bridge the gap between regional cybersecurity initiatives, paving the way for cross-regional knowledge sharing and collaboration. The selection of Indonesia and the Netherlands as a case study for enhanced cybersecurity cooperation is justified by the unique challenges, complementary capabilities, bilateral relations, and cultural diversity they represent. The collaborative efforts between these two countries can lead to significant advancements in cybersecurity governance and offer valuable insights for other nations facing similar cybersecurity challenges. In this spirit, both Indonesia and the Netherlands should continue their collaborative efforts in cybersecurity through bilateral and multilateral partnerships. In addition, the collaboration will help understand and appreciate both countries' different cultural, societal, and geopolitical perspectives, leading to more inclusive and comprehensive cybersecurity policies that reflect the diverse needs and priorities of both nations. Sharing best practices, exchanging threat intelligence, and participating in international forums will facilitate knowledge sharing and strengthen the collective response. ■

About the authors:

Oskar J. Gstrein is an Assistant Professor at the Department of Governance and Innovation at Campus Fryslân of the University of Groningen in the Netherlands, where he is also a member of the Data Research Centre (DRC).

Tais Fernanda Blauth is a PhD researcher at the Department of Governance and Innovation at Campus Fryslân of the University of Groningen (The Netherlands), where she is also a member of the Data Research Centre.

Faiz Rahman is an Adjunct Researcher at the Center for Digital Society (CfDS) and a Lecturer at the Faculty of Law, Universitas Gadjah Mada, Indonesia. He is currently a PhD researcher at The Van Vollenhoven Institute for Law, Governance and Society, Leiden Law School, Universiteit Leiden, the Netherlands.

Anisa Pratita Kirana Mantovani is an Adjunct Researcher at the Center for Digital Society (CfDS), Universitas Gadjah Mada, Indonesia. She currently holds the position of the Head of Public Policy and Government Relations at the Indonesian E-Commerce Association (idEA).

Annisa Paramita Wiharani is an Adjunct Researcher at the Center for Digital Society (CfDS), Universitas Gadjah Mada, a PhD researcher at The Department of International Relations and International Organization, University of Groningen (The Netherlands), and a Lecturer at the Department of International Relations, Catholic University of Parahyangan, Indonesia.

References

Ashari, M. (2020). Keamanan Informasi: Sudah Saatnya Kita Peduli. In Kementerian Keuangan Republik Indonesia. https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/13113/Keamanan-Informasi-Sudah-Saatnya-Kita-Peduli.html

Brooks, C. (2023, March 5). Cybersecurity Trends & Statistics For 2023; What You Need To Know. Forbes. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/

Center, K. insight. (2022). Indeks Literasi Digital Indonesia Masuk Kategori Sedang Pada 2021. In Katadata. https://databoks.katadata.co.id/datapublish/2022/01/20/indeks-literasi-digital-indonesia-masuk-kategori-sedang-pada-2021

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 23(1), 1–11. https://doi.org/10.4102/sajim.v23i1.1277

Council of Europe. (2006, March 1). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189). Treaty Office. https://www.coe.int/en/web/conventions/full-list

Council of Europe. (2022, May 12). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Treaty Office. https://www.coe.int/en/web/conventions/full-list

Council of Europe. (2023, July 7). Chart of signatures and ratifications of Treaty 185. Treaty Office. https://www.coe.int/en/web/conventions/full-list

Dutch Statistics Institute - CBS. (2022, May 12). Dutch digital skills at the top in Europe [Webpagina]. Statistics Netherlands. https://www.cbs.nl/en-gb/news/2022/19/dutch-digital-skills-at-the-top-in-europe

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive), 2022/2555 (2022).

European Union. (2022, September 15). Cyber Resilience Act | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

European Union. (2023a, June 20). The EU Cyber Solidarity Act | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

European Union. (2023b, June 30). The EU Cybersecurity Act | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021 (p. 45). Publication Office of the European Union, Luxembourg.

Fraudehelpdesk.nl. (2023). About Fraud Help Desk. Fraude Help Desk. https://www.fraudehelpdesk.nl

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. Connections, 19(1), 73–86.

Gstrein, O. J., & Zwitter, A. J. (2021). Extraterritorial application of the GDPR: Promoting European values or power? Internet Policy Review, 10(3). https://doi.org/10.14763/2021.3.1576

Hidayat, R. N., & Juaningsih, I. N. (2022). Legal Protection For The Community In Cyber Space Through Regulation Forming With The Omnibus Method. IPMHI Law Journal, 2(2), 143–156.

Indonesia, R. of. (2019). Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan

Ketahanan Siber (Academic Draft of Cyber Security and Resillience Bill).

Indonesia, R. of. (2021). Presidential Regulation No. 28 of 2021 on National Cyber and Crypto Agency.

International Telecommunication Union. (2020). Global Cybersecurity Index 2020. In ITU Publications. ITU Publications.

Jisi, W., & Ran, H. (2019). From cooperative partnership to strategic competition: A review of China–U.S. relations 2009–2019. China International Strategy Review, 1(1), 1–10. https://doi.org/10.1007/s42533-019-00007-w

Kamara, I., Leenes, R., & Stuurman, K. (2020). The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act. Tilburg Institute for Law, Technology, and Society - Commissioned by the National Cyber Security Centre of the Netherlands. https://www.ncsc.nl/documenten/rapporten/2020/oktober/2/the-cybersecurity-certification-landscape-in-the-netherlands-after-the-union-cybersecurity-act

Keohane, R. O., & Nye, J. S. (1998). Power and Interdependence in the Information Age. Foreign Affairs, 77(5).

Kingdom of the Netherlands. (2020, March). Dutch Economic Mission to Indonesia. The Netherlands andYou;MinistryofForeignAffairs.https://www.netherlandsandyou.nl/latest-news/news/2020/04/16/dutch-economic-mission-to-indonesia-march-2020

Kiswondari. (2021). Serangan Siber di Indonesia Meningkat 5 Kali Lipat, Kebocoran Data Salah Satunya. In SINDOnews. https://nasional.sindonews.com/read/527718/12/serangan-siber-di-indonesia-meningkat-5-kali-lipat-kebocoran-data-salah-satunya-1630408129

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

National Information and Communication Technology Council. "Pengembangan Keamanan Siber Nasional," 2018.National Coordinator for Counterterrorism and Security. (2022). Cyber Security Assessment Netherlands (CSAN) 2022 (p. 52). Ministry of Justice and Security. https://english.nctv.nl/binaries/nctv-en/documenten/publications/2022/07/04/cyber-security-assessment-netherlands-2022/Cyber+Security+Assessment+Netherlands+2022.pdf

National Cyber Security Centre. (2019, July 1). National Cybersecurity Agenda—National Cyber Security Centre [Onderwerp]. Nationaal Cyber Security Centrum. https://english.ncsc.nl/topics/national-cybersecurity-agenda

Nuffic. (2023). StuNed Scholarships. Study in Holland. https://www.studyinholland.nl/finances/stuned-scholarships

Rahman, J., Azhari, M. L., Tamba, S. R., Ramadhan, A. N., Fakhriyah, I., Hilmi, M. A., Hartadi, E. E., & Kristallia, R. (2021). Laporan Tahunan Hasil Monitoring Keamanan Siber 2021. In A. Nugroho & F. E. Prasaja (Eds.), Laporan Tahunan. Badan Siber dan Sandi Nasional Republik Indonesia.

Schmitz-Berndt, S. (2021). European Union · Cybersecurity is Gaining Momentum – NIS 2.0 is on its Way. European Data Protection Law Review, 7(4), 580–585. WorldCat.org. https://doi.org/10.21552/edpl/2021/4/14

Schmitz-Berndt, S., & Chiara, P. G. (2022). One step ahead: Mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. International Cybersecurity Law Review, 3(2), 289–311. https://doi.org/10.1365/s43439-022-00058-7

social, W. are & KEPIOS. (2022a). Digital 2022 Indonesia.

social, W. are & KEPIOS. (2022b). Digital 2022: The Netherlands.

