VOLUME 8 (2023) ISSUE 2

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

Expert's View on the War in Ukraine, Russian Cyber Capabilities and Information Warfare

Dr Marina Miron

Ukraine's digital resilience helps the society carry on and fight back to protect our freedom

Interview with Gulsanna Mamediieva

ANALYSES • POLICY REVIEWS • OPINIONS

THE KOSCIUSZKO INSTITUTE

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

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

Editorial Board:

ISSN: 2450-21113

Citations: This journal should be cited as follows:
”European Cybersecurity Journal”
Volume 8 (2023) Issue 2, page reference

THE KOSCIUSZKO INSTITUTE

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

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

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

Contents

The content of this issue of the ECJ was prepared from December 2022 to February 2023. The processes and events described by the Authors may still be developing therefore some information may change as the situation unfolds.

Editorial

Ewelina Kasprzyk

Chief Editor of the European
Cybersecuirty Journal

Dear Readers,

The previous issue of the ECJ came out exactly on the 100th day of the Russian invasion of Ukraine. Today, as we are releasing a new issue of the Journal, Ukraine is still under continuous attacks.

As the war goes on, so does our support for Ukraine – through diplomacy, humanitarian aid, military support, and finally technological assistance, also in the cyber realm.

The war has affected the cyber landscape a great deal. We have experienced new disinformation and propaganda tactics, unprecedented use of digital technologies on the battlefield (both military and civilian applications), tech providers supporting Ukraine by free-of-charge use of their state-of-the-art solutions and services, and so on. Technology is proving to be detrimental in times of crisis, which is why we decided to make this the central topic of the new issue of the ECJ.

We gathered top level experts – from government officials to researchers, to share with you their insights into what is the role of technology in modern crises. You will find here articles analysing both the current war in Ukraine, as well as other critical situations in which human rights are in danger. In this issue we are also proudly publishing an article by the winner of last year's CYBERSEC Young Leaders Initiative – on this occasion, we invite you to join our call for papers for the 2023 edition. Lastly, our authors have also prepared a few critical recommendations regarding cloud security for companies.

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

Signed,

Ewelina Kasprzyk

Ewelina Kasprzyk

CYBERSEC
FORUM / EXPO

SAVE THE DATE

21-22 June 2023

International Congress Centre in Katowice

www. cybersecforum.eu

Ukraine's digital resilience helps the society carry on and fight back to protect our freedom

Interview with Gulsanna Mamediieva – Director General of Directorate for European and Euro-Atlantic integration, Ministry of Digital Transformation of Ukraine; Georgetown University Fellow

The ongoing war is arguably the first conflict to use both kinetic and digital warfare on such a scale. We see clearly that digital technology has become a key tool to achieve strategic objectives. Cyberattacks and disinformation campaigns against Ukraine and your allies were the highlight of the war coverage for months. What is the current state of play? Has the recent experience had any impact on Ukraine's security policy?

Gulsanna Mamediieva: Absolutely. Nowadays, we can observe the first war in which digital warfare is being used not as a supplementary but as an equal component to kinetic warfare and military actions. This proves that the aggressor had given due consideration to digital or cognitive warfare. That, of course, has been reflected in the security policy of Ukraine.

A full-scale Russian invasion of Ukraine provides valuable lessons and calls for action to put in place effective measures that will be vital to protecting the future of the country's democracy. As the war continues, we expect the Russian state and the state-sponsored hackers to continue their cyber operations to paralyse those opposing it and disable Ukraine's energy, transport, and digital infrastructures. Cyberwarfare will be a game changer in any future conflict.

We keep seeing reports of Russia's malicious activity aimed at Ukraine in cyberspace, and yet – your country is still standing strong. What helped you prepare for Russian attacks and how do you manage to fend off new threats?

Prior to the full-scale war, Ukraine had a long-standing Data Protection Law prohibiting government authorities from processing and storing data in the public cloud. This meant that the country's public-sector digital infrastructure was run locally on servers physically located within the country's borders. A week before the Russian all-out invasion, the Ukrainian government was running entirely on servers within government buildings—locations vulnerable to missile attacks and artillery bombardment. Ukraine's government successfully sustained its civil and military operations by acting quickly to migrate its digital infrastructure into the public cloud, where it has been hosted in data centres across Europe.

Digital transformation does not stop in times of war. Your country has used various digital tools and solutions to support your citizens, government, and your army as well – also with the future in mind. In your opinion, what was the best piece of technology or solution you employed in the past year?

It is very hard to choose. Ukraine started the process of digital transformation long before the Russian full-scale invasion. The Ministry of Digital Transformation of Ukraine was created in 2019 to implement the 'state in smartphone' project announced by President Volodymyr Zelenskyy. Headed by Mykhailo Fedorov, the Ministry's main goal was to make Ukraine a user-friendly state for citizens and businesses by providing them with seamless access to public services. We continue to work on it. However, due to the war, the Ministry had to change its priorities. Prior to the Russian invasion, we worked to launch public services for peacetime. Now we are working to launch a wide array of services to support us during war. Ukraine's government has put in place a program of financial assistance to entrepreneurs and employees from the regions where hostilities took place. It also offered assistance services for displaced citizens allowing them to submit applications for compensation for damaged property. The Ministry has also launched eVorog (eEnemy), a chatbot for informing the Armed Forces about the movement of enemy equipment, soldiers or collaborators. It also enabled users of the government-owned Diia app and Diia.Radio to watch and listen to a news marathon by Ukrainian TV channels to provide Ukrainians with accurate information. eDocument, on the other hand, was released to help people who escaped their homes without documents obtain temporary digital papers or pension certificates.

> **Prior to the Russian invasion, we worked to launch public services for peacetime. Now we are working to launch a wide array of services to support us during war.**

2,200 Ukrainians are learning a new profession in IT for free within the framework of the IT Generation project. The full-scale war forced Ukrainians to leave their homes and move to safer regions. Many of them lost their jobs. It is very important to help them move into a new career in a short time and start working again.

We are developing an army of drones. The comprehensive program includes the systematic purchase of drones, their repair, prompt replacement, and a pilot training course.

In addition, we are finding new solutions to maintain operation of important facilities which use satellite internet technology. Ukraine is one of the countries with the largest number of Starlink terminals which amount to 30,000. We received the terminals from Elon Musk's SpaceX company, ministers of digital transformation from the EU countries, and other partners. Starlink makes it possible for the critical infrastructure facilities, including medical, energy, education, and business, to have access to stable and fast internet connection. In addition, Starlink terminals helped restore communication in Irpin, Bucha, Borodyanka, Chernihiv, and other settlements after the Russian occupation had ended.

How did it affect your society and your country's fight against Russia?

Ukraine's digital resilience helps the society carry on and fight back to protect our freedom.

For example, almost 5 million applications were received during March 2022 for the eSupport program, under which nearly UAH 31 billion was paid to those who had lost their jobs because of the war. This program proved extremely successful, helping many of our citizens.

The war forced our citizens immediately to evacuate to safer regions of the country. However, not everyone managed to take the necessary paper documents with them. That's why we created a digital alternative—eDocument. Containing passport data and a taxpayer number, this digital document helped hundreds of people to confirm their identity while moving around Ukraine.

As many as 440,000 Ukrainians use the eEnemy chatbot to report on the enemy's fuel tankers, accumulation and movement of equipment columns, transportation of equipment by rail, location of warehouses with ammunition, radar stations, artillery positions, field airfields for rotorcraft, location of the leadership of enemy troops, deployment or residences of the occupiers.

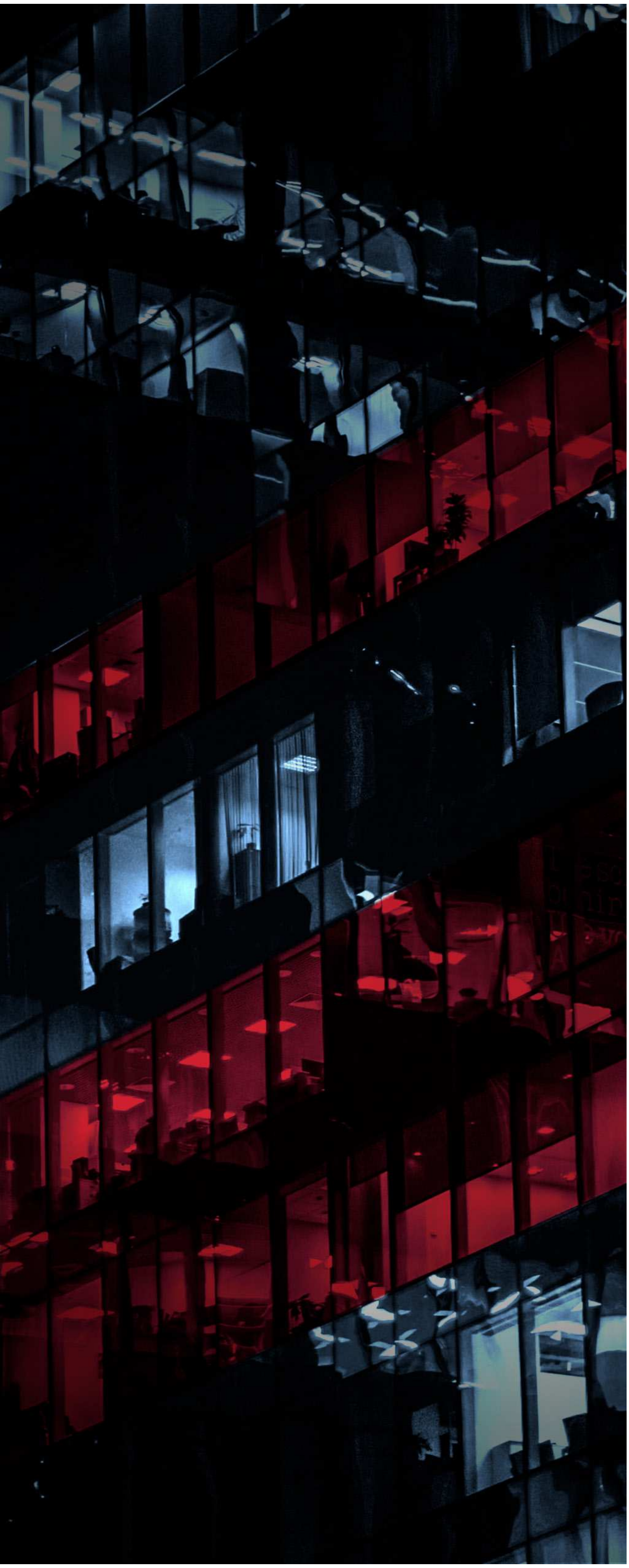
In September 2022, the European Commission and Ukraine signed an agreement inviting Ukraine to the Digital Europe Program which is another great example of how the EU states and Ukraine can work together. What benefits will both parties gain from this 'deal'? What form of collaboration ought to be considered moving forward?

The Program aims to accelerate Europe's digital transition in all sectors, and Ukraine, being called the European Digital Transformation Tiger because of our achievements, logically fits into this ambitious Program. We have already applied to develop the European Digital Identity Wallet as part of the consortium. This great financial mechanism will help us digitize Europe hand in hand with our European colleagues, share our experiences, and get new ones. By the way, our Polish colleagues played an essential role in facilitating Ukraine's joining this consortium. We very much appreciate this opportunity to work together.

We have a unique experience creating a 'state in a smartphone' and we are ready to share it with our partners. In 2.5 years, we have launched 14 e-documents and 23 government services in the Diia app used by 18.5 million citizens. With 22 million users, the Diia portal offers 92 state services. Ukraine is the first state in the world with a digital passport. And even during martial law, we continue developing our flagship products: the Diia application and the web portal by introducing new services. Ukraine is determined to actively participate in all projects that are available to us and involve 4 out of 5 main areas of the Digital Europe Programme: supercomputer, artificial intelligence, digital skills, and the wide use of digital technologies in the economy and society. Associated countries cannot participate in the 5th area – cybersecurity, so this component is excluded for us. Still, we can come back to this question and resume talks in the near future, as the EU and Ukraine should work together on this as well. Considering the EU-Ukraine cyber dialogue, our recent and daily experiences on the cyber front, lessons learned, development of military tech, and Ukraine's participation in this component will be mutually beneficial.

> **Our strategic priority is the integration of Ukraine with the EU's Digital Single Market. To achieve this goal, Ukraine has its own 'digital' homework to do, namely implement a list of EU legal acquis, and do it successfully. In some cases, we are implementing it even faster than the EU member states themselves.**

Our strategic priority is the integration of Ukraine with the EU's Digital Single Market. To achieve this goal, Ukraine has its own 'digital' homework to do, namely implement a list of EU legal acquis, and do it successfully. In some cases, we are implementing it even faster than the EU member states themselves. The European Code of Electronic Communications is an example of that. We are in constant contact



with the European Commission and fruitfully participate in the EU projects that help us align our legislation with the EU ones. In view of EU member candidate status and the desire of Ukrainians to become part of the big EU family, we are very close to this.

Information has been weaponised. We see how the Kremlin uses social media to spread hateful and false stories about Ukraine, your allies like Poland etc. It's not easy to stand against this powerful propaganda machine, now even more powerful thanks to social media. How does your country fight back?

From the first days of the war, the Ukrainian IT community and hackers united to form the so-called IT Army. That army has now more than 300,000 people. They set their own goals every day and coordinate themselves. The IT army has a clear rule—they do not harm ordinary Russians, despite their support for the war. Banks and companies close to the Kremlin and propaganda and disinformation resources are under counterattack. Every day, we see many statements by Russian organisations that we are shut down because of the DDoS attack or that we have been hacked and posted accurate information about what is happening in Ukraine.

One of the key actions to fight against disinformation against Ukraine is to prove it is false. Hence, we have a strong community of fact-checkers. The International Fact-Checking Network, which includes more than 100 organisations, makes a collaborative effort to battle disinformation about Russia's invasion of Ukraine in its project #UkraineFacts. It has three Ukrainian Members: Lead Stories, Vox Ukraine, and StopFake.

For example, StopFake regularly monitors Russian disinformation to spot fake stories. So far, they have debunked over 650 stories and published around 300 other articles and opinions on their website. StopFake fights disinformation also by creating multimedia explanatory video content in 14 languages for social networks like Twitter, Facebook, Telegram, and Instagram. This fact-checking organisation has gathered 6.5 million followers on Facebook. StopFake regularly cooperates with the Center for Strategic Communications and Information Security, the Ministry of Culture and Information Policy, the Ministry of Foreign Affairs, the Ministry of Digital Transformation, and the National Council for Television and Radio Broadcasting.

We also want to share the truth with English-speaking users directly. In the summer, a new rebellious insider digital media was introduced—UNITED24 Media. Initiated by the Ministry of Digital Transformation of Ukraine, its main goal is to show that Ukraine is fighting for freedom and independence, and to encourage the world to collaborate. Moreover, UNITED24 Media is based on the principle of a startup, and a week after the launch, it received more than 400 proposals for cooperation both from Ukrainian and international specialists.

During CYBERSEC FORUM/EXPO 2022, you mentioned that you had also reached out to social media platforms to fight against false information and to spread the truth about what's happening in Ukraine, for example the tragic events in Bucha. Do you feel their support? What do you think could be improved so the coverage of the war on social media is fair, trustworthy and factual?

We are in constant working contact with all social media platforms. We express our concerns or escalate some serious cases, for example, of some bloggers or local volunteers being blocked, government officials' accounts that are under Russian trolls attacks as well as in cases like Bucha, when algorithms blocked the related hashtags. We see some progress. They try to react, but that only partially settles the issues. Platform policies have not been designed to resist propaganda for war and disinformation of such scale, and we are constantly trying to point this out. So definitely more should be done, for example, by creating, in exceptional cases, robust and prompt direct governmental channels to be used as special instruments to escalate efforts if necessary.

The world generally sees how today's tech structure erodes trust and fuels misinformation, polarization, and inequity. That's partly because the applications and algorithms that shape our economies, democracies, and public discourse were developed with few legal restrictions or commonly held ethical standards. This is a global problem that regulatory tweaks or special agreements can't solve. We need comprehensive, collaborative solutions to shape tomorrow's tech infrastructure positively.

Platform policies have not been designed to resist propaganda for war and disinformation of such scale, and we are constantly trying to point this out.

The EU imposed sanctions on the broadcasting of state-owned media outlets RT/Russia Today and Sputnik across the Union. What is the true impact of this type of 'censorship', as some call it, in a world where, technically speaking, we can access whatever we want on the Internet? Does it have a positive effect? What is the value of that?

Indeed, broadcasting media do not play such a unique role anymore and probably have less and less influence, with digital media taking over in scope and coverage. Still, a significant percentage of the population, especially the elderly, rely on TV and broadcasting media. That is why such actions as imposing sanctions on manipulative media outlets are very needed. We should not allow Russian propaganda to spread across the EU. They cannot be considered as 'the media' anymore, they are nothing but a propaganda machine. And I would not call it censorship, or at least I would not give it any negative meaning. We must be aware of the danger that such entities pose. We should not put them under the freedom of speech umbrella. Those who undermine the very idea of democracy and an open society, the only kind of society where freedom of speech can be effectively protected, cannot be called as the media. Voltaire's quotation, 'I disapprove of what you say, but I will defend to the death your right to say it,' stays relevant, yet with the one exception, which is when one's expression aims to undermine the whole system that provides for citizens to express their thoughts freely.

