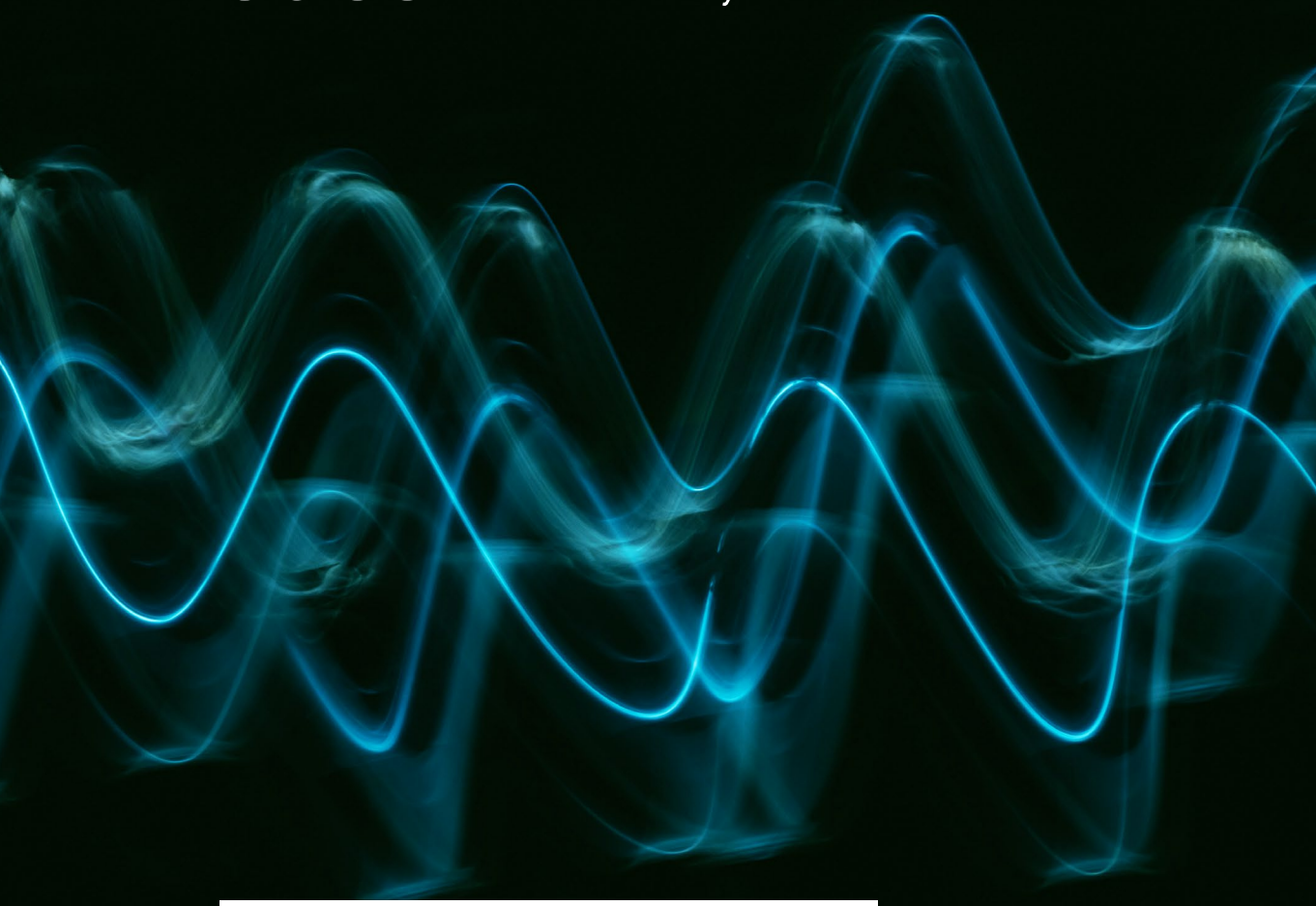
euiss European Union Institute for Security Studies



A LANGUAGE OF POWER?

Cyber defence in the European Union

Edited by
Patryk Pawlak and François Delerue

With contributions from
Hans Boddens Hosang, Raluca Csernatoni, Paul A.L. Ducheine, Aude Géry, Laurent Gisel, Mika Kerttunen, Kubo Mačák, Antonio Missiroli, Peter B.M.J. Pijpers, Matthias Schulze, Eneken Tikk

The EUISS is an agency of the European Union

CHAILLOT PAPER / 176
November 2022

European Union Institute for Security Studies (EUISS)

100, avenue de Suffren
75015 Paris

http://www.iss.europa.eu
Director: Gustav Lindstrom

print	ISBN 978-92-9462-143-6	online	ISBN 978-92-9462-142-9
	CATALOGUE NUMBER QN-AA-22-004-EN-C		CATALOGUE NUMBER QN-AA-22-004-EN-N
	ISSN 1017-7566		ISSN 1683-4917
	DOI 10.2815/067862		DOI 10.2815/57567

Published by the EU Institute for Security Studies and printed in Belgium by Bietlot.
Luxembourg: Publications Office of the European Union, 2022.
Cover image credit: Pawel Czerwinski/Unsplash

European Union
Institute for Security Studies

A LANGUAGE OF POWER?

Cyber defence in the European Union

Edited by
Patryk Pawlak and François Delerue

With contributions from
Hans Boddens Hosang, Raluca Csernatoni,
Paul A.L. Ducheine, Aude Géry, Laurent Gisel,
Mika Kerttunen, Kubo Mačák, Antonio Missiroli,
Peter B.M.J. Pijpers, Matthias Schulze, Eneken Tikk

The EUISS is an agency
of the European Union

CHAILLOT PAPER / 176
November 2022

The editors

Patryk Pawlak is the Executive Officer at the EUISS Brussels office, where he is responsible for inter-institutional relations and coordination of cyber-related projects, including the EU Cyber Direct Project.

François Delerue is an Assistant Professor of Law at IE University and a member of the Jean Monnet Centre of Excellence for Law and Automation (Lawtomation).

CONTENTS

EXECUTIVE SUMMARY

A prosperous digital society cannot exist without a cyber defence posture that adequately addresses vulnerabilities resulting from its reliance on technology and internet-based platforms. By 2021, the share of EU households with internet access had risen to 92 %, some 20 percentage points higher than just ten years earlier. High standards of data protection and civil liberties adopted by the EU are a guarantee that European citizens can safeguard their rights online in the same way they do offline. Digital single market rules ensure that European companies compete in a fair manner and provide consumers with the best value for money. According to some studies, the value of digital goods and services produced in the EU could reach over €2.8 trillion by 2030, which is equivalent to nearly 21 % of the EU's current economy.

However, the benefits of the peaceful use of cyberspace can no longer be taken for granted. The risks to the 'European way of digital life' come not only from cybercriminals seeking financial gain. States, too, increasingly use cyber operations to pursue their strategic interests and compete with one another for influence. The costs of such operations to the safety of citizens and the functioning of companies can be extremely high. The absence of a clear accountability mechanism to curb the impunity of states violating international law and limited options to enforce the agreed norms of responsible state behaviour in cyberspace make it necessary for governments to search for alternative policy solutions, including through cyber defence.

With cyberspace becoming a new battlefield and an arena of strategic competition, this *Chaillot Paper* asks how should the EU shape its cyber defence policy so that it contributes to relearning 'the language of power'? What does it mean to speak the 'language of power' in cyberspace? What is – or should be – the role of armed forces in the event of cyber operations with significant effects on home territory and how does this fit with the military's primary mission of defending their own networks, systems and information? And what rules govern military operations involving cyberspace?

This *Chaillot Paper* approaches the study of 'the language of power' as a quasi-linguistic project that helps to understand the history and functions of cyber defence. At the same time, it aims to provide insights into speech, grammar, or vocabulary that shape the field of European cyber defence. Just as studying the evolution of a language and its functions helps us better understand human history and culture, so the investigation of the role of cyber defence as an element of the EU's defence policy gives us a better insight into the evolution of its strategic culture and defence posture.

Overall, different aspects and perspectives presented in this *Chaillot Paper* provide EU decision-makers with elements for designing a comprehensive policy that guides when and how defence forces may resort to cyber operations in a time of conflict, regardless of whether deployed for military operations or to protect civilian infrastructure. Consequently, the focus of the chapters is on the political and strategic level with the aim to identify:

- Shortcomings and gaps in policies and strategies and procedures, especially regarding the place of cyber defence within a broader EU security strategy;
- Possible dilemmas in the decision-making process;
- Key issues for cooperation between the military and the civilian decision-makers; and
- Opportunities for cooperation with NATO and other international partners.

INTRODUCTION

THE ETYMOLOGY OF EUROPEAN CYBER DEFENCE

by
PATRYK PAWLAK

> *Europeans must deal with the world as it is, not as they wish it to be. And that means relearning the language of power and combining the European Union's resources in a way that maximises their geopolitical impact.*
>
> Josep Borrell Fontelles,
> High Representative of the European Union for Foreign Affairs and Security Policy

A prosperous digital society cannot exist without a cyber defence posture that adequately addresses the challenges posed by our reliance on technology and internet-based platforms. But the open and global cyberspace that promotes economic growth and helps to lift millions of people out of poverty is at the same time a source of vulnerability for European societies.

In peacetime, both state and non-state actors resort to cyberspace operations to disrupt the smooth functioning of democratic societies, undermine legitimate governments, collect intelligence, and steal trade secrets or money. Cyber operations against European targets conducted by state proxies and criminal groups operating from China, Russia, North Korea and Iran seriously damage European competitiveness and our societal fabric. Attacks against military targets and defence contractors with the aim of stealing state secrets are also common. So far, hardly any of these operations have reached the threshold of an armed attack, limiting the role of armed forces to pre-empting and deterring malicious cyber activities that could have a significant impact on the proper functioning of our societies. In such cases, cyber defence capabilities are an important component of the full array of tools deployed to defend our interests and values, including through diplomatic, economic or law enforcement channels.

During wartime, malicious actors conduct cyber operations against adversaries to erode their military advantage and reduce their capacity to act in the theatre. Such operations can be of a defensive or offensive nature and are deployed as part of a broader strategic competition across all domains: air, land, sea and space. In 2008, the communication infrastructure in Georgia was shut down ahead of a Russian military offensive on the ground. In 2010, Iran's nuclear programme was seriously compromised by the deployment of the malicious computer worm Stuxnet. More recently, only during the first six months of 2022, Ukraine has experienced 1 350 cyberattacks against its critical infrastructure in addition

to the kinetic attacks conducted by the Russian forces [1].