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime. ERA Forum, 23(1), 101–108. https://doi.org/10.1007/s12027-022-00707-8

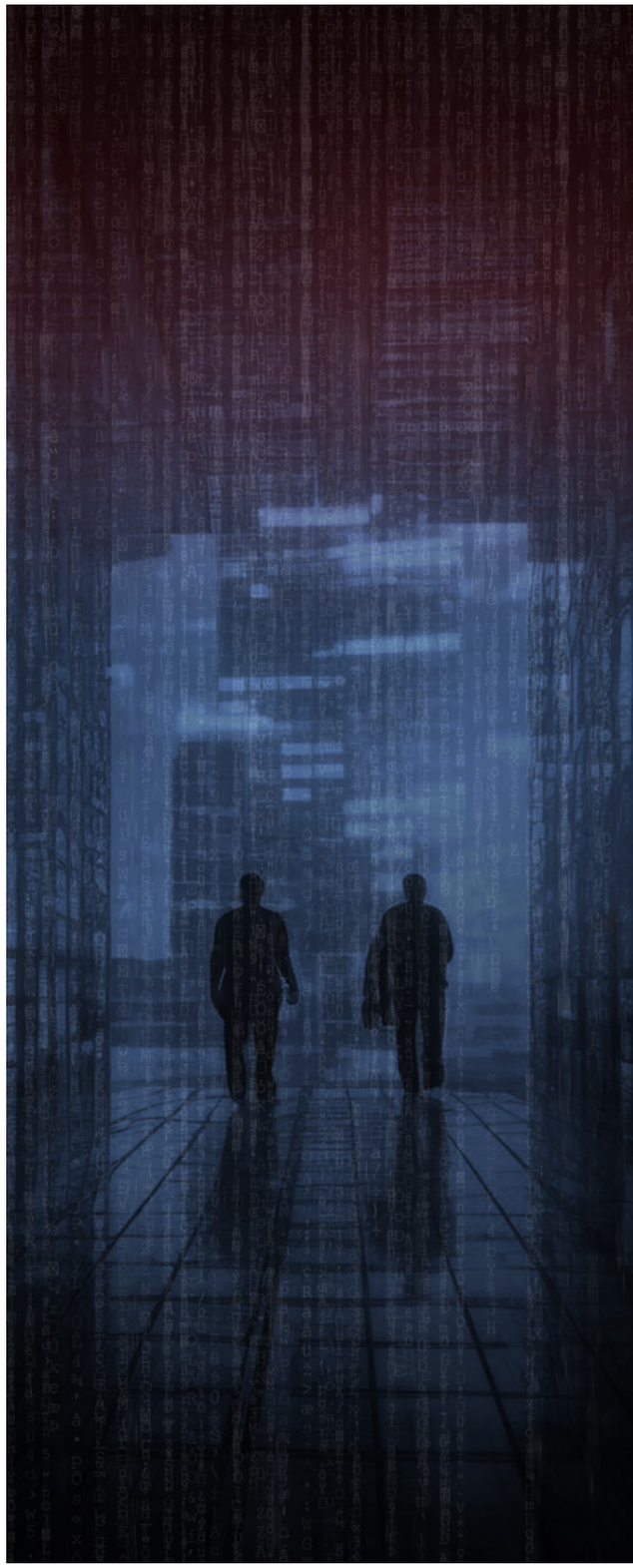
UGM. (2022a). Kecerdasan Digital. Kecerdasan Digital 2022. https://kecerdasandigital.id/

UGM, C. for D. S. (2022b). Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi.

Vermeulen, R. (2020). Cultural cooperation Indonesia-Netherlands 2021-2024. DutchCulture. https://dutchculture.nl/en/cultural-cooperation-indonesia-netherlands-2021-2024

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? International Cybersecurity Law Review, 1(1), 63–72. https://doi.org/10.1365/s43439-020-00012-5

World Bank. (2022, April 5). The World Bank in Indonesia [Text/HTML]. World Bank. https://www.worldbank.org/en/country/indonesia/overvi



ARTICLE

Putting a Humane Face to Digital Transformation & Connectivity in Africa

TEKI AKUETTEH
FOUNDER AND EXECUTIVE DIRECTOR
OF THE AFRICA DIGITAL RIGHTS HUB LBG

Keywords: digital transformation, connectivity, inequality, digital rights, human rights

The potential for accelerated socio-economic growth steered by digital technologies makes digital transformation (Solomona, 2020) an expensive venture to ignore. In the last two decades, we have witnessed the wild embrace of digital technologies in Africa (Ndemo, 2017) and its impact (both good and bad). Indeed, digital transformation is not only hailed in developing economies today as the solution to confronting Africa's myriad challenges, but the key to propelling the much-needed socio-economic development. While there is some truth to these assertions, the Continent of 55 countries continues to lag and faces significant digital divide despite religiously sticking to the prescriptions of digital transformation.

At the bedrock of digital transformation is digital connectivity. No doubt therefore that notwithstanding the bitter pill of the various policies and strategies, Africa's digital connectivity and digital transformation continues to be one of the lowest globally (World Bank, data; Liu, 2019; McKinsey & Company, 2020). And while there have been various interventions by governments, donor agencies and private sector – the big question is: ***Why have we failed to bring everyone on board?*** I do not intend to write a treatise on why many developmental

policies have failed in Africa as this is well documented (Wilson Center, 2017; World Bank, 2015; Kwame, 2003). However, some of the reasons for such unsuccessful policies provide insights into the challenges to digital connectivity and digital transformation in Africa today.

Digital transformation and connectivity are not just a luxury, but a fundamental facet of our society. The past few years have underscored the importance of digital transformation and connectivity to the survival of our planet and the human race (Alper, Miktus, 2019). This article has been adapted from the keynote speech, delivered at the 2022 Annual Conference of the Geneva Human Rights Platform on 18th October 2022 on the 'On/Off – Implications of Digital Connectivity on Human Rights'.

Here are a few stories culled from around the world on the necessity and impact of digital connectivity.

'The pandemic has exposed inequalities across Africa and within our respective countries. With regard to education, the scale of the digital divide and its implications for remote learning are striking. According to the 2021 Ibrahim Forum Report, 89% of learners in sub-Saharan Africa do not have access to household computers. 82% lack internet access and at least 20 million live in areas not covered by a mobile network. Furthermore, wide gender disparities in ownership of and access to digital devices have also limited technology's role in providing solutions, leaving many girls behind.'

– This is a statement from the Mo Ibrabhim Foundation News published in September 2021 on Navigating the Digital Divide in Africa's Classroom.

In April 2021 the New York Times's Shira Ovide, writing on the early concerns of the impact of the pandemic on big tech stated:

'…In the last year, the five tech superpowers — Amazon, Apple, Google, Microsoft and Facebook — had combined revenue of more than $1.2 trillion, as I wrote for The Times on Thursday. It was a strange and amazing year for Big Tech. I can't believe it, but some of the companies are growing faster and are more profitable than they have been in years. The pandemic has made the tech giants and their bosses unfathomably rich…'

'I am an Ewe from the Volta Region, [in Ghana] (emphasis mine) but my nursing profession brought me here. During my registration for both the voter and national ID, the registration officers I met at the two different [registration centres] (emphasis mine) … all doubted my presence here [Widana, Pusiga District near Ghana–Togo border]. They said what shows that I am not Ewe from Togo staying in Ghana. I had to explain everything about me and finally showed them my nursing staff ID card before they continued my registration.'

'My name, either the Sani or Alhassan is also found in the communities just across the river [boundary] you see there. Because of that when I was registering for voter and national ID card it took me a long time and many questions from the registration man if I was not from Burkina Faso. I gave them my birth certificate at the centre but they still asked me several questions if I am truly a Ghanaian.'

These are the stories of Gbolonyo and Alhassan, a 26- and a 24-year-old woman and man respectively from Ghana during a focus group discussion with the Africa Digital Rights Hub on access to IDs by people living in border towns (Africa Digital Rights' Hub, 2020). Interestingly, these IDs, by a recent Government directive, are mandatary (Stash, 2022) for access to SIM cards and connectivity that enables them to fully engage the digital society. And yet, policies and strategies such as these have been implemented in dogmatic ways which have completely failed to look at their impact on the people who should matter the most.

Policies and strategies on digital transformation and connectivity in Africa have again failed

to consider its people as they have mostly been implemented at the beck and call of governments and political interests, industry interests and sometimes even donor interests. Unfortunately, rarely do these initiatives (like many of other failed ones across the Continent of Africa) take into consideration the Continent, its nations, culture, its people and their needs. In this quest for digital transformation and connectivity of African, has anyone dared to ask what does Africa need? What will benefit Africans? Digital transformation strategies and policies will continue to fail if the subject fails to be part of it.

The benefits and impact of digital connectivity are glaringly seen across the world today. The increased economic growth, the reduction in poverty, better access to healthcare and education, access to information, the strengthening of democratic values and principles, the upholding of human rights, the transparency and exposure of societal ills and human rights violations - all that can be felt in Africa, the Americas, Antarctica, Asia, Australia and Europe.

Clearly, no part of our globe has been spared from the impact of digital connectivity. If for nothing at all, it has also brought to light and limited the physical boundaries that once defined us and our societies. However, whilst digital transformation and connectivity have brought us closer, they also have exposed the ills and hypocrisy of our societies today, continuing to undermine and further aggravate the inherent nature of human rights regardless of race, sex, nationality, ethnicity, language, religion, or any other status.

Digital transformation and connectivity are exposing the widening digital divide between the haves and the have-nots. They are bringing to light inequalities in the development and use of digital tools in the world. While many economic opportunities abound under this new dispensation, it is becoming more and more obvious that it may not be realized by Africa and Africans if the approach to these issues remains the same, and continues to blind us to the ills of how it is impacting the Continent.

