VOLUME 8 (2022) ISSUE 1

# European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies


ANALYSES • POLICY REVIEWS • OPINIONS

The Kosciuszko Institute

# European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

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





**ISSN:** 2450-21113

Citations: This journal should be cited as follows:
"European Cybersecurity Journal"
Volume 8 (2022) Issue 1, page reference

The Kosciuszko Institute

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

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

# Contents



# Editorial

**Ewelina Kasprzyk**

Chief Editor of the European Cybersecuirty Journal

Russia's brutal, unjustified and unlawful war waged on Ukraine continues causing a dramatic shift in the security landscape – for Ukraine and its closest neighbours, for the rest of Europe and transatlantic Allies, and even for the rest of the world. With that, we also observe economic and humanitarian crises, both of which affect the communities all over the globe in unprecedented ways. The result of the war in Ukraine will surely influence all of us – and it is high time to stand next to our neighbours and partners, together against the barbarous regime.

This publication is released on the 100th day of the invasion. We all hope that the suffering and violence that the Ukrainian people have been enduring from the hands of the aggressor will end soon enough and that our next conversations will discuss these tragic events as a thing of the past, one that we should draw lessons from. Lessons on cooperation, unity, compassion and humanity.

This June, I present you with this issue of the ECJ, which once again touches upon very timely challenges we are facing right now as a global community. During these trying times it is absolutely key to maintain a united front and join forces to provide Ukraine with strategic, economic, diplomatic, and humanitarian support. We also need to protect the digital world as a whole – and our existence both in and with it. Cyber is a team game, especially now.

Many thanks to our authors for contributing to this publication with their research, ideas and recommendations. I sincerely hope that all of you will be inspired by them and their work.

Have a great read!

Signed,

Ewelina Kasprzyk





**SAVE THE DATE**

**CYBERSEC FORUM / EXPO 2022**

# 13-14 JUNE 2023, ICC KATOWICE




Górnośląsko
–Zagłębiowska
Metropolia

# You cannot get bored in Metropolia!

ENJOY
A WONDERFUL
TIME HERE

from the resources of Tauron Nowa Muzyka Katowice Festival

Górnośląsko-Zagłębiowska Metropolia will surprise you with a multitude of attractions – from post-industrial monuments, cultural routes, concerts, exhibitions, performances, through parks, gardens and nature preserves.

You will find unique places here such as: the Silesian Park – one of the largest urban parks in Europe, the Industrial Monuments Route – the most interesting industrial tourism route in Poland or the Historic Silver Mine – a unique place inscribed on the UNESCO's World Heritage list.

Metropolia is also a place of exceptional cultural events – performances, concerts, or great music festivals – from the classic Gorczycki Festival, through Tauron Nowa Muzyka, to the Off Festival. These events gather tens of thousands of fans from Poland and abroad.

Here you will also be surprised by nature – navigable lakes, such as Pogoria and Paprocany Lake, nature preserves: the Segiet, Murckowski Forest, and even a piece of great natural uniqueness – the Błędowska Desert – unmatched in Europe.

**Together we can do more!**

**41** cities and municipalities
**2.3** million inhabitants
**2,500** square kilometres
of surface area

FOR MORE: METROPOLIAGZM.PL

# HYDROGEN EAGLE

The flagship hydrogen project in CEE region is one of ORLEN Group's initiatives to achieve a net zero carbon footprint by 2050.

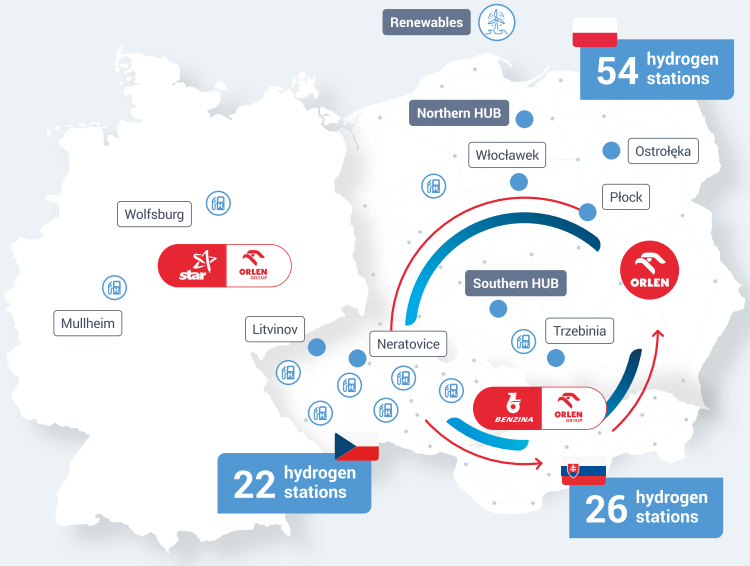
## The ORLEN Group

The largest corporation in Central and Eastern Europe

Operates in: Poland, the Czech Republic, Germany, Lithuania, Slovakia and Canada

Annual processing capacity of over 35 million tonnes of various types of crude oil

Owns the largest network of over 2,800 modern service stations




**Poland**
- **54** HRS,
- **110 MW** electrolysis capacity,
- **15 kt $H_2$** from municipal waste,

**Czech Republic**
- **22** HRS,
- **80 MW** electrolysis capacity,

**Slovakia**
- **26** HRS,
- **60 MW** electrolysis capacity,

**The most important project parametres:**

- **102** HRS
- **250 MW** electrolysis capacity
- **15 kt $H_2$** / year from municipal waste
- over **1 mln tonnes $CO_2$** emission reduction annualy

Hydrogen Production Units (existing and under development)

Hydrogen Refuelling Station (existing and under development)

- Hydrogen Eagle is a staged, comprehensive infrastructure project run by ORLEN in Poland, Czech Republic and Slovakia which aims to establish generation, transport and distribution capacities for zero/low-carbon hydrogen and to utilise it in the mobility sector and, potentially, for energy and industry applications, contributing to the development of a solid supply chain at the European market level.
- Hydrogen Eagle has also the potential to become an important part of the European Hydrogen Backbone vision. This would offer an opportunity to join this pan-European initiative creating systemic interconnections with the neighbouring countries.
- Cross-border coordination in infrastructure development is a prerequisite for the establishment of a European HRS network in the transport sector. Due to Poland, Czech and Slovakia strategic location at the crossways of main European transportation corridors our HRS network will form a part of a bigger pan-European HRS network, it would contribute to the development of a mobility segment relying on hydrogen as a new fuel, and therefore will allow smooth transport along the North-South, as well as East- West European corridors.

## Purpose

- $CO_2$ emission reduction from urban, heavy duty and railway transport
- Shift from conventional fuels to low and zeroemission hydrogen
- Low- and zero-emission hydrogen production on a large scale in CEE region using offshore RES, onshore RES and municipal waste
- Set up a necessary infrastructure in CEE region
- Enhancing Europe's competitiveness and advancing its climate neutrality goals based on environmentally sustainable solutions
- Potential to become an important part of the European Hydrogen Backbone

## Benefits

- Diversified hydrogen generation – Energy security of supply improvement in CEE region
- Hydrogen Eagle will create over **5 000** new jobs
- Solving the municipal waste management problem – Circular Economy solution
- After 2030 logarithmic scalability of hydrogen generation in EU

ANALYSIS

# NATO as a Norm Entrepreneur on Cyber Engagement in a Third-Party Conflict

DR OLESYA TKACHEVA

ASSISTANT PROFESSOR, CENTRE FOR SECURITY, DIPLOMACY AND STRATEGY (CSDS), THE BRUSSELS SCHOOL OF GOVERNANCE (BSOG-VUB)

DR MARTIN LIBICKI

KEYSER CHAIR OF CYBERSECURITY STUDIES, U.S. NAVAL ACADEMY

**ABSTRACT:**

**The ongoing Ukraine-Russia conflict underscored the glaring need for NATO to take the lead on developing shared among NATO Allies norms for engaging in offensive cyber in the new threat environment. As offensive cyber capabilities proliferate within the Alliance, they will become part of the military assistance package offered together with conventional capabilities by Allies to assist one of the conflicting parties in non-NATO conflicts. Subsequently, it will be critical for NATO to ensure that the deployment of these capabilities does not jeopardize its own posture on the conflict. This white paper discusses how to achieve this goal by using a bottom-up approach that emphasizes promoting shared norms for offensive cyber operations. This approach serves as an attractive alternative to the top-down regulation of cyber operations via MoUs or an international convention.**

## Introduction

Shortly after the Russia-Ukraine conflict escalated from a stand-off to conventional warfare, bilateral military assistance from NATO Allies and partners (e.g., Sweden) started pouring into Ukraine. Allegedly, some NATO Allies even started looking into a variety of cyber capabilities as a way to signal to the Kremlin that the cost of conflict for Russia will be rising if the aggression continues. According to NBC News (Dilanian & Kube, 2022), the White House reviewed cyber options ranging from slowing down or shutting the Internet to tampering with electric power or railroad switches. When this information was leaked to the media, a vibrant debate started about the strategic impact that a cyberattack carried out by a NATO Ally may have on the ongoing conflict between Russia and Ukraine, with some experts speculating that it may provoke a tit-for-tat response from the Kremlin.

These deliberations are taking place as NATO Allies are rapidly expanding their toolkits for cyber operations (Marrone & Sabatino, 2021, Pernik, 2021; Muller, 2019, IISS, 2019). Soon, conversations about deploying cyber in a non-NATO conflict could be taking place not only in Washington, but also in Paris, Tallinn, London, and beyond. This raises the following questions:

- What implications may deployment of offensive cyber by an Ally in a non-NATO conflict have on NATO's strategic posture?

- What can NATO do to mitigate the impact of Allies' deployment of offensive cyber on its posture not to engage directly with the third-party conflict?

Answering these questions requires understanding how NATO can bridge the lack of authorities to shape Allies' engagement in a non-NATO conflict with the need to sustain its neutral posture on the conflict. Although a similar dilemma arises when Allies provide conventional military assistance, we argue that the difficulty of attribution and secrecy of cyber operations carry unique strategic implications for offensive operations in cyber space for NATO. As such, in the analysis that follows we explain why the above questions are salient for NATO and outline how NATO can leverage its unique position to promote shared norms of engagement in cyber space to generate a tacit convergence in deployment of offensive cyber in the absence of a formal common framework.

We begin by illustrating strategic dilemmas faced by NATO when its Allies deploy cyber capabilities in a non-NATO conflict and then we will turn to the discussion of how NATO can best position itself to promote shared norms for conducting offensive cyber operations.

**Allegedly, some NATO Allies even started looking into a variety of cyber capabilities as a way to signal to the Kremlin that the cost of conflict for Russia will be rising if the aggression continues.**

## Offensive Cyber Deployment in a Third Party Conflict – Strategic Implications for the Alliance

NATO's approach to conducting offensive cyber operations is based on the voluntary contribution of cyber effects by Allies who retain the Command and Control (C2) over them. This is similar to how NATO uses its strategic nuclear capabilities, in which the three nuclear-holding states the United States, the United Kingdom, and France— retain control of their national capabilities and vest the right to launch a nuclear strike with the civilian leadership who is guided by their countries' nuclear postures that spell out red lines and targets. The latter embodies the country's unique approach to nuclear warfare and this necessitates agreeing on a shared nuclear posture for the Alliance.

One problem, however, with relegating cyber operations to individual nations, even as conventional capabilities come under a supranational organization, NATO, is the prospect

of interference between the two. To illustrate as much, consider the potential disjunction between the U.S. and French nuclear policy in the Cold War when in the early 1960s, U.S. Secretary of Defense, Robert McNamara, took issue with the French nuclear doctrine. In an attempt to stave off the prospects of Armageddon, he offered[1] a strategy in which if nuclear war broke out with the Soviet Union, the United States would limit its nuclear use to taking out Soviet nuclear assets (aka counter-force), but the United States would not target Soviet cities (aka counter-value). The hope was that the Soviets would recognize U.S. restraint, and, likewise, not target U.S. cities. Many lives would be saved. The French nuclear doctrine, however, threatened to complicate this strategy because France lacked the capability to conduct counter-force operations effectively; instead, it threatened to respond to any nuclear attack on France by aiming directly at Moscow. Should war develop (and France be struck) the Soviet Union would lose Moscow, and any attempt by the United States to limit the damage from nuclear war would not work.[2] In any case, with or without France, the Soviet Union was sceptical, to say the least, about McNamara's city-withhold strategy, arguing that it legitimized nuclear war.

Cyberwar, admittedly, is on the far end of the conflict spectrum from nuclear war, but because the Alliance lacks the commonly agreed posture, the two are similar in that states are likely to pursue them independently[3] and operations are highly classified (which means that one state may not know what its Ally is planning). NATO, for instance, has no organic offensive cyber capability, and relies on cyber effects provided voluntarily by the Allies who retain the command and control over cyber effects during joint NATO operations.