The EU Policy on Cyber Defence presented in November 2022 represents the first comprehensive effort by the European Union to outline its strategic, policy and operational goals in cyber defence. Shaped primarily by the military conflict in Ukraine and strategic competition from other major international players, the document aims to allow the EU and its Member States 'to act with self-assurance and assertiveness in cyberspace' [2]. The primary goal of the EU's cyber defence policy is therefore to enhance the EU's ability 'to prevent, detect, deter and defend against cyberattacks aimed at the EU and its Member States using all means available' [3]. Organised around four key pillars – civil-military cooperation, resilience of the defence ecosystem, developing cyber defence capabilities and partnerships – the document sets out many ambitious objectives like the creation of the EU Cyber Defence Coordination Centre (EUCDCC) or developing recommendations on EU cyber defence interoperability requirements. But it also leaves several important questions unanswered, especially regarding how some of the proposed instruments – such as active cyber defence – relate to existing international law or norms of responsible state behaviour in cyberspace. While the document calls out authoritarian regimes for attempting to challenge and undermine the rules-based international order in cyberspace, it does not mention at all the EU's own commitment to the framework of responsible state behaviour in cyberspace.

With cyberspace becoming a new battlefield and an arena of strategic competition, how should the EU shape its cyber defence policy so that it contributes to relearning 'the language of power'? What does it mean to speak the 'language of power' in cyberspace? What is – or should be – the role of armed forces in the event of cyber operations with significant effects at home and how does this fit with the primary mission of defending their own networks, systems and information? And what rules govern military operations involving cyberspace?

CYBER DEFENCE IN THE EU'S LANGUAGE OF POWER

Although most states face a similar challenge of how to respond to the growing intensity and complexity of campaigns by adversarial states and their proxies, the responses developed by individual governments differ and are very much rooted in history and national context. Russia's cyber posture is dictated by its mistrust towards the West which it views as continuously interfering in Russia's 'sphere of influence'. Therefore, cyberwarfare – or information-technological warfare – is an element of information confrontation that aims to ensure superiority in the information sphere [4]. Like Russia, Chinese doctrine locates cyber within the larger operational concept of information operations (IO), which also

(1) State Service of Special Communications and Information Protection of Ukraine, 'War in Ukraine: Pulse of Cyber Defence', June 2022 (https://mcusercontent.com/95750673b8ed58984406ae56e/files/156f7c7b-aa24-818a-ae88-6f77773a5c39/SSSCIP_Weekly_Digest_2022_06_ENG.pdf).

(2) European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, 'EU Policy on Cyber Defence', Join(2022) 49 final, 10 November 2022 (https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf).

(3) Ibid.

(4) The Russian Doctrine of Information Security of 2016 defines the information sphere as 'a combination of information, informatisation objects, information systems and websites within the information and telecommunication network of the Internet (…) communication networks, information technologies, entities involved in generating and processing information, developing and using the above technologies and ensuring information security, as well as a set of mechanisms regulating social relations in the sphere'. See: Hakala, J. and Melnychuk, J., *Russia's strategy in cyberspace*, NATO Strategic Communications Centre of Excellence, June 2021.

includes electronic, space, and psychological warfare [5]. The 2015 Ministry of National Defence paper 'China's Military Strategy' defines as a goal 'winning informationalised local wars' and the People's Liberation Army (PLA) views cyber means as an elemental feature of 'informatised' wars, in which information is both 'a domain in which war occurs' and 'the central means to wage military conflict. [6]' To respond to activities like cyber espionage or attacks below the threshold of armed conflict, the United States has adopted a two-pronged approach that allows the conduct of cyberspace operations to collect intelligence and develop military cyber capabilities to be used in the event of conflict ('persistent engagement') and to disrupt or halt malicious cyber activity at its source ('defend forward') [7]. Accordingly, the Department of Defense seeks to 'pre-empt, defeat, or deter malicious cyber activity targeting US critical infrastructure that could cause a significant cyber incident'. But there are also countries that have adopted a less militarised approach to cyber defence. Japan, for instance, focuses on resilience and non-engagement even though in March 2022 its Self-Defence Forces launched a cyber-defence unit that will centralise cyber countermeasures and combine cyber departments that up to now were dispersed among the ground, maritime and air self-defence forces.

As in the case of individual countries, the evolution of the European Union's cyber posture – including cyber defence – is closely linked to its security environment and the contribution it wishes to make as a global foreign policy and security actor. This orientation is reflected in strategic policy documents, consecutive cybersecurity strategies and specific cyber defence policy frameworks.

At the **strategic level**, the EU's approach has evolved from one focused on threats to one focused on threat actors and competitors. The Strategic Compass adopted by the EU in March 2022 recognises that 'cyberspace has become a field for strategic competition' and a 'contested domain' where state behaviour is driven by historical rights and zones of influence rather than according to internationally agreed rules [8]. It reflects a more state-centric approach to international security compared to the EU Global Strategy of 2016 [9] which defined the challenges in cyberspace in more abstract terms as threatening the EU's security, democracy and prosperity. Consequently, the EU Global Strategy prioritised equipping the EU and assisting Member States in protecting themselves against cyber threats, including through strengthening their technological capabilities, and the Union becoming a 'forward-looking cyber player' protecting its critical assets and values in the digital world. The EU cyber posture outlined in the Strategic Compass takes a more defence-centric turn with the aim to make the EU 'a more assertive and decisive security provider'. It acknowledges that to effectively deal with state-sponsored cyberattacks on critical infrastructure or other malicious cyber activities, the EU must have capabilities to respond 'swiftly and forcefully'.

The EU cyber posture outlined in the Strategic Compass takes a more defence-centric turn.

(5) Department of Defense, *Miltary and Security Developments Involving the People's Republic of China*, Annual Report to Congress, November 2021 (https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF).

(6) Burke, E.J. et al., 'People's Liberation Army Operational Concepts,' RAND Corporation, 2020 (https://www.rand.org/pubs/research_reports/RRA394-1.html),

(7) Department of Defense, 'Cyber Strategy', 2018 (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF).

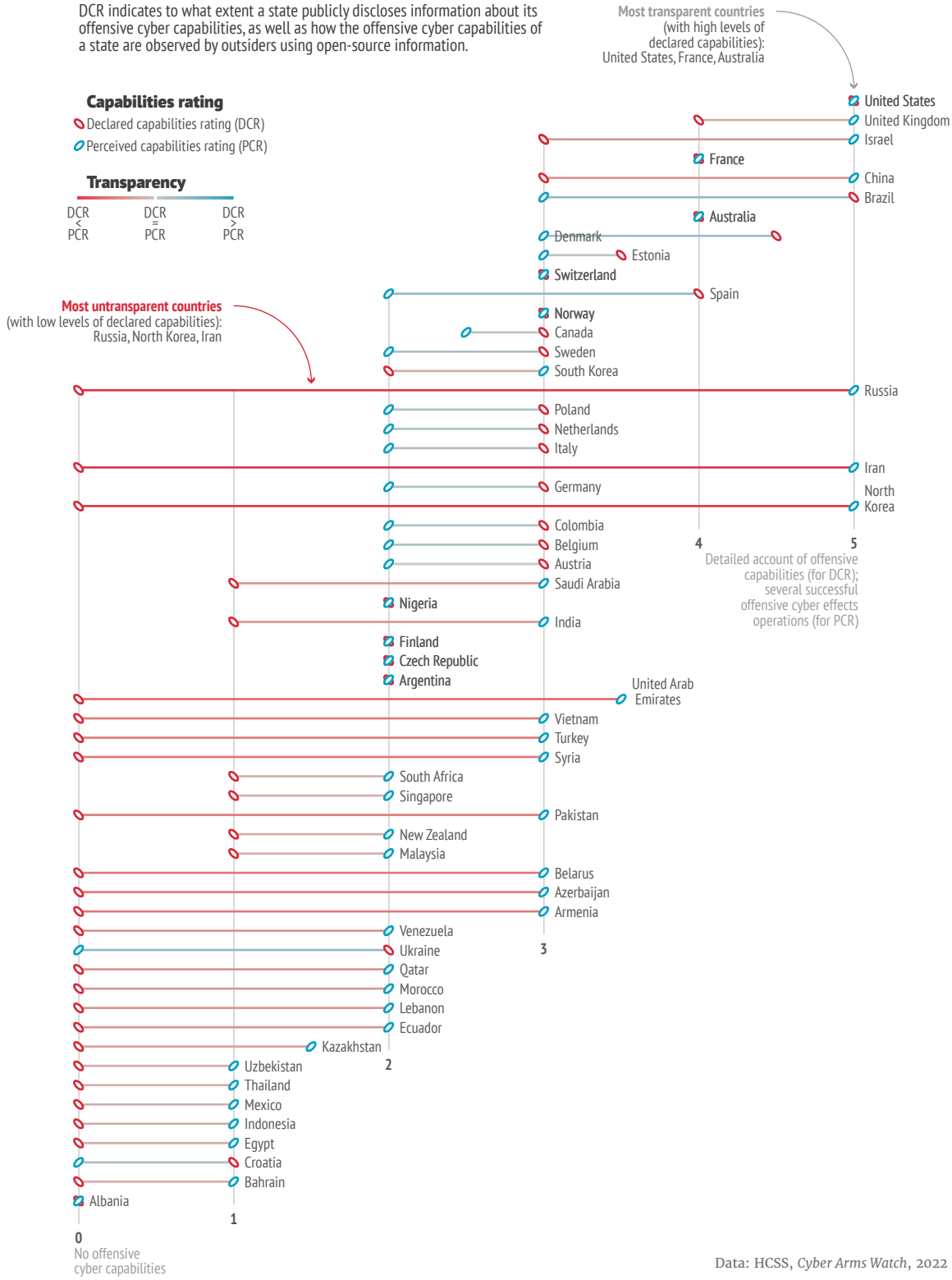
(8) European External Action Service, *A Strategic Compass for Security and Defence*, March 2022 (https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf).

(9) EU High Representative for Foreign Affairs and Security Policy, 'Shared vision, common action: a stronger Europe – A Global Strategy for the European Union's foreign and security policy', June 2016 (https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf).