Humanity loses its meaning when we fail to safeguard all, whether physically or virtually, connected or not connected, on or off the grid. And in today's world, where it is increasingly becoming impossible for us to live outside the connected space, there is an obligation to ensure an equitable distribution and access of this critical resource to everyone, irrespective of who they are or where they come from.

This is indeed a tall order in a world where the language of digital transformation and connectivity is formal, thereby eliminating the majority voices of the informal. How many uneducated and informal populations can effectively engage in the connected world without barriers? Sometimes, it is as if technology has been developed to fail humans. Because even though it has the capability to enable us reach everyone, we turn a blind eye to ensuring that the interest of all is recognized and respected regardless of the language they speak, who they are, or where they come from.

Also, whilst the word 'connectivity' seemingly emphasizes the state of bringing the world together, it has ironically become another tool of inequality, discrimination, abuse and economic woes — just to mention a few. Connectivity-enabling infrastructure in developing countries continues to lag. And while these communities make a significant contribution to the development and use of digital technologies globally, the wealth created rarely trickles into their economies, further worsening the ability of these communities to create and share wealth equitably. This is because the technological tools for digital transformation and connectivity systemically disfavour developing economies such as Africa. And therefore participation automatically creates a power imbalance. Denying equitable participation of Africans in the digital world is in-humane. Perhaps it is no one's problem but Africans; however, what we have seen with Covid should change this narrative.

Digital transformation and connectivity are real and have a strong impact on the lives of people around the world, including Africans. They are affecting the right to live, liberty and security; the right to freedom, dignity and non-discrimination. They are impacting the right to economic freedom, privacy and protection from arbitrary interference in our lives; the freedom of movement, the right to nationality and the right to own property. They are influencing the freedom of association, thought, conscience and religion; the right to education, freedom of expression the list is endless. Is it possible for an African (individual or business situated on the continent) to equitably engage in the digital world today and join the rest of the world in the wealth creation, we so loudly tout digital transformation for? The simple answer is NO. The power dynamics of digital transformation today are favouring the haves and harming the have-nots. And the world needs to re-think digital transformation. Digital transformation and connectivity must cease to be about who is creating the most wealth and be about the equitable distribution of it. It must not be about how many people there are on a platform but about how the people are treated on the platform. It must not be about how I can manipulate digital transformation and connectivity to my selfish gain but to the overall interest of humanity.

While today it is difficult to mention any digital transformation and connectivity and not identify how they have been affecting our lives positively or negatively. Unfortunately, however, the effect of the negatives is fast eroding the essence of humanity and there are minimal efforts to bring everyone along to ensure a fair, justiciable, and equitable distribution of the benefits of digital transformation and connectivity to all.

Bringing everyone along means:

- A fair and equitable development and distribution of the wealth created by digital infrastructure;
- A fair and equitable access to digital infrastructure irrespective of language, culture, race, sex, or other geographical boundaries; and last but not the least;
- The development and implementation of policies and regulatory frameworks that guarantee the protection of human rights in our societies.

The time to evaluate the impact of digital transformation and connectivity on humanity is now. And in doing so, we must ensure that these critical resources is by all and available to all, and not a select few.

In conclusion allow me to quote the words of an illustrious African — Osagyefo Dr. Kwame Nkrumah:

'...The task ahead is great indeed, and heavy is the responsibility; and yet it is a noble and glorious challenge - a challenge which calls for the courage to dream, the courage to believe, the courage to dare, the courage to do, the courage to envision, the courage to fight, the courage to work, the courage to achieve - to achieve the highest excellencies and the fullest greatness of man. Dare we ask for more in life?'

To realize its full digital potential, the Continent of Africa must be 'off the table' as the menu and 'at the table' as an able, willing and equal participant to digital transformation and connectivity globally. It is only then that the policies and strategies will yield benefits for the people of Africa. And while there is the temptation to place this responsibility on the people of the Continent (governments, citizens and business, etc.), putting a humane face to digital transformation and connectivity requires the inputs of all key players and not just Africans. ■

About the author:

Teki is the Founder and Executive Director of the Africa Digital Rights Hub LBG, focusing on digital rights in Africa. She established the Data Protection Commission of Ghana, specializing in data protection and technology law. With two decades of experience, she works across Africa on privacy, data governance, digital economy, and cybersecurity. She's been involved in key ICT legislation development in Ghana and worked with international organizations like the World Bank and the African Union. Teki holds an LLM in Information Technology and Telecommunications Law and is an environmental advocate who enjoys spending time with her family, dogs, traveling, gardening, cooking, exercising, and dancing.

References

Africa Digital Rights' Hub LBG. (2020). Ghana's Identity Ecosystem. https://africadigitalrightshub.org/wp-content/uploads/2022/08/Ghana-Identity-Ecosystem-Brochure-Hyperlink-revised-copy.pdf

Alper, E., Miktus, M. (2019). Digital Connectivity in sub-Saharan Africa: A Comparative Perspective. https://www.elibrary.imf.org/configurable/content/journals$002f001$002f2019$002f210$002farticle-A001-en.xml?t:ac=journals$002f001$002f2019$002f210$002farticle-A001-en.xml

Boafo-Arthur, K. (2003). TACKLING AFRICA'S DEVELOPMENTAL DILEMMAS: IS GLOBALIZATION THE ANSWER? Journal of Third World Studies, Vol. 20, No. 1, THE EFFECTS OF GLOBALIZATION IN TAIWAN AND THE THIRD WORLD (SPRING, 2003), pp. 27-54 (28 pages) Published By: University Press of Florida

Diop, M. (2015). Policymaking in Africa: Reflections from Decades of Experience. World Bank.https://www.worldbank.org/en/news/speech/2015/03/31/policymaking-in-africa-reflections-from-decades-of-experience

Jayaram, K., Leiby, K., Leke, A., Ooko-Ombaka, A., Sun, Y. (2020). Reopening and reimagining Africa. How theCOVID-19crisiscancatalyzechangeacrossthecontinent. McKinsey & Company. https://www.mckinsey.com/featured-insights/middle-east-and-africa/reopening-and-reimagining-africa

Liu, A. (2019). Africa's future is innovation rather than industrialization. World Economic Forum on Africa, Davos. https://www.weforum.org/agenda/2019/09/africa-innovation-rather-than-industrialization/

Signe, L. (2017). Why Do Development Policies Often Fail in Africa? Perspectives on the World Development Report 2017. Wilson Center. https://africaupclose.wilsoncenter.org/why-do-development-policies-often-fail-in-africa-perspectives-on-the-world-development-report-2017/

Stash, B. (2022). Sim Re-registration Ends Today: Unregistered SIM Cards Blocked. GHPage. https://www.ghpage.com/sim-re-registration-ends-today-unregistered-sim-cards-blocked/253328/

World Bank. (2023). Digital Development. https://www.worldbank.org/en/topic/digitaldevelopment/overview#1

ARTICLE

Human Trafficking and Technologies. Adaptation of the Recruitment, Advertising, Communication, and Disbursement Dynamics of Human Trafficking to the New Online Landscape

GRACIA SUMARIVA REYES

PROJECT ASSISTANT,
THE KOŚCIUSZKO INSTITUTE

ABSTRACT:

New technologies have undoubtedly broadened criminals' ability to traffic human beings for different types of exploitation. This brief article delves into the profound shifts brought about by the digital age in the recruitment of victims, advertising of services, communication, and financial transactions within the dark realms of human trafficking. After this initial introductory section, it will proceed to present a brief conceptual framework of human trafficking from the perspective of international legislation. Following that, it will analyse the changes that new technologies have brought about in the dynamics of recruitment, advertising, communication, and financial aspects of human trafficking. The article concludes with a reflection on how the governance of human trafficking must adapt to these historical changes.

Keywords: human trafficking, technologies, online adaptation, human rights

1. Introduction

Human trafficking is millenary phenomenon that has persisted throughout human history. Since its origins, historically associated with the beginnings of slavery, trafficking has taken various forms and has adapted to the changing contexts of civilizational advances. As society has evolved, human trafficking demonstrated a remarkable ability to transform and survive in new environments and proven to be amazingly resilient to the economic, political, and technological transformations that have marked the milestones of human civilization (Bales, 1999).

It is, therefore, worth questioning how human trafficking has transformed itself and adapted to the information era in which we live, characterized by the major role played by communication technologies, especially Internet, in the organization and structure of societies (Castells, 2000). The rise of 'e-trafficking'[1] (Milivojevic, 2012: 73) has not gone unnoticed, remarked by relevant authorities such as the US Federal Bureau of Investigation (2020) and the Europol (2020). As expressed by US Ambassador-at-large to Monitor & Combat Trafficking in Persons at the OSCE, John Richmond:

When financial systems allowed wire transfers, traffickers made use of wire services to move money. When photography advanced and gained widespread adoption, traffickers were quick to take advantage of the technology for use in advertising and coercing victims. When mobile phones became ubiquitous, many traffickers used them as an electronic tether to victims, using them to monitor their movements, control their actions, and keep tabs on them. When video surveillance systems became more common, traffickers wired establishments, like massage parlors, to monitor and control their victims. When online marketplaces arose, traffickers were there seeking customers for their illegal enterprises. (John Richmond, 8 April 2019)

1 Milivojevic (2012: 73) coins the term e-trafficking to reference trafficking in human beings in the context of Internet and the rise of online communication platforms.