Because Allies, as sovereign nations, can deploy their offensive cyber in the third-party conflict any time, it creates a troubling possibility that while the Alliance, as a whole, wants to communicate restraint, the aggressive activities of one of its members may undercut that message in the eyes of the other side – just as McNamara feared that France's nuclear operations would undercut U.S. restraint. Admittedly, in the NATO context, such fears are theoretical: the United States, NATO's *de facto* leader, has the largest, most sophisticated cyber operations and is, as far as known, the most aggressive about using them. But the United Kingdom, Estonia, and the Netherlands, at least, bring some unique cyber capabilities to the mix, and the possibility that one of them (or even another NATO member) may also be more aggressive than the United States, while unlikely, is not impossible.[4]

**Cyberwar, admittedly, is on the far end of the conflict spectrum from nuclear war, but because the Alliance lacks the commonly agreed posture, the two are similar in that states are likely to pursue them independently and operations are highly classified (which means that one state may not know what its Ally is planning).**

This problem becomes more acute if NATO is entangled with a war next door – the Russian invasion of Ukraine, being a case in point. Does such bilateral cyber assistance by NATO Allies in the third-party conflict generate strategic implications for the conflict dynamic beyond what similar activities

1 For an excerpted version see McNamara (2011) at https://www.airforcemag.com/article/0611keeperfile/. His May 1962 remarks to the Ministerial Meeting of the North Atlantic Council (https://history.state.gov/historicaldocuments/frus1961-63v08/d82) essentially said the same thing.

2 In theory, the Soviet Union could recognize that the U.S. strategy still called for restraint and that its own restraint could save its own cities – but in practice, it was far likelier that it would treat NATO as a single entity, which, after all, was the whole point of the alliance.

3 In practice, the United States is likely to coordinate its cyber efforts with the United Kingdom, just as it is likely to coordinate its nuclear operations. Neither has ever been the case with, say, France.

4 Even if offensive cyber is not used, cyberespionage and intelligence sharing could become another way in which Allies can deploy cyber capabilities to assist one of the parties to the conflict. Since these activities are regulated by the intelligence sharing agreements, they go beyond the scope of this paper, it does not mean, however, that norms of cyberespionage cannot or have not yer emerged. See Libicki (2017).

in the conventional domain have? After all, many Allies have already provided or pledged to provide lethal conventional weapons to Ukraine. Will including offense cyber capabilities into the assistance package have any different effects? We argue that several peculiar features of the cyber domain make the impact of offensive cyber different from the overt provision of lethal aid. The ambiguity of attribution under the current C2 structure for offensive cyber effects, and the highly secretive nature of cyber capabilities coupled with the complexities of escalation in a multi-domain environment pose new dilemmas for NATO even when it is not involved in a third-party conflict. We discuss each of them below.

Cyberspace is a crowded domain to operate in. Private actors, who seek economic gains or the desire to fulfil patriotic ambitions, operate concurrently with state actors whose geopolitical goals may or may not overlap with those of the private actors. This complicates *ex post* attribution especially when neither of the private actors nor non-NATO countries claims responsibility for a cyberattack against parties in a non-NATO conflict, it may undermine the credibility of NATO's non-belligerent posture. Such an attack can be even carried out by a NATO Ally, but the secrecy with which offensive cyber is deployed deprives NATO of both *ex ante* verification mechanisms as well as the ability to monitor cyber activities of its member states. If the victim retaliates using conventional capabilities, it forces NATO to deal with the act of aggression unexpectedly. So, anticipating a horizontal escalation of the third-party conflict becomes more difficult for NATO when offensive cyber is deployed because the secrecy of cyber operations obscures the changes in the threat environment for NATO.

If the Alliance understood that one of its members was jeopardizing its own *modus vivendi* with the target state, it might be able to pressure that one member to dial its cyber operations back. If it could not, it may find other ways of convincing the target state that its intentions were unchanged. But one of the defining aspects of an offensive cyber operation is that Allies do not disclose ongoing persistent engagement operations with one of the warring parties in a non-NATO conflict.

Offensive cyber operations also have strategic implications beyond third-party conflicts because they can change the strategic calculus of the conflicting parties. Horizontal and vertical escalation are frequently used concepts to describe dynamics of conventional conflicts. The former refers to the situation when a conflict spills over to a wider geographic area, whereas the latter corresponds to a higher pain level in the form of, for instance, greater casualties and more destruction of infrastructure. Research shows that, unlike conventional, deploying offensive cyber does not map into this topology because it creates non-linear escalation and de-escalation pathways that do not accord to either vertical or horizontal escalation logic (Libicki & Tkacheva, 2021).

Strategic implications of the bilateral use of offensive cyber will be even less linear during the ongoing hot conflict because decision-makers' perceptions of developments in the physical domain will influence the willingness to retaliate against cyber measures. As suggested by the prospect theory, decision makers' risk-taking behaviour is influenced by their perception of the status quo.[5] They become more risk averse when they perceive the status quo as generating gains for them and adopt a more risky behaviour when they perceive the status quo as losing outcome. When a conflict unfolds in multiple domains, the developments in the physical domain shape how decision makers react to a cyberattack. On the one hand, if they perceive that they are winning in a conventional domain, they become risk averse and may avoid a kinetic response, if they even retaliate at all. If, on the other hand, the timing of a cyberattack coincides with defeats in the conventional domain, the kinetic response may be more likely (Balcaen et al., 2022).

**One of the defining aspects of an offensive cyber operation is that Allies do not disclose ongoing persistent engagement operations with one of the warring parties in a non-NATO conflict.**

5 This is a major theme of Copeland (2013)

## How can NATO Leverage Norms to Discourage Excessive Deviations from its Posture?

Can NATO's cyber posture become a potential *ex ante* mechanism for discouraging unilateral risk-taking offensive cyber operations by the members of the Alliance? Although each nation conducts offensive cyber operations within its own legal framework, these frameworks diverge when it comes to the extent of civilian oversight of offensive cyber, its separation from cyberespionage, and the transparency of decision-making on the use of offensive cyber capabilities. Some experts characterized this growing divergence within the Alliance as a "worrisome development" because it deprives NATO of a single path towards cyber maturity and can exacerbate internal divisions on how to address cyber threats. They allege that this diversity should be dealt with by signing the Memorandum of Understanding on Cyber Security Operations (Smeets, 2021).[6] Other experts advocate an international convention on a cyberwar convention to regulate diffusion of offensive cyber worldwide (Geers, 2010; Eilstrup-Sangiovanni, 2018; Kalpokien & Kalpokas, 2020). These proposals use the conventions for controlling chemical weapons as analogy and call for transparency, verification, and communication hotlines to address escalation. Although they have not yet generated buy-ins from the relevant stakeholders, it is conceivable that it may happen in the future, with the EU emerging as the lead actor. The EU Strategic Compass, approved by the European Council on 21 March 2022, laid out an ambitious agenda to strengthen the EU's capacity to counter threats in the cyber domain, including the EU cyber posture, the EU's cyber defence policy, and a new Cyber Resilience Act (EC, 2022). Taken together, these measures may have far reaching implications of the regulatory environment for offensive cyber operations.

6 Max Smeets, "NATO Allies' Offensive Cyber Policy: A Growing Divide?" The Hague Center for Strategic Studies, August 6, 2021: https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/

As such, NATO should become proactive today to position itself as an agenda-setter for discourse on this matter.

One way to achieve this goal is by capitalizing on a bottom-up approach based on a diffusion of shared norms for cyber operations within the Alliance. Norms differ from a top-down regulation because they do not require external enforcement by a third party, as in the case with legal conventions. Norms are mutually-shared forms of behaviour that become self-enforcing because unilateral deviations are suboptimal (e.g. driving on the opposite side of the road). As such, norms have become ubiquitous in the debate on the Internet governance as an alternative solution to the legally enforceable mechanisms; albeit, there is little consensus in the voluminous literature on the type of actors who can contribute to the development of norms, the process by which they disseminate, and the type of cyber operations to which these norms should be applicable. The state-centric approach perceives states as the ultimate protagonists behind norm diffusion. Although non-state actors can contribute to framing and articulation of norms, without state's involvement, norms will not take off the ground. The state-centric approach perceives norms as a transitional phase that will subsequently pave the way to codification of these norms in legally binding rules (Macak, 2017).

The usefulness of the state-led approach to the development of norms has been questioned on several grounds. First, as suggested by norms-evolution theory, norms on how to use new warfare technologies become binding when states perceive them as aligning with their self- interests and when the norms are coherent with already existing norms. Neither of which is the case for cyberspace (Mazanec, 2015). Second, competition from non-state actors impedes the state-led norm development effort. For norms to be biding, they need to be perceived as legitimate by hackers, hacktivists, private-sector players and civil-society actors, but they are frequently left out of negations of terms by states and subsequently are less likely to internalize the norms. This frequently leads

to "normfare" i.e. a competition among multiple norms championed by different actors, a so-called "norm entrepreneurs" (Radu et al, 2022). And that, in turn, reduces the incentives of non-state actors to comply with state norms. Therefore, some authors argue that the emphasis should be on confidence building measures between cyber powers. Bilateral communication hot lines, regular high-level dialogues, and voluntary exchange of information although are not legally binding, could serve as an alternative pathway for developing a shared understanding of acceptable behaviour in cyberspace (Grgisby, 2017). Another limitation of the state-centric approach is the challenges that "normfare" poses among various state agencies, each of whom represents different organizational culture that shapes behaviour in cyberspace.

**The state-centric approach perceives states as the ultimate protagonists behind norm diffusion. Although non-state actors can contribute to framing and articulation of norms, without state's involvement, norms will not take off the ground.**

Multistakeholder approaches to norm settings emerge as an alternative paradigm that focuses on the process by which norms become binding *ex ante* in the absence of *ex post* external enforcement. Three factors contribute to this: shared identity, repeated interactions that facilitate social sanctioning and impose reputational costs, and collective exceptions of compliance with the norms. Although from this perspective any actor can emerge as a norm entrepreneur, it is surprising that this voluminous literature has not considered yet NATO's potential to become a norm setter. This is particularly surprising in the light of the fact that the production of the most frequently mentioned document on cyber warfare, the Tallinn Manual, was led by a group of experts closely linked to NATO. The shared identity of NATO Allies, repeated interactions and shared norms of conducting warfare in other domains makes NATO ideally poised to take the lead on the creation of norms pertaining to conducting offensive cyber operations in cases of the third-party conflict.

Because the context for norm development is much narrower than for the global governance of offensive cyber, this increases the likelihood that norms will become institutionalized. These norms could be communicated within the framework supporting the implementation of the NATO's *AJP-3.20* document (NATO 2020) that spells out NATO's approach to joint cyberspace operations because once norms become internalized in the context of joint NATO operations and trainings, they could become routine behaviour for carrying out cyber effects in non-NATO's missions. Because many NATO Allies still lack offensive cyber capabilities, it makes it easier for them to embrace NATO-specific norms at this stage because they are starting from *tabula rasa*. When they develop their own cyber capabilities, the norms taught by NATO and procedures adopted for NATO's offensive cyber will become the default option. Thus, NATO can still become an effective agenda-setter for norms without having its own offensive cyber capabilities.

## Conclusion

As offensive cyber capabilities continue proliferating within NATO, a day will come when Allies will start including cyber effects into military assistance packages to parties in non-NATO conflicts. As sovereign nations, Allies are free to choose from a wide range of military assistance tools. The secrecy of how cyber operations are implemented my hinder NATO's ability to track and understand how threat levels and operational environment may be reacting to cyber operations conducted by Allies against the parties involved in a non-NATO conflict. Given that cyber operations may have escalatory effects on conflicts, NATO should become an agenda-setter for norms on offensive cyber operations by leveraging effectively its unique position in developing and implementing doctrinal documents on how to carry out operations in cyberspace. Rather than seeking to create a formal regulatory framework for offensive cyber operations, NATO should emphasize

the development of organizational culture based on the shared understanding of escalatory notary of cyber operations, the set of acceptable targets, particularly during non-NATO conflicts, advanced warning of NATO Allies and other type of practices that can contribute to the creation of collective undertaking of norms of conduct in cyberspace. ■

## About the authors:

**Olesya Tkacheva** (Ph.D., University of Michigan, Ann Arbor, 2009) is Assistant Professor at the Brussels School of Governance, VUB. She is affiliated with the Center for Security, Diplomacy and Strategy where she conducts research on the technology-security nexus with particular focus on Russia and Eastern Europe. Prior to moving to Brussels, she worked for the RAND Corporation and the Pentagon where she supported developing and implementing U.S. response to counter Russia's aggression in Ukraine and Syria. Her research was published in leading journals and she is a winner of Fulbright and National Science Foundation Fellowships, and was also a postdoctoral fellow at the Skalny Center for Polish and Central European Studies, University of Rochester.

**Martin Libicki** (Ph.D., U.C. Berkeley 1978) holds the Keyser Chair of Cybersecurity Studies at the U.S. Naval Academy. In addition to teaching, he carries out research in cyberwar and the general impact of information technology on domestic and national security. He is the author of a 2021 textbook on cyberwar, Cyberspace in Peace and War (2nd edition), as well as Conquest in Cyberspace: National Security and Information Warfare and various related RAND monographs. Prior employment includes eighteen years at the RAND Corporation, twelve years at the National Defense University, three years on the Navy Staff (logistics) and three years for the US GAO.