Do you think technologies help you spread the truth about war? To keep people informed, involved, aware of both the atrocities done by Russia and your country's brave fight?

Sure, a good example of how we use technology to spread the truth is the UNITED24 Media project, which I already mentioned. It is an English-language digital media in a modern format centred around a YouTube channel and social media platforms. UNITED24 Media works on individual episodes and covers six themes: culture, history, people, technology, business, and war. Content is designed to reach a broad audience that actively uses social media, YouTube, and other interactive formats. Using technologies, we not only keep our citizens informed and involved, but also reach the international community and even try to affect the public discussion in Russia, even though the latter is only sometimes the case. Russia banned some social networks for showing the truth, making it difficult for people to access it. In authoritarian states, social media platforms may be the only way to learn the facts.

But it works both ways: we can see how social media platforms are being used to glorify aggressive war, hatred, and online abuses. We see many examples of technologies being misused, for example, to spread fake news or support PSYOPs.

This war has shown us how authoritarian and democratic states use technology in a very different way. Do you agree with a statement that technology is neutral by default and that it is up to us whether we use it to do good or bad?

With the exception of technology designed for malicious purposes, I agree that it is largely neutral by default. It is the policy and the law that frames our usage of it. That is why the regulation of technology should be given due consideration. AI technologies are a good example: they can be used both for good (in healthcare, education, public sector) and bad, for example to suppress dissent by using social scoring schemes and similar initiatives. Generally speaking, there is no bad or good technology. What matters is how we use it. ■

The interview was conducted in January 2023.

About the author:

In charge of European integration of digital sector of Ukraine and gradual integration into EU Digital Single Market. Gulsanna and her team have launched development and implementation of the strategy of integration of Ukraine into European Digital Single Market. It consists of many components: electronic communications, online safety, privacy, open data, digital skills, innovation, trust and identification services, e-commerce, etc. Before working in the Ukrainian government, Gulsanna had been an lawyer in private IT sector. She have ve got Master Degree in Information Technology Law, University of Tartu, Estonia and currently pursuing PhD at Kyiv Institute of International Relations with the research in the sphere of Internet Law. Gulsanna speaks Ukrainian, Crimean Tatar, English, Russian, English. Learning French.

EXPERT'S VIEW

On the War in Ukraine, Russian Cyber Capabilities, and Information Warfare

DR MARINA MIRON

POSTDOCTORAL RESEARCHER, DEPARTMENT OF WAR STUDIES,
KING'S COLLEGE LONDON

Russia has been developing its cyber capabilities for several decades now, using its intelligence agencies and relying on the so-called patriotic hackers’ sympathetic to the Russian cause. To understand Russia’s offensive cyber activities, it is important to situate these within a broader framework of information war. Information war is an ongoing activity that takes place both in peacetime and during military conflicts. While there are different definitions of information war within Russia’s academic and military writings, the phenomenon boils down to the domination of the information spectrum. This is an ongoing struggle between Russia and the West and cyber activities fall squarely into the domain of information operations. There are two types of cyber operations: cyber psychological and cyber technical. The former are designed to manipulate and influence public thinking and perception of the adversary. The latter are designed to covertly obtain information and/or overtly degrade the enemy’s IT systems responsible for the functioning of different crucial objects (e.g., critical infrastructure, space assets, and similar). With these definitions in mind, looking at the cyber activities in Ukraine, we can see how the ViaSat hack, which marked the beginning of the ‘special military operation’, was designed to establish information superiority and leave the adversary in the dark (in this case, the Ukrainian military). While this hack was far from being sophisticated in technical terms, it, nonetheless, achieved its objective. Therefore, it is essential to look at the effect that Russia’s cyber operations in Ukraine are designed to achieve rather than analyzing them from their technical perspective.

Looking at the cyber activities in Ukraine, we can see how the ViaSat hack, which marked the beginning of the ‘special military operation’, was designed to establish information superiority and deny information to the adversary (in this case, the Ukrainian military).

What is important to note is that the Kremlin had not been counting on the war taking the turn it did. Therefore, the cyber activities that followed remained relatively benign. This is due to several factors. Firstly, Ukraine has been enhancing its cyber defenses since 2014. To this end, Ukraine has worked together with NATO states to be able to reinforce its cyber capabilities. Thus, Ukraine’s bolstered cyber defenses might explain why Russia has not been as successful as in the case of Sandworm or NotPetya. Secondly, it takes time and effort to prepare for sophisticated cyberattacks. Given that Russia had not been preparing for the kind of war it found itself engaged in, it had no time to prepare such cyberattacks considering Ukraine’s upgraded defenses. Thirdly, if one assumes that Russia has an arsenal of high-end offensive cyber ‘‘weapons’, it would be a ‘waste’ for Russia to deploy its state-of-the-art algorithms since a missile or a drone could accomplish as much. On the one hand, using kinetic weapons ensures immediate effect with an added psychological impact. On the other hand, the damage done is much more challenging to repair. So, in essence, using missiles and drones is much more effective when conducting a cost-benefit analysis. Using missiles and drones also removes the added risk of potential reverse engineering by Ukrainian and NATO cyber forensics.

Instead, what we could witness is that Russia’s GU (formerly GRU) relied on and continues to rely on ‘quick and dirty’ malware, which creates noise in the background without causing substantial damage. More advanced cyberattacks and cyber espionage are being conducted beyond Ukraine’s borders, e.g., the recent attacks against U.S. nuclear scientists by Cold River. Cyberattacks against Ukraine’s supporters are not necessarily something unique. These had been conducted in peacetime, so from this perspective, the strategic approach here did not change. As far as cyber operations in the military domain are concerned, these have been unspectacular, as noted above. A lack of preparation and inability to coordinate cyber operations with kinetic operations (despite some isolated attempts) can be viewed as a gap in Russia’s capabilities. In general terms, combined arms operations have proved to be difficult for the Russians. This gap might indicate poor coordination between Russia’s so-called ‘cyber force’ and ‘military forces’. In theory, overcoming these structural problems and establishing proper coordination should be the main takeaway from the ongoing war for the Kremlin. Given the experiences in the cyber domain so far, it would seem that the Russians will resort to offensive cyber (technical) operations when there are no other (possibly kinetic) means to achieve their strategic objectives.

Russia’s GU (formerly GRU) relied on and continues to rely on ‘quick and dirty’ malware, which creates noise in the background, without causing substantial damage. More advanced cyberattacks and cyber espionage are being conducted beyond Ukraine’s borders, e.g., the recent attacks against U.S. nuclear scientists by Cold River.

As for cyber psychological operations, these have been running in parallel to the military operation; however, due to the blocking of Russian websites and channels in the West, Russia has not proven to be as successful with its psychological operations abroad. Several Russian academics and political figures criticized Russia’s failure to outperform its Western counterparts abroad. Instead, the Kremlin’s focus remained on its constituent population with limited information operations in this domain, targeting countries in the Middle East and Asia. Here the goal was to justify the ‘special military operation’ and to win allegiance and support, which is in line with Russia’s geopolitical thinking à la Aleksandr Dugin. Yet, despite the efforts, it is evident that the creation of 'Russkiy Mir' is still lagging. For example, one can take countries like Belarus or Kazakhstan with a mixed record of support for Russia's cause; in other words, there is a schism between the population and the leadership regarding the 'special military operation'. Notwithstanding, Russia, using information operations and diplomacy, managed to establish favorable relationships with China and Iran. However, it is difficult to assess to what extent designated information operations, as opposed to diplomatic efforts, are responsible for these results. Moreover, China and Iran might cooperate with Russia due to their national interests rather than out of mere sympathy for Russia.

Several Russian academics and political figures criticized Russia's failure to outperform its Western counterparts abroad. Instead, the Kremlin's focus remained on its constituent population with limited information operations in this domain, targeting countries in the Middle East and Asia.

Further, the so-called 'collective West' was targeted with disinformation in relation to several topics including, but not limited to, the negative influence of Ukrainian refugees, Europe's economic collapse, the U.S. ambitions to destroy Europe as an economic power with a particular focus on Germany, and Poland's ambitions to subsume Western Ukraine. Though these kinds of disinformation narratives are proving successful to somewhat polarize societies, Russia still has not achieved the chaos it hoped for.

All in all, in the information psychological spectrum, it should be expected that the Kremlin will try to further pursue its goals of exploiting potential rifts in Western societies while trying to win over the nations of Middle East and Asia. Again, we have seen it before; however, the intensity and themes have naturally changed due to the ongoing war and the overall geopolitical situation. ■

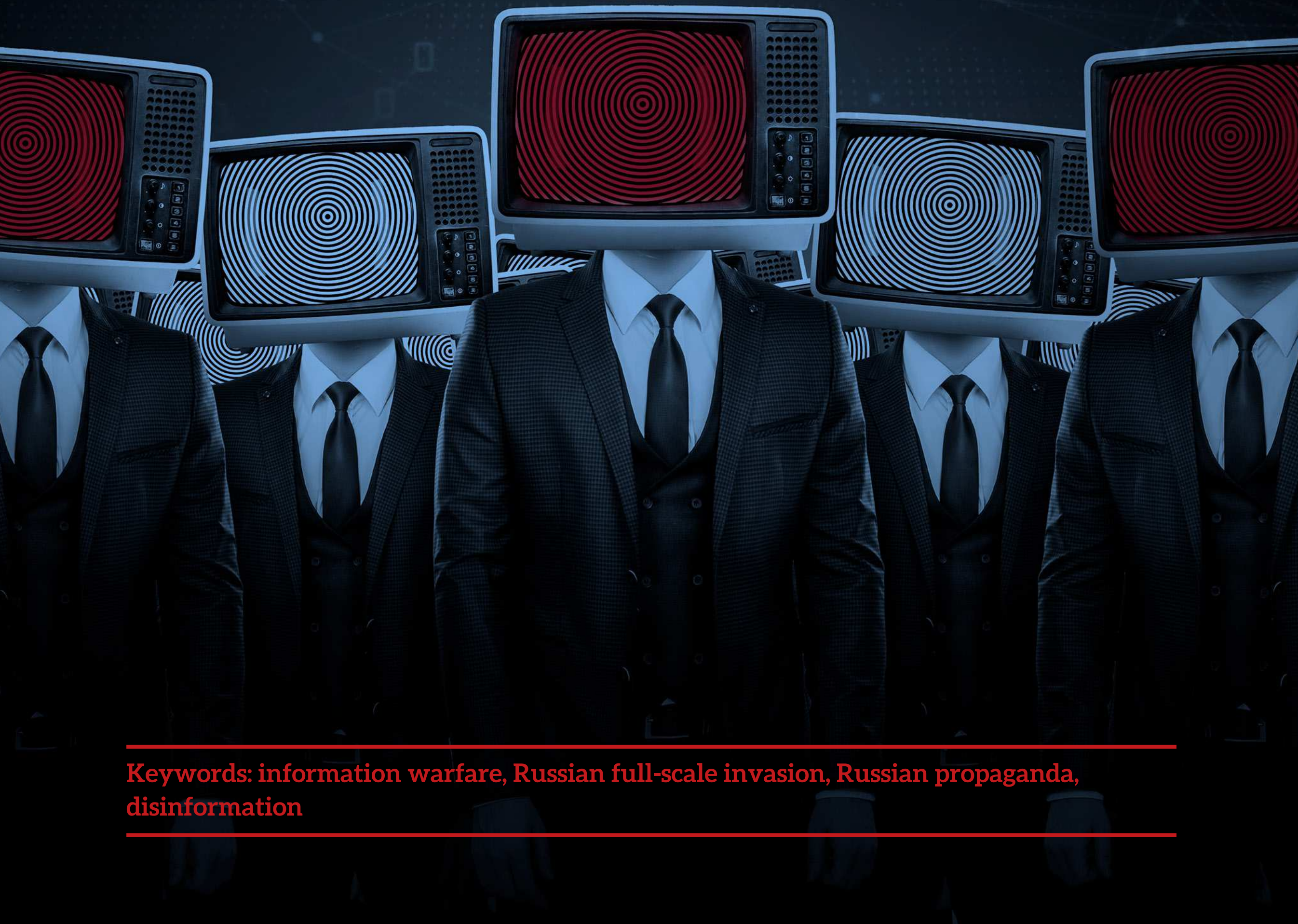
About the author:

Dr. Marina Miron is a post-doctoral researcher at the Department of War Studies. Currently, she is working on a British Academy-funded project on Russia's information warfare which entails analyzing the theoretical underpinnings of Russia's idea of information war and hybrid war and the methods it uses in contemporary settings to pursue its goals in the information sphere. More broadly, Dr. Miron specializes in Russia's security strategy and military doctrine, looking at different domains including but not limited to cyber, space, and the electromagnetic spectrum. Further, she studies Russia's foreign policy, particularly in the Middle East and Southeast and Southwest Asia, focusing on original language publications. Dr. Miron is also concentrating on the war in Ukraine, especially from the military strategic perspective.

ARTICLE

How Russian Propaganda Accompanies War in Ukraine

MARIIA SAHAIDAK
HEAD OF THE STRATEGIC COMMUNICATION DEPARTMENT, STRATCOM CENTRE UA



Keywords: information warfare, Russian full-scale invasion, Russian propaganda, disinformation

Introduction

Disinformation surrounding Russia's large-scale invasion of Ukraine in February 2022 marked an escalation in the Kremlin's ongoing information operations against Ukraine and the entire democratic civilized world. The Russian government used the systematic manipulation of information, disinformation, and propaganda as an operational tool in its attack on Ukraine. Russia had been preparing for a war in Ukraine, not only by mustering an army of soldiers, but also by manipulating the Russian public opinion about the invasion, destabilizing the Ukrainian population, and discrediting it on the international stage.

The formation of the Putin's regime in Russia was accompanied with the cleansing of the media from the opposition and the creation of a powerful state propaganda machine to interact with both domestic and foreign audiences. The Kremlin invested considerable sums in TV channels and news agencies, but also Internet trolls, bot farms, and multilevel agents of influence. Since the beginning of the full-scale war with Ukraine, the Russian government has tripled funding for state media. For example, in the period from January to March 2022, state-sponsored media received 17.4 billion Russian ruble from the federal budget. In 2021, for the corresponding period, this sum was 5.4 billion Russian ruble.[1]

Since 2014, information has become the main tool for a large-scale 'preparation' phase before Russian troops openly attacked Ukraine, inflicting death and injury on civilians. Before the full-scale invasion, the main task of the Russian propagandists was to prepare the ground for the war, namely to form the "right" public opinion in order to brainwash ordinary Russians and make them believe that Ukraine is an artificially created state, and Ukrainians are people who have forsaken their common history with Russia, have become 'Nazis', mere puppets in the hands of the so-called 'collective West' instrumentality using them against the Russian state.

The Kremlin's leaders, especially those controlling the media, showered Russian citizens with lies, exaggerations, and unsubstantiated claims. Russian state media bombarded their viewers with claims that Putin was forced to invade Ukraine to protect Russia and its citizens from a supposedly imminent NATO aggression, Ukrainian Nazis, biological weapons, and 'gender ideology'. Following the full-scale invasion, the narratives of Russian propagandists have become more aggressive, blatantly calling for the destruction of Ukraine, its infrastructure, culture, identity, and people. In addition to justifying or concealing the crimes of the Russian army, Russian propaganda itself has become criminal.

The spread of disinformation by the Russian government and Russian state media, information operations on social media, as well as actions taken in response by the Ukrainian government, Ukrainian civil society, allied governments, and international organisations provide important perspectives and lessons on how to counter the threat posed by information weaponised by dictatorial regimes. The use of disinformation and propaganda has been a common element in all wars, but in the 21st century, the social media landscape has multiplied its reach and potential penetration, and propaganda in the hands of Putin's dictatorship has become a tool to justify the war and genocide.

Following the full-scale invasion, the narratives of Russian propagandists have become more aggressive, blatantly calling for the destruction of Ukraine, its infrastructure, culture, identity, and people. In addition to justifying or concealing the crimes of the Russian army, Russian propaganda itself has become criminal.

[1] Миллиарды на пропаганду. Расходы бюджета на госСМИ подскочили втрое на фоне войны, https://www.moscowtimes.ru/2022/04/12/milliardi-na-propagandu-rashodi-byudzheta-na-gossmi-podskochili-vtroe-na-fone-voini-a19511 (accessed on 27 February 2023)

How Russian Propaganda Prepared the Population for a Full-Scale Invasion of Ukraine

The information policy of Russia acquired the character of a purposeful information war against Ukraine long before the full-scale invasion in February 2022. Prejudice, manipulation, distortion of facts, blatant undisguised lies, Putin-Kremlin propaganda as part of the Kremlin's policy as a whole have become the main tools of the Kremlin in this war.

In his more than 20 years in power, Vladimir Putin managed to almost completely resuscitate all the tools of Soviet propaganda. The media dictatorship has become a proven way for Putin to 'raise a society convenient for his government. And this made it possible to legitimise this brutal war.