2. Conceptual framework: Human trafficking

Article 3 of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Girls, supplementing the UN Convention against Transnational Organized Crime[2], defines trafficking in human beings (THB) as:

The recruitment, transportation, transfer, harbouring, or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.

In the light of the Palermo Protocol, THB is a process made up of three elements: 1) an action of human mobility involving a reception and transfer; 2) coercive, fraudulent or deceptive means that vitiate consent; and, 3) the purpose of exploitation in different modalities such as exploitation of prostitution and sexual exploitation, slavery, forced labour, servitude, removal of organs, for irregular adoption purposes, commission of crimes or begging (Da Silva and Silva Machado, 2016). In addition to the amalgamation of forms of exploitation in which human trafficking can manifest itself, it is a complex phenomenon due its "polyphony" process (Da Silva and Silva Machado, 2016: 2) as it can be understood as a massive violation of human rights, as a contemporary form of slavery, as gender-based violence, as a crime against humanity and/or as a phenomenon linked to transnational organised crime and irregular migration. Human

2 Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children, which complements the United Nations Convention against Transnational Organized Crime, adopted by United Nations General Assembly Resolution 55/25 on November 15, 2000.

trafficking is a complex issue that relates with easiness to other global phenomena such as human mobility or the globalization of economy (Bales, 1999), including rise of the tech society.

3. Changing dynamics: recruitment, advertising, communications, and revenue in the context of e-trafficking

3.1. Recruiting

In the digital age, human traffickers have expanded their reach, exploiting the vulnerabilities of a wide range of people. The landscape is changing, and the tendency for victims to meet their traffickers in person is decreasing. According to research carried out by anti-trafficking NGO Thorn (2018), since 2015 there has been an increased reliance by traffickers on technology in the victim contact and recruitment process. In a study, which surveyed 260 trafficking victims in the US, it was noticed that while 84% of trafficking victims recruited prior to 2015 had made initial contact with the trafficker in person, as of 2015, this ratio dropped to 45%. The remaining 55% of victims indicated that their trafficker used technology in this process, 63% communicated online and 25% communicated through phone calls. Similarly, the study showed that prior to 2015, 85% of the overall sample mentioned that their trafficker spent time with them in person to establish a relationship, while only 58% of those recruited in 2015 reported in-person interaction.

One of the key reasons traffickers are transitioning from in-person recruitment to digital means is that these enable recruitment on a massive scale (Europol, 2002). Indeed, online channels afford traffickers the convenience of engaging with numerous potential victims concurrently (Kunz et al, n.d.).

Another significant factor is that the online realm, especially social media, ease the process of identifying and targeting new victims. While in the pre social media era uncovering and understanding the vulnerabilities of potential victims was a considerably more laborious endeavour, the rapid development of online relationships and the increasing share of personal problems online have significantly bolstered traffickers' ability to pinpoint and exploit the vulnerabilities that individuals openly display on their social media profiles. This acceleration has transformed the landscape of human trafficking, granting traffickers an unprecedented advantage in identifying and targeting their victims (Kunz et al., n.d.; Jones, 2010).

Online vulnerabilities to human trafficking can arise from two sources: individuals turning to the Internet as a coping mechanism for emotional states or the sharing of personal information during difficult situations. On the one hand, these online vulnerabilities can be linked to emotions that render individuals susceptible. These encompass a deep need for understanding, feelings of emptiness, the pursuit of love, desires and allure, experiences of disappointment, a longing for connection, the quest for freedom, feelings of fear, the search for success, and the need for confidence (Kunz et al., n.d.). On the other hand, online platforms offer traffickers an opportunity to identify potential victims, particularly those who openly divulge personal information related to their financial hardships, low self-esteem, or family problems (FBI, 2020). Human traffickers exploit these vulnerable individuals by capitalizing on their personal circumstances. They focus on comprehending the vulnerabilities of young people, then manipulate and exploit these vulnerabilities to gain control over them (FBI, 2020).

Highlighting the two points made so far, an anti-trafficking expert interviewed by Kunz et al. (n.d.: 5) concluded the following:

Social media itself tends to offer easy access to identifying vulnerabilities, whereas in the past, traffickers might have had to gradually discern these vulnerabilities over time. Now, they can simply go online, search for individuals displaying indicators they typically exploit – such as substance abuse, runaway tendencies, or instability within their home environment. Sometimes, social media posts even reveal histories of multiple substance abuse. This allows traffickers to target these vulnerabilities more efficiently, and they can even incorporate a narrative element into their grooming strategies. All of these factors enable them to tailor the grooming process when engaging with young individuals [...].

Furthermore, new technologies lower the barrier for new traffickers, as they allow them to engage into trafficking activities without the previous development of a physical criminal infrastructure and a criminal network (Europol, 2020).

The recruitment of victims online takes place especially in social media. The nexus between online recruitment of victims and social media is evident in mediatic cases such as the West Brides of ISIS. It is estimated that during the insurgency of ISIS (2014-2015) almost 550 women from the West were trafficked by the organization. Most of them were recruited via Facebook and averaged 18 years of age, as a number of young, under-age girls were targeted. Most of these women were recruited for purposes of sexual exploitation, serving as 'jihadist brides' that facilitated the captivation and retention of male foreign fighters (Binetti, 2015).

Authorities such as the FBI (2020) and Europol (2020) have warned that the Internet, particularly social networks, is used by traffickers to ensnare potential victims into human trafficking. Among the most commonly used applications for online recruitment are Facebook, Instagram, Snapchat, Tinder, Blendr, WhatsApp, and KIK (Kunz et al., n.d.). According to data gathered from the Polaris Project (7 February 2019), covering the period from January 2015 to July 2018, the US Human Trafficking Hotline documented 969 potential victims of sex trafficking who were recruited online, some of whom were targeted on multiple platforms. Among them, 300 potential victims could have been recruited through Facebook; 147 from dating websites; 113 via Instagram; and 502 through various other internet platforms, such as Craigslist, chat rooms, or websites that could not be identified during the hotline calls.

In the recent months, alarm bells have been ringing about advertisements by transnational travel traffickers on social media, especially video platforms with an emphasis on TikTok, using the reference 'game'. This term has been coined to advertise the illegal movement of people across borders who often end up as victims of trafficking (Bhuiyan, 23 October 2022; Malik, 9 July 2023). Traffickers post testimonial videos on social media about the hassle-free journeys or 'games' of their former "clients" (victims) aimed at attracting customers, as it is showed in the following extract taken from one of these videos:

Great game of Baba Haji. [Our] group has reached Italy non-stop. The game is direct. We reached Italy in 8 to 9 hours [...] The trip was great and so is the game (cited in Malik 9 July 2023).

Social media are designed to foster community, connect users, and establish online relationships. In this sense, any platform that facilitates connections with individuals of varying motives and intentions, inherently carries risks. However, it is the susceptibility of the online user, rather than the social media themselves, what ought to be the matter of concern (Kunz et al., n.d.).

3.2. Advertising

Online advertising is increasing while advertising on the street is decreasing. According to the above-mentioned Thorn study (2018), victims recruited before 2004 stated that traffickers predominantly used the street in-person as their main forum for advertising them (78% street vs. 38% online). After that year, the trend reversed: street advertising had dropped to 61% while online advertising increased to 75%. However, this trend appears to be reversing due to the scrutiny and actions taken by the preferred advertising sites for trafficking, such as Craigslist and Backpage (Thorn 2018).

One of the main reasons for this change is the impact of online versus street advertising. To this effect, while 14% of the victims promoted on the street claimed to have more than 10 customers per day, this percentage rose to 25% in the case of those who had been promoted online (Thorn, 2018). Another question to take into consideration is that the online arena not only facilitates the procurement and delivery of trafficking services but also allows traffickers to free themselves from the constraints of physical locations, enabling them to advertise victims and connect them with clients while avoiding any form of in-person engagement (Europol, 2020). In this regard, during Thorn's study (2018), one third of trafficked victims who advertised online claimed that they posted their ads themselves, with an average of 8 ads per day but as many as 65 postings per day. Furthermore, in the online environment it is much easier to disguise the age of the victims, who are very often minors (Thorn, 2018).

While we often associate human trafficking with the hidden corners of the deep and dark web, it's important to recognize that advertising for trafficking victims is also prevalent on the clear web. Indeed, traffickers generally lack the sophistication to use the dark web and its use has not been found to be as widespread with the exception of forms of exploitation involving children (Williams and Muhammad, 2021). In the clear web, Backpage and its successor Bedpage have emerged as prominent platforms for online advertising related to sex trafficking, as indicated by Thorn (2018) and Kunz et al. (n.d.). Traffickers have strategically leveraged escort and dating websites, including Cityxguide, Skipthegames, Seekingarrangement.com, and Sugar-babies.com, to promote the services of their victims. Other frequently used clean sites are Babylon, Facebook, Airbnb and Twitter (Williams and Muhammad, 2021).