# References


Blacaen, Pieter, Du Bois, C. & Buts, C. The hybridisation of conflict: a prospect theoretic analysis. *Games* 12 (4): 81-95; https://doi.org/10.3390/g12040081.

Dilanian, K. and Kube, C. (2022, 24 February 24). Biden has been presented with options for massive cyberattacks against Russia. *NBC News.* Retrieved from https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558.

EC, (2022, 21 March). *A strategic compass for security and defence.* Available at https://eeas.europa.eu/headquarters/headquarters-homepage/113273/strategic-compass-security-and-defence_en.

Eilstrup-Sangiovanni, M. (2018). Why the world needs an international cyberwar convention. *Philosophy & Technology* 31: 379-407; doi 10.1007/s13347-017-0271-5;

Geers, K. (2010). Cyber weapons convention. *Computer Law & Security Review* 26: 547-551; doi:10.1016/j.clsr.2010.07.005.

Grigsby, A. (2017). The end of cyber norms. *Survival* 59(6): 109-122, DOI:10.1080/00396338.2017.1399730.

Copeland, D. (2013). *The origins of major war*. Cornell University Press.

IISS (2021, 28 June). Cyber capabilities and national power: A net assessment," International Institute for Strategic Studies (IISS) Research Paper; https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

Kalpokienė, J. & Kalpokas, I. (2020). Contemplating a cyber weapons convention: an exploration of good practice and necessary preconditions. *Baltic Journal of Law & Politics* 13(1): 51-80.

Libicki, M. & Tkacheva, O. (2021). Cyber escalation: ladder or lattice? In Stevens, T, Floyd, K. & Pernik, P. eds. *Cyber threats and NATO 2030: horizon scanning and analysis*. NATO Cooperative Cyber Defence Centre of Excellence.

Libicki, M. (2017). The coming of cyber espionage norms, in Rigas, H, Jakschis, R, Lindstr L, & Minrik, T (Eds.) *2017 9th International Conference on Cyber Conflict Defending the Core* CCD COE, at https://ieeexplore.ieee.org/document/8240325.

Macak, K. (2017). From cyber norms to cyber rules: re-engaging states as law-makers. *Leiden Journal of Integration Law* 30: 877-899.

Marrone, A. & Sabatino, E. (2021, Februrary). Cyber defence in NATO countries: comparing models. Instituto Affari Internazionali Paper; https://www.iai.it/sites/default/files/iaip2105.pdf.

Mazanec, B. M. (2015). *The evolution of cyber war: international norms for emerging-technology weapons*. University of Nebraska Press: Potomac Books.

Muller, Lilly Pijnenburg (2019, 29 January). Military offensive cyber-capabilities: small-state perspectives, Norwegian Institute of International Affairs.

NATO (2021). AJP-3.20: Allied joint doctrine for cyberspace operations; https://isnblog.ethz.ch/defense/military-offensive-cyber-capabilities-small-state-perspectives.

Pernik, P. (2021, October). Cyber deterrence: a case study on Estonia's policies and practice. The European Center for Excellence for Countering Hybrid Threats, October 2021; https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf.

Radu, R., Kettemann, M.C., Meyer, T. & Shahin J. (2021, July). Normfare: Norm entrepreneurship in internet governance. *Telecommunications Policy* 45 (6)): 102148. https://doi.org/10.1016/j.telpol.2021.102148

Smeets, M. (2021, 6 August). "NATO Allies' offensive cyber policy: a growing divide? The Hague Center for Strategic Studies; https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/.

ANALYSIS

# Cyber Conflict During the War in Ukraine

MIROSŁAW MAJ

FOUNDER AND PRESIDENT,CYBERSECURITY FOUNDATION; CO-FOUNDER, OPEN CSIRT FOUNDATION; VICE-PRESIDENT, COMCERT.PL

*Disclaimer: This article is based on observations made since the outbreak of the war in Ukraine until March 22. The situation may have changed since then.*

The war in Ukraine is being waged not only at a kinetic layer, within the well-known physical domains of warfare, but also in cyberspace. The "cyber" layer, however, is not the one where the most critical or dangerous activities take place. The ongoing Russian invasion in Ukraine proves that wars are still not won in cyberspace, although the role of this domain increases with each new conflict. Activities in cyberspace consist of cyber and intelligence operations – both of which are interrelated. In the past, Russia proved that it has considerable capabilities in this sphere, and is able to combine technical attacks with disinformation attacks. The effects and scale of the use of cyber weapons are unpredictable and, given today's interconnectedness, can affect the attacked and the attacker alike, which perhaps to some extent deters the parties from using this arsenal. Moreover, in today's interconnected world and decentralized Internet, it is difficult to predict who will fall prey to the attacks in the end.

There are currently three players whose cyber activities we are observing during the war in Ukraine, and who are also involved in this cyber conflict: Ukraine, Russia, and the Anonymous

World community. Their narrations, however, differ significantly from one other. What is known at this point is that cyber activities are on the rise, but they are still not that different from what we have been observing for years. The attack vectors are already known: DDoS (Distributed Denial of Service), data leaks, and attempts to attack data, with data destruction (for example, through wipers) being ousted by ransomware attacks. However, up until now there have not yet been attacks that have led to serious consequences, such as damage to critical infrastructure, although such incidents are historically known (e.g. power outage in Ukraine in 2015 and 2016). It is important to keep in mind that cyber threats have yet to show their devastating impact, having the potential of inflicting serious damage to Western countries for example.

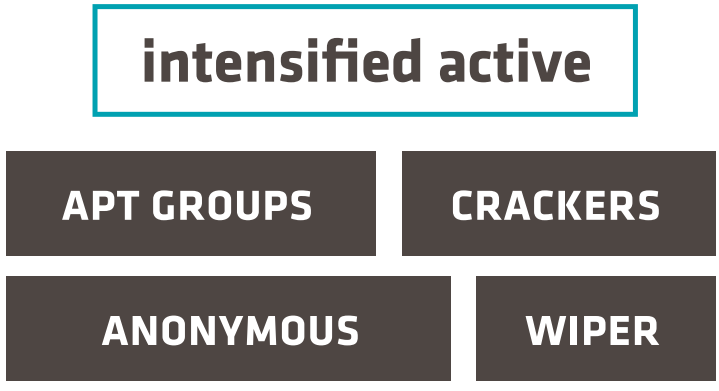
"Operation Russia", as announced and executed by the Anonymous, is one of the largest in the history of the group's existence. Their actions are seemingly countless, however their effectiveness should be assessed thoroughly. The Moscow Exchange, which was supposed to be unresponsive due to a DDoS attack, was unavailable only in certain areas, and the Russian Federation reported very few similar problems overall. Uncoordinated actions by hacktivists can be an additional complication for those who formally seek to coordinate cyber efforts. After all, these ventures do not involve professionals, but average Internet users who are not fully aware of what they are installing on their computers. Their attacks may not always coincide with the actions of others.

**The ongoing Russian invasion in Ukraine proves that wars are still not won in cyberspace, although the role of this domain increases with each new conflict.**

## ACTIVITY OF APT GROUPS

Interestingly enough, there are no clear traces of activities of the most threatening APT groups in connection with the ongoing war, which are usually backed by state actors who are capable of conducting dangerous operations in cyberspace on a very large scale using advanced techniques. However, this situation may still change very soon, as there is a possibility that preparations for a specific operation are just underway, and the public will find out about it in the near future. There are reports of increasing exploitation of new vulnerabilities of systems, but at the same time these actions are neither new nor critically dangerous. However, it may turn out that we will have to redefine the TTPs (Tactics, Techniques, Procedures) used by the Russian APT groups. After all, the observation is still ongoing. Careful analysis of the workings of systems that may turn out to be targets of attacks may reveal entirely new attack sequences.

There is no doubt that APT groups continue to remain active. They may be using old methods or preparing their operations to enter a decisive phase; alternatively, they may be operating in ways that we cannot even recognize. It is also



possible that the already known cyber problems will emerge and affect the Ukraine's allies, rather than Ukraine itself. This could be a way to retaliate for sanctions and destabilize the aid coming from the West. Unfortunately, it is likely that the most dangerous activities that will manifest themselves in cyberspace are yet to come and turn a conflict in this realm into a full-fledged war.

There is also little information regarding the activities of the Chinese APT groups in relation to the war in Ukraine. China is a country that operates strategically and co-ordinately in cyberspace as well, and Chinese groups often conduct long-term espionage activities. For example, the APT41 group is known to have continuously attacked U.S. government agencies and governmental institutions around the time the war began. They managed to compromise at least 6 government networks, also by means of the 0-day Log4J vulnerability they discovered.

## WIPER

Before and after the outbreak of war in Ukraine, there has been a lot of talk about malware – during the first large-scale eruption of the conflict, many governmental institutions were infected with ransomware. In relation to the most recent events, we can observe modified malware that no longer allows for recovery of data, irretrievably deleting it. These are the so-called wipers, an example of which is called the HermeticWiper (thankfully, most antivirus engines already detect the presence of this particular malware). Another threat is the HermeticRansom which encrypts files found on partitions using the AES-GCM algorithm. Running it triggers generation of a string of 32 characters used as a key. The AES-GCM key in turn is encrypted using RSA. Interestingly, in the process of implementation of this ransomware a mistake has been made, making it possible to exploit and create a free decrypter.

It seems that this is not the end of the destructive activity of wiper-type malware in Ukrainian networks. This seemingly simple attack is extremely effective in paralyzing the activities of still functioning institutions and critical infrastructure, including the systems used by the border services which are also gradually becoming the target of such attacks. However, there is no evidence that the said attacks have been carried out on a large scale. We will have to wait a bit longer for precise analyses of the methods of defence and how to deal with such hostile activities. The extent to which malware errors contributed to the lack of effective operations (effective meaning leading to a total disorganisation of systems) remains an open question.

**It seems that this is not the end of the destructive activity of wiper-type malware in Ukrainian networks. This seemingly simple attack is extremely effective in paralyzing the activities of still functioning institutions and critical infrastructure, including the systems used by the border services which are also gradually becoming the target of such attacks.**

## ACTIVITY OF CYBERCRIMINALS

Old methods, but new targets – this is how we can sum up the activity of cyber criminals who are trying to take advantage of the current situation. One of such "new-old" ventures is bitcoin wallets, where one can deposit funds, supposedly to support Ukraine. There are also phishing scams related to sending aid and exploiting people's natural willingness to help Ukraine.

The topic of sanctions is also used in phishing campaigns targeting the private sector. Companies receive emails to convince the recipients that the imposed sanctions will harm them in some way. These messages are meant to scare employees or pressure them to react in a certain way. Influencing through emotions (especially negative ones) is a standard tactic used by cybercriminals. They often exploit current events to make their actions seem credible in order to profit from them, which may go against the interests of any party involved in the conflict.

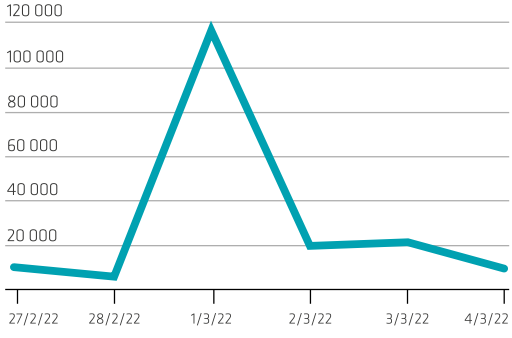
We can also observe other vectors of attacks that are aimed at higher management. The recent buzzword is "supply chains", which is used in cybersecurity and a myriad of other contexts. However, when it comes to phishing, "supply chain" is primarily targeting executives, trying to pressurize them into infecting equipment that stores company information. This time, it is not about delivering vulnerable libraries, but merely attempting to deceive recipients through fake surveys.

## THE ROLE OF DISINFORMATION

Disinformation activities have always accompanied armed conflicts, so it is not surprising that we are being flooded with false information from both sides. Propaganda and disinformation activities have been Russia's domain for years, so also this time we can observe a lot of false information being sent by Russian botnets. As a result of that, in Poland we have observed reports of fuel shortages or problems with ATM withdrawals.

As observed, disinformation groups linked to Russia became more active in the second half of February. However, the biggest wave of disinformation swept through the Polish Internet at the beginning of the war in Ukraine, and included as many as 120,000 disinformation attempts in Polish social media just on 1 March alone. At that time, mainly anti-refugee groups were active, creating a sense of threat by spreading information about the so-called "non-Ukrainian refugees". Additionally, information about fuel shortages appeared online, leading to giant queues at petrol stations across Poland and, consequently, to fuel shortages at many petrol stations (mainly due to difficulty in delivering fuel in such a short period of time). These are not the only activities that will be conducted in the Western countries by the Russian Federation. Therefore, especially during the conflict, we should be particularly cautious and critical about information spread online, even that distributed by "trusted", that is, well-known sources. Journalists play a big part in it, and have a huge responsibility to verify the sources when disseminating information.