On the eve of Russia's invasion, disinformation messages were generally intended to demoralise Ukrainians, sow division between Ukraine and its allies, and strengthen Russia's public perception of Ukraine as a threat and an enemy.

The first narrative that Russia began to actively intensify in 2014, when it launched a hybrid war against Ukraine, presented Ukraine as a failed state. Its main function was to deny the existence of the Ukrainian people as separate from the Russians and discredit the Ukrainian statehood.

The second narrative of the Russian propaganda claimed that the Ukrainian government was 'neo-Nazi, illegitimate, and discredited'. However, references to the 'denazification' of Ukraine in the Russian media have appeared at least since 2015–2016. It was around 'Nazism' that Russia decided to build its anti-Ukrainian rhetoric. This narrative was aimed at creating an image of Ukraine as evil in order to make it easier to mobilise the Russian population against the 'enemy'. Finally, one of the goals in this war, which Russia voiced in February 2022, is the so-called 'denazification'.

The third narrative promoted by Russia on the eve of the full-scale invasion of Ukraine was about the so-called 'external governance' and 'the West exploiting Ukraine and being destructive to the world order'. In particular, it was aimed at creating distrust in Western countries in Ukrainian society and presenting the West, led by the United States, as an exploiter of Ukraine in its geopolitical interests and a threat to the world order.

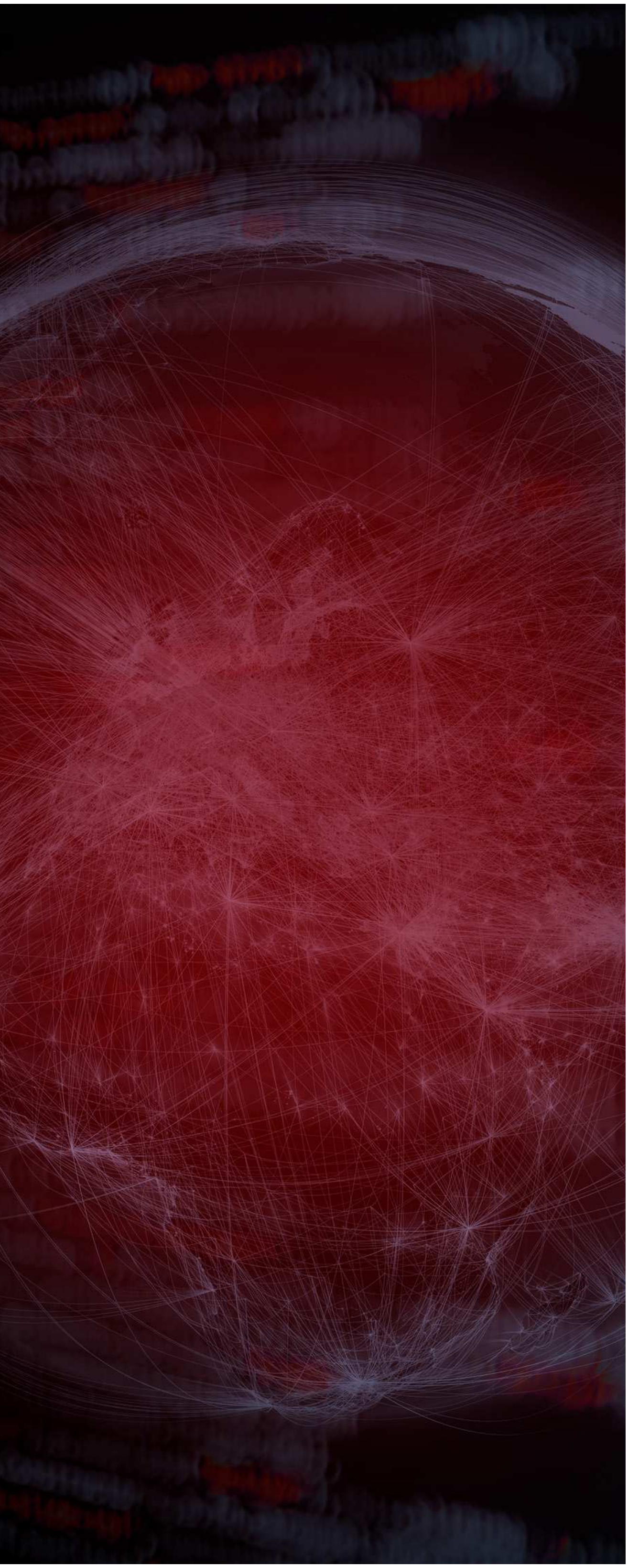
The fourth narrative presented the Russian minority as the object of oppression in Ukraine. This narrative, in particular, was aimed at forming beliefs about the illegal and violent ousting of everything Russian in Ukraine: language, church, history and culture, the Russian minority, pro-Russian media, and politicians.

Finally, **the fifth narrative** of Russian propaganda was that there was an external threat to Russia. It was aimed at intimidating NATO and the United States and Ukraine by war, presenting them as aggressors in the society that plan to return the territories of Ukraine occupied by Russia by military means.

Russian disinformation has accompanied the military actions and crimes of the Russian army on the territory of Ukraine since the start of the war. Now, it is controlled by the Kremlin in at least three ways:

Roskomnadzor. The Federal Service for Supervision of Communications, Information Technology and Mass Media which blocks any attempts of alternative naratives, not in line with the Kremlin's propaganda.

Law 'on Fakes'. On March 3, 2022, the State Duma Committee on State Building and Legislation approved an amendment introducing liability and a fine of up to 5 million or imprisonment for up to 15 years for 'publicly disseminating deliberately false information about the use of the Armed Forces of the Russian Federation'. Thus, the law has become a tool in the hands of the Kremlin for full control of the media space of Russia, since it is the Kremlin who defines what is 'true' and what is 'fake'.



The Prosecutor General's Office of Russia. The entity with the right to shut down information outlets without legal proceedings for disseminating information that discredits the Russian army. And this means that Russian state media works as an information support for the conduct of the war.

The aggressiveness of Russian propaganda increased simultaneously with the increase in defeats of the Russian army. If at first no one, except the head of the Chechen Republic, Ramzan Kadyrov, directly said they were ready to seize Kyiv and Kharkiv, after the retreat of the Russian troops from Kyiv , the leading propagandist of the Kremlin, Olga Skabeyeva, announced the Kremlin's intention to seize the whole of Ukraine.

> **The media dictatorship has become a proven way for Putin to 'raise a society convenient for his government. And this made it possible to legitimise this brutal war.**

Hate Speech and Genocidal Rhetoric in Russian Propaganda

The use of hate speech as a way to dehumanize the enemy and the use of 'disguise words' to distort reality have become key methods of Russian propagandists during the war. During the military aggression against Ukraine, Russian propaganda created an entire Orwellian 'newspeak' that helps justify the criminal actions of Russia. Thus, the all-out war has become a local 'special military operation', which is conducted allegedly for objective reasons, such as 'denazification'. The invasion, accompanied by all the atrocities of the war, is called 'liberation', 'salvation', or 'cleansing from Nazis, fascists, Satanists, Banderites, punishers', etc.

The Russian propaganda channels have shown to increase aggressive rhetoric, extremism, direct calls for war and blurring of borders in the Russian information space between those who are supposed to be enemies and all Ukrainians. If earlier the Russian propaganda called the Ukrainian military and government officials "Nazis," now, this message is used to demonise the entire population of Ukraine.

In April 2022, at the Russian state-run news agency Ria Novosti, a pro-Kremlin journalist, Timofey Sergeytsev, called for the destruction of Ukraine's national identity and a campaign of brutal reprisals against its people.[2] He called for imprisonment, forced labour, and the death of those who refused to abide by the Kremlin's rule in Ukraine. In the programme of the famous propagandist, Vladimir Solovyov, one of the guests said: 'Ukraine cannot be fixed. You cannot repair this structure. It needs to be destroyed because it is anti-Russian; it is an entity that threatens Russia.'

On October 20, 2022, the Kremlin's propagandist Anton Krasovsky called for the drowning of Ukrainian children and burning them in their own houses in the 'Antonyms' programme on the Russian state multilingual TV channel RT. The 'Krasovsky's case' is actually a pattern, not an isolated incidence.

The use of hate speech and disrespectful attitude towards Ukrainians through offensive language is also part of the rhetoric of Russian propaganda. In an article published on the website of the official news agency RIA Novosti, Victoria Nikiforova called Ukrainians 'mentally unhealthy people', and Dmitry Medvedev in his Telegram channel called them 'cockroaches'.

Concealment of War Crimes

In addition to creating a distorted reality, Russian propaganda also performs other tasks of the state, in particular, the concealment of war crimes committed by the Russian army on the territory of Ukraine. After the course of the war began to change, and the invading army suffered defeats, Russia intensified shelling of civilian infrastructure throughout Ukraine. To conceal these crimes or to shift responsibility for them to the Ukrainian side, the Kremlin's disinformation apparatus tried to deny, reject, and distract the world from the crimes committed by the Kremlin.

When Russia attacked a maternity hospital in Mariupol, pro-Kremlin media called the victims 'Nazis'. When Russian missiles struck a railway station in Kramatorsk filled with civilians, propagandists falsely accused Ukraine of killing innocent people fleeing the horrors of war. When Russian pilots fired missiles at a shopping mall in Kremenchuk, Russia denied the attack, claiming it was only striking military targets. And the attack on several civilian targets in Vinnytsia was justified by pro-Kremlin disinformers with the fact that they allegedly hid the Nazis. After the Ukrainian army de-occupied towns and villages in the Kyiv region, photos of the bodies of executed civilians scattered in the streets of Bucha quickly spread throughout the world. The Kremlin immediately tried to occupy the information space with contradictory 'explanations' of the events in Bucha—this was allegedly a Ukrainian provocation, atrocities were staged, and the West was to blame for everything. Pro-Kremlin adepts tried to mount a disinformation campaign to cover up Russia's war crimes. It is currently difficult to assess the impact of the Kremlin propaganda directed against Ukrainians because Russia's full-scale war against Ukraine continues. But even now, we can trace the obvious relationship between the consumption of content of Russian propaganda resources and the degree of support for the war against Ukraine. First of all, this is evidenced by the absolute majority of Russian society, which supports the war of Russia in Ukraine. According to the Levada-Center, as of October 2022, 73% of Russians supported the actions of the Russian military in Ukraine.

[2] Сергейцев Т. Что Россия должна сделать с Украиной, https://ria.ru/20220403/ukraina-1781469605.html (accessed on 27 February 2023)

The Kremlin immediately tried to occupy the information space with contradictory 'explanations' of the events in Bucha—this was allegedly a Ukrainian provocation, atrocities were staged, and the West was to blame for everything.

How Propaganda Becomes a Crime

Hate speech, genocidal rhetoric against Ukraine and Ukrainians are commonplace in the Russian information space. TV shows with statements similar to those of Krasovsky or Timofey Sergeytsev are not an exception, but part of the system. The term 'genocidal rhetoric' means public incitement to such actions. Prosecutors of the International Tribunal for Rwanda accuse the founder of Radio of the Thousand Hills, Rwandan oligarch Félicien Kabuga, of using such rhetoric, creating 'the most powerful weapon for committing genocide'.[3] The number of victims during the 1994 genocide in Rwanda amounted to about 800,000 people. Researchers from the Institute of Mass[4] (Ukraine) analysed the indictment against Félicien Kabuga dated March 1, 2021 and identified the following signs of genocidal rhetoric:

1. Direct calls for the destruction or commission of genocidal acts, for example, attacks on civilian infrastructure, the abduction of Ukrainian children, and the destruction of Ukrainians.

2. The use of euphemisms, softening words or statements to conceal what is really happening to minimise the scale of the tragedy and the essence of war crimes.

3. Euphemisms that dehumanise the victim group. Rwandan radio called the Tutsis 'cockroaches that need to be destroyed'; Russian propagandists call Ukrainians 'Nazis', 'rats', 'worms from which you need to clear the territory'.

4. The sacralisation of war, the speculative use of religious narratives and theological concepts. Justification of crimes with supposedly good intentions.

5. Ignoring genocidal appeals in the speeches of officials in a situation where media employees should have paid attention to them is considered as indulgence and incitement to their continuation.

6. Favourable (or neutral) coverage in the media of already committed acts with signs of the crime of genocide.

7. The Court also considered the popularity of the media on which genocidal rhetoric was voiced.

Analysing Russian propaganda, particularly after the full-scale Russian invasion of Ukraine in February 2022, we see that hate speech, the dehumanisation of Ukrainians, calls for the destruction of Ukraine and the state, Ukrainian identity, as well as genocidal appeals have become a rule rather than an exception.

First of all, the complete subordination of Russian media to the Kremlin indicates that there is no free media in Russia and everyone is responsible as an accomplice in the Kremlin's crimes given the lack of journalistic standards, conscious creation of facts and the production of fakes instead of news.

Hate speech in journalistic materials and on television only confirms that Russian propaganda and the Russian state media work as information support for the war against Ukraine and should be punished for it.

[3] Félicien Kabuga: Rwanda genocide suspect goes on trial at The Hague// https://www.bbc.com/news/world-africa-63068598

[4] How state propaganda is driving Russia`s genocide of Ukraine // https://imi.org.ua/en/monitorings/how-state-propaganda-is-driving-russia-s-genocide-of-ukraine-i49066

The example of the Russian federal media and those who work for them gives a distilled example of the support for the war in the 21st century. International communities and organisations need to undertake a comprehensive study and prosecution of this phenomenon because aggressive regimes are likely to adopt it. ■

About the author:

Mariia Sahaidak is Head of the Strategic Communication Department and Analytical Department at the Centre for Strategic Communication and Information Security under the Ministry of Culture and Information Policy of Ukraine.
Mariia is an expert on Russian propaganda, Russian hybrid threats and countering disinformation. She obtained her master's degree in History at the Ukrainian Catholic University in 2015 and completed a second master's degree in International Relations in Munich in 2020. Her master's research paper concerned "Hybrid Warfare. Compliance with International Law in Resolving Conflicts in the Post-Soviet Space."

ARTICLE

The Impact of Digitalization for Cybersecurity in the Humanitarian Sector

CHARLOTTE LINDSEY

CHIEF PUBLIC POLICY OFFICER, SENIOR HUMANITARIAN ADVISOR,
CYBERPEACE INSTITUTE

ABSTRACT:

The humanitarian sector is undergoing incredible transformation through the use of technologies to enhance the reach and impact of humanitarian responses to populations in need. Concurrently, the security and threat landscape is rapidly changing with a rise in the sophistication and impact of cyberattacks in times of peace and war. This has increased the requirement to address the challenges arising from these evolutions, and to learn important lessons in particular to improve capacities of organisations and to inform and influence ongoing normative negotiations which guide responsible behaviour in cyberspace and advance accountability. The role of civil society organisations, such as the CyberPeace Institute*, can contribute knowledge, expertise and policy guidance in light of these global challenges to peace and security in cyberspace.

Keywords: assistance, beneficiaries, data protection, digital transformation, humanitarian organisations, peace, privacy, protection, resilience

* The CyberPeace Institute is an independent and neutral non-governmental organisation, headquartered in Switzerland, whose mission is to reduce the harms from cyberattacks on people's lives worldwide, provide assistance to vulnerable communities, and call for responsible cyber behaviour and accountability. The Institute analyses cyberattacks, exposes their societal impact and how international laws and norms are being violated, and advances responsible behaviour to enforce cyberpeace.

Introduction

'When you're pulling people from rubble after missile strikes, or tending to injuries in a tent, or worrying about getting the next truck with medical and food supplies past military checkpoints in a war zone, the latest transformations from technology and digitalization might seem distant – but not for long.'[1]

In the 6 years since this statement was published, accelerated by a global pandemic and the increasingly *connected beneficiary*[2] for humanitarian action, digital transformation is now part of the strategy of many humanitarian organisations reshaping the delivery of assistance and protection, providing more agile and efficient ways of meeting beneficiaries' needs. Against this backdrop is also the use of cyber means as a feature of today's armed conflicts changing and expanding the threat landscape.

Technologies are enablers for change in the humanitarian sector in facilitating digital proximity to stakeholders, informing and engaging with beneficiaries (information as aid), connecting people to services including scaling up programs such as the use of online programs for survivors of violence, to distribute cash as aid, to connect large data sets to aggregate and disaggregate needs of different populations, to name but a few examples. The same technologies can also be exploited by threat actors for malicious purposes and weaponised to identify groups for persecution, to hack and leak data, to collect and analyse data on individuals such as human rights defenders, to surveil people including tracking their communications. Social media platforms and messaging services are leveraged to control the information space, spread misinformation and disinformation and influence policies and/or undermine trust amongst populations. This includes disinformation about humanitarian organisations to undermine their credibility and the trust that they depend upon to reach, assist and protect persons in need, as well as to ensure their 'license to operate' from stakeholders and to receive donations to carry out their work.

Cynically alongside the incredible transformations the use of technologies is facilitating to enhance the reach and impact of humanitarian responses to populations in need, the security and threat landscape is rapidly changing and creating new challenges to the delivery of these critical activities. Recognising that cyber hygiene and security has not been a high priority in many humanitarian organisations, threat actors now view humanitarian actors as valuable targets for cyberattacks. The digitalization and connectivity of organisations and beneficiaries have increased their attack surface and their associated risk profile. There is a requirement to address the challenges arising from these evolutions, and to learn important lessons in particular to improve capacities of organisations and to inform and influence ongoing normative negotiations. This is not a theoretical exercise but an essential requirement to ensure the protection and rights of people.