3.3. Communication

Another aspect to consider when analysing the relationship between human trafficking and technologies is the adoption of encryption technologies, especially by human traffickers. Currently, traffickers are shifting towards communicating through applications that offer end-to-end encryption. These applications encrypt all communication between traffickers, their workforce, and/or their victims, making it challenging for law enforcement agencies to trace and investigate. The most popular application among traffickers is Telegram, although the use of Signal, Wickr, WhatsApp, and even Apple's iMessage with end-to-end encryption has also been observed. There is also evidence that traffickers use applications that allow them to encrypt their entire device, making it difficult to access the content or discover the necessary information and evidence in the new landscape of e-trafficking (Vilím, Eržen and Weber, 13 January 2023).

3.4. Revenues

Although the great majority of human trafficking revenues are still collected in cash (Europol, 2020), a review of how technologies have influenced trafficking cannot end without referencing to the adoption of digital tools for financial transaction. The decentralized nature of cryptocurrency, coupled with its ease of use and global reach, has made it an attractive tool for criminal enterprises. Human trafficking, given its significant profitability and the necessity of handling substantial sums of money, has faced challenges with traditional credit card companies refusing to process transactions for websites suspected of facilitating sex trafficking. Consequently, cryptocurrency has emerged as an effective workaround and is increasingly employed to facilitate such criminal activities, as noted by Khodarkovsky, Russo, and Britsch in 2021. Furthermore, although not yet widely prevalent, the recent emergence of trafficking "cryptoprofiles' suggests potential shifts in the trafficking business model (Europol, 2020).

4. Conclusion

The present article originated from Bales' observation (1999) regarding human trafficking's capacity to transform and adapt to the realities and progress of human societies. Faced with this, we wonder how the emergence of the information society has impacted it. The impact of the digital revolution is undeniable. The proliferation of smartphones, social media, and encrypted communication platforms has created a virtual breeding ground for traffickers, enabling them to manipulate, recruit, advertise, and facilitate their illicit activities with unprecedented efficiency. The recruitment of victims, once confined to the shadows, now unfolds in plain sight on the screens of our connected world. Advertising their "services," traffickers have ventured into the open web, often cloaked beneath a veneer of legitimacy, while communication among criminal networks has become encrypted and elusive. Financial transactions, too, have migrated into the digital realm, rendering traditional traceability efforts obsolete.

As e-trafficking continues to evolve, it becomes increasingly evident that the battle against it needs a global governance framework that adapts to the new context. The complex interplay between technology, criminality, and the vulnerabilities of victims demands a multidimensional response that transcends international borders as well the conventional realm of law enforcement, calling for multi-sectoral cooperation. In this new context, the need for international cooperation and coordination takes centre stage. The challenges posed by e-trafficking transcend national jurisdictions and demand a united front. The response must be proactive, leveraging the same technological tools that traffickers employ to both detect and prevent these crimes. This entails strengthening cross-border partnerships, sharing intelligence, and harmonizing legal frameworks to effectively combat the digital tendrils of trafficking networks. Additionally, to truly confront this evolving threat, we must bridge the gap between governments, law enforcement agencies, non-governmental organizations, and the private sector. Collaborations with tech giants, who possess both the power and resources to combat online exploitation within jurisdiction of their platforms are pivotal, as well as the establishment of public-private partnerships against e-trafficking. Engaging these industry leaders as active stakeholders in governance efforts is crucial. Together, through a fusion of government initiatives, civil society advocacy, and private sector innovation, we can forge a resilient defence against e-trafficking, safeguarding the vulnerable and upholding virtual human security.

All in all, the fight against e-trafficking stands at the intersection of human rights, technology, and global cooperation. The malleability of traffickers in adapting to the digital frontier compels us to respond with even greater agility and resolve. Through concerted international efforts, informed by a deep understanding of the digital dynamics at play, we can hope to confront e-trafficking effectively, safeguard vulnerable lives, and construct a more equitable and compassionate society in an age defined by digital transformation. ■

About the author:

Gracia Sumariva Reyes currently pursuing a master's degree in international Organisations and Crisis Management. In the age of Internet, she is particularly drawn to exploring how it is harnessed "by the bad guys do bad things", such as spreading damaging narratives, disinformation, foreign influence and extremist ideologies. She loves using and learning OSINT techniques to answer all her questions.

References

Bales, K. (1999) Disposable people. New Slavery in the Global Economy. Berkley, University of California Press

Buhiyan, J. (23/10/2022) Revealed: how coyotes and scammers use TikTok to sell migrants the American dream. The Guardian. Retrieved from https://www.theguardian.com/technology/2022/oct/22/tiktok-coyotes-scammers-migrants-american-dream-revealed

Castells, M. (2000) La Era de la Información: Economía, Sociedad y Cultura. Madrid, Alianza Editorial

Correa da Silva, W. & Silva Machado, R. (2016). Re-aproximaciones y posibles aplicaciones del concepto de seguridad humana. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades, vol. 18, No. 36, DOI: 10.12795/araucaria.2016.i36.10

EUROPOL (2020) The challenges of countering Human Trafficking in the Digital Era. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

FBI (2020) Human Traffickers Continue to Use Popular Online Platforms to Recruit Victims. Public Service Announcement – Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/Y2020/PSA200316

Jones, K. (6 October 2020) Date or Target: The Dangerous Link between Human Trafficking and Online Dating. Anti-Trafficking International. Retrieved from https://preventht.org/editorial/human-trafficking-and-online-dating/

Khodarkovsky, J., Russo, A.N., & Britsch, L.E. (2021) Prosecuting Sex Trafficking Cases in the Wake of the Backpage Takedown and the World of Cryptocurrency, Journal of Federal Law and Practice, vol. 69, No. 3

Kunz, R., Baughman, M., Yarnell, R., & Williamson, C. (n.d.) Social Media and Sex Trafficking Process. From Connection and Recruitment, to Sales. University of Toledo. Retrieved from https://www.utoledo.edu/hhs/htsji/pdfs/socmedia.pdf?platform=hootsuite

Malik, A.M. (09/07/2023) The 'game' of human trafficking on social networks. Dawn. Retrieved from https://www.dawn.com/news/1763746

Milivojevic, S. (2012). The State, Virtual Borders and E-Trafficking: Between Fact and Fiction. In: McCulloch, J., Pickering, S. (eds) Borders and Crime. Transnational Crime, Crime Control and Security. Palgrave Macmillan, London. https://doi.org/10.1057/9781137283825_5

POLARIS PROJECT (7 February 2019) Looking for Love Online this Valentine's Day? Polarisproject.org. Retrieved from https://polarisproject.org/blog/2019/02/looking-for-love-online-this-valentines-day/

Richmond, J. (08/04/2019) Taking a Lesson From Traffickers: Harnessing Technology To Further the Anti-Trafficking Movement. US Mission to the OSCE. Retrieved from https://osce.usmission.gov/taking-a-lesson-from-traffickers-harnessing-technology-to-further-the-anti-trafficking-movement/

Thorn (2018) Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking. Retrieved from: https://www.thorn.org/wp-content/uploads/2019/12/Thorn_Survivor_Insights_090519.pdf

Williams, K., & Muhammad, J. (2021) How does the Dark Web Influence Human (and Sex) Trafficking? What Security Implementations are Involved in the Dark Web?. ADMI 2021: The Symposium of Computing at Minority Institutions. Retrieved from https://par.nsf.gov/biblio/10284706

ARTICLE

Questionable Smart Devices and Their Hidden Dangers

LILIANA KOTVAL
JUNIOR PROJECT COORDINATOR AND ANALYST,
THE KOSCIUSZKO INSTITUTE

ABSTRACT:
Smart devices were made to make life simpler, yet, in many aspects, they have done quite the opposite. Invasion of privacy through location tracking, eavesdropping, and spying can be relatively simply achieved by hackers, and the users themselves may find it too late to escape from a device addiction.

Keywords: smart devices, smart home, privacy, surveillance, data exploitation, device addiction

1. Introduction

The concept of technology is as simple as applying scientific knowledge to the practical aims of human life or manipulation of the environment – even a stone tool or a wheel are technologies. Conversely, the huge advancements being made in the technological realm are far from simple and have allowed complex smart home devices to be integrated into everyday life. This integration has been mostly welcomed for being efficient and practical, however having a smart device, constantly monitoring its surroundings, may not be completely safe. According to a survey conducted by Panda Security, 55% of Europeans believe that IoT devices do not respect their privacy and 62% are concerned about these devices collecting and storing personal data. Furthermore, with constant technological advancements being difficult to track and with tactful marketing by manufacturers, smart home devices that are otherwise dangerous are perceived by a growing number of people as being essential and beneficial to daily life. From smart vacuums to smart watches, these gadgets are invading privacy and providing an avenue for hackers to gain access to personal information.