**Disinformation on the Polish Internet at the beginning of the war**




*Author's own compilation based on data from the Institute for Internet and Social Media Research*

For many years the problem of disinformation went under the radar – these days, we are undergoing a quick and painful learning curve. The other side acts methodically, conducting strategic and well thought-out operations, therefore our defence must be equally well prepared. The role of education is pivotal, of course, but it is also crucial to combat disinformation through technical means, including proper identification. No matter how much effort we put into getting Internet users to be able to think critically to recognize "fake news", adequate technical tools are still necessary to assist in removing news that is false and intended to cause panic or generate hostility. Disinformation does not just happen online though; specific individuals or organizations are subject to those types of narratives and used to spread and legitimize false opinions – oftentimes these individuals do not even realize they are working for the enemy. There is no system to counteract this and perhaps special hubs dedicated to fighting disinformation are needed. After all, disinformation can be detected by technical means: it is often botnets or other forms of technical manipulation and gaining advantage in a network battle.

**For many years the problem of disinformation went under the radar – these days, we are undergoing a quick and painful learning curve.**

**How to protect yourself against online disinformation?**

1. consciousness
2. verification
3. using various sources of knowledge
4. vigilance

First of all, one has to be aware that in the current abundance of information, verification and filtering (rather tedious activities) have become even more difficult. Manipulative content is often created in such a way that it cannot be classified as false at first glance. Frequently, verifying the information at source is required to either confirm or dismiss it as false. Therefore, as informed Internet users, we should follow various trusted channels. Frequently searching for the latest information is pointless as all parties to the conflict create their own narratives with which they want to influence morale. Moreover, military actions cause a lot of chaos, including information chaos. It is key to remember that the information coming from the front is distorted because the fog of war is still superimposed on the typical disinformation activities.

There is an ongoing conflict in the cyber zone, however something much more serious may strike us soon. It is hard to believe that the APT groups who have been responsible for major cyberattacks so far are now weaker and unable to deal with the infrastructure of the wider West. So we should stay vigilant and continue to prepare for major cyberattacks on critical infrastructure. Cyber criminals we fight every day do not sit idle – they want to take advantage of the situation to achieve their goals. Here, too, it is important to remain vigilant and fight new scams which this time are taking advantage of the war in Ukraine. It is likely that the "cyber" zone has not revealed all its cards yet. ■

## About the author:

Over 20 years of experience in ICT security. Founder and president of the Cybersecurity Foundation, Vice-president of the ComCERT company, a former leader of CERT Polska team. The member of the Digital In 2017-2018 he was the adviser to the Minister of National Defence of Poland on planning cyberdefence capabilities and building organizational structures and establishing international cooperation in the field of cyberdefence. In March 2021 was appointed a member of the Digitalization Council at the Ministry of Digital Affairs.

Initiator of Polish Civic Cyberdefence organization. Co-founder of Open CSIRT Foundation - the stewardship organisation for SIM3 model and co-provider of Trusted Introducer service for CSIRTs, including processing of CSIRT formal certifications. Lecturer of cybersecurity courses on few universities.

European Network Information Security Agency expert and co-author of many ENISA publications including CERT exercises and papers on improvement CSIRT maturity. He organised 10 editions of cyber exercises (Cyber-EXE™) in several countries for most essential sectors (e.g energy, banking, telecommunication). Speaker on many international conferences including the FIRST conferences. He is also the originator and organiser Security Case Study conference, one of the largest cybersecurity event in Poland.

ANALYSIS

# The Power of Layered Resilience

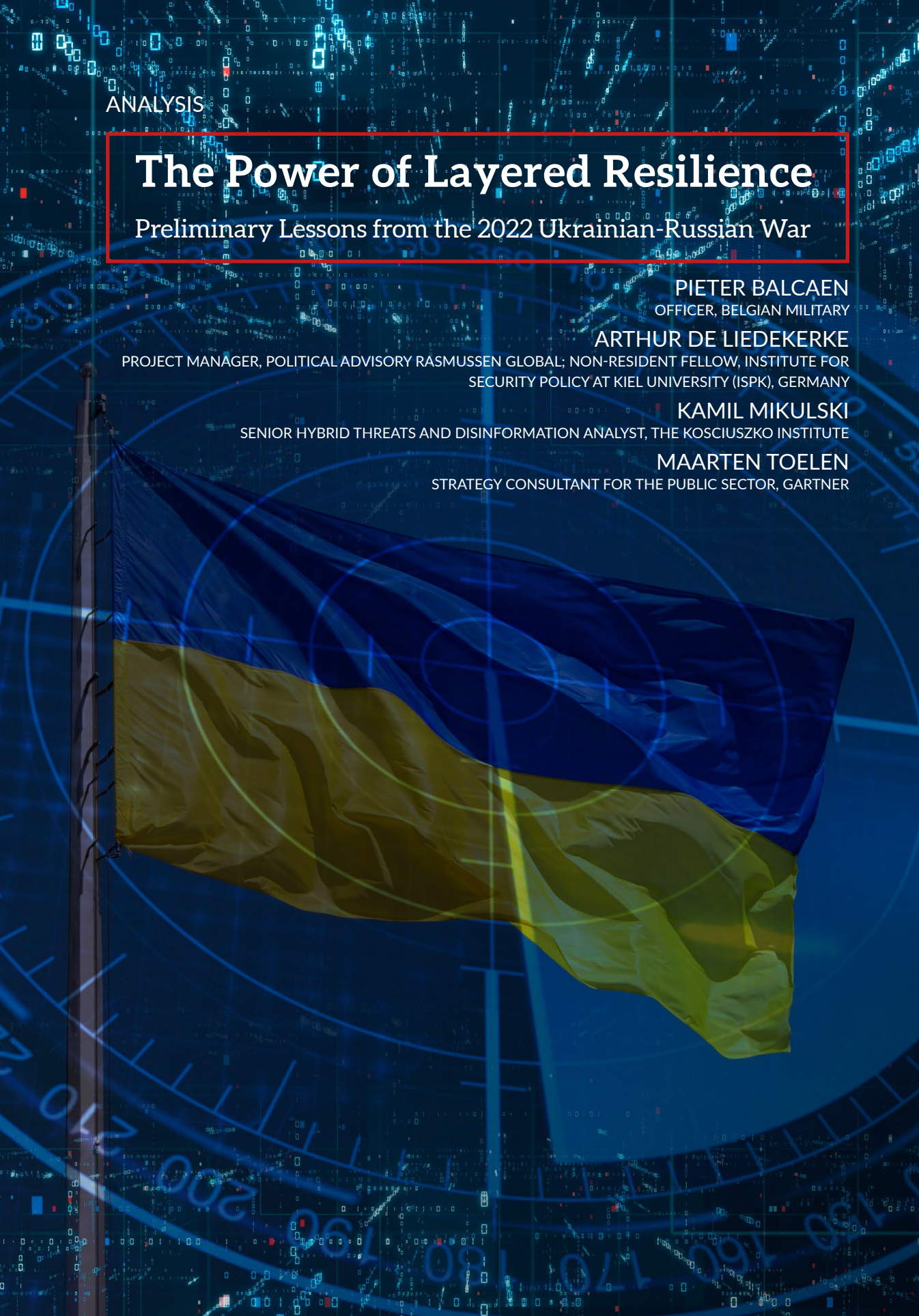
## Preliminary Lessons from the 2022 Ukrainian-Russian War


PIETER BALCAEN
OFFICER, BELGIAN MILITARY

ARTHUR DE LIEDEKERKE
PROJECT MANAGER, POLITICAL ADVISORY RASMUSSEN GLOBAL; NON-RESIDENT FELLOW, INSTITUTE FOR SECURITY POLICY AT KIEL UNIVERSITY (ISPK), GERMANY

KAMIL MIKULSKI
SENIOR HYBRID THREATS AND DISINFORMATION ANALYST, THE KOSCIUSZKO INSTITUTE

MAARTEN TOELEN
STRATEGY CONSULTANT FOR THE PUBLIC SECTOR, GARTNER

*All authors are writing in a strictly personal capacity and the views expressed in this contribution should not be construed with any of their professional or academic affiliations.*

## Introduction

The unprovoked Russian invasion of Ukraine will certainly go down in history as a blatant violation of standing international law and the territorial integrity of another sovereign and peaceful nation. While discussions on these issues will certainly shape scholarship and policy-making for the near future, it must be noted that the peoples of Ukraine have thus far defied all odds by containing the Kremlin's offensive.

Despite the considerable human toll and suffering of this war, the unwavering courage of the Ukrainians – be they in uniform or not – is not only commendable but equally captivating, since it provides other nations with a practical, but terrible, example of how the concept of 'layered resilience' is essential for any contemporary integrated defence strategy. With dwindling support in Western nations to take up arms for one's country, the conflict in Ukraine clearly illustrates just how crucial this notion can suddenly become for NATO Allies on the Eastern flank and beyond (Gallup, 2015).

The article is structured as follows. First, we discuss briefly how the conflict evolved into a war of attrition. Second, this paper proceeds to illustrate how Ukraine has demonstrated resilience, serving as a good demonstration of NATO's concept of 'layered resilience' and which lessons can be drawn therefrom. As we show in the article, resilience was not only demonstrated in the physical domain, but also in the cyber and the cognitive domain. All these efforts have contributed to the current state of affairs, i.e. Ukraine being able, for the time being, to repel the Russian offensives across all domains. To conclude and based on some of these observations, the authors formulate recommendations applicable for NATO Allies. After all, the current crisis shows Western societies have much work ahead. The further strengthening of society-wide resilience is undoubtedly needed to address the challenges associated with the return of great power competition.

## The case of Ukraine: attrition warfare unfolding

Being the fifth largest military in the world,[1] Russia probably expected a swift victory following the surprise attack that occurred on the 24th of February, shortly after decreeing a 'special military operation' and demilitarization of Ukraine during a television speech. The blitzkrieg-like victory the Kremlin expected has not materialized. Instead, the preparations and efforts made by Ukrainian people, in the years following the 2014 invasion of Crimea, to increase their deterrence and if necessary, resist Russia, have paid off, as we will explain later on.

Whereas modern conflicts are more urban in nature and have seen changing practices – including hybrid tactics – increasingly target society as a whole, the Ukrainian conflict clearly demonstrated how civilians are ever more impacted by the consequences of war. They can play a pivotal role in the defence of the nation, alongside regular combatants. In other words, no longer does it suffice to defeat the conventional forces of a nation to subdue it. More often than not, contemporary wars – if at all – only end after a prolonged phase of insurgency on one side and suppression or (faltered) nation-building on the other.

**The blitzkrieg-like victory the Kremlin expected has not materialized. Instead, the preparations and efforts made by Ukrainian people, in the years following the 2014 invasion of Crimea, to increase their deterrence and if necessary, resist Russia, have paid off.**

1 In terms of active military personnel and reserve military personnel (IISS, 2022).

Unfortunately, the fierce resistance demonstrated by the Ukrainian population, resulting in a large number of casualties at both sides, has forced the Russian military to alter its strategy. The gradual degeneration of the conflict as observed over the last months can be best described by the definition of 'total war' (Freedman, 2017).[2] Defence analysts and various independent security experts have already noted this clear shift in the Russian strategy following the first weeks of the invasion, characterized by the increasing use of indiscriminate violence (e.g. artillery fire) resulting in an increasing number of civilian casualties. The tenacity – or 'resilience' – of the Ukrainian armed forces and civilians in occupied areas, have left Moscow with little choice other than resorting to attrition warfare. While the Russian army is certainly experienced in ruthless tactics, as their handling of the decade-long 'Chechen conflict' amply demonstrates, the fact that the Kremlin is now facing the distinct possibility of a 'frozen conflict' and the definitive prospect of a considerable international backlash,[3] is in itself a great indication of the effectiveness of Ukraine's layered resilience.

As its military operations falter, the Russian armed forces are now resorting to intense bombardments of several major Ukrainian cities and attempting to encircle or isolate others. Gruesome and illegal as such non-discriminatory methods might be, there are several lessons about resilience that one could note from this situation. Before discussing these observations in Section 4, we give a brief overview of NATO's concept of layered resilience within NATO's Warfighting Capstone Concept (NWCC).

## Layered resilience and the role of civilians in enhancing a nation's security

Being one of the five pillars of the NWCC, layered resilience focuses on enhancing a nation's ability to persist during long and protracted campaigns (NATO, 2021). In doing so, multiple layers of resilience can be distinguished in the NWCC: military resilience, military-civilian resilience and civilian resilience. Without entering into much details, which is beyond the scope of the article, the concept of layered resilience emphasizes the importance of the civilian population in the context of ensuring a nation's ability to absorb shocks, to increase resistance and to fight through (HCSS, 2020). Moreover, the concepts of the NWCC and the nested pillar of layered resilience recognize the importance of strengthening a nation's resilience in the cognitive and cyber domain, beyond the well-known traditional physical domain. The concept of layered resilience in the context of the Ukrainian conflict is further discussed in Section 3.2.