Cyber Threat Landscape for Humanitarian Organisations

Humanitarian organisations provide critical services to those most in need of assistance and protection, especially people living in areas of conflict or natural disasters. These organisations – international organisations and non-governmental organisations (NGO) – are also the targets of cyberattacks, and in many cases have limited capacity to respond. They are attacked because of the work they do, as well as to steal funds, exfiltrate data, including highly sensitive data on people that they are processing, and to or disrupt their ability to operate. Many NGOs may not have the resources, expertise, or time to properly secure their ICT infrastructure and digital assets or to develop a robust incident response system that could deal with a range

[1] The digital transformation of the humanitarian sector, Anja Kaspersen and Charlotte Lindsey, International Committee of the Red Cross (ICRC), ICRC Law and Policy Blog, December 2016.

[2] This refers to beneficiaries or potential beneficiaries who have access to mobile and online to leverage digital channels to seek information, support and engagement.

of cyberattacks. Consequently, essential programs and activities are impacted, which puts the already vulnerable people they serve at even greater risk.

Recent cyberattacks have affected both large international organisations such as the International Committee of the Red Cross (ICRC)[3] and UN agencies[4] as well NGOs such as Roots of Peace.[5]

Many NGOs may not have the resources, expertise, or time to properly secure their ICT infrastructure and digital assets or to develop a robust incident response system that could deal with a range of cyberattacks. Consequently, essential programs and activities are impacted, which puts the already vulnerable people they serve at even greater risk.

There are many ways the civilian population have been harmed by cyberattacks.

1. **Destructive attacks** often lead to the deletion of data or damage to systems rendering them unrecoverable, such as through wiper malware targeting Ukrainian entities and organisations, e.g. a wiper attack on a border control station on 25 February 2022 was reported to have slowed the process of enabling refugees to cross into Romania.

2. **Disruptive attacks** leading to the interruption of services and operations, e.g. D-DoS attacks have been targeting the public and financial sectors with civilians impacted in their ability to access online payments and applications as a result.

3. **Data weaponisation** leading to the theft or exfiltration of data or the acquisition of data for espionage, surveillance or intelligence purposes. This includes hack and leak attacks through the theft and leak of data for political or ideological purposes. This sows distrust, demonstrates an inability to secure sensitive data, and potentially places individuals at risk.

4. **Disinformation or propaganda attacks** leading to the spread and circulation of false information and political propaganda attempts to influence the information space and limit access to timely, reliable and official information for the population.

The cybersecurity of humanitarian organisations is crucial for the people who depend on them. To better understand the potential threat landscape for humanitarian organisations it is important to look at several key focus areas which must be understood and addressed, as follows:

- Digitalization of an organisation's response capacities exposes the organisation and potentially its beneficiaries, staff and other stakeholders to the risk of cyberattacks to disrupt or disable the operations in a particular

[3] The targeted cyberattack against the ICRC led to compromise of personal data and confidential information on more than 515,000 vulnerable people, including those separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention. Because of the attack, the ICRC had to shut down the systems underpinning their Restoring Family Links work, affecting the Red Cross and Red Crescent Movement's ability to locate missing people and reunite separated family members. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know#:~:text=Update%3A%2024%20June%202022.,in%20a%20sophisticated%20cyber%20attack.

[4] https://www.cpomagazine.com/cyber-security/united-nations-data-breach-hackers-obtained-employee-login-from-dark-web-are-executing-ongoing-attacks-on-un-agencies/
The breach affected dozens of servers in three separate locations: the UN Office at Vienna; the UN Office at Geneva; and the UN Office of the High Commissioner for Human Rights (OHCHR) headquarters in Geneva. These servers hold a range of data, including personal information about staff. https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack

[5] Roots of Peace, an NGO working to remove landmines from agricultural land in Afghanistan to allow people to replant crops, experienced a financial loss of USD 1.34 million as threat actors tricked the employees to transfer money. CyberPeace Institute, "Hackers Trick Humanitarian Non-profit into Big Wire Transfers," July 14, 2020, available from: https://cyberpeaceinstitute.org/news/2020-07-14-hackers-trick-humanitarian-non-profit-into-big-wire-transfers/

context, program of activities,[6] or globally;

- The inability to safeguard this data, and/or the misuse of data collected for purely humanitarian purposes puts individuals at risk as well as the humanitarian organisation itself, for example when an NGO is required to hand over data which is then used in counter terrorism operations;

- Misinformation, disinformation, cyber influence operations, use of deep fakes, against the humanitarian organisation to undermine its credibility and trust amongst the population and with authorities, which can impede the ability to operate and increase physical security risks for staff and volunteers;

- Surveillance of a humanitarian organisation and/or its staff members, through the hacking of telecommunications devices, and or the leveraging of metadata generated by digital assets, which lead to the targeting of individuals and or compromise the reputation and operational capacity of an organisation to function;

- The potential of cyberattacks and operations to increase humanitarian needs for people, which could be the case if infrastructure essential for the survival of the population is targeted disrupting the provision of power supplies, health care, clean water, etc.[7];

- Cyberattacks to disrupt an organisation's ability to collect donations or to fraudulently divert funds out of or from reaching the organisation through fake websites, social engineering schemes, disruption of the organisation's website and donation portals;

- Applicable legal and normative frameworks which apply to the use of cyber and which afford protection for civilians, civilian infrastructure, ICT systems and data, which must be advanced by organisations to try to increase the protection of people from the malicious use of cyber. For example, international humanitarian law restricts the use of cyber during armed conflicts as a means and method of warfare, and governs the conduct of hostilities.

Humanitarian organisations, of all sizes, generally lack cybersecurity capabilities to both understand their individual threat landscape and to put in place the relevant cyber skills, capacity building and capabilities to appropriately detect threats to their systems, to respond in the case of a cyber-incident and secure their digital operations, network and infrastructure. The adage that it is not if but when a cyberattack will happen is just as applicable to the humanitarian sector organisations as it is to other sectors. Organisations will be evaluated by their stakeholders not on the fact they were attacked which is increasingly happening to organisations in all sectors but on how prepared the organisation was for such an eventuality, how long it took them to identify the attack and the processes in place to mitigate the impact of the attack, recover operations and assets, and to inform persons whose data may have been violated or exfiltrated, and donors if financial resources were stolen, and the cost of the recovery operation necessary.

Information on cyberattacks affecting the humanitarian sector are being reported in the public domain. The level of transparency of organisations about such attacks depends on several factors such as its mandate, modus operandi, the scale and scope of the attack, potential criminal

[6] For example, the family links activities of the ICRC were targeted disrupting the abilities to carry out activities to reunite persons separated by war and disasters. There has been no indication from the ICRC that other activities were targeted by cyberattack, or attempts to disable the whole organisation. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know#:~:text=Update%3A%2024%20June%202022.,in%20a%20sophisticated%20cyber%20attack

[7] The ongoing international armed conflict between the Russian Federation and Ukraine has witnessed a prolific use of cyber, and the CyberPeace Institute has been monitoring and aggregating data in a publicly available platform with regard to cyberattacks and operations against critical infrastructure. Four types of cyberattacks have been documented —Destructive, Disruptive, Disinformation and Data Weaponisation—including incidents of attacks against humanitarian organisations. See Cyber Attacks in Times of Conflict Platform

investigations underway, physical security risks for individuals, reporting obligations such as in relation to data protection. Organisations feel very uncomfortable with communicating about cyberattacks, however, supporting organisations who do so, building means and methods to report to help others in the sector whilst ensuring the necessary safeguards are in place are essential to helping other organisations understand the threats, risks and vulnerabilities that may have been exploited.

A Collective Approach to Cybersecurity in the Humanitarian Sector

To improve the capacity and capabilities of humanitarian organisations will require a collective effort across the sector and involving a range of state and non-governmental stakeholders, including actors who can support the overall cyber resilience of NGOs, provide resources to help them better detect and respond to threats, and assist them to understand the overall threat landscape. This will enable different perspectives, lessons learned and good practices, and resources to be shared across the sector and to leverage the essential expertise and skills of a range of practitioners. This could be inspired by the approach and resources developed for the healthcare sector elaborated in the Compendium of Multistakeholder Perspectives on Protecting the Healthcare Sector from Cyber Harm.[8]

The CyberPeace Institute has also developed and is implementing key cybersecurity support to humanitarian NGOs to help them build cybersecurity capacities to respond to the threats of malicious cyber use. Through its CyberPeace Builders program,[9] over 100 humanitarian NGOs across the world are currently assisted with free and tailored cybersecurity assistance to enable and empower each organisation's adoption of cyber preparedness and resilience measures. The number of NGOs assisted with end-to-end cybersecurity services through a network of experts and volunteers is increasing every week, with an ambition to be assisting 1,000 NGOs by 2025. Recognising the growing and diverse needs of the sector, and building on the activities of the CyberPeace Builders program, the Institute launched the Humanitarian Cybersecurity Center[10] (HCC) on 27 February 2023.

> **Through its CyberPeace Builders program, over 100 humanitarian NGOs across the world are currently assisted with free and tailored cybersecurity assistance to enable and empower each organisation's adoption of cyber preparedness and resilience measures.**

Through partnerships, networks and volunteers, the HCC provides tools, expert support and practical free cyber assistance to NGOs, tailored to their needs wherever they are located in the world. From detection and analysis of cyberattacks, to the sharing of actionable threat intelligence, to hands-on technical support and the fostering of collaboration, standards and advocacy efforts for the protection of the sector, there is a real opportunity to make progress. The Institute will also launch a report in 2023 based on a collection and analysis of data on cyberattacks against a sample of NGOs that are part of international Geneva. An improvement of information and analysis about cyberattacks will contribute to a great understanding and recognition of the challenges, informing policy-makers with the ambition to put an end to such

[8] Workshops, key recommendations, lessons learned, and good practices were collected from a diverse group of experts, practitioners, and stakeholders to support efforts to safeguard the healthcare sector from cyberattacks. This was developed into a Compendium of Multistakeholder Perspectives on Protecting the Healthcare Sector from Cyber Harm that offers healthcare institutions, governments, international organisations, and other stakeholders a useful resource to support their efforts to safeguard the healthcare sector from cyber threats. https://cyberpeaceinstitute.org/wp-content/uploads/Compendium-of-Multistakeholder-Perspectives.pdf

[9] https://cyberpeaceinstitute.org/cyberpeace-builders/

[10] https://cyberpeaceinstitute.org/humanitarian-cybersecurity-center/

attacks and ensuring a greater protection of humanitarian organisations.

The CyberPeace Institute has also called for greater protection from attacks against the humanitarian sector in diplomatic and multilateral fora, such as the United Nations Open-ended Working Group.[11] States have already identified the need to address the existing gaps in capacity and/or knowledge connected to critical infrastructure sectors, including specific concerns about the threats of cyberattacks targeting humanitarian organisations.[12] The Institute has made the following policy recommendations:

- **Clarification on the applicability of international law.** States need to act in line with their obligations under international law and agreed-upon norms to protect the humanitarian sector from malicious activities in cyberspace. States need to clarify the applicability of international law in the use of ICTs toward sustained protection of humanitarian action, including how international law applies.

- **Protection of the humanitarian sector.** States should respect and ensure respect for existing laws and norms, and advocate for strengthened protection for humanitarian organisations to enable them to fulfil their missions and mandates. Attacks on NGOs in wartime and peacetime should be off limits, including both kinetic and cyberattacks against staff and volunteers, resources, systems, services, programs, property, and data.

- **Protection of data under domestic legal frameworks.** States should maximise the protection under domestic legal frameworks and introduce safeguards that effectively protect humanitarian organisations and their operations within their territory. The specific nature of humanitarian action should inform the design of data protection frameworks and the legislative approach to safeguarding humanitarian interests.

- **Study of existing and potential threats.** States should study existing and potential threats to build knowledge about the cyber threat landscape and cyber threats to the humanitarian sector. Toward this goal, States need to increase transparent reporting on the cyberattacks against NGOs, including the impact of these incidents on the organisations and the beneficiaries of their services and programs, within the constraints that ensure protection of personal identifiable information, the mandates and modus operandi of the organisations. This will require cooperation and clear communication between the organisations, donors, and government entities to ensure transparent and accurate reporting, which should be limited to data necessary to understand the cybersecurity and operational implications of the attack. Reporting must ensure that it does not subject individuals to further harm or is used as a tool to disclose information on beneficiaries. Reporting can make the humanitarian sector safer, increase its resilience, prevent further re-victimization, and provide a body of knowledge for decision-makers about trends in cyberattacks such as the vector of the attack and its impact, tools used, and the malicious actors.

- **Capacity building.** States need to build capacity at the national and local levels to create policies and initiatives to support the humanitarian sector and to reduce the proliferation of cyberattacks against NGOs. States should engage in broad participation when building the capacity of NGOs. Actors from the humanitarian, development, academic, corporate, and private sectors should be encouraged to participate in a multi-stakeholder

[11] CyberPeace Institute, Submission on the Protection of the Humanitarian Sector to the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025, 13.07.22 https://cyberpeaceinstitute.org/news/submission-on-the-protection-of-the-humanitarian-sector-2/

[12] United Nations, Kingdom of the Netherlands, "National intervention under agenda item 5: Discussions on substantive issues," available from: https://documents.unoda.org/wp-content/uploads/2022/04/220329-Netherlands-Existing-and-Potential-Threats.pdf

process to break the remaining silos and support transparency, sharing of best practices, and increased mutual understanding.

- **Secure digital infrastructure.** Efforts should be increased to build the capacity of organisations to:
    - strengthen their protection against cyber incidents,
    - enable the establishment of secure channels of communications for humanitarian actors with staff/offices and with beneficiaries,
    - increase protection for the confidentiality of data gathered, managed, processed, and stored,
    - securely leverage technology for the provision of digital services,
    - understand the cybersecurity threat landscape,
    - procure cybersecurity capabilities commensurate with the level of threat, and widely deploy encryption,
    - ensure understanding of jurisdictional issues, financing, viability, and sustainability of cybersecurity.

Addressing threats to NGOs emanating from cyberspace will require a joint commitment of all relevant stakeholders: leveraging their diverse contributions, experience, and expertise. Humanitarian organisations make a vital contribution to humanity, assisting and protecting people around the globe. Cyberattacks against such organisations demonstrate a clear disregard for lives and suffering, and the vital mission of these humanitarian organisations. Such attacks must stop. Ultimately, the peace and security of cyberspace is a collective goal that requires collective action. ■

About the author:

Charlotte Lindsey is responsible for Public Policy and is the Senior Humanitarian Advisor at the CyberPeace Institute. Charlotte is an experienced senior executive in digitalization of organizations, tech policy and diplomacy, multilateral engagement, data and digital risk, as well as in security and crisis management, and communication. Charlotte has spent 30 years in the humanitarian sector, including as Director of Communication and Information Management and Director of Digital Transformation and Data at the International Committee of the Red Cross (ICRC) as well as a number of other positions in the Headquarters and in contexts of armed conflicts. She is the author of Women facing War: a study of the impact on armed conflict on women. Charlotte holds an MSc in Communication Management and a BA in Business Studies, and has studied both Digital Disruption and Digital Transformation. She is an Executive Fellow, Digital Strategies Roundtable, SDA Bocconi. Charlotte was voted one of the 100 Digital Shapers in Switzerland in 2019.

ARTICLE

The Eye of Providence: Surveillance. Ukrainian Battlefield. Human Rights.

TETIANA AVDIEIEVA

LEGAL COUNSEL AT THE DIGITAL SECURITY LAB UKRAINE;
MEMBER OF THE INDEPENDENT MEDIA COUNCIL;
EXPERT OF THE EXPERT COMMITTEE ON ARTIFICIAL INTELLIGENCE,
MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE

ABSTRACT:

This article provides an overview of the surveillance technologies applied by Ukraine as a response to Russian aggression. It focuses on creating a human-rights-centered environment aimed at protecting civilians' personal data while considering the interests of national security and territorial integrity. It also addresses the most notable cases of applying AI-driven surveillance tools dealing with biometric data, such as the infamous Clearview AI and less criticized FindClone applications.

Keywords: wartime surveillance, Clearview AI, facial recognition, AI surveillance, human rights

Introduction

Modern wars are won not by the number of missiles shot but by the amount of data available for predicting future attacks, detecting enemy soldiers, and neutralizing potential military operations. Starting from the 2014 occupation of Crimea by Russia, Ukraine employed various surveillance tools to collect intelligence data, identify the occupying powers and plan the counter-operations. In 2021, right before the Russian illegal full-scale invasion, Ukrainian authorities resorted to satellite surveillance to track Russian military vehicles in the occupied Donbas region.[1] However, things changed after 24 February 2022, with the level of threat reaching the never expected heights. In this respect, new technological means to address illegal aggression were sought by the state, including ones in the area of surveillance. Meanwhile, the previously used tech tools were adjusted to wartime reality.