Cyber Transparency Index

Greater transparency regarding states' cyber capabilities helps reduce misunderstandings and offers more predictability in the international security environment, ultimately contributing to reducing the risks of conflict. However, states are usually reluctant to release such data.

DCR indicates to what extent a state publicly discloses information about its offensive cyber capabilities, as well as how the offensive cyber capabilities of a state are observed by outsiders using open-source information.



Data: HCSS, *Cyber Arms Watch*, 2022

To support this vision, the Strategic Compass enumerates a series of concrete initiatives, including further developing the EU's Cyber Defence Policy, boosting research and innovation, stimulating the EU's industrial base, increasing cooperation among the EU's and Member States' partners in cyber defence, including interoperability and information sharing through cooperation between military computer emergency readiness teams (MilCERTs), as well as in the conduct of defensive cyber operations. Regarding cyber capabilities, the document commits the EU to develop and make intensive use of new technologies, notably quantum computing, artificial intelligence (AI) and Big Data, in order to achieve comparative advantages, including in terms of cyber responsive operations and information superiority.

At the **policy level**, the place of cyber defence in the EU's cybersecurity strategies has also evolved significantly [(10)]. The 2013 Cybersecurity Strategy [(11)] lists developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP) as one of the strategic priorities. To support Member States' defence and national security interests, the 2013 Strategy defines the goals for cyber defence capability development as detection, response and recovery from sophisticated cyber threats. It also notes the need for enhancing synergies between civilian and military approaches in protecting critical cyber assets. The document addresses extensively the need for a comprehensive approach to cybersecurity built on three pillars: (i) network and information security; (ii) law enforcement; and (iii) defence, each with their own legal and institutional framework. Developing cyber defence policies in conjunction with the CSDP was given priority, as well as developing industrial and technological resources for cybersecurity. The Strategy intended to encourage the demand for highly secure information and communications technologies (ICTs) products and to stimulate technology research and development plans by the EU Member States in collaboration with the European Defence Agency (EDA) so as to create competent and competitive technical resources for cyber defence.

Its successor – the 2017 Cybersecurity Strategy [(12)] – takes a more elaborate position regarding building the EU's 'cybersecurity deterrence' through defence capabilities, in particular concerning the cyber-resilience of CSDP missions and operations. Some of the key components mentioned in the document include standardised procedures and technical capabilities to support both civilian and military missions and operations, their respective Planning and Conduct Capability structures, and European External Action Service (EEAS) information technology service providers. Recognising the blurring lines between cyber defence and cybersecurity and the dual-use nature of cyber tools and technologies, the 2017 Strategy highlights the importance of promoting synergies between military and civilian efforts. It also stresses the importance of investments in research and innovation in critical areas such as encryption systems based on quantum technologies, cyber situational awareness, biometric access control systems, Advanced Persistent Threats (APTs) detection, or data mining.

The 2020 revision of the EU Cybersecurity Strategy [(13)] frames cyber defence as part of a broader digital strategy. According to the document, 'cybersecurity must be integrated

(10) The term 'defence' was used 25 times in the 2013 strategy, 55 times in 2017 and 39 times in 2020.

(11) European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace', 7 February 2013 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN).

(12) European Commission, Joint Communication to the European Parliament and the Council, 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', JOIN(2017) 450 final, 13 September 2017 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en).

(13) European Commission, Joint Communication to the European Parliament and the Council, 'The EU's cybersecurity strategy for the digital decade', Join 2020 18 final, 16 December 2020 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN).

into all digital investments, particularly key technologies like AI, encryption and quantum computing, using incentives, obligations and benchmarks'. The EU and its Member States should provide further impetus for the development of state-of the-art cyber defence capabilities through different EU policies and instruments, notably the Cyber Defence Policy Framework (CDPF) and encouraging Member States to make use of the full potential of Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF). Over time, strengthening the EU's cyber defence has become an important horizontal priority across other policy areas, especially those addressing hybrid threats, strategic autonomy, industrial strategy, and broader defence policy, in particular military mobility.

Finally, at the **operational level** the EU continued to advance the notion of cyberspace as a domain of operations. [(14)] Enshrined in the 2013 Cybersecurity Strategy and adopted by the European Council in November 2014, the EU Cyber Defence Policy Framework highlighted five priority areas: supporting the development of cyber defence capabilities related to CDSP with EU Member States; enhancing the protection of CSDP communication networks used by EU entities; promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies, as well as with the private sector; improving training, education and exercise opportunities; and enhancing cooperation with key international partners, including the North Atlantic Treaty Organization (NATO) and other major stakeholders. The Framework put forward more than forty proposals, including: the enhanced voluntary cooperation between military Computer Emergency Response Teams (CERTs) of EU Member States in light of prevention actions and for the handling of incidents; promoting real-time cyber threat information sharing between Member States and relevant EU bodies; exchanging best practice on exercises, training and other areas of possible civilian-military synergies; the involvement of international partners such as NATO or the Organization for Security and Co-operation in Europe (OSCE); and reinforced cooperation between the CERT-EU, relevant EU cyber defence bodies and the NATO Computer Incident Response Capability (NCIRC). Significantly, the 2018 update of the Cyber Defence Policy Framework also identified several technology innovation priorities, such as the development of cyber defence capabilities, joint research and technology efforts, and enhanced civil-military cooperation.

Concerning institutional structures, the main EU actors dealing with cyber defence-related issues are the EU Military Staff (EUMS) and the EDA. The former bears the primary responsibility for the EU Cyber Defence Concept for EU-led Military Operations and Missions (2016); the latter has become a key driver of EU cyber defence initiatives and research and technology (R&T) activities. The EDA set up the Cyber Defence Research Agenda (CDRA), considered as a research and technology roadmap for the coming years for identifying dual-use cyber technologies, while considering ongoing and future civil research under the EU's Research and Technology Framework Programmes. Different levels of cyber defence capabilities and the varying speed of digital transformation of Member States' armed forces made capability development one of the priorities for action at the EU level. Development of cyber defence capabilities occurs through two primary channels: the Member States-driven PESCO and the game-changing potential for technological research and innovation of the European Commission's EDF. However, many questions still remain concerning how Member States can capitalise on various EU instruments and funding opportunities aimed to boost the research and innovation potential of the European Defence Technological and Industrial Base (EDTIB).

(14) Council of the European Union, 'EU Cyber Defence Policy Framework', 14413/18, Brussels, 19 November 2018 (https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf).

LINGUISTICS OF THE EU'S CYBER DEFENCE

This *Chaillot Paper* approaches the study of 'the language of power' as a quasi-linguistic project that helps to understand the history and functions of cyber defence. At the same time, it aims to provide insights into speech, grammar or vocabulary that shape the field of European cyber defence. Just as studying the evolution of a language and its functions helps us better understand human history and culture, so the investigation of the role of cyber defence as an element of the EU's defence policy gives us a better insight into the evolution of its strategic culture and defence posture.

Tenses: present and future of cyber defence

In grammar, tense is a verb-based method of indicating the time of action. The correct use of tenses helps us understand how certain events relate to each other in time: how the past impacts the present, and what will or might happen in the future. Two contributions to this *Chaillot Paper* play exactly that role.

Antonio Missiroli offers a discussion on the anatomy of a cyber conflict and provides an introduction to the theme of this volume. His contribution helps us better understand the distinction between traditional and cyber warfare and challenges associated with drawing the line between the two. He argues that not all hostile cyber activities are of equal importance, not all pose significant threats to national or collective security, and not all can be prevented. The hostile cyber operators themselves may range from states or state-sponsored groups to criminal organisations, from 'hacktivists' to terrorist franchises. While cyber *warfare* proper (i.e. as carried out *only* in cyberspace) seems still a remote possibility, the war in Ukraine has reinforced the sense that any future armed conflict or high-end military operation will most likely contain a significant enabling or disabling cyber component (cyber *in* warfare).

Raluca Csernatoni looks into the future of cyber defence and the role of emerging disruptive technologies. She also highlights how in a complex network of state and non-state actors, cyberspace becomes a domain where the lines between the orthodox understandings of war and peace are increasingly blurred. This means that cyber incidents and threats are moving conflicts into a grey zone below the threshold of conventional warfare. In her view, the disruptive impact of new and emerging technologies and an accelerating race to deploy autonomous and intelligent systems has led to a paradigmatic transformation regarding armed conflicts. Such technological advancements are seen as critical to dominance in future warfare and for the militaries of tomorrow. As enabling technologies such as AI enter cyberspace and cyber war scenarios, they transform the way in which conflicts are fought. The fielding of AI cybersecurity systems may lead to new approaches and transformations in cyber system engineering and cyber defence architectures. AI-enhanced cyberattacks, communications jamming, electronic warfare, and other attacks on a system's software will become as important as those that target hardware, if not more so.

Together, these contributions highlight the importance of the information environment as a central element for commanding the conflict space and illustrate challenges that states might face without a clear distinction between cyber and traditional warfare, in particular ensuring that decisions taken during a conflict are justified and proportional.

Semantics: security, resilience, defence and cyber defence

Semantics is the study of meaning in language used in reference to entire texts or single words. It also plays an important role in improving the general understanding of the role that cyber defence plays in the broader security strategy of the European Union.

Eneken Tikk and **Mika Kerttunen** address the complex relationship between cyber defence and other key concepts in the European security vocabulary like resilience, security and defence more broadly. But as their contribution demonstrates, clear definitions, the precise use of words, and giving them meaning in specific contexts has very concrete policy and operational implications. The challenge, however, is that such clear definitions are still lacking in the EU Member States with many politicians still using cyber defence as a catch-all term that also encompasses strengthening cyber resilience. In France, for instance, cyber defence refers to the protection of the state's networks, including those of the Ministry of Defence, with the national framework prescribing a clear overall responsibility to the director general of the National Cybersecurity Agency (*Agence nationale de la sécurité des systèmes d'information* – ANSSI) with the commander of cyber defence (COMCYBER) in charge of military cyber defence at the Ministry of Defence [(15)]. This implies that cyber defence is understood as a shared responsibility that requires a clear division of labour within different components of the armed forces, the Ministry of Defence as well as their industrial partners outside of government.

Tikk and Kerttunen argue that questions that have underpinned cyber defence efforts in individual countries and defence organisations – such as the nature and extent of cyber defence, triggers of defence engagement, cooperative defence efforts, optimal capabilities and command – now need to be accommodated in, and resolved as part of, broader European security and defence policy. Their contribution addresses a complex question of civilian-military relations that needs to be addressed to provide integrated cyber capabilities to support military operations.