## Preliminary lessons-learned from the conflict

Studying the Ukrainian-Russian conflict in light of the concept of (layered) resilience bears several interesting findings. This article discusses the following: the paramount role of maintaining superior morale and the utility of organizing a nation's resilience across different layers. More precisely, we focus on the role the civilian society can (should) play in enhancing a nation's resilience.

### Resilience in contemporary conflict: the importance of enduring morale

Broadly speaking, the war in Ukraine can be perceived as testament to the fact that the capacity to absorb 'layers' of hardship without losing hope, is an integral part of the defence against total war – the key concept behind the NATO term of 'layered resilience'. Like most wars, the Russian invasion has inevitably resulted in the loss of swathes of territory in the first two weeks, including major cities

2 A concept of a conflict in which a nation is willing to make as many sacrifices as needed to obtain a complete victory and in which all types of weapons and tactics (such as the targeting of critical infrastructure) are envisaged (Freedman, 2017).

3 For example illustrated by the large number of sanctions implemented against Russia and the decision to ban multiple Russian banks from the SWIFT system. This debate lies, however, beyond the scope of this article.

such as Kherson and Melitopol. The Ukrainians even scuttled the Hetman Sahaidachny – the navy's flagship frigate – an act of defiance and resistance in order to prevent this asset from getting in Russian hands (Evans, 2022).

Moreover, the war in Ukraine highlights another crucial aspect of layered resilience: support of like-minded peoples and values or/and beliefs they stand for. Despite the presence of some far-right elements within Ukraine's self-defence forces and the foreign volunteers signing up, the international support Kyiv has received from the European Union and other NATO Allies is truly remarkable. On top of the provision of military equipment, thousands of foreign volunteers have signed up for service against the Russian invaders.

**The war in Ukraine highlights another crucial aspect of layered resilience: support of like-minded peoples and values or/and beliefs they stand for.**

Additionally, resilience played a critical role in buying time for the international community to respond to the tragic events unfolding in Ukraine. The fierce resistance demonstrated by the Ukrainian population and the images of civilians picking up weapons certainly made a strong impression on the Western society. The resilience observed by the Ukrainian population against the Russian brutality accelerated the decisions taken in the domain of arms deliveries and economic sanctions, decisions that had a strong impact on the further course of the conflict. Indeed, little opposition or debate was observed in light of the decisions made to support Ukraine. One could even say the European Union has rarely appeared this strong and united. Although the effects of sanctions are not visible immediately, they are assessed to have a substantial effect on the Russian economy in the longer term, rendering it gradually more and more difficult to continue their war efforts in Ukraine. Nothing of the sorts would have been possible if the Ukrainian army had surrendered in the early days of the invasion.

**Reinforced resilience across different layers: the role of civil society and the military**

The Ukrainian-Russian conflict also serves as a good case-study, demonstrating how 'layered resilience' can be implemented in practice and how these mutually reinforcing layers result in an overall increased resilience. First and foremost, the strength of military resilience has already been mentioned. It is, however, interesting to see how partner nations contributed to increasing this resilience, both in terms of the quality of Ukrainian soldiers and the equipment available to face the Russian numerical superiority. The Ukrainian army was not entirely unprepared for the clashes with Russia and has gone through a lessons-learned process since 2014. While the Ukrainian army was suffering from poor conditions for military service men and inadequate training in 2013, it has become more performant due to years of combat experience in the Eastern Donbas. Moreover, several NATO countries have provided the Ukrainian army with military trainers and non-lethal military supplies (Davis, 2016). While the West decided not to intervene militarily in 2022,[4] they have, however, played an important role in increasing Ukrainian resistance through numerous arms deliveries, making the difference on the battlefield. It was mainly anti-tank weapons (such as the Javelin, the AT-4 and the NLAW) and anti-aircraft systems (such as the Stinger missile and Starstreak missile system) which inflicted significant losses on the Russian army. The EU even unanimously agreed on a €1bn fund to finance the delivery of arms and equipment to Ukraine (European Commission, 2022). In terms of intelligence, the US also provided Ukraine with classified information, which is believed to have helped the Ukrainian military to target and kill several Russian generals (Barnes et al., 2022). As a result, this had a strong impact on the Russian morale and leadership.

Most notably for the conflict, Ukraine turned its civilian support and infrastructure into a strength rather than a vulnerability (i.e. civil-military resilience).

4 Following the immediate Russian declaration that a Western intervention would lead to a disastrous outcome.

While Russia hoped to reach Kyiv swiftly, the city was turned into a stronghold of resistance, bringing the fight to the streets and forcing the Russian army into urban warfare. As shown by King (2021), conquering a city takes time and forces the attacker to engage in a series of 'micro-sieges', as combatants fight for individual buildings, streets and districts. The Ukrainian population strongly contributes to this resistance by cooperating fiercely with its armed forces. Most notably, civilians have engaged in making Molotov cocktails, booby-traps and other military equipment. Important to note, Russia's strategy of encircling major cities has shown the necessity for cities to be prepared to sustain challenging situations over longer periods of time (NATO, 2022), as demonstrated by the lack of food, power and medicines in Kherson.

Finally, the conflict has so far demonstrated Ukraine's capability to deny its competitors the opportunity to unlock civil vulnerabilities (i.e. civilian resilience). The psychological and material preparations that followed the illegal annexation of Crimea in 2014 made the Ukrainian society brace for war, resulting in its peoples being able to bear the brunt of a conventional conflict without collapsing under the military weight of its conventional superior adversary. As the war in Ukraine makes abundantly clear, it is the collective societal state of a Nation that determines its capacity to put up effective resistance in the face of aggression. The Ukrainian population has also demonstrated its resilience in the cyber domain. Over the last years, Ukraine adapted its systems following the numerous cyberattacks it had had to endure. More precisely, the country created numerous back-up systems and increased the number of Internet providers throughout its territory. Moreover, Ukraine was supported by Elon Musk who offered its services by means of its 'Starlink terminals'. This provides a good example of a non-military Western support, enabling Ukraine to gain more strength in the informational domain. Although the above-mentioned examples could be defined as rather 'defensive', Ukraine was even able to launch counter attacks in the digital domain. Already on the 26 February 2022, the Ukrainian Vice Prime Minister, Mykhailo Fedorov, called out to create an 'IT army'. This army is now assessed to consist of thousands of digital talents, organizing cyberattacks on the Russian government, media and financial institutions (Schechner, 2022).

While Russia has a dreaded reputation for launching disinformation campaigns, Ukraine has for the time being also taken a strong stance in the cognitive realm. Throughout the conflict, president Zelensky has been emphasising the difficulties the Russian army is facing, such as the declining motivation of the soldiers, the logistic difficulties in resupplying the Russian army and the large number of casualties (amongst which multiple generals) it was suffering. The narrative put forward is clear: Ukraine will sell its skin dearly and Russia should better prepare itself for major losses. Ukraine's efforts to provide a counter narrative extend even beyond its own media environment. While Russia is well-known for its 'controlled' media-environment, Ukraine succeeds in reaching the Russian population by launching millions of advertisements, countering Russian psychological operations by overwhelming their websites and flooding their intelligence officers with spam (Harwell and Lerman, 2022).

**The narrative put forward is clear: Ukraine will sell its skin dearly and Russia should better prepare itself for major losses.**

## Conclusions and recommendations

With the conflict in Ukraine, the EU is (for the first time in a long time) being confronted with a major conventional conflict at its Eastern borders. Indeed, the terrible scenes observed, and the confrontation with the humanitarian consequences stemming from the conflict, leave a strong impression. Nevertheless, analysing the current conflict and the way Ukraine resisted to the Russian invasion enables us to draw lessons in the light of the evolving strategic landscape of great power competition. More specifically, this article focuses

on NATO's concept of 'layered resilience', which focuses on the role of civil society and the civilian-military collaboration in increasing a nation's resilience. We draw the following conclusions and related recommendations.

First, the Ukrainian-Russian conflict demonstrates the need to invest in logistic stocks: food, medicine, ammunition or weapons. The parallel with strategic stocks of mouth masks and medical supplies during the Covid crisis is certainly valid. Finland provides a good example in this respect, as the country has strategic stockpiles containing 6 months-worth of all major fuels, grains, and 3-10 months' worth of medical drugs (Milne, 2022). Moreover, nations need to think about plans and transport lines to ensure the supply of resources needed to resist and fight over a long period. The tons of ammunition and weapons sent to Ukraine perfectly illustrate the means needed to wage a conventional conflict over longer periods of time. Therefore, the crisis also provided a good stress test for NATO nations, which suddenly had to gather and ship ammunition and weapons to Ukraine at a rapid pace. From the Alliance's perspective, contingency plans need to be drafted, allowing re-supplies from diverse neighbouring countries and other partner nations, taking a wide array of scenarios into consideration (disruption of supply lines, degraded ground infrastructure, contested airspace etc.). Indeed, this conflict has demonstrated how a rapid and strong support of one country in need by the others can lead to decisive outcomes, i.e. not succumbing to a surprise attack but being able to slow down the enemy by means of fierce resistance.

Second, the conflict demonstrates the necessity of quickly being able to absorb shocks and to provide early resistance during the initial phase of a conflict. A country's combat potential can be raised in multiple ways, both in quality and in quantity. First, the military assistance the Ukrainian army received after 2014 certainly enhanced the quality of the official Ukrainian armed forces, allowing them to inflict damages to the Russian army consisting of a large number of young and inexperienced soldiers. Second, a country can raise its combatants by investing more in operational reservists. Training reservists has the advantage of sparing costs, to contribute to the 'Whole of Governance Approach' (since these persons are also working in other civilian sectors but learn to think how to enhance national security). We again refer to Finland as a proper example. As a country of only 5.5 million people, it is capable of augmenting its 280.000 men army with 900.000 reservists. Moreover, National Defence courses are organized annually, teaching politicians and business leaders which role they can fulfil during a wide range of crises (Milne, 2022). Importantly, training reservists does not only serve the purpose of increasing a country's capacity to deliver kinetic effects. As seen during the Ukrainian-Russian conflict, the 'IT-army' can also add strong value and inflict considerable damages.[5] In addition, the enhanced civilian-military cooperation with the industrial sector could allow the accelerated production of goods needed during a crisis, such as body armour. ■

5 The Military Intelligence apparatus could for example train people working in the ITsector how to conduct cyberattacks or teach how to better protect the industrial sector against cyberattacks, increasing civilian resilience.

## About the authors:

**Pieter Balcaen** is an Officer in the Belgian Military. Academically, he holds masters' degrees in Social and Military Sciences (Royal Military Academy), Economics (Ghent University) and Advanced Studies in Economics (Catholic University of Leuven). He has a PhD in Defencse Economics (Free University of Brussels and Royal Military Academy). His research focuses on Hybrid Threats and Resilience.

**Arthur de Liedekerke** is a Project Manager at political advisory Rasmussen Global and a non-resident fellow at the Institute for Security Policy at Kiel University (ISPK), Germany. He has previous experience advising senior officials in the French Ministry for the Armed Forces and the institutions of the European Union (Commission and Parliament) on security and defencse matters. He holds two masters' degrees – in international relations from the University of Maastricht and in geopolitics from King's College London.

**Kamil Mikulski** is a senior hybrid threats and disinformation analyst at the Kosciuszko Institute, and a PhD student in strategic communication against hybrid threats at the Rey Juan Carlos University. He advises within the EU Commission Expert Group on Tackling Disinformation and Promoting Media Competences through Education and Training. Furthermore, he is a fellow of NATO StratCom CoE, the Center for European Policy Analysis, and an alumnus of the Visegrad School of Political Studies' s United 4 News: Building Democratic Resilience against Disinformation programme. Academically, Kamil holds an advanced M.A. in EU International Relations and Diplomacy Studies from the College of Europe, and an L.LM from the Wroclaw University.

**Maarten Toelen** is a strategy consultant for the public sector at Gartner, with previous experience in the Cyber and Hybrid Threats Working Parties of the Council of the EU and PwC's Crisis Management and Resilience Practice. Furthermore, he is an active reserve officer in the Ministry of Defence dealing with NATO/EU matters. Academically, Maarten holds an LL.M. in European Law from Leiden University, a Master MA in EU External Relations & Security Policy from the Vrije Universiteit Brussel (VUB) and a MAaster in International Security & Contemporary War from King's College London.

# References


Barnes, Julian E., Cooper, H. & Schmitt, E. 2022. U.S. Intelligence Is Helping Ukraine Kill Russian Generals, Officials Say. *The New York Times*. Accessed on 05 May 2022 on https://www.nytimes.com/2022/05/04/us/politics/russia-generals-killed-ukraine.html

Davis, Christopher M. 2016. The Ukraine conflict, economic-military power balances and economic sanctions. *Post-Communist Economics*, *28* (2), pp. 167-198.