Apparently, the full-scale military intervention caused a need to defend the sovereign borders, triggering additional limitations upon the rights of Ukrainian citizens and foreigners within its territories. The regimes of martial law and derogations from certain obligations under international treaties, imposed in February 2022,[2] extended the State's discretion in choosing the means for responding to armed aggression. In the privacy realm, they included the limitations on constitutional rights but lacked clarity on the scope and form of such restrictions.

Even despite the imposed restrictions, the margin of appreciation cannot become unlimited concerning human rights, which should remain at the center of the discourse around any limitations. Accordingly, the main question is whether surveillance tools applied by Ukraine reflect the minimum standards in the area of human rights and provide the necessary safeguards against abuse from both the State's and private actors' sides, as required by the international conventions and the practice of international judicial bodies. Namely, according to *Big Brother Watch and Others v. the UK*, any surveillance measures shall be duly reasoned and authorised by a competent authority, subjected to an independent oversight and notified to an individual concerned.[3] Akin to that, there are requirements towards a limited period for storage of collected personal data, its destruction after the expiration of such period, and limited access by the third-parties throughout of storing the personal data for some legitimate purposes.[4] For example, as follows from *Peck v the UK*, it is illegal to distribute biometrics obtained via street surveillance for law enforcement purposes to media entities, since it violates the right to privacy.[5]

Modern wars are won not by the number of missiles shot but by the amount of data available for predicting future attacks, detecting enemy soldiers, and neutralizing potential military operations.

Importantly, the remarkable military technologies shall be likewise compatible with the applicable standards as the peace-time measures employed for security reasons. So, what are the types of surveillance applied by Ukraine in the context of the armed conflict?

[1] Карбунар, Н. (9 October 2021). Україна запустить супутник, який дозволить стежити за Донбасом та Чорним морем. Главком. https://glavcom.ua/country/incidents/ukrajina-zapustit-suputnik-yakiy-dozvolit-stezhiti-za-donbasom-ta-chornim-morem-789806.html

[2] Decree of the President of Ukraine on Introduction of the Martial Law №64/2022 (24 February 2022); Ukraine: Notification under Article 4(3) of the ICCPR (28 February 2022) UN Doc C.N.65.2022. Treaties-IV.4

[3] *Big Brother Watch and Others v the UK* Apps no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021), paras 320-350

[4] UNCHR 'Report of the Special Rapporteur on the right to privacy' (2018) UN Doc A/HRC/37/62, paras 55, 125-126

[5] *Peck v the UK* App no 44647/98 (ECtHR, 28 January 2003), paras 57-63, 87

See you Soon: Dimensions of Surveillance

Surveillance in Ukraine is only partially covered by privacy and criminal procedure laws, whereas a general legislative framework addressing the powers of competent authorities, independent oversight, and remedial safeguards is lacking. For example, peacetime surveillance is mainly left at the discretion of the municipal councils,[6] which both lack powers to regulate such issues and generally provide imprecise and unforeseeable regulations. The Law on Protection of Personal Data is outdated, addressing only general standards on the collection and storage of biometrics,[7] while the reform in this area has been recently blocked by the Ukrainian parliament.[8] The procedural laws, though, grant wide discretion to law enforcement in accessing information-communication systems following the court authorization. Notably, the limitations under martial law also need more clarity on the conditions for using surveillance and identification measures.

1. Street surveillance. Ordinary street surveillance, i.e., street video cameras recording or transmitting video in real time, is also used to identify and track Russian saboteurs. Since some street surveillance cameras are equipped with a facial recognition function, they are also used to prevent sabotage and identify the perpetrators of war crimes after the de-occupation of certain territories. For instance, it has been reported that thousands of dead occupants have been identified via street surveillance.[9]

Another example can be found in the Sumy region, where the population of the border zone decided to install border surveillance to monitor the location of the adversaries and plan defence operations.[10] According to the available media descriptions, the cameras are connected to a unified system, having analytical capacities and predictive functions. Although used primarily for military purposes, deployed cameras are similar in their design to the Hikvision surveillance installed in the biggest Ukrainian cities, while the access is granted to the same actors, i.e., military units, local administration, government structures, border guards, and security services. However, media have also reported instances of misidentification, which proves the imperfect precision of the facial recognition incorporated into street surveillance.[11] This, in turn, means that apprehension of the perpetrators and subsequent court proceedings over them cannot be based on the data obtained from such systems.

Since some street surveillance cameras are equipped with a facial recognition function, they are also used to prevent sabotage and identify the perpetrators of war crimes after the de-occupation of certain territories.

Moreover, the newly adopted legislative changes to the Code of Criminal Procedure of Ukraine ensured the access of law enforcement to the information-communication systems (among which the street surveillance is categorized) without the court order during the martial law period.[12] This tendency is dangerous from the perspective

[6] Avdieieva, T. (30 June, 2021). Cameras With Facial Recognition on City Streets. Is It Legal? *CEDEM*. https://cedem.org.ua/en/analytics/cameras-facial-recognition/b

[7] Law of Ukraine on Protection of Personal Data (2010), Articles 6-7

[8] Draft Law №5628 on Protection of Personal Data (2021), Articles 17

[9] Italiano, L. and Orecchio-Egresitz, H. (21 March 2022). Ukraine and Russia have both weaponized facial recognition — in very different ways. *Insider*. https://www.businessinsider.com/ukraine-russia-have-both-weaponized-facial-recognition-2022-3

[10] Solonyna, Y. (16 June 2022). В Україні створили програму для миттєвої перевірки осіб. Розробники просять пришвидшити розгляд застосунку в Play Store. *ComeBackAlive*. https://savelife.in.ua/en/materials/texts-en/the-shield-effect-what-video-surverveill-en/

[11] Андрєєва, В. (28 May 2022). Ймовірно, штучний інтелект помилився: розслідувачі встановили іншу особу мародера з Ірпеня. Українська правда. https://life.pravda.com.ua/society/2022/05/28/248849/

[12] Draft Law №7147 on Amendments to the Laws of Ukraine 'On the National Police' and 'On the Disciplinary Statute of the National Police of Ukraine' in order to optimize the activities of the police, including during martial law (2022), Part 1(7)

of the potential transition of martial law norms into peaceful periods, leaving law enforcement authorities with excessive discretion regarding access to sensitive data and its use for investigation purposes. While no specific regulation on surveillance is present, personal data protection laws, civil legislation, and regulations on law enforcement still need detailed provisions for the mass collection of biometrics. Therefore, no procedural safeguards against abuses have been provided either for peaceful times or martial law periods.

Even with the relatively successful application of street surveillance as a defensive tool and a source of intelligence, another possible risk is that occupying powers might capture the employed technologies and the data the systems retain. As a result, they can identify and track local journalists, human rights defenders, activists, and anti-occupation protesters. They can also download the databases containing the biometrics of civilians to use for further persecution and oppression. In this regard, particular care shall be given to the application of surveillance technologies in the border areas which remain under the threat of occupation. At the same time, servers storing sensitive data shall be moved to more secure regions.

2. Mobile surveillance. A few changes happened in the area of mobile surveillance after the full-scale invasion. Luckily, Ukrainian authorities abstained from using overly intrusive means, such as Pegasus, a spyware highly criticized by human rights defenders worldwide. Allegedly, the purchase of this technology for military purposes was blocked by Israel[13] but regardless of the reasons, mobile communications remain relatively safe from the mass spyware technology from the Ukrainian side, which cannot be said regarding Russian mobile operators.[14]

Meanwhile, the domestic 'State in Smartphone' mobile application 'Action' (ukr. '*Diia*') is still widely used by the population, providing access to most of the state registers and the individual's personal documents therein. Setting aside the technical security of the system, which is debatable inside the Ukrainian society, there are concerns regarding the potential capture of the technology by the Russian side or data leakage from this most extensive database containing all biometric data of the Ukrainian citizens. Right before the full-scale invasion, this application was hacked, but no leaks of personal data happened[15] while no attacks have been reported since the Russian full-scale aggression started almost a year ago.

... there are concerns regarding the potential capture of the technology by the Russian side or data leakage from this most extensive database containing all biometric data of the Ukrainian citizens.

Apart from that, at the end of 2022, there was an extensive debate regarding the use of AirTags – a tool that, by design, assists in detecting missed objects (keys, mobile phones, headphones, etc.). Yet, some individuals decided to apply it for surveillance purposes, tracking persons via putting AirTags in their bags or pockets.[16] This, in turn, might create severe risks if a person tracked is a public official or a serviceperson. Fortunately, a design has been changed with an AirTag having a voice alarm between 8 and 24 hours after its activation.[17]

3. Military surveillance. The Ukrainian Armed Forces use numerous military intelligence tools, which *de facto* amounts to mass surveillance given their all-encompassing nature from the data

[13] Kirchgaessner, S. (23 March 2022). Israel blocked Ukraine from buying Pegasus spyware, fearing Russia's anger. *The Guardian.* https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia

[14] Burgess , M. (21 September, 2022). Shadowy Russian Cell Phone Companies Are Cropping Up in Ukraine. *Wired.* https://www.wired.co.uk/article/ukraine-war-mobile-networks-russia

[15] Маслюкова, І. (14 January 2022). Атака на сайти МОН, МЗС, вимкнена «Дія»: ситуацію пояснюють чиновник, експерт і військовий. *Радіо Свобода.* https://www.radiosvoboda.org/a/ukrayina-kiberataka-sayty-uryadu/31654840.html

[16] Що таке AirTag, та як уберегтися від стеження. *ГоловнеInUA*. (22 December 2022). https://glavnoe.in.ua/news/science/shho-take-airtag-ta-yak-uberehtysya-vid-stezhennya

[17] *Ibid*

collection perspective. To exemplify, Palantir provides Ukraine with the capacity for large-scale data exchange, uniting various sources, from commercial satellites to secret data from foreign intelligence offices.[18] Different types of data overlap, creating a comprehensive picture of what is going on within the battlefield, especially in the regions under occupation and the so-called grey zones. It enables the planning of military operations without endangering people in the field and the timely evacuation of civilians.

There are also some local databases maintained primarily by the border guards. For instance, in the Volyn region, a server centre collecting data from the borders with Belarus and Poland is established,[19] enabling the monitoring of the mentioned regions on the presence of threats to national security. Notably, such surveillance precludes unexpected operations from Belarus, providing Ukraine with sufficient time to reorganize its military and border forces.

Another widely used tool is a system called Delta, applied for real-time surveillance over the battlefield and prediction of the further steps the invaders might undertake.[20] In particular, this system enables total control over the information on military vehicles, units, and any facility used by the enemy armed forces. However, since the armed activities are taking place on the Ukrainian territory, the data about civilians can be likewise incorporated into the system as a side effect of the collateral collection of intelligence data. No doubt is expressed regarding the necessity and proportionality of the application of such systems during wartime. It is essential, however, to remove all civilian data after the end of the conflict to ensure their privacy.

Meanwhile, the Russian forces are also conducting (or rather trying to conduct) indistinctive satellite surveillance over the Ukrainian territory.[21] Contrary to military surveillance from the Ukrainian side, the occupying powers neither provide the minimum safeguards for the collected personal data nor generally develop an adequate human rights protection framework on the domestic level. Thus, the unlawful processing of the personal data of Ukrainian civilians, which can be easily retained after the war ends, cannot be challenged without an effective remedy for the population of the territories subjected to such surveillance techniques.

It is essential, however, to remove all civilian data after the end of the conflict to ensure their privacy.

4. AI-driven surveillance. One of the most significant controversies in the area of AI tools employed for surveillance was the infamous Clearview AI. The company gained a highly negative reputation by collecting personal data from social media without the users' consent. Following the full-scale invasion, it offered its services to the Ukrainian authorities. Specifically, according to the Clearview AI founder, six different state agencies currently have access to the system with a low possibility of their accounts being hacked.[22] No algorithm, however, was provided for the cases when individuals with access to the database are captured

[18] Ignatius, D., (19 December 2022). How the algorithm tipped the balance in Ukraine. The Washington Post. https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/

[19] Дем'янчук, О., (24 December 2022). Україна відкрила сучасний центр стеження на кордоні з Білоруссю. Кореспондент. https://ua.korrespondent.net/ukraine/4547213-ukraina-vidkryla-suchasnyi-tsentr-stezhennia-na-kordoni-z-bilorussui

[20] Добровольський, В., (27 October 2022). Україна показала НАТО унікальну систему керування боєм та стеження за противником. Speka. https://speka.media/ukrayina-pokazala-nato-unikalnu-sistemu-stezennya-za-protivnikov-9g1zd9

[21] Коновал, В., (26 May 2022), "Роскосмос" хоче запустити супутники для стеження за війною в Україні. *PravdaTutNews*. https://pravdatutnews.com/tehnologiyi/2022/05/26/16588-roskosmos-hoche-zapustyty-suputnyky-dlya-stezhennya-za-viynoyu-v

[22] Temple-Raston, D. and Powers, S. (17 May 2022). At war with facial recognition: Clearview AI in Ukraine. *The Record*. https://therecord.media/at-war-with-facial-recognition-clearview-ai-in-ukraine/

by Russians. Thus, there is a threat of using this technology against Ukrainian civilians, activists, and other vulnerable groups.

At first, the software was supposed to be used to identify dead soldiers – an area where few privacy concerns can be raised. However, according to the Clearview AI website, facial recognition is also used for providing refugee assistance, debunking of false information on social media, checking identity at checkpoints, as well as the detention of Russian infiltrators.[23] In only four months of its use, a specially designed military personnel checked more than 60,000 individuals, identifying 7,500 suspects and leading to charges against 127 Russian militaries.[24] Yet, the crucial issue, indeed, is the retention of the personal data of those persons who are not among the suspects. Although some ideas have been expressed regarding the destruction of such data after the end of the martial law, this legal regime may last for ages constantly endangering people's privacy.

International organisations, such as Privacy International, actively condemned the use of Clearview AI during armed conflicts.[25] OpenDemocracy expressed their fears regarding the potential loading of the search results into the automated weapons for further targeted killings, which may result in mistaking civilians for soldiers.[26] Apart from lethal capacities, Clearview AI can be applied to identify individuals at checkpoints, which also creates certain human rights dangers, especially when it is followed by subsequent apprehension. Lastly, human rights defenders are worried about the good use of evil technologies[27] which can be later employed to justify illegal means for obtaining personal data. In numerous jurisdictions, Clearview AI has already been brought to justice for violation of privacy laws,[28] making its application in Ukraine even more disputable.

Other options, although less infamous as Clearview AI, still resort to the same technology of opensource search for similar images and are also applied to identify illegal invaders. One of such tools was the FindClone application, used by the investigative media Bellingcat to recognise faces on recorded videos.[29] Notably, both Clearview AI and FindClone enable the identification of individuals whose pictures are not even published on their own social media profiles, but who are merely tagged by their friends.[30] Respectively, any presence of military persons on the Internet is enough to subject them to facial recognition. Yet, since FindClone is a free tool, it is important to ensure that the aggressor state does not use it to track Ukrainian citizens.

At the same time, some technologies have been subjected to cyberattacks, such as the servers of Ukrainian border control stations that have

[23] Avdieieva, T. (2022) Facial Recognition Technologies and Their Influence on Human Rights: International and Comparative Law Aspects. http://ekmair.ukma.edu.ua/bitstream/handle/123456789/23548/Avdieieva_ Mahisterska_robota.pdf?sequence=1&isAllowed=y, p.90

[24] War in Ukraine, *Clearview AI*. https://www.clearview.ai/ukraine

[25] The Clearview/Ukraine partnership - How surveillance companies exploit war. *Privacy International*. (18 March 2022). https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war

[26] Meacham, D. and Gak, M. (30 March 2022). Does facial recognition tech in Ukraine's war bring killer robots nearer? *Open Democracy*. https://www.opendemocracy.net/en/technology-and-democracy/facial-recognition-ukraine-clearview-military-ai/

[27] O'Leary, L. (26 April 2022). How Facial Recognition Tech Made Its Way to the Battlefield in Ukraine. *Slate*. https://slate.com/technology/2022/04/facial-recognition-ukraine-clearview-ai.html

[28] Harwell, D. (15 April 2022). Ukraine is scanning faces of dead Russians, then contacting the mothers. *The Washington Post*. https://www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/

[29] Roth, A. (21 November 2019). Man who filmed beheading of Syrian identified as Russian mercenary. *The Guardian*. https://www.theguardian.com/world/2019/nov/21/man-filmed-killing-torture-syrian-identified-russian-mercenary-wagner

[30] Clayton, J. (13 April 2019). How facial recognition is identifying the dead in Ukraine. *BBC*. https://www.bbc.com/news/technology-61055319

been processing large amounts of personal data.[31] Since the attacks were directed not at stealing data, but at disabling the systems, no significant damage has been caused. Yet, the period for obtaining refugee assistance became longer and much more complicated.