Syntax: defensive and offensive capabilities

Syntax is about the right order in a sentence: what word comes before and after another word. The chapter by **Matthias Schulze** demonstrates that the issue of order plays an important role in the discussion about cyber defence. This is for two main reasons. First, for any democratic society, it is important to establish the role of armed forces during day-to-day competition in cyberspace when most attacks – sometimes with significant effects – occur below the threshold of armed conflict. Second, prior to taking decisions about which tools to use in order to control the conflict space and prevent adversaries from using their resources, states need to establish doctrines and rules regarding the use of offensive and defensive capabilities within and outside a state jurisdiction.

So far, states have adopted different approaches. For instance, France's 2018 *Public Elements for the Military Cyber Warfare Doctrine* defines military offensive cyberwarfare as 'all military actions undertaken in cyberspace, in support or not of other military capabilities. Cyber weapons aim, in accordance with international law, at producing effects against adversarial computer systems to alter availability or data confidentiality' [(16)]. The United States, on the other hand, has adopted a different approach that allows the conduct of cyberspace operations to collect intelligence and develop military cyber capabilities to be used in the event of conflict (*persistent engagement*)

(15) Delerue, F., Desforges, A. and Géry, A., 'A close look at France's new military cyber strategy', *War on The Rocks*, 23 April 2019 (https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/).

(16) The document consists of two components: the Ministerial Policy for Defensive Cyber Warfare (*Politique ministérielle de lutte informatique défensive*) and the Public Elements for the Military Cyber Warfare Doctrine (*Éléments publics de doctrine militaire de lutte informatique offensive*). Ministère des Armées, 2018 (https://www.defense.gouv.fr/sites/default/files/ministere-armees/Politique%20minist%C3%A9rielle%20de%20lutte%20informatique%20d%C3%A9fensive.pdf and https://www.defense.gouv.fr/sites/default/files/ema/doctrine_de_lutte_informatique_dinfluence_l2i.pdf).

and to disrupt or halt malicious cyber activity at its source (*defend forward*) [17]. Against this background, Schulze's contribution signals potential challenges for transatlantic efforts to deter malicious cyber operations as a result of incompatibility between the US approach and the EU's understanding of a rule-based international order.

Affirmation and negation: armed forces and attribution

In grammar, affirmation and negation are used to express the validity or truth of a basic assertion. In cyber defence, this translates into concrete capacities and mechanisms to ascertain who is responsible for harmful activities or who may pose a threat to a state's key interests. If anonymity is an enabler for malicious cyber activity by state and non-state groups, attribution is an antidote that needs to be a fundamental part of an effective cyber defence toolkit. More than that: attribution is a key element for ensuring accountability in cyberspace and the rules-based international order.

Aude Géry takes a deep dive into the contribution of the armed forces to different types of attribution, the role of attribution in military cyber operations, and the role of the armed forces in attribution. She demonstrates how, depending on the type of attribution and the goal pursued, attribution can play different roles in the context of military cyber operations: as a tool in supporting military cyber defence, a legal prerequisite before conducting cyber operations, and to leverage an operational advantage. Géry also argues that if the EU wants to build a solid cyber defence, both at the military and civilian level, it will not be able to do so without involving the armed forces from EU Member States and framing attribution collaboration.

Morphology: cyber espionage and defence

Another key conceptual category in linguistics is morphology: the study of word structure and its relationship both to sentence structure and to meaning. One of the issues in international relations among states in cyberspace that requires such careful study – both in terms of relations and long-term implications – concerns cyber espionage activities to acquire military or trade secrets. This has become one of the most problematic aspects in relations among states in cyberspace.

François Delerue explores the topic of espionage in cyberspace and the implications it has for the armed forces. Cyberspace has broadened the scale of espionage, making it possible to spy on almost everybody from a remote location and give access to an unprecedented amount of information, including trade or military secrets. He demonstrates that the demarcation line between espionage activities and other military activities in cyberspace tends to become blurred in most circumstances. In this context, this chapter contributes to the debate on how the EU and its Member States should apprehend and react to alleged state-sponsored cyber espionage campaigns. A measured response to cyberwarfare requires both deterrence and escalation levels, therefore a better understanding of cyber espionage is important in order to determine what constitutes a legitimate and proportionate response to such malicious activities.

Grammar: rules in cyber conflict

The grammar of a natural language is its set of structural rules and constraints regarding the composition of clauses, phrases and words. In the context of cyber defence, this role is played

[17] United States Department of Defense, *Department of Defense Cyber Strategy*, 2018 (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF).

by international law, in particular international humanitarian law.

Kubo Mačák and **Laurent Gisel** stress that the increasing use of military cyber capabilities and the related humanitarian concerns underscore the urgency of reaching shared understandings on the legal constraints that apply to the use of cyber operations during armed conflicts. Their chapter sets the scene by defining the notion of cyber operations during armed conflicts and discusses the threshold question of whether international humanitarian law (IHL) applies to cyber operations. They also address specific issues related to how IHL principles and rules apply to cyber operations during armed conflict.

Dialects: collective cyber defence in EU and NATO

Finally, this volume would be incomplete without an analysis of dialects: a regional variety of language distinguished by vocabulary, grammar and pronunciation from other varieties and constituting together with them a single language. In cyber defence, the EU and NATO share obvious similarities but can they be considered dialects of the same language of power?

Peter B.M.J. Pijpers, Hans Boddens Hosang and **Paul A.L. Ducheine** offer a comparative analysis of the EU's and NATO's approaches to collective cyber defence. Though both organisations build on the customary international law standard regarding the right of self-defence as laid down in Article 51 of the UN Charter, the wording of the EU and NATO collective defence clauses differs. Where NATO's collective defence is a proven asset, the EU's mutual defence clause is still waiting for its full operationalisation and is therefore mainly a paper tiger. However, when cyber-attacks are outside the remit of the use of force – which characterises most cases these days – the collective defence systems appear to be of limited relevance. Given that the EU has a wide array of instruments of power at its disposal - from diplomatic measures via economic sanctions and financial fines to legal retorsions - could this mean that the EU is better equipped to provide a security umbrella against modern cyber threats?

Overall, different aspects and perspectives presented in this *Chaillot Paper* provide EU decision-makers with elements for designing a comprehensive policy that guides when and how defence forces may resort to cyber operations in a time of conflict.

CHAPTER 1

PRESENT TENSE: CYBER DEFENCE MATTERS

by
ANTONIO MISSIROLI

INTRODUCTION

When the President of the European Commission, Ursula von der Leyen, announced during her 2021 State of the Union address in the European Parliament the EU's intention to develop a cyber *defence* policy, officials in the European External Action Service wondered what she had in mind. It soon became clear that she was referring to a broader cyber *resilience* posture of the European Union. Such confusion between cyber *defence* and cyber *security,* however, is not unusual. While there is no universally accepted definition [(1)], cyber *security* encompasses – broadly speaking – measures to protect cyberspace from hostile actions. Nowadays, every business and public institution has staff responsible for protecting its networks against unauthorised intrusion from outside of the organisation. Cyber *defence*, on the other hand, refers to those measures and authorities that that are within the remit of the military or impinge on military capabilities (starting with signal intelligence).

Yet, cyber *defence* may also be used more generally to convey an action rather than a specific actor. At any rate, different definitions reflect different mandates, with many variations across governments and countries: as a result, strengthening cyber 'defence(s)' does not necessarily entail involving (only) the military.

Among *state* actors, cyber 'power' overlaps only partially with other conventional indicators of capability and influence, including size and international outreach. Most assessments place the United States (through the National Security Agency - NSA), Israel (*inter alia* Mossad's Unit 8200), China and Russia in the 'top tier', with the United Kingdom (GCHQ) close behind, and Iran and North Korea considered highly capable especially in terms of offensive skills. Other countries like Japan, South Korea, Australia and Canada are seen as quite well prepared, primarily thanks to their intelligence cooperation with the United States. In the EU, France and Germany, most Nordic and Baltic countries as well as the Netherlands are

This chapter draws substantially upon: Missiroli, A., 'Geopolitics and strategies in cyberspace', Hybrid CoE Paper no. 7, The European Centre of Excellence for Countering Hybrid Threats, published in June 2021.

(1) The section that follows relies on a number of different sources that cannot be listed in full. For most of the definitions, however, see Kello, L., *The Virtual Weapon and International Order*, Yale University Press, New Haven, 2017 (the author also coined the notion of 'un-peace' to characterise the current state of play). For the conceptual implications for security and defence, see Rid, T., *Cyber War Will Not Take Place*, Hurst & Co., London 2013. For a general introduction, see Dunn Cavelty, M., 'Cyber-Security', in Collins, A. (ed.), *Contemporary Security Studies*, 5th edition, Oxford University Press, Oxford, 2019, pp. 410-426. See also Maurer, T., *Cyber Mercenaries: The State, hackers, and power*, Cambridge University Press, 2018.

also assessed as quite mature cyber powers, with others like Spain and Italy catching up quickly. According to the National Cyber Power Index released by Harvard's Belfer Center, all of the countries mentioned above are placed in the 'Top Ten' cluster. The high score of Iran and North Korea, however, may also be ascribed to their usage of cyber tools for surveillance and control purposes [(2)]. Researchers from the International Institute of Strategic Studies (IISS) came to similar conclusions, ranking 15 selected countries along three main tiers, with the United States as the only one in the first tier, China as its most likely future challenger, and other states assessed differently in light of their respective defensive and offensive capabilities [(3)].

Yet, such state-centric assessments not only neglect the important role often played by non-state actors and proxies, especially in the context of so-called 'hybrid' campaigns. They also show the ever-widening digital gap between the 'haves' and the 'have-nots', which makes the so-called Global South a potential battleground for geopolitical and technological influence between competing camps. The discussions at UN level already reflect this growing tension between different approaches to cyberspace, its regulation and future governance.

ANATOMY OF CYBER CONFLICT

Not all hostile cyber activities are of equal importance, not all pose significant threats to national or collective security, and not all can be prevented. The hostile cyber operators themselves may range from states or state-sponsored groups to criminal organisations, from 'hacktivists' to terrorist franchises.