European Commission. 2022. Speech by Commissioner Gentiloni hosted by the University of Oxford: Turning point: the implications of Putin's war for Europe's economic and political choices. *European Commission*. Accessed 23 March 2022 on https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_1969

Evans, Michael. 2022. Ukraine scuttles its flagship frigate as Russians close in. *The New York Times*. Accessed on 06 May 2022. https://www.thetimes.co.uk/article/ukraine-scuttles-its-flagship-frigate-as-the-russians-close-in-wtd07bbqp

Freedman, Lawrence. 2017. *The Future of Warfare: A History*. New York: Hachette Book Group.

HCSS. 2020. The NATO warfighting capstone concept. Key insights from the global expert symposium summer 2020. *The Hague Center for Strategic Studies*. Accessed on 01 May 2022. https://hcss.nl/report/nato-warfighting-capstone-concept-key-insights-from-the-global-expert-symposium/

Harwell, Drew & Lerman, Rachel. 2022. How Ukrainians have used social media to humiliate the Russians and rally the world. *The Washington Post*. Accessed on 02 May 2022 on https://www.washingtonpost.com/technology/2022/03/01/social-media-ukraine-russia/

IISS. 2022. The Military Balance 2022. *International Institute for Strategic Studies*. Accessed on 23 March 2022. www.iiss.org

King, Anthony. 2021. Urban Warfare. Polity. 288 pg.

Leonard, Mark et al. 2016. Connectivity wars. Why Migration, Finance and Trade are the Geo-Economic Battlegrounds of the Future. *European Council on Foreign Relations*. Accessed 20 March 2022. https://ecfr.eu/archive/page/-/Connectivity_Wars.pdf

NATO. 2020. "Resilience and Article 3." Accessed 21 March 2022. https://www.nato.int/cps/en/natohq/topics_132722.htm

NATO. 2021. NATO's Warfighting Capstone Concept: anticipating the changing character of war. Accessed on 28 March 2022 on https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html

Milne, Richard. 2022. War with Russia? Finland has a plan for that. *The Financial Times*. Accessed 30 March 2022. War with Russia? Finland has a plan for that | Financial Times (ft.com)

Schechner, Sam. 2022. Ukraine's 'IT Army' Has Hundreds of Thousands of Hackers, Kyiv Says. *The Wall Street Journal*. Accessed 24 March 2022. https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX

OPINION

# Gender and Cyber Resilience: Challenging Assumptions and Broadening Commitments

ESTHER NAYLOR

FORMER RESEARCH ANALYST, INTERNATIONAL SECURITY PROGRAMME, THE ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS, CHATHAM HOUSE

AMRIT SWALI

PROJECT COORDINATOR, INTERNATIONAL SECURITY PROGRAMME, THE ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS, CHATHAM HOUSE

ISABELLA WILKINSON

RESEARCH ASSOCIATE, INTERNATIONAL SECURITY PROGRAMME, THE ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS, CHATHAM HOUSE

**ABSTRACT:**

**An intersectional, gendered approach is integral to a whole-of-society approach to enhancing cyber resilience. Cyberspace amplifies offline gender norms and ingrained biases impact whole-of-society cyber resilience. First, this article explains why gender should be at the heart of human-centric cyber resilience, diagnosing reductionist approaches that focus on victimhood and 'women' as synonymous with gender. Then, this article proposes key principles for integrating intersectional, nuanced, sensitive and appropriate gender considerations into national cybersecurity strategies.**

**Keywords: gender, cybersecurity, online harms, intersectional feminism, cyber resilience.**

## Introduction

It is a misnomer that technology is simply 1s and 0s, and that the technological tools that people use in their daily lives are neutral. Much like the offline world, the 'online' world is far from a neutral space: the very inequalities and biases that have existed before the advent of cyberspace and technology are embedded into the very ways they are governed. In particular, offline gender bias and stereotypes can be amplified in cyberspace: for example, the assumptions that all hackers are young boys in hoodies and that all cyber and information security professionals are men, or that the only policy priority for gender and cyberspace is addressing gender-based violence online.

As more and more countries define their cybersecurity strategies and improve their national cyber resilience to serious threats in cyberspace, understanding the field's gender considerations in a holistic and comprehensive manner is an urgent priority. In this article, the authors define gender considerations as a systematic and comprehensive attempt to understand the way in which gendered experiences inform and impact the design, production and implementation of policies and strategies and mitigate biased outcomes and consequences from the outset. If cyberspace is to provide all the benefits of the digital world that it promises, incremental steps towards equality, equity, diversity and inclusion must be done in tandem and meaningfully across domains. We emphasize *national* cyber resilience because cyberspace is neither a monolith nor is it homogenous; it is shaped and informed by the actors, stakeholders, people and realities closest to an individual's social and political ecosystem, thereby mirroring offline contexts and landscapes. Different societies are at different stages along the journey of gender emancipation and inclusive and tolerant societies, which in itself looks different in different contexts. International cyber resilience is dependent on national cyber resilience.

**If cyberspace is to provide all the benefits of the digital world that it promises, incremental steps towards equality, equity, diversity and inclusion must be done in tandem and meaningfully across domains.**

Recognizing the gendered harms of technology is the first of many steps addressing gender inequalities and bias in cyberspace. Expert communities have explored and advocated for the meaningful inclusion and mainstreaming of gender considerations in national and international security for many years – including in cybersecurity strategies and approaches to cyber resilience. However, much of this understanding is rooted in a series of insufficient assumptions about women and cyberspace such as 'gender' referring solely to white, cis women – leading to the exclusion of due considerations of the experiences of people of colour – and the categorization of women as solely victims, denying them agency elsewhere. This ultimately leads to strategies and commitments that pay little more than lip service to incorporating gender considerations into policies and strategies and conceive of gender as just a representation issue.

Important and necessary work has been done to understand gender-based online harms and the experience of marginalized people in cyberspace, but the assumptions above have created a gap in the literature on gender in cyber resilience.[1] Building on the history of scholarship and policy measures which are addressing online

1 Important policy-orientated works on gender, cyber and international security include: https://unidir.org/publication/gender-approaches-cybersecurity; https://www.reachingcriticalwill.org/resources/publications-and-research/publications/14677-why-gender-matters-in-international-cyber-security; https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda. Works on gender and online violence and harm: https://rm.coe.int/gender-mainstreaming-toolkit-15-gender-equality-and-cyber-crime-cybervi/168092e9b4; https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19; https://www.oii.ox.ac.uk/blog/design-ethics-for-gender-based-violence-and-safety-technologies/https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf.

harms faced by women in cyberspace, this article seeks to provide both an overview, direction and guiding principles for taking gender considerations to the next step. This article takes a three-pronged approach to filling this gap. First, the authors explore the concept of a human-centric, whole-of-society approach to cyber resilience – and how gender fits within this framework. Second, the authors problematize existing discourse on gender and cyber, drawing out some common narratives which have been perpetuated in existing literature. Emphasizing the need to ensure that pre-existing assumptions are challenged, and commitments are meaningful, the article's final section outlines three policy recommendations for integrating gender considerations as a central part of a human-centric, whole-of-society approach to improving national cyber resilience.

## Gender and whole-of-society, human-centric approaches to cyber resilience

While there is no single, authoritative definition of cyber resilience, it commonly refers to an organization's ability to prepare for, respond to and recover from cyberattacks and security breaches.[2] Some scholars adopt a broader approach, defining cyber resilience as 'the ability to continuously deliver the intended outcome despite adverse cyber events' (Bjork et al 2015).[3] Embracing cyber resilience (as policymakers, practitioners or scholars) indicates a significant shift in thinking about cybersecurity in terms of *reacting* to threats and *preventing* incidents toward *preparing* for breaches and *mitigating* the impact of the threats themselves. This shift in thinking reflects not only the pervasiveness of threats in the cyber domain, but also the challenges they pose for the people and processes that govern technology, not just the systems behind it.

The Covid-19 pandemic has underlined the importance of focusing on and practicing resilience as businesses and activities globally have overwhelmingly moved online. During this time, countries, businesses and individuals have faced a wave of cyberattacks and an uptake in cybercrime, both increasing in sophistication and scope.[4] In part due to this uptake, some governments have embraced the concept of cyber resilience at the national level. The UK's National Cyber Strategy (released in 2022) contains a whole pillar dedicated to cyber resilience, rooted in understanding the risk, minimizing the impact of, and securing systems to prevent cyberattacks.[5] Another example is Singapore's Cybersecurity Strategy (released in 2021),[6] which contains two strategic pillars on building resilient infrastructure and enabling a safer cyberspace. Both strategic pillars focus on securing systems and networks to reduce threats posed to Singapore's digital infrastructure and economy.

Resilience in cyberspace has traditionally focused on networks, systems and infrastructure, reflecting the primacy of national security and a broadly technical approach to the securitization of assets.[7] However, across organizations and governments, there is a growing recognition that *societal resilience* to cyber threats is an important component of resilience. In a cyberspace that is innately non-neutral and not just technical, societal resilience must be human-centric. *It must centre and protect the needs of the most vulnerable and marginalized if it is to be truly resilient.*

Deibert (2018) defines a human-centric approach to cybersecurity as 'fundamentally [resting] on a political architecture of "distributed security," at the heart of which are institutional mechanisms of power

2 https://www.gov.uk/government/collections/cyber-resilience

3 Björck F., Henkel M., Stirna J., Zdravkovic J. (2015) Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham. https://doi.org/10.1007/978-3-319-16486-1_31

4 INTERPOL report shows alarming rate of cyberattacks during COVID-19

5 National Cyber Strategy 2022 - GOV.UK (www.gov.uk)

6 The Singapore Cybersecurity Strategy 2021 (csa.gov.sg)

7 Dunn Cavelty, M. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Sci Eng Ethics 20, 701–715 (2014)

restraint most often associated with the concept of 'checks and balances.'[8] A system-centric approach to cybersecurity may lead to the assumption that technology itself is the primary security object to be secured or protected; however, a human-centric approach also focuses on individuals as the *users* of technology and prioritizes the protections of their rights and freedoms both offline and online. 'Cybersecurity should not only address the security needs of the state, but also (if not primarily) the needs of people' (Liaropoulos, 2015, 15).[9] A human-centric approach to cyber resilience is one that contains a measured balance of resilient systems, networks, infrastructure, and *people*.

**In a cyberspace that is innately non-neutral and not just technical, societal resilience must be human-centric. It must centre and protect the needs of the most vulnerable and marginalized if it is to be truly resilient.**

A whole-of-society approach is broadly defined as a policy response which meaningfully engages diverse stakeholder groups both horizontally and vertically, and with due consideration for social and cultural norms.[10] These stakeholder groups may be comprised of state and non-state actors, which all have an important role to play in mitigating threats in cyberspace and thus enhancing overall resilience. Security is not confined to the social contract between the state and the individual; the state is not the only actor deciding what needs to be secured. The notion of multi-stakeholderism in cyberspace[11] in itself contains a series of underlying assumptions about the centrality of human rights considerations, and should and may rationally be extended to include gender considerations, many of which are represented by non-state stakeholder groups (such as victims associations or research institutes with programmes focusing on gender and cyber policy issues).

Adopting a human-centric approach to cybersecurity requires actively integrating gender considerations from the get-go, reconceptualizing whole-of-society and human-centric in such a way that the safety, protection and resilience of society's most vulnerable groups are prioritized in a meaningful way. By default, this requires looking beyond gendered impacts and harms, and considering different intersectional identities,[12] too (intersectionality being broadly defined as the recognition that individuals and groups can experience amplified oppression, discrimination and bias as a result of belonging to multiple identity groups).

In practice, this may mean developing and adopting a flexible, dynamic set of gender mainstreaming principles in both policy response and overarching strategy design, which ensure gender is at the heart of whole-of-society cyber resilience. For instance, in *risk assessment* this approach would mean adopting a human-centric lens to gauging and quantifying different risks faced by and vulnerabilities brought by different stakeholders, communities and individuals across society in addition to assessing technical securitization. In assessing cyber risk/s, policymakers would need to adopt an intersectional and holistic approach (i.e. prioritizing reaching a meaningful understanding of potential risks or harms faced by individuals as a result of their belonging to different gender identity groups, for example).

## Problematizing existing discourse on gender and cyber

While research on gender and cyber has proliferated considerably in recent years, several assumptions

8 Deibert, Ronald J. "Toward a human-centric approach to cybersecurity." Ethics & International Affairs 32, no. 4 (2018): 411-424.

9 Liaropoulos, Andrew. "A human-centric approach to cybersecurity: securing the human in the era of cyberphobia." Journal of Information Warfare 14, no. 4 (2015): 15-24.

10 The UK Government's New Cyber Strategy: A Whole of Society Response | Royal United Services Institute (rusi.org)

11 Full article: A multi-stakeholder foundation for peace in cyberspace (tandfonline.com)

12 Intersectionality, explained: meet Kimberlé Crenshaw, who coined the term - Vox

persist at both the policy practitioner level and the academic level, which may lead to the inadequate inclusion of gender considerations and commitments in resilience. These assumptions – which are evident in national security strategies by both their presence and/or lack thereof – can be categorized as follows: the pervasive equation of gender considerations with 'women's considerations' and thus classifying gender considerations predominantly as a representation issue that ignores people who are gender-nonconforming or non-binary and intersectionality; the categorization of women as victims in cyberspace; and finally, the 'male by default' technical and policy approach.