> **The crucial issue, indeed, is the retention of the personal data of those persons who are not among the suspects. Although some ideas have been expressed regarding the destruction of such data after the end of the martial law, this legal regime may last for ages constantly endangering people's privacy.**

In response to the criticism towards the facial recognition applications, Ukrainian developers of YouControl and Artellence united with the Security Service of Ukraine to create the 'Who Are You' (ukr. TyKhto) application[32] which can identify the numbers of personal IDs and names to find the matches with the databases of dangerous individuals, such as 'Myrotvorets'. In practice, however, these tools have shown low performance, with numerous misidentifications taking place despite well-defined data types and absence of facial or emotional recognition. This, in turn, served as an additional argument for supporters of Clearview AI and related services. Nevertheless, one shall bear in mind that effectiveness does not always mean security, let alone compliance with basic human rights standards. Accordingly, the proportionality of applying any surveillance tools shall be regularly assessed, especially where the environment is rapidly changing.

After the Epilogue: What Can Be Changed?

Although much more effective than human monitoring, modern surveillance tools create many risks when applied in armed conflicts. If during peacetime the gravest consequence of misidentification implies a wrongful apprehension of an individual, wartime risks include mislabelling somebody as a combatant, which might lead to civilian causalities. Moreover, the cessation of hostilities, end of the armed conflict, and transition to a peaceful period will require additional reviews of the applied policies and filtering out the overly intrusive ones to prevent their application after the war is over. Therefore, the most crucial issues to be addressed by Ukrainian state authorities include the following:

- Considering the nearly one-year anniversary of the full-scale invasion and the nine-year-long aggression in Crimea and Eastern Ukraine, the state shall develop a comprehensive legal framework addressing the issues of surveillance in times of war to make domestic legislation foreseeable. The discretion of the state shall be defined in the relevant laws to avoid excessive intrusions into privacy and other rights;

- Abstain from resorting to surveillance tools designed exclusively or mainly for armed conflict periods during peacetime. Notably, it is essential to ensure that, subsequently, data collected to ensure security in wartime is not used illegally when the martial law limitations are lifted;

- Be careful and conscious of applying surveillance technologies which are disputable from the human rights perspective. In cases where the risks of human rights abuses cannot be mitigated, the use of surveillance tools shall be limited to a possible minimum. Also, it is crucial not to legitimise dangerous or overly intrusive technologies by referring to their effectiveness in a military context. The proportionality of the means employed to an end sought shall always be maintained;

[31] Alspach, K. (27 February 2022). Ukraine border control hit with wiper cyberattack, slowing refugee crossing. *VentureBeat.* https://venturebeat.com/security/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/

[32] Harbuzova, A. (9 April 2022). В Україні створили програму для миттєвої перевірки осіб. Розробники просять пришвидшити розгляд застосунку в Play Store. *DOU.* https://dou.ua/forums/topic/37637/?from=fb-repost&utm_source=facebook&utm_medium=social&fbclid=IwAR2fFbnavDxRD46xIkfYQg0OsvMnKYkfUp25YBe8N-t0bU6CCHY1atsM9Gk

- Grant persons a possibility to effectively appeal the application of surveillance tools, both on the general level and in individual cases. Abstain from using AI-driven tools in cases where a human being cannot review the decision of the autonomous system. For example, the use of AI for the development and deployment of autonomous weapon systems shall be outlawed;

- Abstain from making decisions based purely on the results provided by AI-driven tools where such results might have serious human rights implications. Mainly, identification to apprehend or prosecute individuals cannot rely exclusively on facial recognition technologies or other forms of automated programs;

- Develop a comprehensive system of technical safeguards and effective crisis protocols for data destruction and transfer. Additional guarantees shall necessarily be provided for the territories in the border regions of the state and those which border with the occupied territories or remain under risk of occupation.

About the author:

Tetiana Avdieieva is a Legal Counsel at the Digital Security Lab Ukraine, a Member of the Independent Media Council, and an Expert of the Expert Committee on Artificial Intelligence under the Ministry of Digital Transformation of Ukraine. She has cooperated with various international intergovernmental and non-governmental organizations, including the European Commission, the Organization for Security and Cooperation in Europe, the Council of Europe, Article 19, Access Now etc. Tetiana is a graduate of the National University of Kyiv Mohyla Academy with a specialization in human rights. Her areas of professional interest include human rights, international public and international humanitarian law, legal regulation of innovative technologies and the Internet.

ARTICLE

The Nexus Between New Technologies, Migration Management and Human Rights

PAULINA GÓRSKA

PROJECT MANAGER, THE KOŚCIUSZKO INSTITUTE

ABSTRACT:

The use of new technologies in migration management has become increasingly prevalent in recent years. While these technologies hold great promise for improving the efficiency and effectiveness of migration management, they also raise important human rights concerns. This article explores the nexus between new technologies, migration management, and human rights. Drawing on a review of the literature, the article examines the various ways in which new technologies are being used in migration management, including biometric identification, artificial intelligence and blockchain. The article then discusses the human rights implications of these technologies, focusing on issues such as privacy, discrimination, and due process. Overall, the article highlights the need for careful consideration of the human rights implications of new technologies in migration management, and the importance of ensuring that these technologies are designed and implemented in a manner that upholds the rights of migrants and other affected individuals.

Keywords: digital technology, migration, human rights, AI, blockchain, biometrics

'Before you even cross a border, you will be interacting with various technologies. Unpiloted drones are surveilling the Mediterranean and Aegean corridors under the guise of border control. Biometrics like iris scanning are increasingly being rolled out in humanitarian settings – where refugees, on top of their already difficult living conditions, are required to get their eyes scanned in order to eat.' - says an anonymous refugee in the report 'Technological Testing Grounds. Migration Management Experiments and Reflections from the Ground Up', in which the authors describe refugees' early encounters with technology and how common it has become to use technology in migration control activities.

The development of new technologies has undeniably accelerated in recent decades, and the scope of their application is constantly expanding. Digital technologies are now used in almost every aspect of human life, and both the private and the public sector are finding new ways to use them. Asylum seekers and immigrants are no exception. State and non-state organisations are looking for innovative solutions to manage migration due to its increasing flows.

On the one hand, new technologies have the potential to make migration management more efficient and systematic. Biometric identification technologies such as fingerprint and facial recognition can be used to verify migrants' identities, making it more difficult for people to enter a country illegally or claim false identities. This can aid in improving security and managing the flow of people across borders.

On the other hand, new technologies can be used to restrict migration and violate migrants' human rights. Governments, for example, may use surveillance technologies to monitor and track people's movements, or they may use algorithms to identify and target people for deportation. The data collected by these technologies may also be mishandled, misused, or shared with third parties without the migrants' consent.

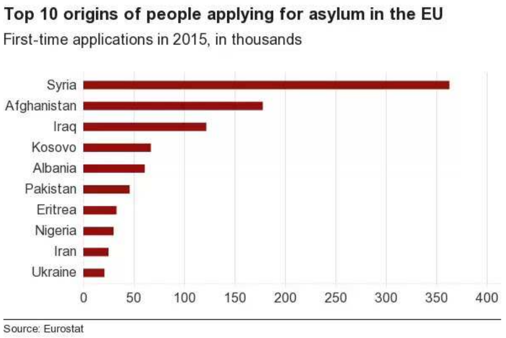


Figure 1. Top 10 origins of people applying for asylum in the EU. Eurostat.

The changes in migration management and the impact of this process on human rights are certainly visible in Europe, which has been experiencing a migration crisis – since 2015 more appropriately referred to as the refugee crisis. More than 911,000 refugees and migrants arrived at Europe's borders at the end of 2015, with more than 75% fleeing conflict and persecution, primarily in Afghanistan, Syria, and Iraq[1].

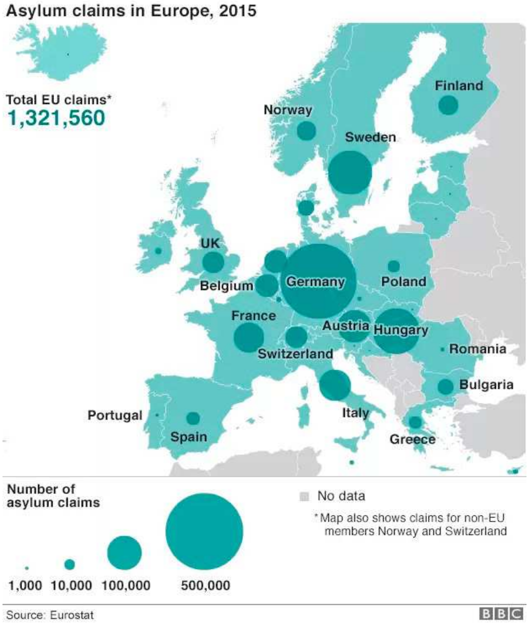
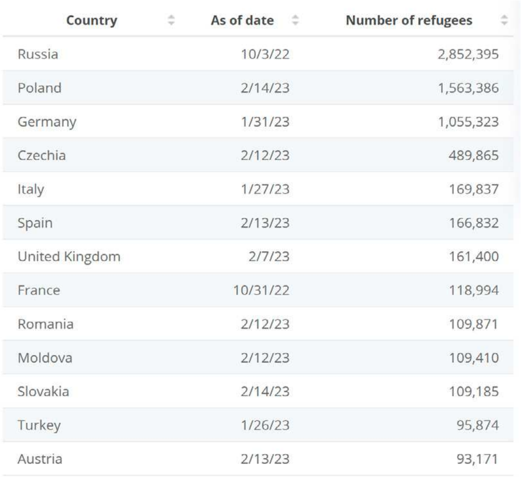


Figure 2. Asylum claims in Europe, 2015. Eurostat.

[1] https://www.unhcr.org/news/stories/2015/12/56ec1ebde/2015-year-europes-refugee-crisis.html

It was undoubtedly a watershed year for the then-28 European Union countries, Norway, and Switzerland, which recorded 1.3 million of asylum applications, nearly doubling the number of applications recorded in 1992, following the collapse of the Soviet Union[2].

Seven years after the aforementioned events, Europe (particularly Central Europe) was flooded by a wave of Ukrainian refugees fleeing their country to avoid Russian aggression. The majority of them are in Poland and Germany, and nearly 500,000 have made their way to the Czech Republic, but a significant number have also fled to Italy, Spain, and the United Kingdom.



Country	As of date	Number of refugees
Russia	10/3/22	2,852,395
Poland	2/14/23	1,563,386
Germany	1/31/23	1,055,323
Czechia	2/12/23	489,865
Italy	1/27/23	169,837
Spain	2/13/23	166,832
United Kingdom	2/7/23	161,400
France	10/31/22	118,994
Romania	2/12/23	109,871
Moldova	2/12/23	109,410
Slovakia	2/14/23	109,185
Turkey	1/26/23	95,874
Austria	2/13/23	93,171

Figure 3. Estimated number of refugees from Ukraine recorded in Europe and Asia since February 2022 as of March 2023. Statista.

As of January 2023, the UN reported nearly 8 million Ukrainian refugees in Europe with 4.9 million of them registered for temporary protection or similar national protection programs across Europe.

Given the instability of the situation beyond Poland's eastern border and in the Middle East, and in other regions from which refugees are arriving in Europe, managing the influx of refugees/migrants will remain a challenge for the European Union in particular.

New Technologies in Migration Management

The technological revolution has left its stamp on the migration management process. In addition to fundamental phenomena—like the expansion of total digital connectivity—new, more sophisticated technology applications have surfaced.

Karim the AI chatbot, designed by the Silicon Valley start-up X2AI, provides virtual psychotherapy to Syrians detained in Lebanese refugee camps. Carrying out personalised discussions in Arabic, Karim simultaneously analyses the interlocutor's emotional conditions while addressing pertinent queries, suggestions, and comments.

DoNotPay—an AI-powered robot lawyer—originally designed to help people wriggle out of petty fines and parking tickets, was expanded to assist asylum seekers across the United States, Canada and the United Kingdom. Offering free legal aid to refugees, the chatbot helps obtain financial assistance from governments by facilitating communication and filling out immigration forms.

But not only individuals can benefit from new migration management technologies. States utilize them primarily to oversee immigration procedures and employ techniques such as biometric identification to enable identification and tracking by way of iris scanning, facial recognition and fingerprints.

Using geographic information systems (GIS) enables mapping and identifying potential migration hotspots, while computer-assisted translation (CAT) tools help overcome linguistic challenges when registering and interviewing migrants.

Database management systems are another example of technological measures employed by governments. Designed for storing information and sharing

[2] https://www.pewresearch.org/global/2016/08/02/number-of-refugees-to-europe-surges-to-record-1-3-million-in-2015/

data among agencies involved in the migration process, they support tracking and management of individuals. Blockchain technology secures and shares migrants' data for the purpose of identification and tracking while artificial intelligence improves the efficiency and accuracy of immigration processes and helps identify anomalous patterns.

The latter also gives ample options for managing migration.

For instance, artificial intelligence-driven predictive modelling can be used to detect unusual migratory trends and forecast incoming migrant flows. This is supported by numerous and varied prediction technologies, such as improved high-resolution satellite imagery, geo-referenced data, cell phone data, or social media. Data science tools enable an in-depth analysis of new data to examine survey and asylum statistics, conflict indicators, environmental elements, economic or market data sets, or information sets directly related to migratory patterns. One of them is the Displacement Tracking Matrix (DTM), developed by the International Organization for Migration (IOM).

Switzerland and Sweden are testing a tool to predict asylum claims. The European Union Agency of Asylum is exploring potential models as part of an early warning and preparedness system while Germany is using data science and machine learning to conduct early monitoring of crises. Chatbots similar to the aforementioned Karim, or Free Robot Lawyers, can assist migrants in receiving the necessary information or support. In the migration management process, picture, video, and audio analysis is becoming more and more prevalent. It may be used to track and identify migrants as well as monitor migration routes and dismantle organised smuggling operations. A language and dialect identification assistance system, or DIAS, is an intriguing tool. The instrument can identify Arabic dialects and is designed to help German authorities determine the potential country of origin of an asylum applicant. Artificial intelligence is also employed to identify fraud, primarily to validate the documentation provided by applicants for citizenship or refuge. This is how the Netherlands, for example, detects document fraud. And it is not an isolated case but a widespread practice. Similar AI-based procedures have been used by Germany, the United States, Canada, and Australia to verify identity based on biometric data. Hungary has harnessed facial recognition to prevent fraud. Artificial intelligence is also widely used in the visa application process, particularly in the processing of asylum and visa requests and in decision-making, as well as in the identification of security threats, the detection of ominous travel patterns, and the reduction of irregular and illegal entry. Created by Stanford University and the ETH Zurich Immigration Policy Lab, the algorithm aims to place accepted asylum seekers and refugees in areas or cities where it is most likely that they find employment.

Artificial intelligence is also employed to identify fraud, primarily to validate the documentation provided by applicants for citizenship or refuge. This is how the Netherlands, for example, detects document fraud. And it is not an isolated case but a widespread practice.

What about the application of artificial intelligence in border control? It is currently being rigorously tested, and innovative projects are being carried out. One of them is the EU-funded 'iBorderCtrl' project, which is being piloted in Greece, Hungary, and Latvia, and involves the use of an avatar posing a series of filtered questions to travellers at a border crossing in the AI-powered module. By merging cutting-edge technology including biometric verification, automated fraud detection, document authentication, and risk, iBorderCtrl aims to standardize the procedure, expedite border crossings at the EU's external borders, and increase security.

The physiological or behavioural characteristics used to identify or verify identity are known as biometrics, and they play a significant part in the migration management process. The most popular methods of physiological feature verification are fingerprinting, facial recognition, and iris scanning. Identification and tracking of people are the two basic functions of biometrics. And it does not necessarily stop at a country's border and may extend to monitoring their movements within that country. Biometrics may be used to confirm person's identity to issue documents as well as for the fair distribution of assistance. Additionally, digital identities drawing on biometric data are being created, maintained on a blockchain-based platform, and then used to access services.

In order to validate people's identities, the World Food Program (WFP) or the United Nations High Commissioner for Refugees (UNHCR) register refugees and migrants with biometrics. This authentication is typically a requirement for decisions on access to food, healthcare, or other services.

For instance, the Building Blocks program, a WFP initiative, enables users to access monetary services or make grocery purchases by scanning their irises to the refugees' biometric database. Sharing biometric data is currently required to cross borders, and physical land borders, ports, and airports are the sites where governments can lawfully gather this information on non-citizens.

It is interesting to note that the original intent of the aforementioned blockchain technology was to facilitate the production and trade of Bitcoin and other cryptocurrencies during the financial crisis. Even though it has only been in use for 15 years, the technology is already being employed in immigration administration.

It is generally used to reduce superfluous tasks, such as redundant registration processes, and to better coordinate the operations of the institutions taking part in the process. The major goal of the blockchain technology is to safely store and distribute data on migrants, such as personal data (identification documents and biometrics), their migration status and history. Germany, Estonia, and Portugal are currently managing migration with the use of technology. Estonia offers a comprehensive ecosystem of online identity and government services. Germany has established a blockchain infrastructure named FLORA in order to administer national protection and as an additional linking mechanism to accelerate the exchange of information between the participating institutions. On the other hand, Lithuania is experimenting with the blockchain technology at its borders and as a tool to show verification history and to determine where and how frequently a document has already been certified.

Identification and tracking of people are the two basic functions of biometrics. And it does not necessarily stop at a country's border and may extend to monitoring their movements within that country.