While cyber *warfare* proper (i.e. as carried out *only* in cyberspace) seems still a remote possibility, even the ongoing war in Ukraine – despite its mainly 'conventional' aspects – has reinforced the notion that any future armed conflict or high-end military operation will most likely contain a significant enabling or disabling cyber component (cyber *in* warfare).

Furthermore, most hostile cyber activities based on the *use of code* do not fit neatly in the category of 'armed attack' and do not entail or elicit the *use of force* for self-defence, at least in a kinetic sense. It is sometimes even difficult to ascertain precisely what harm – defined as injury or death of individuals as well as damage to or destruction of property – is the result of a cyber operation. In fact, digital technologies have dramatically lowered the entry barriers for new threat actors (the 'democratisation' effect) and extended the scope and *modus operandi* of hostile activities (the 'weaponisation' effect) that were already quite common, for instance, during the Cold War. Yet they have also decreased the overall level of *direct* physical violence.

Hostile cyber activities lying below the level of armed attack represent comparatively low-cost, low-risk but high-impact operations that are difficult to detect, deter and defend against. For state actors, in particular, resorting to digital 'weapons' – including through proxies – is a very effective way to externalise the material and reputational costs of warfare while lowering public accountability.

The main vectors of a cyberattack – intended as the use of code to interfere with the functionality of a computer system for political or strategic purposes in order to damage, disrupt or destroy – are networks, supply chains and human insiders (whether malicious or just careless). Cyberattacks can be generalised (no machine connected to the internet is

(2) Voo, J. et al., *National Cyber Power Index 2020*, Belfer Center for Science and International Affairs, Harvard University, September 2020. The International Telecommunications Union (ITU), which is part of the UN, also publishes a *Global Cybersecurity Index* (the latest released in 2018) based, however, on self-assessments.

(3) Austin, G. et al., *Cyber Capabilities and National Power: A net assessment*, IISS, London, June 2021.

Examples of significant cyber operations against military and defence actors

2022
OCTOBER
Sensitive data from Australia's Department of Defence may have been compromised after a ransomware attack targeted a military communications platform.

2022
MARCH
At the beginning of the Russian invasion, some **internet services throughout Europe** were interrupted by a cyberattack on Viasat, an American satellite broadband provider. Ukraine military communications that relied on Viasat services were affected.

2022
SEPTEMBER
Mexico's Defence Ministry was targeted by hackers claiming to be an anti-imperialist group pursuing the protection of the environment. **Six terabytes of data gleaned from over four million emails** were released, detailing how the military has gradually increased its influence over the civilian government, ignored human rights investigations, and spied on journalists.

2022
FEBRUARY
US authorities report that Russian state-sponsored cyber actors have targeted US cleared defense contractors (CDCs) from at least January 2020, through to February 2022. The actors obtained **sensitive data about US defence and intelligence programmes and capabilities**. Compromised entities have included CDCs supporting all branches of the US military. In one case, threat actors exfiltrated hundreds of documents related to the companys' products, relationships with other countries, and internal personnel and legal matters.

2021
DECEMBER
A cyberattack against Belgium's Ministry of Defence left staff unable to send **external emails** for up to four weeks.

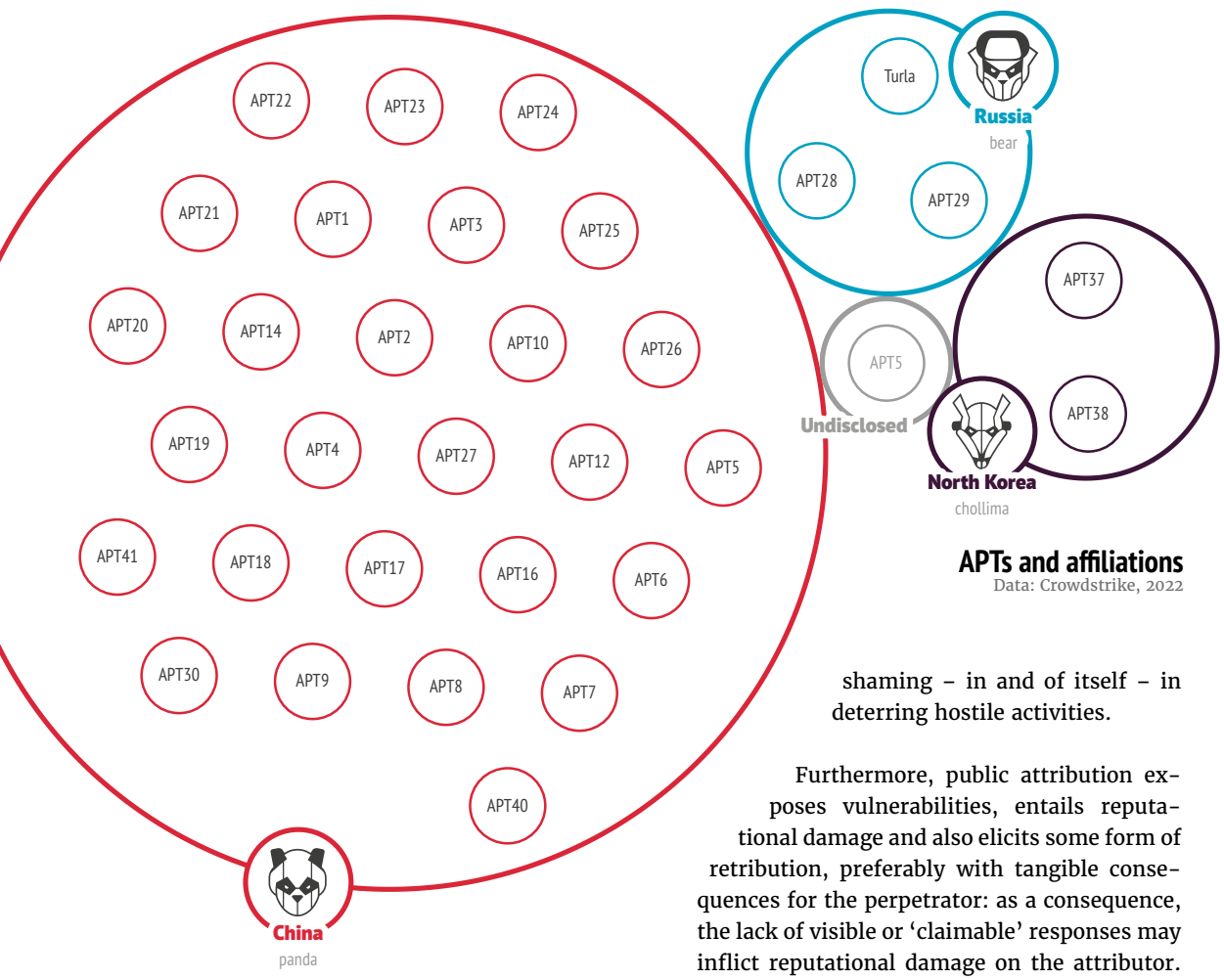
2021
MARCH
Chinese hacking group thought to have government backing targeted security flaws in Microsoft Exchange Servers to gain **access to data from over 30 000 companies**, including defence contractors.

2020
MAY
Hackers posing as employees of large US defence companies, and affiliated with the North Korean Lazarus group, compromised the systems of at least two defence and aerospace firms in Central Europe by spreading **malware** via fake job offers on LinkedIn.

2020
MAY
Japan's Ministry of Defence discovered that 59 out of 20 000 **compromised files** from a cyberattack against Mitsubishi Electric Corp. may have impacted Japan's National Security.

in principle spared), as with the 2007 attack against Estonia, or customised, as with the 2009/10 Stuxnet operation against Iran's nuclear programme, notably the Natanz power plant. They can be stand-alone operations or part of broader and well-coordinated destabilising and disruptive 'hybrid' campaigns. They may entail cyber exploitation, i.e. the penetration of an adversary's computer system for the purpose of exfiltrating data (a quintessential *espionage* activity practised also by Western agencies and governments); yet they may also lead to the disablement of the adversary, which amounts to *sabotage* (a potential *casus belli*). More often than not, they cross multiple jurisdictions, putting into question the traditional separation between the domestic and the foreign sphere. Their opacity also blurs the distinction between crime and war as well as between peace, crisis and conflict: there are no tanks crossing borders, no visible insignia or soldiers, no debris or minefields ('what you *cannot* see is what you get'). Finally, attacks can occur anytime and anywhere: the attack surface is virtually infinite.

As a result, attributing a cyberattack or even just malicious activity can be an extremely complex and challenging process. It includes a sophisticated technical component (forensics proper, often carried out also by private companies) and, particularly for state actors, an equally sophisticated all-source intelligence component to assess circumstance and hostile

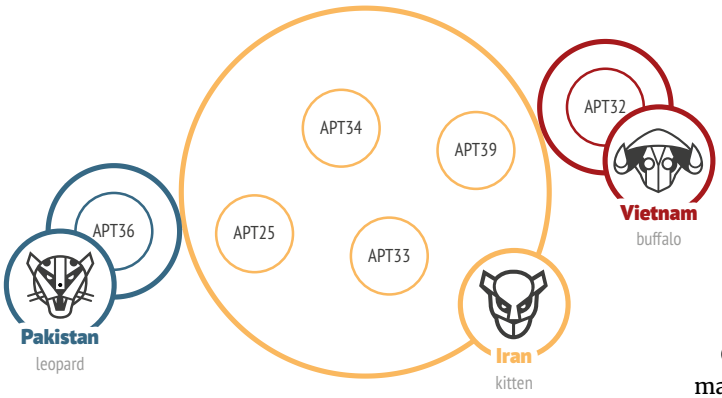


APTs and affiliations
Data: Crowdstrike, 2022

intent. Deception – through 'spoofing' and 'false flag' techniques – is quite common in the cyber domain: even knowing the true location of the originating machine is not the same as identifying the ultimate instigator of an attack, although skilled investigators can reduce the list of potential aggressors. Attribution, in other words, is a matter of degree (it can rarely be 100 % conclusive) as well as political judgement, especially when made public by governments and/or specialised agencies. Moreover, disclosing forensic methods and/or intelligence sources to corroborate attribution may actually diminish or even compromise their value for future contingencies; not doing so, however, could open the door to 'plausible deniability' and a potential loss of international support. In other words, while inaction and silence could signal weakness, the jury is still out as to the effectiveness of naming and shaming – in and of itself – in deterring hostile activities.