The number of professionals working in cybersecurity who identify as women is low; while conclusive country-relevant studies are not available, it is estimated that in the UK approximately 16% of the cyber workforce are 'female' and only 3% of senior positions are held by women and people from ethnic minorities.[13] In contrast, in some countries the percentage of women in, for example, professional medical careers that require several years of education is nearer 50%.[14] With increasing emphasis on STEM education for young children in school, why does cybersecurity still have a representation problem, and how does this representation issue fare in the non-technical aspects of cyber resilience?

One reason for the lack of diverse representation in cybersecurity could be traditional and pervasive international relations theories (IR) that conceive of security in masculine terms.[15] The masculinity of IR theory has been heavily – and importantly – studied elsewhere, but it is crucial to emphasize that this prevalent masculinity frames matters of security in terms that de-centre human security and individual experience (often at the expense of national security) and works to deter inclusive hiring and engagement. This is problematic because it is not only detached from contemporary or updated thinking on 'security risks' but also misconstrues security priorities and how we should think about cyber resilience in such a digitized age; it conceives of a security that is detached and kept separate or at bay from lived experiences (Young, 2004).[16] Re-framing cybersecurity and cyber resilience as a human-centric problem, rather than a system-, state- and strategy-centric problem, could be one way of inspiring and incentivizing a workforce that is diverse and representative by identifying the individual as the object of protection.

**The number of professionals working in cybersecurity who identify as women is low: while conclusive country-relevant studies are not available, it is estimated that in the UK approximately 16% of the cyber workforce are 'female' and only 3% of senior positions are held by women and people from ethnic minorities.**

This shift could also help in moving away from harmful notions that working towards greater diversity and representation is the job of those already under-represented. Gender, identity security and cybersecurity are intrinsically linked; this connection should be sufficiently represented and respected. Furthermore, outdated assumptions such as the bifurcation or superficial dichotomy created between masculine, technical approaches and feminine, human-centric approaches to securitization and resilience-building must be recognized as being more nuanced than they appear.

13 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

14 https://www.kingsfund.org.uk/projects/time-think-differently/trends-workforce-overview

15 See: Hoffman, J. "Patriarchy, Sovereignty and Realism" in Gender and Sovereignty: Feminism, the State and International Relations, (Palgrave), 2001; Connell, R. W., and James W. Messerschmidt. "Hegemonic Masculinity" Gender & Society, 19.6 (2005), pp. 829–859; Marysia Zalewski on Unsettling IR, Masculinity and Making IR Theory Interesting (Again) (ethz.ch).

16 Young, G. 'Feminist International Relations: a contradiction in terms? Or: why women and gender are essential to understanding the world 'we' live in', International Affairs, 80.1 (2004), pp. 75-87.

These issues are further problematized in how gender considerations are summarized in both international and national cyber policy documents, some of which are considered below. While many strategies, communiques and policies mention gender, most do so with regard to representation only. Very few go into detail about what is meant by 'gender considerations'. Often, the consideration of gender is implied and sometimes explicitly incorporated under the umbrella term of human rights, because gendered rights are and should be human rights. However, the disproportionate discrimination that occurs on the basis of gender warrants particular attention in and of its own accord.

In March 2021, UN member states and non-state stakeholders as part of the UN OEWG agreed to a final report, which reaffirmed the previously agreed upon 11 norms of cyberspace.[17] These 'norms' are non-binding, guiding principles on how states should behave in cyberspace in order to create a stable and secure domain. None of these norms, however, refer explicitly to gender and the OEWG report itself mentioned 'gender' in just two paragraphs: firstly, in recognition of women delegates who participated in the OEWG and the importance of promoting women in leadership, and secondly, in a brief nod to ensuring gender sensitivity in capacity building. The lack of a comprehensive passage on gender considerations – or gender mainstreaming across the report in general – is significant, because the norms and the OEWG final report are two of the most prominent instances of countries agreeing in principle on how to behave and build resilience in cyberspace. They represent a focal point in synthesizing national and international understandings about working towards human-centric, whole-of-society cyber resilience, being developed in consultation with global multi-stakeholders. However, neither the norms nor the final report made any reference to mainstreaming gender beyond simple representation – nor elaborated on precisely what gender considerations are important in developing capacity building programmes. Granted, the UN OEWG's mandate has been renewed for the 2021-2025 period, with new initiatives such as a Programme of Action to assist with norm implementation and thus has potential to elaborate on previously under-explored areas: it has the resources, platforms, networks and political buy-in to make meaningful progress on integrating gender into cyber resilience at the international level, but it is yet to be seen how many and which states participate.

Elsewhere, the UK's National Cyber Security Strategy of 2022 – as aforementioned, a recent example of a comprehensive approach to cyber resilience – refers to gender or women just four times in a 130-page document; this is in spite of a welcome recognition of the importance of considering gender equality in the 'design, development and use of cyberspace', and a commitment to increasing the number of women in the cyber workforce.[18] The strategy also referred to the 'shadow pandemic of gender-based violence' as one of the cyber threats the UK faces. Again, while this was a welcome recognition, it falls short of a comprehensive assessment of the unique gender dynamics that are exhibited in cyberspace and manifest themselves in cyber resilience. If building cyber resilience is a whole-of-society responsibility, then policymakers and policy communicators are tasked with the important work of adding substance to their commitments to making cyberspace a safe space for people of all gender identities.

Adding substance to gender commitments means several things. It means directly referring to people who identify as part of the LGBTQIA+ community, people who are non-binary or gender-nonconforming, and people who have intersecting protected characteristics that make them more vulnerable in cyberspace. It means recognizing, preventing and breaking the biases and stereotypes that are amplified by data and in technology. It means expressing and embedding meaningful awareness

17 https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

18 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

of the unique systemic barriers that vulnerable groups face when it comes to access to justice or victim support. It means committing publicly to better understand the way cultural behaviours and gendered power hierarchies manifest themselves in policies and in implementation. Commitments to 'gender considerations' or 'gender sensitivity' are important. At the international level, commitments from several delegations to the OEWG process and in the recent ad-hoc committee process to develop a convention on cybercrime were notable and welcome, However, these commitments do little to advance mitigation of gender bias in cyberspace if they are not accompanied by concrete plans of action, or treating these as substantial and intricate issues in the very first instance.

Much important work has been done to address the unique online harms faced by women in cyberspace, including by the Council of Europe, UNIDIR and in the UK's upcoming Online Safety Bill, where violations such as 'cyber-flashing' are due to be criminalized.[19] Recognizing new forms of harms is vital, as increased awareness of the unique harms that people who identify as women, non-binary or gender-non-conforming experience is the only way to ensure that cyber resilience centres the most vulnerable in our societies. But victimization in cyberspace is not exclusive to women. It is important to recognize that anyone – regardless of their gender identity – can be a victim in cyberspace. Furthermore, proposed initiatives to address online harms must adhere to international human rights standards, rather than allowing crimes (gender-based or otherwise) to be politically-determined As such, categorizing *just* women as *just/nothing more than* victims in cyberspace not only reduces their role and agency in creating a more resilient and secure cyberspace, but also ignores the unique risks that cyberspace can pose to all.

**Victimization in cyberspace is not exclusive to women. It is important to recognize that anyone – regardless of their gender identity – can be a victim in cyberspace.**

19 https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women; https://www.bbc.co.uk/news/technology-60750463

A further problematic trope in discourse is the synonymizing of gender with women and the subconscious conceptualizing of women as white and cis. This is particularly emphasized by the 'male-by-default' dynamic which, in reality, is not just 'male' but 'white, cis male'. 'Male-by-default' design has been explored extensively elsewhere, but largely draws from the androcentric school of thought, where the needs of (white) men are centred and prioritized (Perez, 2019).[20]

Multistakeholderism in cyber resilience is not just about advocacy and representation; industry is key in the implementation of these strategies. The cybersecurity industry suffers from a 'male by default' problem that is pervasive across its technical and policy layers. From the physical design of devices to the algorithms behind platforms and applications, technology reflects and amplifies the bias and values of the engineers behind it. This leads to a bias in cybersecurity that continues to favour those who have been historically favoured. As Millar et al explain: '[T]echnology design is gendered: it misunderstands, omits and consolidates certain gendered uses. Cybersecurity design inherits these issues', amplifying gender bias (such as privileging masculine and patriarchal practices and behaviours) in security, threat models and user-control protocols (Millar et al, 2021).[21]

On the policy side, a 'male by default' bias complicates a whole-of-society approach to cyber resilience, as the actors involved in delivery or implementation and the primary users, recipients or targets of cybersecurity or policy responses may embody gender bias. This can be seen through the initiatives that seek to increase the number of women in STEM that are designed to be successful in privileged educational establishments and are ill-equipped to replicate these successes in less privileged schools and institutes, which ultimately perpetuates elitist

20 Caroline Criado Perez, Invisible Women: Exposing Data Bias in a World Designed for Men, 2019; Also see Tickner, J. A. Gender in International Relations: feminist perspectives on achieving global security (New York, Columbia University Press), 1992.

21 Gender Approaches to Cybersecurity | UNIDIR

recruitment rather than socio-economically diverse recruitment.[22] It is also seen in the design of critical national infrastructure (CNI) in the health services, for example, where technological medical equipment is less effective at detecting problems in people of colour.[23] These biases create technology-based systems and structures that reinforce power hierarchies that prioritise the needs of one group above others, essentially contributing to ineffective policy solutions, informing a type of ineffective or inequitable cyber resilience.

Understanding and identifying the nuances of these assumptions and how to overcome them is key to ensuring the meaningful inclusion of gender considerations in approaches to cyber resilience. Assumptions must be challenged about gender and cyber that conceive of diversity as solely a representation issue, synonymize gender with women, discard intersectionality, categorize women as victims in cyberspace and do little to dismantle male-by-default technology and policies.

## Guiding Principles: Gender and Cyber Resilience

This article concludes with three guiding principles for challenging assumptions and meaningfully embedding gender considerations into cyber resilience on a national strategy level.

In national strategies, 'gender considerations' should go beyond the issue of 'women and representation' and prioritize a deeper understanding of local social norms and conceptions of gender and how that can be manifested in cyberspace. This means that when conceptualizing cyber threats, policymakers should consider the various ways in which cyberspace and the people that use and govern cyberspace are working towards the shared goal of security: security should not privilege some users and interests over others. Policymakers should be encouraged to consider more deeply and substantively what precisely they mean by 'gender considerations' and how precisely they are going to commit to addressing gender concerns in cyberspace.

National strategies for cyber resilience must empower decision makers and relevant stakeholders to identify what the gendered impacts of cyber technology are on various social groups and how their needs should be safeguarded accordingly. Impacts and consequences should be considered from an intersectional angle – if policies and responses do not centre or validate the online experiences of the most vulnerable in society, they are failing. One of the ways in which policymakers can address this is by understanding the risk landscape and how these risks impact different groups of people. Evaluating the effectiveness of cyber policy interventions and adapting the strategy on a recurring basis will allow policymakers to work towards a more resilient cyberspace for all.

Finally, a strong strategy for cyber resilience should recognize that it sits alongside various other government priorities and strategies and should, therefore, complement human rights obligations and pre-existing commitments to gender equality. As policy is playing catch up to the adoption and development of technology, and the boundaries between the offline and online space continue to blur, it is only prescient that strategies reaffirm existing commitments to human rights and work both within and outside of existing commitments to strengthen the case for meaningfully embedding gender considerations into cyber resilience.

We are all stakeholders in the future of cyberspace. Building an inclusive, safe, open cyberspace for all is a strategic priority; integrating gender considerations into cyber resilience is all the more urgent as the cyber threat landscape evolves. This can only be done by rethinking and challenging assumptions and the substance of gender-based commitments. ■

22 An initiative that seeks to address this issue specifically is #ShareTheMicInCyber, which aims to amplify and promote the stories of Black Practitioners in the cyber field. https://www.sharethemicincyber.com/

23 https://www.theguardian.com/society/2021/nov/21/from-oximeters-to-ai-where-bias-in-medical-devices-may-lurk; https://www.wired.com/story/how-algorithm-favored-whites-over-blacks-health-care/.

## About the authors:

**Esther Naylor** is a former research analyst in the International Security Programme at Chatham House. Her main research focus is cyber policy which covers cyber security within international security, cyber capacity building, data security and governance, and cyber diplomacy.
Esther also works on the Journal of Cyber Policy, which is published by the programme and places a strong emphasis on topics that are international in scope and can address national and international cyber policy challenges.
She obtained her masters degree in Security and International Law from the University of Manchester, and received her bachelors degree in International Relations and French from the University of Birmingham.

**Amrit Swali** is a project coordinator in the International Security Programme, working on various cyber policy projects, and on the editorial team of the Journal of Cyber Policy. She co-hosts Undercurrents, the Chatham House podcast, and is the co-chair for gender on Chatham House's EDI Working Group.
She holds an MSc in the History of International Relations from the London School of Economics and Political Science, and a BA in History from the University of Southampton.