2. The Rise of Smart Devices

Smart home technologies that are able to perform tasks requested per voice commands or from a remote device, like Amazon Alexa or Google or Apple Home speakers, smart thermostats, keyless door locks, robot vacuums, smart lightbulbs, and smart watches have become an integral part of households across the globe. They provide automatic and chained functions that expedite everyday tasks. In 2022 there were about 307 million worldwide users of smart home devices (Statista) – the US being a leader in smart home market with about half of all households owning at least one smart home device (Wise, 2023). These numbers are only expected to rise in the coming years, with a prediction that 20% of the world's households will own smart technology by 2025 (Wise, 2023). With more and more people being connected to smart home devices, the technological security risks of smart devices will also rise.

Almost all smart home devices are a part of the internet of things (IoT) and are embedded with sensors and software that allow for the exchange of information over an internet connection (Old Dominion University, 2021). By 2025, there will be over 75 billion connected devices, and by 2030, 124 billion IoT devices (Silva-Trujillo, 2023). The birth of the IoT realm began in the 1980s when a group of researchers from Carnegie Mellon University connected a Coca-Cola vending machine to the Internet, and ever since, the IoT has greatly expanded, with engineers integrating sensors into all types of physical machines in order for them to be controlled remotely by a smart phone, networked device, or by voice commands (Buil-Gil, 2023).

3. When the Benefits Don't Outweigh the Risks

3.1 Hacking and remote exploitation

Having a smart vacuum programmed to run at a certain time each week or telling an Amazon Echo a grocery list instead of manually writing it down indubitably brings numerous benefits, yet being constantly connected to the internet comes with its downsides. The main issue is related to the sensitive data collected from users. Smart devices operate with cameras and voice control, making an entire smart home ecosystem insecure to cyberstalking, spying, and more (Buil-Gil, 2023). Compromised smart locks can allow hackers to control who comes in and out of a house; voice-activated devices can enable hackers to control their commands; hacked smart refrigerators can make grocery orders online and so generate considerable costs; smart lightbulbs can be turned off and on at random times; smart vacuums may provide information about a home's layout to hackers; compromised smart children's toys can record a child's activities or send them manipulative audio; smart speakers can save user voice recordings (TrendMicro, 2019).

According to tests conducted by Kaspersky, lab researchers found that smart hubs, a mobile application or a web-based service used to program smart home devices could be hacked remotely without even gaining access to the Wi-Fi network.

If an attacker knew the serial number of the hub, they could send it a custom configuration file that would be accepted without any further steps. This enabled the hacker to access the username and encrypted password, which – once broken – granted them control over an entire smart home system. Serial numbers are not typically thought of as being private, so publishing a photo of a smart hub with its serial number can be a dangerous action (Perekalin, 2018).

Buying second-hand smart home devices could potentially be worrisome, as their firmware could have been modified by previous owners to allow continued remote access (Perekalin, 2018). Although attackers may not find these used devices to be as hack-worthy compared to more sensitive data, such as credit card details, Internet-enabled smart home devices can be compromised and used to gain access to other devices, hence the importance of taking precautions by securing passwords and admin access.

3.2 Eavesdropping

Smart speakers are the most commonly owned type of smart device and Amazon dominates the smart speaker market with 28% of global market shares in 2022 (Statista). The Amazon Echo is able to access online information, make phone calls, purchase items, control other smart home devices, among others. Voice interaction activated by a "wake word" automates and simplifies everyday tasks, yet with unanticipated security concerns. There have been over 130,000 Alexa Skills (voice-driven capabilities, like ordering a pizza) developed, and these skills can be exploited by attackers with "skill squatting", where phonetic errors are exploited, and normal requests are routed to a malicious skill (Pathak, 2022). In a test conducted by Deepak Kumar which examined twenty-seven pairs of skills (target skill and squatted skill), twenty-five of the pairs were squatted at least once, giving a success rate of 92.6%. Furthermore, with Voice Masquerading Attacks, a user is unaware of skill eavesdropping, while through the impersonation of a malicious skill as a target skill, they reveal potentially sensitive information to the device (Pathak, 2022).

The Amazon Echo developed a cloud system to store user recordings following a 2017 case of an Echo ordering a dollhouse after a girl asked, "Can you play dollhouse with me and get me a dollhouse?". Multiple households' Echo devices purchased dollhouses after hearing the girl's news story on the television (Pathak, 2022). The Echo now stores voice recordings in the cloud in order to distinguish users' voices which raises obvious suspicions. Trouble occurred in May of this year when the U.S. Department of Justice filed a claim on behalf of the Federal Trade Commission (FTC) due to Amazon retaining children's voice recordings indefinitely while falsely informing users that voice recordings and geological information could be deleted (Fair, 2023). Over a one-year period, Amazon gave 30,000 employees access to Alexa users' voice recordings for no apparent reason (Fair, 2023). Amazon paid a $25 million settlement after violating the COPPA (Children's Online Privacy Protection Rule) and the company can no longer use "geolocation, voice information, and children's information for the creation or improvement of any data product" and must delete inactive child Alexa accounts (Fair, 2023).

One of the most commonly asked questions about smart speakers has been whether or not they are always listening.

Based on a study carried out by Marcia Ford and William Palmer, the answer is: Yes. Through a twenty-one-day experiment, which analyzed network traffic over an Amazon Echo Dot, it was found that 70% of logged response cards were television sounds and 30% were of human voices. Amazon speakers claim that they do not record conversations without first hearing the "wake word", but as seen here, this is not true.

3.3 Compromising location

Another aspect of smart devices to be wary of is location tracking. Smart watches and smart phones have microphones and cameras and come with similar related security concerns as smart speakers, yet a key distinguishing feature has to do with the fact that these devices tend to be constantly on the user wherever they go. Smartwatches use accelerometers for motion sensors, and they can be tracked through a spying smartphone app that reads accelerometer data to determine the wearer's actions – sitting, standing, running, typing etc. (Lurye, 2018). Although difficult, it is possible to identify exactly what a user is typing when the user's typing patterns are observed over a long period of time and their activity is paired with location tracking to distinguish when the user will be typing something important (i.e. a password when entering work) (Lurye, 2018).

Furthermore, parents have been giving smartwatches with location tracking capabilities to their children in order to make sure they are safe throughout the day when away from home. Such a watch, however, can be hacked and followed, providing attackers with information about the child's whereabouts and more. This occurred in 2020 with Thinkrace smartwatches when at least forty-seven million devices were thought to be compromised. Security researchers found out that each device connected to the Thinkrace cloud platform could be accessed with a device's unique identification number and a default password, and once past this, a hacker could track the child's location, reset passwords, send and receive voice recordings, and activate cameras (Ikeda, 2020).

Smartphones, like smart watches, are constantly on the user and pose location tracking risks. A Ph.D. student, Evangelos Bitsikas, and his research group from Northeastern University found a vulnerability in text messaging that can enable attackers to track a smartphone simply by knowing the phone number and having normal network access (Thomsen, 2023). Once a hacker sends a sequence of text messages to a victim's phone, the timing of the automated delivery leaves a location fingerprint that can be tracked through an algorithm (Thomsen, 2023). Moreover, a smartphone uses location tracking for a variety of applications and for its own security purposes, like Find My iPhone. Even if location services are turned off, it is still trackable (McAfee). Find My iPhone uses Bluetooth to locate an offline phone, and public Wi-Fi and spyware allow a smartphone to be constantly tracked (McAfee).

3.4 Invasion of privacy

What about smart devices that know the ins and outs of a user's own home? Robotic vacuums that use Wi-Fi, webcams with night vision, and smartphone-controlled navigation can be hacked to spy on the owner or house. The Roomba i7 was the first of iRobot's smart vacuums able to remember up to ten floor plans of a home (Schroeder, 2018). This entails security risks, and although iRobot CEO, Colin Angle, has stated that this data will never be sold to third parties, IoT devices are always prone to security failures (Schroeder, 2018).

In 2020, workers in Venezuela posted a series of photos of intimate household scenes captured from low angles – from the iRobot's Roomba J7 series robot vacuum (Guo, 2022).

These types of photos are regularly captured and sent to the cloud, but with stricter storage and access controls. MIT obtained fifteen screenshots and they included a young woman on a toilet, a young boy laying on the floor, and other miscellaneous images of furniture and décor. Roomba claimed that these images came from 'special development robots' used for testing by paid collectors and employees and are not consumer products for purchase (Guo, 2022). Despite all this, smart vacuums still have the potential to be hacked, revealing house plan information and possibly photos

of the owner.

Cars have been reviewed to be the worst product in terms of privacy. Automobiles have been advancing to include more smart technological aspects, such as cameras, inertia sensors to gather information about their surroundings, voice command features, and AI-powered autopilot. The Mozilla Foundation, an American open-source community project, researched 25 car brands in terms of their privacy. All the studied cars were found to collect large amounts of personal data on how a user interacts with the car and third-party sources with Sirius XM or Google Maps. 84% of them shared or sold a user's data with service providers, data brokers, and businesses. 56% also can share information with the government or law enforcement based on just a simple informal request. Only 2 out of the 25 brands studied allowed the users to have control over their own data and privacy. This study brings alarming new truths to cars with smart features and how they can be even more dangerous than smart speakers.