Furthermore, public attribution exposes vulnerabilities, entails reputational damage and also elicits some form of retribution, preferably with tangible consequences for the perpetrator: as a consequence, the lack of visible or 'claimable' responses may inflict reputational damage on the attributor. Attribution is indeed also a form of strategic communication: it is about messaging (bilaterally and discreetly, or jointly and publicly), and it is about perceptions. It requires credibility at source, including the capability to retaliate. In turn, however, retaliation in kind – i.e. 'intra-domain' – is complicated by the particular nature of cyberspace (a man-made ecosystem, mostly privately owned and operated) and carries the risk of unintended consequences, collateral damage, miscalculation and escalation: so-called offensive cyber 'effects' are in fact one-shot weapons ('you launch it, you lose it') whose ultimate impact and outreach cannot always be controlled, as they can also be reverse-engineered, repurposed and reused[4]. What is more, all of this is amplified by the lightning speed at which action unfolds in cyberspace, which compels responders to (re)act quickly on the basis of incomplete or ambiguous information and in compromised

[4] On the other hand, cyberattacks were carried out by the US first against Daesh/ISIS on the battlefield in 2015/16 and, later on, in response to a *kinetic* operation by Iran-supported militias in the Gulf.



MAPPING THREAT ACTORS

environments: nowhere is von Clausewitz's 'fog of war' thicker than in cyberspace.

Finally, not only is global governance of cyberspace highly fragmented [5], but digital 'weapons' are neither banned nor controlled internationally, despite ongoing efforts at UN level to set rules of responsible state behaviour (the general norms endorsed most recently by the General Assembly in 2021 are voluntary, non-binding and not enforceable) and attempts at OSCE level to implement confidence-building measures and early-warning protocols. Classical arms control-type arrangements and mechanisms seem indeed inapplicable to the cyber domain: the intrinsic ubiquity and dual-use nature of information technology would make inspections pointless, verification of stockpiles virtually impossible, and compliance hardly enforceable. In fact, cyber assets and capabilities can be promptly and easily recreated.

Needless to say, reliable and releasable information about cyber threat actors, their strategies and their methods is for the most part difficult to access, often shrouded in (legitimate) secrecy, and quite easy to contest. Nevertheless, it is possible to sketch some profiles and to identify distinctive patterns of behaviour [6].

Organised crime has been and remains the main perpetrator of hostile cyber operations, at least in quantitative terms. Cybercrime – i.e. crime committed mostly or entirely by digital means – has increased and intensified during the Covid-19 pandemic (also due to the shift to remote working), especially through hacking attacks where victims' files are locked until a ransom is paid, often in cryptocurrency. Such groups seem to operate in a decentralised fashion – unlike drug cartels or mafias – and often cultivate links to states interested in their know-how or in the data they have plundered.

Recently these activities have become hugely profitable, creating a peculiar business called Ransomware-as-a-Service (RaaS) run through the Dark Web and based on renting out malware and taking a cut in the earnings. The 2021 Colonial Pipeline hack, which blocked the petrol supply across the southern and south-eastern United States (and has been attributed to Dark Side, a gang of Russian-speaking hackers based somewhere in the territory of the former USSR), is a typical case in point. Law enforcement and intelligence agencies are struggling to keep up with this constantly evolving and growing threat and are considering specific forms of deterrence, including compelling targeted companies to report attacks, delaying or blocking ransom payments altogether, or 'doxing' the perpetrators, i.e.

[5] Intellectual property is dealt with in the World Intellectual Property Organization (WIPO), digital commerce in the WTO, privacy protection in the UN Human Rights Council, and IP numbers in ICANN, a non-profit legal entity incorporated in California. The Budapest Convention on Cybercrime, originally drafted within the Council of Europe and which entered into force in 2004, has been ratified by 65 countries. Finally, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, originally signed in 1995, now includes a 2015 provision for systems that 'command and control' intrusion software – but not all signatories have translated it into law yet.

[6] The section that follows is based on information that circulates widely among analysts and experts. Compelling accounts are provided *inter alia* by two well-known *New York Times* reporters, namely Sanger, D.E., *The Perfect Weapon: War, sabotage and fear in the cyber age*, Scribe, London, 2018; and Perlroth, N., *This is How They Tell Me the World Ends: The cyber weapons arms race*, Bloomsbury, London, 2021.

making their details and coordinates publicly available [7].

So far, terrorist groups and militias have mainly used cyberspace for recruitment, funding as well as operational purposes – in-theatre (Levant, Libya), in Europe and elsewhere. While there is still no evidence or credible prospect of 'cyber-terrorism' proper, there is concern about the possible use of unmanned vehicles for jihadist attacks in urban environments, and cyber-enabled sabotage operations against transport or energy infrastructure. Yet most analysts believe that such activities could be carried out only with the backing of capable state or state-sponsored actors.

None of these criminal or terrorist groups, in fact, normally qualify as an APT, that is, as an actor equipped with the full spectrum of intelligence-gathering techniques, pursuing specific objectives rather than just opportunistically seeking information for financial or other gain, and guided by both intent and capability, i.e. executing attacks by coordinated human actions rather than mindless and automated pieces of code. The best known APTs identified so far are the Russia-based Fancy Bear (also known as APT 28), Cozy Bear (APT 29), and Sandworm; a number of China-based APTs (often codenamed Pandas) supported by either the PLA or the Ministry of State Security; North Korea's Lazarus Group (APT38) and Iran's APT 39.

Their strategies and techniques, however, differ significantly [8]. North Korea's APTs, for instance, focus mainly on criminal-type operations designed to seize financial resources for the cash-strapped regime, as in the case of the 2016 SWIFT bank 'heist' and the 2017 WannaCry ransomware attack. Yet they have also carried out politically symbolic cyberattacks like the one against Sony Pictures, in 2014, to prevent the company from releasing a film on the North Korean regime – the first cyber incident to be formally sanctioned and publicly attributed by the US government. Deterring groups like Lazarus, however, remains challenging due to North Korea's minimal reliance on public networks [9].

Iran's posture is highly political. On the one hand, Tehran was the first victim of a targeted cyberattack (Stuxnet), later attributed by the international media to a joint US-Israeli intelligence operation. On the other hand, Iranian actors are considered to have been behind the malware attack on the Saudi Aramco oil company in 2012 as well as the distributed denial of service (DDoS) attack against the Sands Casino in Las Vegas, owned by pro-Israel billionaire Sheldon Adelson, in 2014. Other targets are, predictably, the United States and the domestic opposition to the regime.

Russian 'Bears' are widely credited with a high degree of technical sophistication and ingenuity.

Russian actors – which also include the (in)famous Internet Research Agency based in St. Petersburg as well as a number of contractors – tend to act geopolitically, with a disruptive and/or strategic intent, combining opportunistic and carefully tailored campaigns. Their range of operations has gone from compromising the networks of the World Anti-Doping Agency (WADA) and the Organisation for the Prohibition of Chemical Weapons (OPCW), which

(7) See the interview given by the former US cyber security 'tsar', Chris Krebs, to the *Financial Times* (6/7 February 2021) after being fired by President Trump for certifying the regularity of the November 2020 elections. See also 'Spam, scam, scam, scam', *The Economist*, 8 May 2021, and Glenny, M., 'Colonial cyberattack is a warning of worse to come', *Financial Times*, 15/16 May 2021.

(8) For a detailed description of the main APTs and their *modus operandi*, see for instance the website of FireEye, one of the more prominent private cybersecurity companies (www.fireeye.com), as well as the 2021 Global Threat Report released by CrowdStrike, another well-known private company (www.crowdstrike.com).

(9) See White, G., *The Lazarus Heist: From Hollywood to high finance – North Korea's global cyber war*, Penguin Business, London-New York, 2022.

failed spectacularly in October 2018, to the 2017 NotPetya supply chain attack that inflicted huge financial damage on the world economy; from 'hack-and-leak' and political interference operations against democratic processes (e.g. in the United States in 2016 and France in 2017) to large-scale disinformation and misinformation campaigns through social media worldwide. Russian 'Bears' are widely credited with a high degree of technical sophistication and ingenuity, a focus on strategic targets (including energy infrastructure and military command and control systems), and a remarkable ability to create havoc and engineer new ways of doing old things [(10)], albeit within the context of cyberspace as we know it.

One of the most recent and alarming cases has been the SolarWinds software exploitation that affected government and business networks around the world in late 2020. A typical supply-chain attack, the SolarWinds hack was soon attributed by experts and officials to a group, Nobelius, backed by Russia's Foreign Intelligence Service, which was previously linked to the theft of emails from the Democratic National Committee ahead of the 2016 US presidential elections – also showing how the boundaries between economic, political and security data exploitation and theft are fading [(11)]. On the one hand, Moscow appears to tolerate (and occasionally use) hackers who operate *from* Russia but not *against* Russia, only (or primarily) against Western or other interests – and it likely is not alone in doing this [(12)]. On the other hand, there seems to be little evidence of bilateral cooperation or coordination between hostile state actors proper – only efforts at disguising the origin of attacks and shifting the blame onto others [(13)].

Finally, the recent Russian military aggression against Ukraine provides additional evidence of the extent to which hostile cyber operations have become tools in warfare, albeit in a less decisive way than initially expected or feared [(14)]. On the one hand, in fact, cyberattacks against Ukrainian communication networks and critical infrastructure had already started before the invasion proper and have continued since, often extending also to neighbouring NATO and EU countries supporting Kyiv in the conflict [(15)]. On the other, their impact has been significantly mitigated by a number of factors – ranging from Ukraine's increased preparedness and resilience (thanks also to Western training and assistance) to the large number of Ukrainian internet-service providers (that reduced the network's chokepoints and resulting vulnerabilities), from the mobilisation of international hackers and IT communities against the aggression to Moscow's own reluctance to disrupt or destroy critical infrastructure and communication networks it might need during or after the war [(16)] – and has even led some to wonder (rightly or wrongly, or perhaps just

(10) Rid, T., *Active Measures: The secret history of disinformation and political warfare*, Farrar, Straus and Giroux, New York, 2020. For a special focus on cyber operations see Greenberg, A., *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*, Doubleday, New York, 2019.

(11) Murphy, H. et al., 'Cyberspace's "silent cold war"', *Financial Times*, 19/20 December 2020; Murphy, H., 'Russians behind *SolarWinds* hacking target 150 global foreign policy bodies', *Financial Times*, 29/30 May, 2021; Willett, M., 'Lessons of the *SolarWinds* Hack', *Survival*, Vol.63, No 2, April-May 2021.