**Isabella Wilkinson** is a research associate in the International Security programme at Chatham House, specializing in cyber policy, including cyber diplomacy and capacity-building, countering cybercrime, and digital transformation, and is also part of the editorial team for the Journal of Cyber Policy.
Previously Isabella was a policy and research associate at the Portulans Institute in Washington D.C., covering technology competitiveness and innovation readiness, in addition to working with the Network Readiness Index and Global Innovation Index.
Working at the intersection of technology and future-ready governance, Isabella has gained international experience at various research institutes and non-profits, and often provides briefings and comments on modernising electoral policy.
Isabella has a master's degree in Democracy and Governance at Georgetown University, where she focused on digital disruptions to political systems. She has a bachelor's degree from the London School of Economics and Political Science.

ANALYSIS

# Four Foundations for Achieving a Successful Cyber Risk Management Program

ADAM PALMER
CHIEF INFORMATION SECURITY OFFICER (CISO), FIRST HAWAIIAN BANK; EXPERT OF THE KOŚCIUSZKO INSTITUTE
JOHN MORGAN SALOMON
INFORMATION SECURITY ADVISOR AND LEADER

The basis of strong cybersecurity is risk management – the identification, analysis, avoidance, reduction, and mitigation of risk. In the past, many cybersecurity programs focused solely on technical operations. However, cyber risk management has become a more quantifiable and critical component of security governance. It is now the 'compass' that guides a security program. Even more encouraging, cyber risk management is now recognized as an integral factor in overall enterprise risk strategy, receiving increasing executive attention.

Cyber risk management sets the organization's security strategy by identifying risk, prioritizing risk, and reporting on the effectiveness of the security team's efforts to reduce risk. Modern approaches to cybersecurity risk management now rely on detailed frameworks and risk measurement tools. However, despite improvements in these practices, key elements of building an effective cyber risk management program may still be confusing. Large organizations face uncertainty as to how to assign 'responsible/

accountable' risk roles internally. Some organizations also continue to struggle with how to prioritize security activities and then assess the measurable success of those activities in reducing risk.

This article addresses these concerns and outlines four 'foundational' elements for a successful cyber risk management program that will help support a strong overall cybersecurity plan.

Risk management is a *positive and constructive* function. Rather than seeing risk management as an 'obstacle', consider that identifying risk is a positive opportunity. It is an opportunity for the organization to mitigate security gaps, learn about key risks, and prevent harm to the enterprise.

## Foundation 1: Identify Clear Roles and Responsibilities for Managing Cyber Risk

Cyber risk management should be part of an overarching enterprise-wide risk management program. Defining specific roles and responsibilities to accomplish this objective, however, can be a challenge. Variations on oversight structure may depend on an entity's size and needs. Creating an agreed upon RACI (Responsible, Accountable, Consulted, Informed) matrix is an important step that will help meet an organization's specific requirements. This should be done early in a security program development process to avoid duplication of functions or confusion of roles.

The US Federal Financial Institutions Examination Council (FFIEC) provides some limited guidance on specific responsibilities within a cyber risk program. However, the FFIEC guidelines are broad and do not clearly define the roles across the three lines of the defence risk management model. The CISO function is one of the only areas specifically outlined by the FFIEC as:

*'The board should delegate responsibility to the CISO or other appropriate personnel for assessing whether IT operations conform with policies. The CISO should ensure appropriate consideration of risks involved with new products, emerging technologies, and information systems.'* [1]

1 See Management Examination Guidebook, Federal Financial Institutions Examination Council (Nov. 2015)

The exact structure of a cyber risk organization, including authority, size, etc. is based on a number of factors that vary depending on the organization. The Information Systems Audit and Control Association (ISACA) provides guidance on functional roles for security, risk and audit functions.[2] At a more strategic level, board and senior management accountability for cybersecurity risk is generally guided by an evolving body of best practices, such as those outlined in the US National Association of Corporate Director's (NACD) Handbook on Cyber Risk Oversight.[3]

Reviewing, and clearly defining, roles and responsibilities across the security, audit, risk management, and senior executive level, should be an early step in the cybersecurity risk management planning process. Organizing this early supports successful collaboration and avoids confusion, especially within larger organizations.

**Cyber risk management should be part of an overarching enterprise-wide risk management program. Defining specific roles and responsibilities to accomplish this objective, however, can be a challenge.**

## Foundation 2: Map Cyber Risk Management to an Enterprise-wide Standardized Framework

Cyber risk is a relatively new risk domain. However, cyber risk is no longer just a set of technical capabilities and controls designed for protecting an organization. Cyber risk management has evolved in terms of understanding where it fits into the overall business. Frameworks and standards such as ISO 27002, NIST 800-53, and the NIST Cybersecurity Framework, provide a detailed and predictable basis for cyber risk management. The choice of framework may depend on unique needs of an organization, but efforts should be made to take a consistent holistic approach.

2 See https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance

3See generally the National Association of Corporate Directors Handbook (Feb. 2020)

Alignment to a standardized risk management framework, across the organization, ensures that the capability is based on accepted, proven good practices. A framework may need adaptation to fit an organizations unique size and needs; adaptation and flexibility are helpful approaches to security. An excessive 'cafeteria' style approach, however, may defeat the goal of using a standardized framework. Avoid a patchwork approach to risk management as much as possible. Leverage the consistency of a framework, with some flexibility, for best results.

## Foundation 3: You can only protect what you can see

What assets are part of the security program? Who owns them? What is their value? 'Assets' may refer to information, infrastructure components, people, and processes – anything of value to the organization. Before creating a proper risk management program, it is necessary to define what an 'asset' is and have a clear system for describing the value to the organization. How these values are assigned depends on each organization – its type of activity, the potential impact of the asset's loss or degradation on its ability to perform that activity, etc. The only rule is – the method of assigning value ratings must be rational and consistent.

Once an asset inventory identification, tracking, and evaluation mechanism is approved by leadership, it is critical to identify a 'business owner' (i.e., a person or function who has the authority and competence to be accountable for the asset and its impact on continued operation). This sounds simple in theory, but can be tricky – how are assets identified and tracked? How are changes handled? With what frequency are they reviewed? And most importantly, who are the business owners and what are their responsibilities? Various tools are now available for discovery of assets, both internal and external to the traditional security perimeter. At its simplest, asset discovery and tracking can be a manual process, linked to purchasing, tech support, or human resources. Alternatively, asset discovery may be done using a specific software or service tasked with IT asset identification. Even vulnerability scanning can help support this.

Clearly establishing a reliable asset inventory, assigning values for assets, and have a 'data ledger' of the information contained on, or managed, by each asset, is critical to effectively prioritizing risk management activities. The classic vulnerability approach is that 'you can only protect what you can see,' Therefore, having visibility and good awareness of assets is indispensable for strong cybersecurity risk management. As cloud infrastructure expands, good visibility should also extend to all cloud data-based data and resources.

## Foundation 4: Align Cyber Risk Management with other Business Reporting Metrics

The biggest risk to organizations is sometimes stated as 'how you measure risk'. Effective cyber risk management should apply methodologies that are similar to other types of business risk analysis. Quantifiable metrics should be preferred as much as possible over qualitative reporting. As an example, rather than using ambiguous 'heat maps' for cyber risk reporting, there may be use of statistically sound metrics to evaluate the probability of risks when there is limited data available. Tools such as FAIR, Monte Carlo Scenarios, and the ORX risk taxonomy help organizations to measure and report risk effectively. Using a rating mechanism such as 'CIA123' or Red – Amber – Green ('RAG') scores offers little value unless supported by clear and systematic underlying criteria that can support business decisions. Communicate in objective, quantifiable terms that business leaders can understand.

A key part of the risk management process should also be the development of cyber risk profiles for each business unit. This may include taking account of cyber risks that have a material impact to business processes, interdependent processes, IT stack components, and critical dependencies on third parties. Cyber risk profiles serve as a vehicle to regularly inform business and IT leaders of business-process-specific impacts, assess material risk propagation to/from critical dependencies, and enable more effective risk remediation and investment prioritization.

It is hard to prioritize remediation efforts without using a unifying business-focused language. Address this concern with a cyber risk quantification program designed to describe cyber risk in quantifiable terms that help business executives make informed decisions. Align cyber risk management reporting with

other similar business reporting methods. And finally, maintain updated risk profiles for business units.

**The classic vulnerability approach is that 'you can only protect what you can see'. Therefore, having visibility and good awareness of assets is indispensable for strong cybersecurity risk management. As cloud infrastructure expands, good visibility should also extend to all cloud data-based data and resources.**

### Conclusion:

Implementing strong risk management practices is an important part of successfully building an overall cybersecurity program. Rather than building generic security capabilities because they seem like a good idea at the time, organizations should rely on effective cyber risk management to prioritize those areas that require the most attention and provide the most value for risk reduction.

Effective cyber risk management practices guide the entire cybersecurity program to identify security gaps and achieve success. If an organization has a clear understanding of the foundational elements of risk management such as ownership (who), assets/scope (what), measurement and reporting (how), and business context (why), there is a good foundation for establishing a dependable, consistent, and sustainable risk management capability. ■

## About the authors:

**Adam Palmer,** CISSP, JD, MBA, is an Expert of the Kosciuszko Institute, Poland. Adam is a former U.S. Navy Officer and previously led the United Nations Global Program against Cybercrime. Adam is currently based in Hawaii where is he is the Chief Information Security Officer (CISO) at First Hawaiian Bank.

**John Salomon** is an information security and cyber risk management professional with 25 years of worldwide experience in financial services, healthcare, and other critical infrastructure sectors. John has an extensive security technology, risk management, and leadership background. He is based in Spain, and currently coordinates the activities of FS-ISAC in continental Europe, the Middle East, and Africa.

# 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:

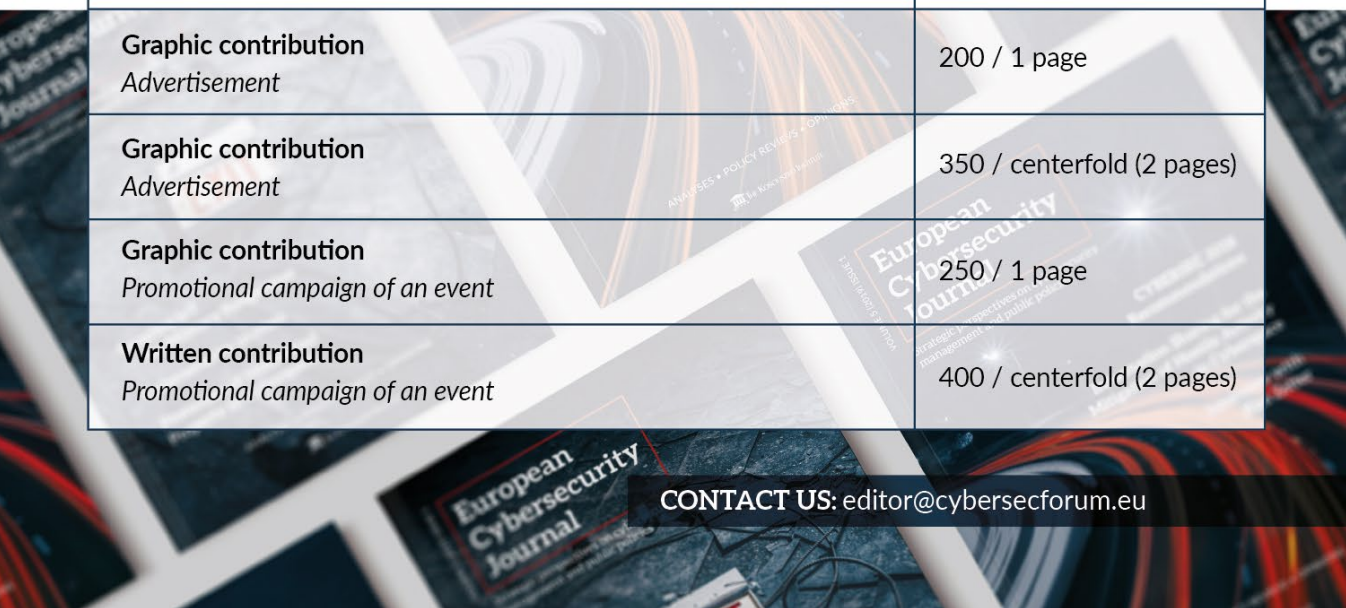
- Policy review / analysis / opinion – a Partner's article or a series of articles on crucial issues related to cybersecurity;
- Interview with Partner's representative;
- Research outcomes and recommendations;
- Advertisement of a firm, product or an event (graphical);
- Promotional materials regarding 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**<br>*Analyses, Opinions, Policy Reviews, Interviews, Research Outcomes* | 100 / 1 page |
| **Graphic contribution**<br>*Advertisement* | 200 / 1 page |
| **Graphic contribution**<br>*Advertisement* | 350 / centerfold (2 pages) |
| **Graphic contribution**<br>*Promotional campaign of an event* | 250 / 1 page |
| **Written contribution**<br>*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**