3.5 Surveillance and harassment

Not only are unknown stalkers or hackers the main culprits of smart home device manipulation, but abuse can occur right from within one's own household. Smart devices have become a tool used in domestic violence to harass, monitor, and control. One of the first known court cases for IoT-related abuse occurred in 2018 with an 11-month prison sentence for a husband found guilty of eavesdropping on his wife through a tablet (Riley, 2020).

Smart home devices can be controlled by an abuser to physically and psychologically torment a victim by adjusting the home's temperature to be very hot or cold via smart thermometers or heaters, stalking when a victim enters or exits the house via smart doorbells, spying on phone calls or what the victim may be doing inside the home, preventing a victim from entering or leaving the house through smart locks, among others (Khan, 2023). Women continue to be disproportionally affected by domestic abuse, and the United Nations has noted that violence against women was at its height during the COVID-19 pandemic, with tech ill-use playing a huge role in this growing issue (Health Hub, 2023). In the UK, for example, there has been a 93% increase in the use of spyware and stalkware apps since COVID-19 lockdown measures were implemented (Health Hub, 2023).

Having admin control of smart devices or Wi-Fi and passwords, shared either willingly or unwillingly, are just some ways a domestic abuser can maltreat a vulnerable victim who may not understand the possibilities of tech-facilitated abuse nor how to protect themselves. The population should not only be cautious about outside hackers and big companies gaining access to personal information through smart devices, but also aware of potential manipulation of devices by partners or family members in domestic abuse.

3.6 FOMO, information overload and other psychological risks

The threat spectrum of smart devices would not be complete without mentioning the psychological aspects. Users of smart phones, smart watches, and tablets are typically very attached to their devices and use them on a daily basis. Smart phones are especially addictive, and former Google design architect, Tristan Harris, believes they were designed to be so by seizing the focus of the user to profit the tech companies (Bosker, 2016).

Application software has been designed to hook the user in and keep them scrolling through simultaneous rewards and feedback, such as likes and messages.

Chronic phone use is a recently developed behavioral addiction that negatively affects the person over time and may lead to sleep deficiency, lower concentration, creativity blocks, anxiety, stress, depression, loneliness, insecurity, impaired relationships, and poor academic performance (Addiction Center). Intense phone overuse has been proven to change the reward circuits of the brain, particularly the GABA neurotransmitter that produces a calming effect in the body and reinforces addictive behavior. Additionally, excessive phone use changes the grey matter of the brain (responsible for controlling movement, memory, and emotions). A study conducted by scanning multiple phone addicts' brains showed the physical shape and size of the brains resembled that of drug users (Addiction Center).

Teenagers and adolescents, particularly girls, are prone to this risk of addiction, and according to the CDC (Centers for Disease Control and Prevention), between 2010–2015 (a time where smart phone use was increasing at a high rate), suicide rates rose by 12% and reporting of severe depression increased by 58% in adolescent girls in the U.S. (Price, 2017) Economic struggles are also a key factor in the explanation of this sharp rise in suicide and depression during this time frame, however, researchers at San Diego State University found that those that spent more time online have an increased risk for mental health issues (due to online abuse and the effect screentime has on an adolescent brain), and the rise in device usage during these years was one of the biggest changes in teenagers' lives. The university researchers recommend 1-2 hours of device use per day as a safe limit.

The constant influx of messages, calls, notifications etc. from smart devices leaves a user feeling as if they should be available around the clock. This can overwhelm an individual and lead to message dependency. On the other hand, an absence of messages and notifications can lead a user to feel lonely and neglected, causing anxiety, stress, and depression. Either way, an expectation to be up to date with all notifications induces preoccupation and distraction from the present moment (Harwood, 2014). Furthermore, the excessiveness of stimuli becomes a new normal, and typical everyday events and situations become boring and are then replenished with smart device usage. In-person communication can turn into a hassle, as a reliance on smart devices fuels the avoidance of real-life communication and increases social stress and the likelihood of emotional instability when forced not to communicate via a smart device (Harwood, 2014).

Smart devices do not need to consume a person's life.

Precautionary measures can be taken to avoid addiction, such as designated time away from smart devices and connecting with the present world or limiting the number of smart devices owned altogether. Indeed, smart devices are interesting and expedite everyday tasks, yet slipping into a device addiction can happen seamlessly and have devastating mental health effects.

4. The Way Forward

International laws are lagging regarding the security and regulations of smart devices. For instance, smart watches may have stricter medical regulations in terms of fitness tracking; however, they have no particular regulation for location tracking and its data (Ikeda, 2020). In the UK, until recently, there were no legal requirements for a smart product to be secure, leaving the quality of a device's safety up to the manufacturer (Khan, 2023). At the end of 2022, the Product Security and Telecommunications Infrastructure (PSTI) Act was passed in the UK to bring minimum security standards for new smart devices.

In the EU, the EU Cyber Resilience Act was proposed in 2022 by the European Commission to set a standard of rules that apply to IoT devices, implementing mandatory cybersecurity requirements for smart products before they can enter the market and reporting actively exploited vulnerabilities and incidents (European Council, 2023). It

additionally includes monetary repercussions for not complying with the new standards (Lomas, 2022). In July 2023, the Council of the EU met and reached an agreement on the proposal, advancing the EU's commitment towards a safe and secure digital market (European Council, 2023). This proposal still must go through various steps before it can be approved and implemented, meaning the act will most likely not take effect until 2025 (Lomas, 2022).

In the U.S., there are also not many policies in this respect at the federal or state levels. Most guidance comes from NIST standards and compliance to meet security standards lies with the vendors, leaving many security issues regarding where data is collected, who has access to this data, and what type of data should be illegal to collect, unaddressed (Beyer, 2023).

IoT safety legislation can be ambitious, as single acts will attempt to cover a wide range of different products with different functions. Some industry leaders, like Director-General of DigitalEurope, Cecilia Bonefeld-Dahl, believe the acts will not be enough to secure users. Regarding the EU Parliament's vote in favor of the Cyber Resilience Act, Bonefeld-Dahl has stated:

Today's votes move this important piece of legislation forward, but the issue remains that the Cyber Resilience Act aims to cover a very broad scope of products – including hardware and software – within a very short timeframe, while industry and governments are struggling with stretched cyber resources.

Securing IoT devices through legislation will not be a quick and seamless process – we can expect security improvements in the years to come, however personal precautions should still be prioritized.

Smart devices are engineered to be practical, not necessarily safe. Users must take precautions when using any IoT device, as being constantly connected to the Internet and Bluetooth comes with security and privacy risks. The vulnerabilities mentioned above are just the tip of the iceberg, with more smart device weaknesses being discovered and exploited each day. Since there are no set international laws regarding the security of IoT devices yet, it is up to the consumer to monitor their own safety and conduct in-depth research on the products they are consuming as well as to be aware of who could be a potential threat. With any advanced technology that makes everyday tasks a breeze, comes privacy risks. The real question lies with whether or not we are prepared and willing to sacrifice our privacy, security, and more in favor of keeping these devices an essential part of daily life. ■

About the author:

Liliana Kotval is a Junior Project Coordinator and Analyst at Instytut Kościuszki. She holds a BA in Global Cultural Studies from Suffolk University with a concentration in European Affairs and two minors in Mathematics and Spanish Language. Throughout the completion of her BA in Boston, Prague, and Madrid, she worked with different think tanks, such as Europeum in Prague and Fundación Civismo in Madrid. At these think tanks, she published various articles on topics ranging from TransAtlantic and European Affairs, Culture, and Cybersecurity, and continues to do so in her current position. Her other main interests include journalism and anthropology.