(12) Younger, A. 'Ransomware attacks have to be stopped – here's how', *Financial Times*, 12/13 June 2021; and 'Over there in the shadows', *The Economist*, 19 June 2021.

(13) Rugge, F. (ed.), *Confronting an 'Axis of Cyber'? China, Iran, North Korea, Russia in cyberspace*, ISPI, Milan, 2018.

(14) Manjoo, F., 'The Ukrainian cyberwar that never materialized', *The New York Times* (International edition), 12/13 March 2022; Rid, T., 'Why you haven't heard about the secret cyberwar in Ukraine', *The New York Times* (International edition), 21 March 2022.

(15) Cerulus, L., 'Don't call It warfare: West grapples with response to Ukraine cyber aggressions', *Politico*, 18 January 2022. See also the long interview ('Are we ready for Putin's Cyberwar?') given by Anne Neuberger, the current US deputy national security adviser for cyber and emerging technology, to *The New York Times*, 10 March 2022, as well as: 'Dealing with degradation', *The Economist*, 26 March 2022; Srivastava, M., 'Russian hacking warriors fail to land heavy blows', *Financial Times*, 29 March 2022; Black, D. and Cattler, D., 'The myth of the missing cyberwar', *Foreign Affairs*, Vol.101, No 2, March-April 2022.

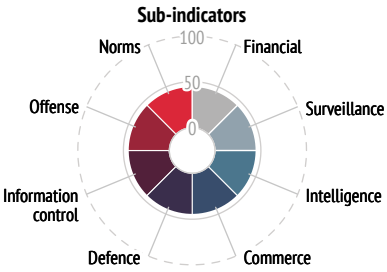
(16) Srivastava, M., 'Pro-Ukrainian hackers launch "unprecedented" attack on Russia', *Financial Times*, 7/8 May 2022; Tett, G. 'Inside Ukraine's open-source war', *Financial Times*, 23/24 July 2022; Scott, M., 'How Ukraine used Russia's digital playbook against the Kremlin', *Politico,* 24 August 2022.

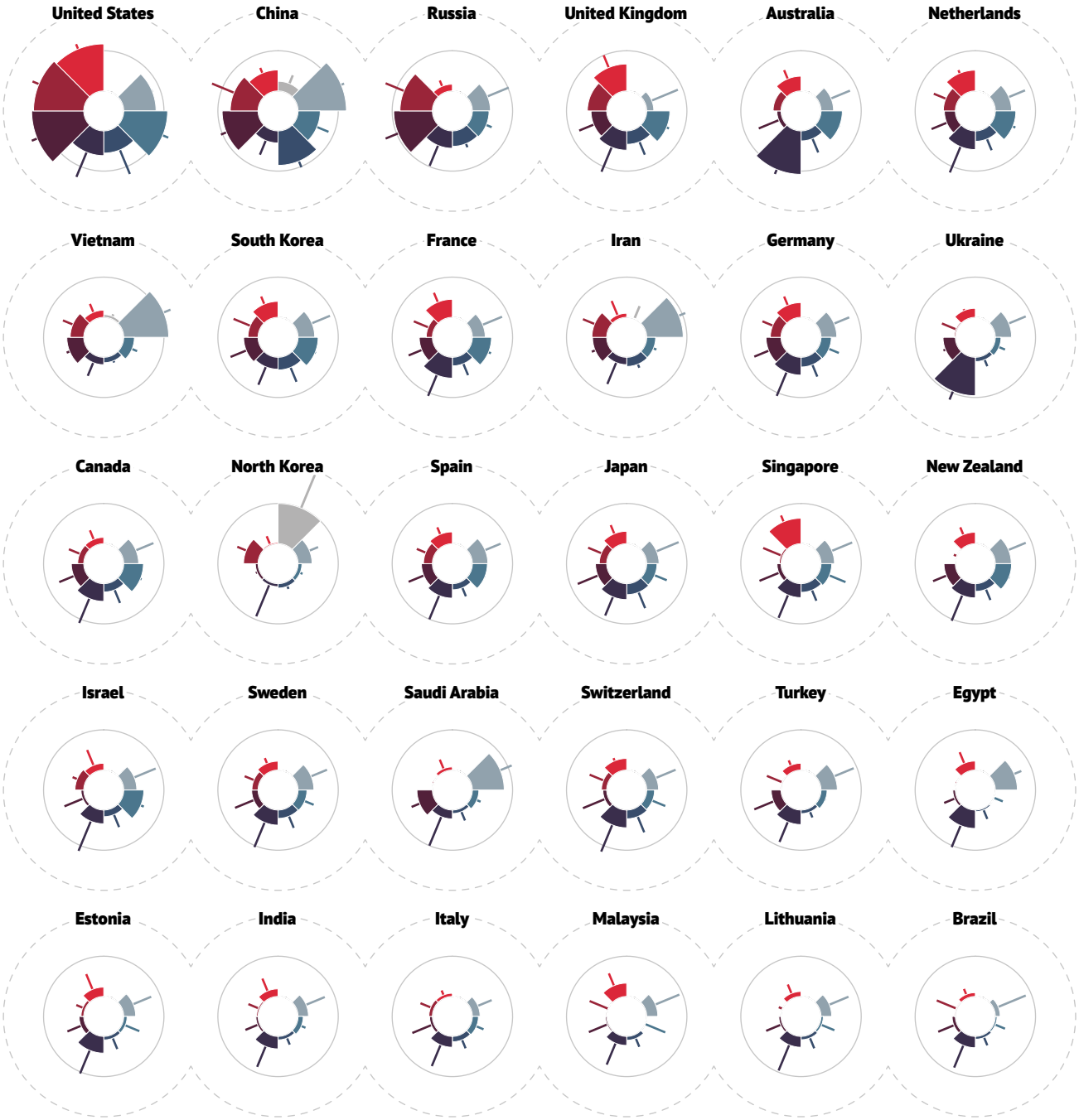
National Cyber Power Index

2022

Measuring cyber power is a complex and nuanced process. Methodologies used to assess cyber power of individual states are also evolving. This visual represents a snapshot captured by Harvard University in 2022.

In a first step, a country's capabilities to exert cyber power are gauged by eight sub-indicators (from 0 to 100). In a second step, these capabilities are weighted according to a country's intent to leverage specific capabilities (from 0 to 1).





Data: Harvard, *National Cyber Power Index*, 2022

prematurely) whether Russia's cyber 'power' had been somewhat overrated [17].

By contrast, Chinese state and state-sponsored 'Pandas' have long focused on cyber espionage aimed at commercial gain (including through intellectual property theft), soon followed by asset acquisition and network control (first along the so-called New Silk Road and then worldwide), and have only recently become more assertive also in the global battle of narratives, especially after the Covid-19 outbreak. China, however, is explicitly aiming not only at comprehensive technological predominance in the medium term but also at (re)shaping cyberspace and the internet. The Chinese 'model', as opposed to the still dominant 'Californian' model, is centred upon the so-called Great Firewall at home and technological control abroad, and it relies on huge manpower resources and close coordination between state authorities and private players – thus potentially threatening US cyber superiority and fostering a 'bipolar' cyberspace.

DETERRENCE AND DEFENCE IN CYBERSPACE

The emphasis on *offensive* cyber capabilities – which cover the full range of active operations, regardless of whether they are run by civilians or the military – is quite recent and reflects growing frustration over the proliferation of hostile activities during the past few years. Despite different interpretations of the applicability of international law (including humanitarian law) to cyberspace, most experts believe that it is already entirely possible to justify retorsions for such activities and even to apply – in certain conditions – 'countermeasures' that do not include the use of force [18]. Most importantly, such responses need not be limited to the cyber domain: on the contrary, several national strategies now make reference to diplomatic, information, military, economic, financial, intelligence and legal (DIMEFIL) measures as part of a comprehensive, 'cross-domain' toolbox.

At multilateral regional level, both the EU and NATO have equipped themselves to prevent, mitigate and respond to hostile cyber activities by building on their respective strengths and mandates. The EU has boosted its cyber resilience by adopting new legislation aimed at strengthening the resilience of critical entities and critical information infrastructure. It has also strengthened its diplomatic response thanks to a dedicated Cyber Diplomatic Toolbox that allows the imposition of sanctions against individuals and entities in cases of significant attacks (an option that has already been used on a couple of occasions).

For its part, NATO has adopted stricter technical criteria for its own networks and beefed up its Baseline Requirements to ensure the resilience of critical national infrastructure. The Alliance has also agreed in 2019 a Guide for Strategic Response Options to Significant Malicious Cyber Activities (those falling below the level of armed conflict), created a mechanism for integrating some offensive cyber tools – the so-called Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) – into its missions and operations [19] and, in 2021, adopted a new Comprehensive Cyber Defence

[17] Srivastava, M., 'Kremlin's cyber abilities may be overhyped, says UK spy chief', *Financial Times*, 11 May 2022.

[18] While the initial broad consensus reached at UN level with the 2013 and especially the 2015 GGE Reports on the general applicability of international law to the use of digital technologies has gradually waned, significant work has been carried out at academic level through the two iterations of the so-called 'Tallinn Manuals': see Schmitt, M.N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013; and Schmitt, M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.

[19] Several Allies have already made their national 'effects' available, in principle, to Supreme Allied Commander Europe (SACEUR), while a Cyber Operations Center (CyOC) – though not a Cyber Command proper – has been set up at NATO Military Headquarters (SHAPE) in Mons. NATO had declared cyber as a domain of military operations – alongside land, sea and air – in 2016.

Policy, updating its 2014 Enhanced Cyber Defence Policy.

Last but not least, in addition to EU regulation and NATO standardisation, in February 2016 the computer emergency/incident response teams of the two organisations (CERT-EU and N-CIRC) signed a bilateral Technical Agreement on the exchange of information about threat actors and techniques, and cyber elements have regularly been incorporated in crisis management exercises involving the Union and the Alliance [(20)]. Cyber-related intelligence sharing and capacity building with partner countries have also increased significantly and take place more or less informally between government agencies.