Similar to the previously described technologies, the Internet of Things (IoT) is also used to track the movement of people both within and outside national borders. This may involve using GPS-enabled smartphones and other IoT gadgets like RFID tags and cameras. IoT has numerous uses in refugee camps as well where it monitors things like temperature, humidity, and occupancy levels. In addition to identifying possible issues, such as overcrowding which would necessitate additional resources, this can assist aid organisations in ensuring that the living arrangements in the camps are safe and comfortable.

Another phenomenon that turns futuristic scenarios into real life challenges is robot dogs which I had the opportunity to discuss with Dr. Petra Molnar, a lawyer, a fellow at Harvard's Berkman Klein Center and a researcher specializing in migration, technology, and human rights. As she stated, this is one of the most extreme examples because it is quite visceral.

'It makes us think of the Black Mirror series [British TV series – author's note], you will see those videos where the robots are huge they are running around, they have four legs and they are essentially a military-grade technology', adducing an example from New York and Honolulu, 'In Hawaii, the police were using them for all sorts of training and live action events, including monitoring unhoused people on the streets during COVID. I think at some point there were even concerns that these robo-dogs would be armed. This is an autonomous machine that makes some decisions on its own and it is concerning.

Now, also the U.S. Department of Homeland Security is exploring rolling it out in the Sonora corridor, which is the border between the U.S. and Mexico. 'Where a lot of people come and a lot already died' – adds Dr. Molnar.

'When my colleagues and I were there, it was probably one of the most surreal moments of my career to date. We were on the sand in the desert when the DHS announced that they are going to roll out the robot dogs. We were also seeing graves of people who died in the Sonora desert trying to cross into the U.S. and it really made me think "Is this the space that you are going to be rolling out this technology?" And they were making really terrible jokes, even the official press release from the DHS made light of it, saying things like the robot dog is going to lend a helping hand 'or a paw' to border enforcement.

The Impact on Human's Rights

New technologies and their impact on human rights are two inseparable topics that will always be linked. The profound intertwinement with digital technologies in migration management has prompted questions about rights to life and liberty, rights to equality and freedom from discrimination, privacy, and procedural justice.

Privacy violation is the biggest concern. After all, the use of surveillance tools and the gathering of private information, particularly the biometric data, can present privacy issues. Every person has the right to respect for their private lives and correspondence, and this right extends to digital correspondence, as per international human rights legislation. In addition, the availability of data and its transfer between various information systems raises concerns about the acquisition, storage, and processing of sensitive personal data. Anyone disclosing sensitive information runs the risk of seriously impairing refugee's right to privacy, frequently without their knowledge or consent.

Discrimination is another important process risk. For instance, it is possible for visa applications to be denied on the ground of the skin color. The initial triage AI algorithms may not accurately identify applicants with darker skin tones. When compared to the faces of white men, facial recognition technology is substantially less accurate when used to identify the faces of women with darker skin tones. In addition to this, it has already been established that current AI systems are more likely to incorrectly verify the faces of black persons and match them to those who have previously been detained by the police, leading to **erroneous arrests and deportations.**

Because it is imprecise and not always accurate, biometrics are vulnerable to interference. It is likely that when more and more data is gathered and collected over time, the relative reliability of fingerprint checks will decrease.

> **Anyone disclosing sensitive information runs the risk of seriously impairing refugee's right to privacy, frequently without their knowledge or consent.**

The inability to **access one's own information** is another major issue. New technology may effectively hamper access to personal information, human rights and the services accessible to those in need. Additionally, data is frequently used in ways that is not intended or approved of when it was gathered.

Displaced people are at danger of harm in a variety of contexts, not only during the asylum or citizenship application process. One illustration is the website Ukraine Take Shelter, which was created by a Seattle youngster to assist Ukrainian refugees in finding a safe home in neighbouring nations. The website has come under fire for failing to thoroughly check out prospective hosts and for breaking the EU's Data Protection Regulation (GDPR).

Can we determine which technologies are the most harmful given their wide range and widespread use?

According to Dr. Molnar, the answer is twofold.

'There is this sharp surveillance that is preventing people, even killing them, arguably because they are forced to take more dangerous routes. That is something that you see in the Sonora Desert a lot because with this rise of surveillance tech and this dragnet that encapsulates the border, people do not stop coming just like they do not stop coming across the Aegean or the Mediterranean, they just take more dangerous routes. But from a legal perspective, and an anti-discrimination perspective, what actually worries me, too, is the way that the algorithmic decision-making is kind of baked into the immigration and refugee systems because we know that data is not neutral, right? Data and technology are always a political project, often used by powerful actors on less powerful communities. And as we already know, the immigration system is very biased. Immigration law is also super discretionary. Anytime you cross a border, it kind of depends on whom you meet, how the officers feel, and what questions they will ask you.'

New technologies and the private sector go hand in hand, which is also not conducive to improving the state of human rights. As Dr. Molnar mentions, 'the private company that decides, yes, this is the solution to border enforcement. The norms in this kind of decision are made often behind closed doors without thinking about how it is manifesting on the ground, and what it is doing to people's human rights.'

'From a legal perspective, and an anti-discrimination perspective, what actually worries me, too, is the way that the algorithmic decision-making is kind of baked into the immigration and refugee systems because we know that data is not neutral, right?'

The Future

Today, it is widely known that new technologies will not stop developing; in fact, they will develop even faster, more money will be invested in them, and their presence in our lives will only grow.

States also do not intend to stop using the tools that are currently in use, but rather to improve them and seek new solutions. This also applies to migration management.

'Now there has been this big proliferation where, I think, countries are not scared anymore to show what they are doing,' adds Dr. Molnar. 'And different countries, are testing different technologies, depending on their localization and needs. For example in Greece, we can notice more frontline kind of technology, stuff tested out in the land border, the maritime borders, in refugee camps whereas, in Germany, which is in the middle of Europe, people are already in the process of moving, and so, different types of technologies are being used in the asylum process, as already mentioned voice printing technology used for purposes of refugee status determination,' Dr. Molnar reminds.

It is especially worth observing the development of technologies in migration management in the EU.

As Dr. Molnar says, 'There has been a great diversity of projects, except the robot dogs that are being used in the US (for now). In the EU, we see voice recording, different types of surveillance stuff in camps, predictive analytics, different kind of surveillance through the land, cameras, maritime surveillance, algorithmic decision-making, and lie detectors. So it does seem to be this kind of laboratory of experiments.'

Indeed, individual countries are more and more keen to increase their resources and capacity to use artificial technology. And this does not just apply to States that are struggling with waves of refugees.

As Dr. Molnar explains, 'I think there is also another element, and that is the conversations that are happening around the AI Act, the first regional attempt to try and govern something as amorphous as artificial intelligence, which is hard to do. How can the act go further to strengthen protections for people on the move? It does not go that far, to be honest. And one of the concerning uses that we want to target particularly is the use of predictive analytics for border enforcement and potential interdictions or pushbacks.'

Indeed, individual countries are more and more keen to increase their resources and capacity to use artificial technology. And this does not just apply to States that are struggling with waves of refugees.

Dr. Molnar continues saying that 'an act like that will set a global precedent on what can be governed and regulated by law when it comes to tech and development and deployment and sharing and all of that. And the concern is that when it comes to migration management, the current political climate in the EU is one that is characterised by extreme permissiveness when it comes to tech development. The thinking almost boils done to "let's develop it and ask questions later," especially because it is done on people on the move who are already a community that does not have a lot of rights, so let's just test it out there. Plus, the general kind of feelings around migration including the need to beef up border enforcement and strengthen detentions and removals and encampment and all of that. I mean, it all plays into this greater conversation around migration needing to be something that is managed and then managed through technology.

In conclusion, Dr. Molnar adds, 'I think that is where the geopolitics of it plays into, where some of my colleagues call it "AI arms race", where countries really want to position themselves, as the leaders in AI, in technology. It is all part of the global messaging of who fits where on the hierarchy. There is a lot of learning, sharing, and selling of technology across borders. Money, money, money. It always comes down to money, does it not?' ■

About the author:

Paulina Górska has been working for the Kosciuszko Institute since 2021. She graduated from the University of Warsaw with a degree in international relations, and did her specialization in security and strategic studies. She gained experience working in both the public and private sectors as well as at French universities, where she spent a year studying at Sciences Po in both Paris and Strasbourg. Her master's thesis is focused on digital technologies and their impact on state power in the international arena. Her professional interests also include the impact of digital technology on society.

References

Mohan M. (2017, 9 March). The 'robot lawyer' giving free legal advice to refugees. BBC. https://www.bbc.com/news/blogs-trending-39205935

Solon O. (2016, 22 March). Karim the AI delivers psychological support to Syrian refugees. The Guardian. https://www.theguardian.com/technology/2016/mar/22/karim-the-ai-delivers-psychological-support-to-syrian-refugees

Thomas R. (2005, 1 March). Biometrics, Migrants, and Human Rights. Migration Policy Institute. https://www.migrationpolicy.org/article/biometrics-migrants-and-human-rights

Molnar P. (2020). Technological Testing Grounds. Migration Management Experiments and Reflections from the Ground up.

European Migration Network (2022). The Use of Digitalisation and Artificial Intelligence in Migration Management. ENM-OECD Inform. European Commission.

Bither J., Ziebarth A. (2020). AI, digital identities, biometrics, blockchain: A primer on the use of technology in migration management. Migration Strategy Group on International Cooperation and Development.

Nedelcu M., Soysüren I. (2022). Precarious migrants, migration regimes and digital technologies: the empowerment-control nexus. Journal of Ethnic and Migration Studies.

Goel A., Sharma A., Gupta D., Khanna A. (2020). Immigration Control and Management System using Blockchain. International Conference on Innovative Computing And Communication (ICICC 2020)

Nalbandian L. (2022). An eye for an 'I:' a critical assessment of artificial intelligence tools in migration and asylum management. Comparative Migration Studies.

Kent J. (2018). The Role of Technology in Addressing the Global Migration Crisis. Conference Report — Berkeley, California.

McAuliffe M., Blower J., Beduschi A. (2021). Digitalization and Artificial Intelligence in Migration and Mobility: Transnational Implications of the COVID-19 Pandemic. MDPI.

Molnar P. (2019). Technology on the margins: AI and global migration management from a human rights perspective. Cambridge International Law Journal.

Tyler H. (2022). The Increasing Use of Artificial Intelligence in Border Zones Prompts Privacy Questions. Migration Policy Institute.

Kinchin N. (2022, 21 June).New technology is producing mixed outcomes for Ukrainian refugees. Blog LSE. https://blogs.lse.ac.uk/europpblog/2022/06/21/new-technology-is-producing-mixed-outcomes-for-ukrainian-refugees/

Access Now. (2022). Uses of AI in migration and border control:
A fundamental rights approach to the Artificial Intelligence Act. https://www.accessnow.org/cms/assets/uploads/2022/05/Uses-of-AI-in-migration-and-border-control.pdf

ARTICLE

Building Consumer Cyber-Resilience in the European Union

DOMINIKA SYROCIAK

ADVOCATE, CIPP/E, CYBER SCIENCE SILESIAN CENTRE FOR LEGAL ENGINEERING, TECHNOLOGY AND DIGITAL COMPETENCE

Consumer Protection in the European Union

New Consumer Agenda

Consumer rights are widely regulated in the European Union. The obligation to consumer protection is already laid down in the Treaty on the Functioning of the European Union, where Article 12 TFEU establishes a horizontal approach to consumer policy, whereby, for the achievement of the objectives of the internal market, it is necessary to take into account the interests of consumers in all relevant political and economic areas in order to ensure a high level of consumer protection in the European Union.[1] The European Commission is thus taking actions to protect competition and consumers by, among others, creating regulations that keep up with economic and technological changes.[2] The New Consumer Agenda sets out a consumer protection policy for 2020–2025

[1] Miąsik, D., Półtorak, N., Wróbel, A. (Eds.). (2012), Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I: (Art. 1-89) komentarz do art. 12 TFUE. Warszawa: Wolters Kluwer

[2] Podrecki, P., & Uchańska, J. (Eds.). (2018), Prawa konsumentów w Unii Europejskiej. Praktyczny poradnik dla przedsiębiorców. Warszawa: Polska Agencja Rozwoju Przedsiębiorczości

called 'Strengthening consumer resilience for sustainable recovery.'.[3] According to communication from the Commission to the European Parliament and the Council, the new consumer agenda encompasses, among others, digital transformation to create a safer digital space for consumers where not only are consumer rights protected, but a level playing field is ensured in order to provide newer and better services to all Europeans through innovation.[4] The aim of this policy is to ensure that consumers can fully benefit from the potential of digital transformation, while taking into account consumer interests at the same time.

Considering the EU's consumer protection policy framework, the question arises whether current legislation provides adequate consumer protection for the Internet of Things (IoT) devices commonly used in everyday life. In order to answer this question, it is necessary to formulate the definition of a consumer and to present the IoT definition under the current legal regulations.

...the new consumer agenda encompasses, among others, digital transformation to create a safer digital space for consumers where not only are consumer rights protected, but a level playing field is ensured in order to provide newer and better services to all Europeans through innovation.

Definition of a consumer

There is no uniform definition of a consumer in the generally applicable EU legislation.[5] So far, different definitions have been usually created for the needs of specific normative acts.[6] For the purposes of this article, it seems reasonable to adopt the definition of a consumer set out in Directive (EU) 2019/770 of 20 May 2019 where a consumer is defined as a natural person who, with regard to contracts covered by this Directive, is acting for purposes which are not related to that person's trade, business, craft, or profession. It should be stressed that the premise of Directive 2019/770 is to harmonise rules for the provision of digital content or services in order to guarantee equal rights to consumers across the EU. According to Article 4 of Directive 2019/770, Member States shall not maintain or introduce, in their national law, provisions diverging from those laid down in this Directive, including more or less stringent provisions to ensure a different level of consumer protection, unless otherwise provided for in this Directive.

Definition of the Internet of Things

For the purposes of this article, the Internet of Things will be understood as an infrastructure in which billions of sensors embedded in common, everyday devices – 'things' as such, or things linked to other objects or individuals – are designed to record, process, store, and transfer data. As they are associated with unique identifiers, they interact with other devices or systems using networking capabilities.[7]

[3] EC. (2020), Communication from the Commission to the European Parliament and the Council: New Consumer Agenda: Strengthening consumer resilience for sustainable recovery. COM(2020) 696 final. Retrieved: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0696&from=PL

[4] Ratcliff, C., Martinello, B., Kaiser, K. P. (2022), Consumer policy: Principles and instruments. In European Parliament, Fact Sheets on the European Union. Retrieved: https://www.europarl.europa.eu/factsheets/en/sheet/46/polityka-ochrony-konsumentow-zasady-i-instrumenty

[5] Szczepańska, K. (2011). Pojęcie konsumenta w "dyrektywach konsumenckich" Unii Europejskiej i orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej – wybrane aspekty prawne. Zeszyt Studencki Kół Naukowych Wydziału Prawa i Administracji UAM, nr 1, 161-178

[6] Łętowska, E. (2004). Europejskie prawo umów konsumenckich. Warszawa: C.H. Beck

[7] Article 29 Working Party. (2014), Opinion 8/2014 on the on Recent Developments on the Internet of Things. 14/EN WP 223. Retrieved: https://www.pdpjournals.com/docs/88440.pdf

Thereby, this definition refers to devices with sensors which, after being combined with other similar devices within more advanced devices (machines), observe with their sensors a certain fragment of the reality surrounding them.[8]

The Internet of Things – Development and Risks

Development

The European Parliament resolution of 10 June 2021 indicated that 22.3 billion devices worldwide are anticipated to be linked to the Internet of Things by 2024.[9] Additionally, it is estimated that the number of IoT devices in the EU Member States will increase to 7.43 billion and hence, on average, there will be 29 radio devices per household in 2030.[10]

Risks

Despite the growing number of IoT devices in use, many IoT products do not have adequate security features, which significantly increases the risk of cyber-attacks against consumers. IoT devices use default passwords, lack encryption and do not pay attention to the principles of security by design or security by default during the manufacturing process. The above practices of IoT device manufacturers lead to increased risks in the network, which as a result may violate the fundamental rights set out in other legislation, such as the right to privacy.[11] There is, for instance, a risk of a network attack through the use of BotNets which take over a user's device and create a botnet, a network of computers infected without the users' knowledge. It can be used by the attacker to transmit viruses and engage in other acts of cybercrime, such as Distributed Denial of Service (DDoS) attacks.[12]

Despite the growing number of IoT devices in use, many IoT products do not have adequate security features, which significantly increases the risk of cyber-attacks against consumers.