References

Addiction Center (n.d.). Phone Addiction: Warning Signs and Treatment. https://www.addictioncenter.com/drugs/phone-addiction/#:~:text=Chronic%20phone%20use%20is%20a,medical%20professionals%20and%20researchers%20worldwide

Beyer, J., Su, D. (2023, March). U.S. Federal and State Regulation of Internet of Things (IoT) Devices. The Henry M. Jackson School of International Studies, University of Washington. https://jsis.washington.edu/news/u-s-federal-and-state-regulation-of-internet-of-things-iot-devices-2019-2022/

Bosker, B. (2016, November). The Binge Breaker. Tristian Harris Believes Silicon Valley is Addicting Us to Our Phones. He's Determined to Make it Stop. The Atlantic. https://www.theatlantic.com/magazine/archive/2016/11/the-binge-breaker/501122/

Buil-Gil, D., et al. (2023). The Digital Harms of Smart Home Devices: A Systematic Literature Review. Computers in Human Behavior 145.. https://doi.org/10.1016/j.chb.2023.107770

Caltrider, J., Rykov, M., MacDonald, Z. (2023, September). It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy. Mozilla Foundation. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

Council of the EU. (2023, July). Cyber Resilience Act: Member States Agree Common Position on Security Requirements for Digital Products. https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/

Fair, L. (2023, May). Out of the Mouths of Babes? FTC says Amazon Kept Kids' Alexa Voice Data Forever – Even After Parents Ordered Deletion. Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2023/05/out-mouths-babes-ftc-says-amazon-kept-kids-alexa-voice-data-forever-even-after-parents-ordered

Ford, M., Palmer, W. (2019). Alexa, are you listening to me? An Analysis of Alexa Voice Service Network Traffic. Pers Ubiquit Comput 23. https://doi.org/10.1007/s00779-018-1174-x

Guo, E. (2022, December). A Roomba Recorded a Woman on the Toilet. How did Screenshots End Up on Facebook? MIT Technology Review. https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

Harwood, J., et al. (2014, May). Constantly Connected – The Effects of Smart Devices on Mental Health. Computers in Human Behavior 34. https://doi.org/10.1016/j.chb.2014.02.006

Health Hub. (2023). Top 10 In-Home Devices Used for Tech-Enabled Domestic Abuse. https://hubpublishing.co.uk/top-10-in-home-devices-used-for-tech-enabled-domestic-abuse/

Ikeda, S. (2020, Janusary). Location Tracking Cloud Vulnerability Impacts Millions of Smartwatches Worn by Children. CPO Magazine. https://www.cpomagazine.com/cyber-security/location-tracking-cloud-vulnerability-impacts-millions-of-smartwatches-worn-by-children/

Irwin, L. (2023, July). European Parliament Votes in Favour of Cyber Resilience Act. IT Governance. https://www.itgovernance.eu/blog/en/european-parliament-votes-in-favour-of-cyber-resilience-act

Khan, C. (2023, April). 'Smart' Tech is Being Weaponized by Domestic Abusers, and Women are Experiencing the Worst of it. The Guardian. https://www.theguardian.com/commentisfree/2023/apr/04/smart-tech-domestic-abusers-women

Kumar, D., et al. (2018). Skill Squatting Attacks on Amazon Alexa. University of Illinois

Urbana-Champaign. https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kumar.pdf

Lomas, N. (2022, September). The EU Unboxes its Plan for Smart Device Security. Tech Crunch. https://techcrunch.com/2022/09/15/eu-cyber-resilience-act-draft/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMz6tNUVnZe77jxWEDsNFEH2d8ypvNH2lqYUrNZ10CdKBLBsGECJP5HYLT9NjnILnsolTz1TKEujt64aITSGI3nW7P028P5DnBzO5LoLRNPn39u8iq_hbWOxXnsTKal1h7QiqFl9nmNxM1oeow-pdwtoGDidY7oy4N9gXW65W9ki

Lurye, S. (2018, May). Experiment: How Easy is it to Spy on a Smartwatch Wearer? Kaspersky. https://www.kaspersky.com/blog/smart-watch-research/22536/

McAfee. (n.d.). Can My Phone Be Tracked If Location Services Are Off? https://www.mcafee.com/learn/can-my-phone-be-tracked-if-location-services-are-off/

Old Dominion University. (2021, September). The Risks and Rewards of IoT Tech and Smart Devices. https://digitalskills.odu.edu/cybersecurity/the-risks-and-rewards-of-iot-tech-and-smart-devices/

Panda Security. (2023, August). Cybersecurity Survey: 36% of Europeans Don't Even Have an IoT Device. https://www.pandasecurity.com/en/mediacenter/press-releases/cybersecurity-survey-iot/

Pathak, S., et al. (2022). A Survey on Security Analysis of Amazon Echo Devices. High-Confidence Computing 2, 4. https://doi.org/10.1016/j.hcc.2022.100087

Perekalin, A. (2018, February). Smart Home Apocalypse. Kapersky. https://www.kaspersky.com/blog/mwc2018-insecure-iot/21343/

Price, M. (2017, November). Screen Time Might Boost Depression, Suicide in Teens. San Diego State University NewsCenter. https://newscenter.sdsu.edu/sdsu_newscenter/news_story.aspx?sid=77017

Riley, A. (2020, May). How Your Smart Home Devices Can Be Turned Against You. BBC. https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse

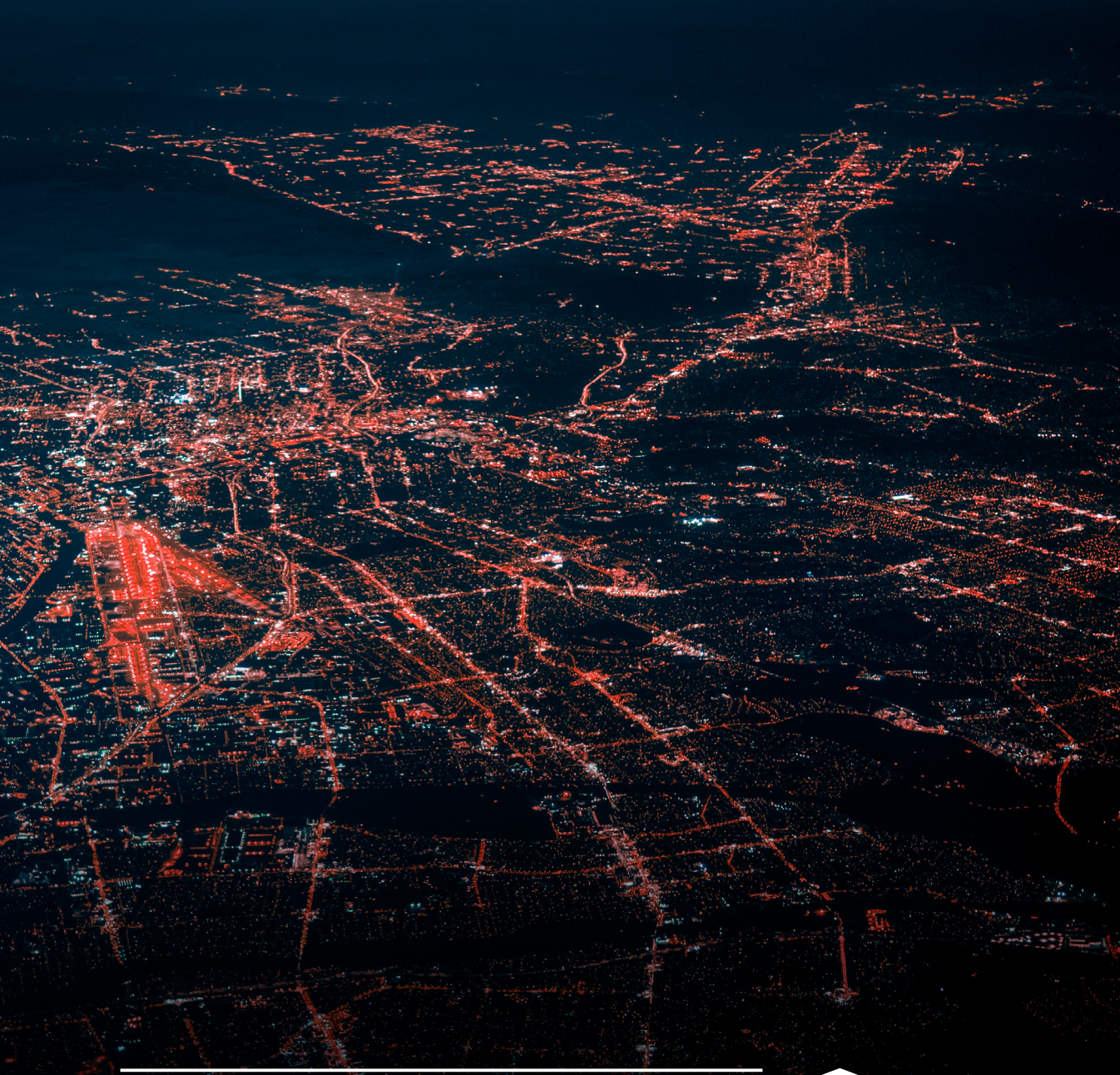
Statista (n.d.). Market share of global smart speaker shipments from 3rd quarter 2016 to 1st quarter 2022. https://www.statista.com/statistics/792604/worldwide-smart-speaker-market-share/#:~:text=Amazon%20is%20the%20leading%20vendor,percent%20in%20the%20same%20quarter

Statista. (n.d.). Number of Users of Smart Homes Worldwide from 2018 to 2027. https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world

Thomsen, I. (2023, July). New Smartphone Vulnerability Discovered by Northeastern Ph.D. Student Reveals Hackers Could Track Your Location. Northeastern Global News. https://news.northeastern.edu/2023/07/27/phone-location-tracking-research/

TrendMicro. (2019, July). Inside the Smart Home: IoT Device Threats and Act Scenarios. https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios

Wise, J. (2023, August). Smart Home Statistics 2023: How Many Smart Homes are There? EarthWeb. https://earthweb.com/smart-home-statistics/



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