Actions Taken by the European Union

Commission Delegated Regulation (EU) 2022/30 of 29 October 2021

Due to the growing number of Internet-connected devices, machines or network sensors which make up the Internet of Things, and also due to the increasing scale of cybersecurity threats, on 29 October 2021, the European Commission adopted a delegated regulation[13] which aims to improve the cybersecurity of wireless devices available on the European market.[14] Taking legislative actions in this area was related to the European Parliament Resolution of 10 June 2021 setting out the EU Cyber Security

[8] Prabucki, R. (2020). „Inteligentne" rzeczy jako „świadkowie" w postępowaniu dowodowym. In L. Lai & M. Świerczyński (Eds.), Prawo sztucznej inteligencji. Warszawa: C.H. Beck

[9] EP., The EU's Cybersecurity Strategy for the Digital Decade: European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)). (2022/C 67/08). Retrieved: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021IP0286&from=PL

[10] EC. (2021), Commission staff working document impact assessment report: Accompanying the document: Commission Delegated Regulation supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive. SWD(2021) 302 final. Retrieved: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021SC0302

[11] Ibidem

[12] Ibidem

[13] EC. (2021), Commission delegated regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive. Retrieved: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0030

[14] EC. (2021), Commission strengthens cybersecurity of wireless devices and products. Retrieved: https://ec.europa.eu/growth/news/commission-strengthens-cybersecurity-wireless-devices-and-products-2021-10-29_en

Strategy for the Digital Decade, which concluded that action was needed to ensure that all products connected to the Internet in the EU, whether for consumer or industrial use, had adequate security features by design. These mechanisms should be resilient to cyber-attacks and allow for immediate updates when a vulnerability is discovered.[15] One of the reasons why the EU decided to introduce changes at the EU level was the need to harmonise national rules and avoid fragmentation of the internal market. The current EU regulations do not allow Member States to withdraw from the market IoT devices that either lack adequate security features or have been manufactured without considering the principle of security by design, which results in increased cybersecurity risks.[16]

The Delegated Regulation stipulates that the RED Directive will cover 'internet-connected radio devices', which will be regarded as any radio device that can by itself communicate via the Internet, whether directly or through any other device. Article 3(3) (d),(e) and (f) of the RED Directive refers to network protection, safeguards for the protection of personal data and privacy, respectively, and also aims to strengthen protection against fraud. Thus, by implementing the Delegated Regulation and including the interconnected radio equipment in the scope of the RED Directive, it will be possible to enforce the implementation of the security by design and the security by default principles and to ensure an appropriate level of network security or confidentiality of communications. Applying the principles of security by design and security by default will reduce the risks associated with cyber threats, as device manufacturers will be obliged to make their systems as resistant to attacks as possible by applying basic security measures such as continuous testing, authentication security and best programming practices. Thereby, as envisaged by the Delegated Regulation, safety aspects will become an integral part of product development and will be embedded into devices at the manufacturing stage prior to entering the EU market, and not dealt with after a security incident has occurred.[17] Therefore, once the Delegated Regulation enters into force on 1 August 2024, Internet-connected wireless devices will also be required to have built-in security systems to ensure the protection of the end user's personal data and privacy. Thus, the RED Directive will cover wireless devices which are capable of communication via the Internet (e.g. telephones, smartwatches, household appliances), as well as interactive toys or childcare equipment (e.g. baby monitors). These changes will increase the safety of wireless devices placed on the EU market.

Applying the principles of security by design and security by default will reduce the risks associated with cyber threats, as device manufacturers will be obliged to make their systems as resistant to attacks as possible by applying basic security measures such as continuous testing, authentication security and best programming practices.

Cyber Resilience Act

It should also be noted that, in addition to the amendments to the RED Directive, consumer protection against cyber threats is to be further enhanced with the planned Cyber Resilience Act. This act aims to introduce common and horizontal EU cybersecurity resilience standards. The Cyber Resilience Act will cover the security of products throughout their entire life cycle. To address this issue, the proposed regulation introduces the essential cybersecurity requirements in order to ensure that all products with digital elements, which are placed on the Union market, are designed and developed securely. The definition of the product with digital elements is defined as any software or hardware

[15] EP., The EU's Cybersecurity Strategy for the Digital Decade: European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)). (2022/C 67/08). Retrieved: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021IP0286&from=PL

[16] EC. (2021), Commission staff working document impact assessment report, op. cit.

[17] Ibidem

product and its remote data processing solutions, including software or hardware components, to be placed on the market separately. According to the proposal, manufacturers should comply with all essential requirements related to vulnerability handling and ensure that all their products are delivered without any known exploitable vulnerabilities.[18] In addition, the essential cybersecurity requirements should also contribute to enhancing the protection of personal data and the privacy of individuals. In particular, non-compliance with the essential cybersecurity requirements shall be subject to administrative fines of up to EUR 15 million or up to 2.5 percent of its total worldwide annual turnover, whichever is higher. As underlined by the European Commission, the regulation of the life cycle of a digital product is justified as the life cycle requirements are crucial for digital products because software needs to be updated regularly.[19] The European Commission also stressed in its recommendations that in view of the introduction of 5G networks, the protection of the networks and all participating devices should take place throughout the entire life cycle, starting from the design, to development, to purchase, to implementation, and to the operation and maintenance of 5G networks.[20]

Impact of the new regulations

It should be underlined that the changes introduced by the EU may contribute to creating trust in digital technology by ensuring basic security rules for networks, services and terminal equipment. Furthermore, due to the development of 5G network technology, the regulations in question will help to minimise the risks identified by the European Commission in the implementation of 5G networks, such as improper network configuration, lack of access control caused by inappropriate security measures or the use of IoT devices to carry out cyber-attacks in order to disrupt or destroy systems and data.[21]

As underlined by the European Commission, the regulation of the life cycle of a digital product is justified as the life cycle requirements are crucial for digital products because software needs to be updated regularly.

The Delegated Regulation is not intended to enter into force until 1 August 2024, since, as we read in recital 18, economic operators should be given sufficient time to adapt to the requirements of this regulation. Similarly to the GDPR, the premise of this delegated regulation, is to maintain technological neutrality. Therefore, specific technological solutions to the risks identified by manufacturers are not indicated in the provisions in order not to unnecessarily curb innovation.[22]

Best Practices and Guidelines

It should be noted, however, that manufacturers of radio devices can already start the process of implementing appropriate solutions that are compliant with the new Delegated Regulation by using already existing good practices. Helpful information on applicable security measures can already be found in the Code of Practice for Consumer IoT

[18] EC.(2022), Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Retrieved: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

[19] EC. (2022), Call for evidence for an impact assessment: Cyber Resilience Act. Ref. Ares(2022)1955751 - 17/03/2022

[20] EC. (2019), Commission recommendation (UE) 2019/534 of 26 March 2019 Cybersecurity of 5G networks. Retrieved: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019H0534&from=PL

[21] EC. (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Secure 5G deployment in the EU - Implementing the EU toolbox. COM(2020) 50 final. Retrieved: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0050&from=PL

[22] EC. (2021), Commission staff working document impact assessment report, op. cit.

Security,[23] which is a set of good practices for IoT device security. The Code has become the basis for the Product Security and Telecommunication Infrastructure Bill, which, among other things, will introduce regulations for IoT devices in order to increase the UK's resilience to cyber-attacks using these products as their probability of occurrence is greater because of the universality of IoT devices. In accordance with such legislation, consumer connectable products will be considered consumer products which can connect to the Internet or other networks and can transmit and receive digital data. The regulation will require transparency about the length of time for which the product receives important security updates and will also ban the use of default passwords. Non-compliance will entail fines of up to GBP 10 million and 4 percent of an organisation's global turnover. Thus, manufacturers, importers and distributors will be obliged to abide by the Bill, particularly with security requirements, or investigate and take action in relation to compliance failures.[24]

Information about appropriate security of IoT devices can also be found in the EDPB guidelines about processing personal data in the context of connected vehicles and mobility related applications. Since autonomous vehicles involve machine-to-machine communication, the solutions indicated in the EDPB guideline may also be helpful for designing IoT devices. The design should consider, for example, adopting measures such as encryption of communication channels by means of a state-of-the-art algorithm, implementation of an encryption-key management system that is unique to each device, not to each model, regular renewal of encryption keys, protection of encryptions keys from any disclosure, authentication of data-receiving devices, maintenance of data integrity (e.g., by hashing) or access to personal data subject to reliable user authentication techniques (password, electronic certificate, etc.).[25]

Consumer As the Fundamental Link of Regulations

Since the consumer is an individual who requires special protection in business transactions, it is necessary to develop appropriate regulations aimed at increasing consumer protection against cyber threats. Therefore, in order to build consumer cyber resilience, it seems reasonable not only to disseminate knowledge about cybersecurity, but also to introduce regulations which, through the use of security by design or security by default solutions, will allow the fundamental rights of the individual to be secured. Actions undertaken by the EU will contribute to improving the digital position of consumers and result in uniform regulation of IoT devices. As the consumer is the most vulnerable actor, building grassroots cyber resilience will allow us to unite in cyber power and thus minimise cyber risks that consumers face when using IoT devices.

> **In order to build consumer cyber resilience, it seems reasonable not only to disseminate knowledge about cybersecurity, but also to introduce regulations which, through the use of security by design or security by default solutions, will allow the fundamental rights of the individual to be secured.**

[23] UK Department for Digital, Culture, Media & Sport. (2018), Code of Practice for Consumer IoT Security. Retrieved: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

[24] Buckley, JP., Morrow, S. (2022), DCMS publishes Product Security and Telecommunications Infrastructure Bill. Retrieved: https://www.lexology.com/library/detail.aspx?g=73531fa9-7f1b-444c-820c-f95135ad6bfe

[25] EDPB. (2021), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 2.0. Retrieved: https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

About the author:

Dominika Syrociak is an advocate, CIPP/E, with an interest in data protection, information security and cybersecurity, CYBER SCIENCE Silesian Centre for Legal Engineering, Technology and Digital Competence.

References

Centre for Strategy & Evaluation Services LLP. (2020), Final Report. Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment. 716/PP/GRO/IMA/18/1133/10768 IMPLEMENTING FRAMEWORK CONTRACT 575/PP/2016/FC. Retrieved: https://ec.europa.eu/docsroom/documents/40763/attachments/2/translations/en/renditions/native.

Koman, K. (2021), Umowy o dostarczanie treści i usług cyfrowych a ochrona konsumentów na rynku wewnętrznym: dyrektywa 2019/770 i perspektywa jej implementacji do prawa polskiego. Warszawa: UOKiK.

CYBERSEC
YOUNG LEADERS

5TH EDITION OF CYBERSEC YOUNG LEADERS INITIATIVE

PARTNERSHIPS FOR CYBER RESILIENCE
CALL FOR PAPERS IS OPEN!

ABOUT CYBERSEC YOUNG LEADERS

Launched in 2018 by the Kosciuszko Institute, the CYBERSEC Young Leaders Initiative is dedicated to students and young professionals who are passionate about all things cyber.

From digital divide to data privacy, from disinformation to critical infrastructure security, from ethics of AI to supply chain risk management – the list of cyber challenges is growing. You can help solve them!

CYBERSEC Young Leaders Initiative aims to find promising cyber specialists and boost their careers through the Institute's flagship projects like CYBERSEC Forum and the European Cybersecurity Journal.

Take part in our CALL FOR PAPERS and join the CYBERSEC Community!

ANALYSIS

Security & Lowering Costs in the Cloud

ADAM PALMER

CHIEF INFORMATION SECURITY OFFICER (CISO), FIRST HAWAIIAN BANK; EXPERT OF THE KOŚCIUSZKO INSTITUTE

DAVE COLE

CEO AND CO-FOUNDER, OPEN RAVEN

Three Strategies to Support Strong Security & Reduce Costs in the Public Cloud

The evolution of many organizations from an on-premises IT environment, with a static security perimeter, to modern cloud environments, often results in tension between cloud teams and security groups. Cloud engineers are focused on speed. Their natural obstacle is the security team. The security team commonly introduces security controls or 'guardrails' that slow the pace of cloud engineering. These controls are designed to prevent the data leaks and breaches, the prevention of which, are a measurement of the security team's success. Both cloud developers and security teams also have a shared problem: managing costs.

The following 3 strategies help mature and build a secure cloud environment while also providing stronger control of an organization's budget. Supporting developer innovation, managing costs, and implementing successful security, creates good relations within the IT team and positions the CISO as a business enabler.

Shift From an "Asset" Visibility Strategy to a Focus on Cloud Resource & Data Management

The security maxim for vulnerability management has always been 'you can only protect what you can see'. In the on-premises environment, this meant having a firm grip on fixed assets like laptops, servers and endpoints. These assets also depreciated in value over time. In the cloud, having an inventory of data and other infrastructure is even more critical due to the fact that these assets are not fully controlled and they also have ongoing variable costs based on usage. The classic asset management strategy has now shifted to resource and data management in the cloud. Good visibility of cloud data helps determine the scope of security controls and may reduce the costs for cloud infrastructure.

One sometimes overlooked place to look to reduce costs and improve security is to look in the 'shadows'. Shadow data, unexpected or forgotten storage services, and the data they hold, are a potential source of data breaches. The volume of data in the cloud, the number of people handling it, and the dynamic nature of the cloud, make shadow data a potential problem. Maintaining an updated data inventory can make it easier to identify shadow data. Eliminating this 'shadow' data can help reduce overall data management costs and reduce risk.

Creating a solid inventory of resources in the cloud is not simple, but it can be straightforward and does not need to be expensive. Begin by identifying infrastructure resources using a cloud security posture management solution (CSPM). Free tools exist that will inventory compute and services with only a little extra work required for analysis and reporting. Data mapping is more challenging. Platforms such as AWS and Google offer a limited free capability tier and there are commercial tools also available that are optimized for this task.[1] If there is a small amount of data, start by using the free tier of your cloud platform's data inventory and classification service (AWS, Google, etc.) on externally facing services (e.g., public AWS S3 buckets). If there is more data than can be accommodated by the free tier of a cloud platform, then a commercial tool may be considered to help with cost reduction and improved performance.

One sometimes overlooked place to look to reduce costs and improve security is to look in the 'shadows'. Shadow data, unexpected or forgotten storage services, and the data they hold, are a potential source of data breaches.

Assure Visibility of Data Centres Across the Organization

In the on-premises IT world, occasionally there would be a mystery server or even an entire rack whose purpose had long since been forgotten. In the cloud, entire data centres can be hiding in plain sight and out of reach of both DevOps and security teams. How can this happen? Anyone with a credit card can setup a data centre within minutes in the cloud. These individual accounts may be set up by business units or development teams and be entirely unknown to the security team.

The solution to the problem of 'shadow accounts' is to move to an organization model that serves as a centralized place to manage all cloud accounts. Any new accounts are forced into the organization versus existing outside of the control of DevOps and security. This not only provides full visibility from a single location, but also streamlines actions such as applying security policies across all accounts. Using an organizational approach to the cloud, versus managing each cloud account separately, is one of the most fundamental actions that can be taken to manage both costs and security.

[1] The co-author is the CEO of a company offering a commercially available cloud data mapping tool. See openraven.com for information.

Consider All Costs When Evaluating Managed Services

One of the key advantages of the cloud is the ability to selectively outsource the management of services to improve security and reduce costs. Contrast this approach to the prior approach of wholesale IT outsourcing to various tech industry giants and you get a sense of just how fundamentally different cloud outsourcing decisions are. The decision to outsource a service versus doing it yourself (DIY) can sometimes be confusing to organizations transitioning to the cloud, however, there may be significant advantages for cost savings and risk reduction by outsourcing to managed services providers.

Managed services can offer security benefits, eliminating a myriad of security configuration options which are notoriously difficult to get right. From a cost perspective, using a cloud service provider (CSP) can free up expensive DevOps resources that are likely already overburdened. So, while the direct costs from the CSP may appear higher than self-management, the actual cost may be significantly less when security and DevOps resource costs are fully considered. No matter whether you choose to DIY or lean on a managed services approach, the decision should be made thoughtfully and consider the full scope of costs as well as the operational trade-offs and security risks.

> **The decision to outsource a service versus doing it yourself (DIY) can sometimes be confusing to organizations transitioning to the cloud, however, there may be significant advantages for cost savings and risk reduction by outsourcing to managed services providers.**

Final Insights

The shift from on-premises IT to cloud infrastructure does not need to cause anxiety. If approached correctly, this can be an opportunity to reduce costs while also supporting both the business and security goals. Focus on data visibility, organizational control of cloud data centres, and leverage the potential opportunity for cost savings with managed services. Successfully reducing cloud risk and controlling costs can help an organization's CISO to support a key area of business growth. ■

About the authors:

Adam Palmer is a former U.S. Navy Officer and now the CISO at First Hawaiian Bank. Adam previously worked as a cyber risk executive at a large EU bank. He also previously led the United Nations global program against cybercrime. Adam is a cybersecurity expert for the Kosciuszko Institute.

Dave Cole's fingerprints are visible across the cybersecurity industry from his 25+ years working as a leader in consulting (Deloitte, ISS), enterprise products (VP Foundstone, CPO CrowdStrike, CPO Tenable), and consumer products (VP Norton). Currently, he is CEO and Co-Founder of Open Raven, a post Series B company solving the modern challenge of securing data at cloud scale.

CYBERSEC
FORUM / EXPO

SAVE THE DATE

21-22 June 2023

International Congress
Centre in Katowice

www. cybersecforum.eu

European Cybersecurity Journal

Strategic perspectives
on cybersecurity management
and public policies

Readers' profile

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

Types of contribution:

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

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

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

Prices of contribution

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

CONTACT US: editor@cybersecforum.eu

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

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

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

We invite you to follow our initiatives and get involved.

The Kosciuszko Institute

is the publisher of

European Cybersecurity Journal