These steps show that cyber defence encompasses a whole range of civilian and military concepts, authorities and resources which, in turn, require a high degree of coordination and convergence at both domestic and international level. The measures taken to date by individual countries as well as organisations like the EU and NATO in response to hostile cyber activities may not amount to *strategic* deterrence as we know it, i.e. the classical combination of denial and punishment – if anything, because in the nuclear domain weapons are *not* meant to be used, while in the cyber domain they are constantly used. Yet they may contribute to *tailored* deterrence by appropriately combining a higher degree of denial (resilience), propensity to expose and stigmatise hostile activity (attribution), and readiness for punishment (not necessarily in kind); by constantly adapting defences to one's own vulnerabilities and the type of threat actors involved; and by calibrating responses accordingly. Rather than reacting to each individual hostile action or specific effect, for instance, it may prove strategically more efficacious to respond – preferably jointly and in a coordinated fashion – to repeated actions and cumulative effects by one and the same perpetrator.

After all, policy cooperation and convergence among like-minded countries are also necessary to support and facilitate global efforts to preserve a free, open and secure cyberspace and to deter (or at least discourage and contain) operations that go well beyond what is considered acceptable by the international community – including by the military, increasingly confronted by the 'unknown unknowns' and ethical dilemmas generated by the new technologies. If digital weapons cannot be banned, at least certain targets and techniques could – and indeed should.

(20) More detailed information about these EU and NATO initiatives can be accessed through their respective websites.

CHAPTER 2

SEMANTICS: CYBERSECURITY, DEFENCE AND CYBER DEFENCE

by
ENEKEN TIKK AND MIKA KERTTUNEN

INTRODUCTION

Defence is an inherently national prerogative that comprises a wide range of predominantly military means and measures. Typically, the role of defence organisations is to safeguard national aspirations and activities *against* the potential, even likelihood, of violence and destruction. Defence policy helps situate a country in the international security environment. Where foreign policy efforts fail to prevent spiralling insecurity and conflict, defence policy provides the state with operational resources and capabilities to ensure military deterrence and, ultimately, response.

In the current fragile and deteriorating international security environment, national defence postures have come to employ elements of security, intelligence and trade. However, even close political allies within dedicated international defence frameworks prioritise independent national capabilities alongside, or over, collective security and defence mechanisms [(1)]. Countries continue to withhold not just intelligence and operational know-how but also the wider considerations and factors that inform and frame their security policy decisions.

Matters of defence have been difficult to settle in the EU. The idea of European defence was originally conceived in the context of the post-war drive towards increased cooperation. Along with agriculture, European defence became one of the challenges in European integration after the Cold War. A functional and autonomous defence for Europe has remained a utopian aspiration with fluctuating ups and downs over the past few decades. For the time being, European defence remains limited primarily to the EU's defence policy, including (some) capability development [(2)].

Meanwhile, it is imperative that Europe's critical infrastructure be better safeguarded and protected in cyberspace. In an unstable and adversarial international climate, most advanced information societies have proven a lucrative and relatively easy target for cyber-attacks and various influence operations. The intersection of digitalisation and security is a complex and demanding phenomenon. On the

(1) See for example Jensen, M. S., 'Five good reasons for NATO's pragmatic approach to offensive cyberspace operations', *Defence Studies*, May 2022 (https://doi.org/10.1080/14702436.2022.2080661).

(2) Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Lisbon, 13 December 2007 (http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0007.01/DOC_19).

one hand, European cyber defence will remain subject to the pitfalls and challenges of general defence cooperation, thus requiring a meaningful division of competences, mandates and tasks between Member States, the EU and NATO. On the other, cyber defence is not the only, and certainly not the primary, way of securing European cyberspace.

This chapter revisits two discussions deriving from the EU Cyber Defence Policy Framework (CDPF). 'To respond to changing security challenges', the framework argues, 'the EU and its Member States have to strengthen cyber resilience and to develop robust cyber security and defence capabilities' [3]. The first part of the analysis focuses on respective challenges. In the face of potentially violent military (cyber) activities, what is to be secured and defended, and against what or whom? – what are the EU's cyber defence imperatives? The second part, emphasising the necessary distinctions between resilience, cybersecurity and defence, focuses on two security-oriented relationships, the first between cybersecurity and cyber defence and the other between defence proper and cyber defence.

Cyber defence is not the only, and certainly not the primary, way of securing European cyberspace.

EUROPE'S CYBER DEFENCE NEEDS

Weighing EU cyber policy measures against EU cyber threat assessments does not necessarily provide conclusive evidence of their security relevance. The cyber threat picture is not uniform in the EU. The EU's cybersecurity strategy underscores the role of states as major threat agents and concludes that the EU is targeted by malicious cyberattacks against which deterrence is needed [4]. Malicious cyber activities are also considered a key element of hybrid campaigns [5]. Meanwhile, in the assessment of the European Union Agency for Network and Information Security (ENISA), state-sponsored entities have entered the threat landscape, but largely driven by economic motivations and with a technical and functional, rather than operational, focus [6].

The 2022 Cybersecurity Strategy contains parallels to the 2021 *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.* Experts have recognised 'states and other actors' as persistent threat actors potentially posing 'a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals.' Rather similarly to the *Final Substantive Report* of the Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, the Group of Governmental Experts (GGE) Report specifying the diversity of state and non-state actors, including criminal groups and terrorists, notes that:

> A number of states are developing information and communication technologies

[3] Council of the European Union, 'EU Cyber Defence Policy Framework (as updated in 2018)', No 14413/18, 19 November 2018 (https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf).

[4] See European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, 'The EU's cybersecurity strategy for the digital decade', JOIN(2020) 18 final, 16 December 2020 p. 3, pp. 16-17 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN).

[5] Council of the European Union, 'Council conclusions on a Framework for a coordinated EU response to hybrid campaigns', para 19, 21 June 2022 (https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/).

[6] ENISA, *ENISA Threat Landscape Report 2018: 15 top cyberthreats and trends*, January 2019, p. 7, p. 14 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018). As the ENISA Report states (p. 14), the report targets security professionals or scholars but that also 'decision makers, security architects, risk managers, auditors clearly belong to the target group' [of the Report].

(ICTs) capabilities for military purposes; and that the use of ICTs in future conflicts between states is becoming more likely;

- States' malicious use of ICT-enabled covert information campaigns influencing the processes, systems and overall stability of another state are potentially escalatory and threatening to international peace and security as well as posing direct and indirect harm to individuals;

- Harmful ICT activity is being directed against critical infrastructure which provide services domestically, regionally or globally, including critical information infrastructure, infrastructure providing essential services to the public and the technical infrastructure essential to the general availability or integrity of the internet and health sector entities;

- New and emerging technologies expand the attack surface and create new vectors and vulnerabilities;

- The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, may threaten international peace and security [(7)].

It is hard to say, however, to what extent these observations are directly relevant to Europe's cyber defence. Recent trends in cyber conflict, on the one hand, support and even amplify the UN GGE and OEWG assessments. In addition to problematising political cyber espionage, state-sponsored cyberattacks have been targeting Covid-19 vaccine research; there have been state-linked cyberattacks against trust services; revenue operations intended to subvert economic sanctions or steal money from other states and the financial sector; targeting of online elections and elections infrastructure; indiscriminate cyber operations that undermine trust in online products and services; and cyber operations against international organisations and events [(8)]. On the other hand, the numerous cyberattacks Russia has launched against Ukrainian networks and critical infrastructure before and during its current military offensive have not managed to achieve notable strategic or operational effect. The employment of Russian cyber capabilities did not enable Russians to capture Kyiv, silence the president, derail Ukrainian railways, or stop the autumn Ukrainian counter-offensive [(9)].

In this light, national and nationwide perspectives on threats and ways of addressing them are worth considering. In the context of national strategies and policies, the question of what we are securing and defending goes beyond the defence sector and purely military means. Most European national cybersecurity strategies recognise state, proxy and politically driven malicious cyber activities but seek to address them by all-of-government and multistakeholder approaches rather than military measures. Although defence forces are mandated to support civil authorities in various emergencies, military cyber capabilities, even dual-useable ones, are predominantly

(7) United Nations, Office for Disarmament Affairs, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*. Advanced copy, 28 May 2021, paragraphs 6-14; United Nations General Assembly, Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, *Final Substantive Report*, A/AC.290/2021/CRP.2 (10 March 2021), paragraphs 15-23 (https://ict4peace.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf).

(8) Tikk, E., Hovhannisyan, K. and Kerttunen, M., *Cyber Conflict Factbook*, Cyber Policy Institute, 2021.

(9) Truth perhaps having become a victim also in 'cyber war', diverse accounts and analyses tell of hundreds of Russian cyber-attacks. See, for example, 'Cyber attacks on Ukraine: Not what you think', *PCMag UK*, 19 May 2022 (https://uk.pcmag.com/antivirus/140473/cyber-attacks-on-ukraine-not-what-you-think); Smith, B., 'Defending Ukraine: Early lessons from the cyber war', 22 June 2022 (https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/); BleepingComputer, 'Ukraine targeted by almost 800 cyberattacks since the war started', 30 June 2022 (https://www.bleepingcomputer.com/news/security/ukraine-targeted-by-almost-800-cyberattacks-since-the-war-started/).

developed for military operations [10]. In liberal democracies they are developed and employed for military purposes only. Domestic prerogatives are civilian, and pragmatically focus on securing the continuity of critical and essential societal, industrial and corporate cyber-digital services [11].

In sum, threat perceptions and models differ in terms of their perspective and subsequent recommendations. UN-based concerns echo superpower competition and focus selectively and rather incoherently on international peace and security. All-European threat assessments and strategies seek to promote such European norms and values as the rule of law, fundamental rights, freedom and democracy [12]. They also are a result of political bargaining among Member States with different ambitions and interests. National strategies, while following relatively fixed technical and functional imperatives, are subject to domestic political changes and fluctuations in resource allocation, and even in value prioritisations.

As it stands, the EU and its Member States cannot rule or single out any particular model or threat. It is paramount to seek to find a balance, or suitable compromise, between justifiable threats-and-measures demands. It is therefore essential to carefully analyse whether a top-down foreign and security policy-centric or a bottom-up domestic needs-based approach is most relevant for European cyber defence aspirations. Conceptually, while the former securitises and, at least partially, militarises the use and development of ICTs, the latter centres around information security as understood in terms of confidentiality, integrity and accessibility of information. Whether the former is too much and the latter too little, and who gets to define the agenda, are strategic questions that remain to be answered.

CYBER DEFENCE, CYBERSECURITY AND DEFENCE: WHAT IS WHAT?

Apart from the question of threat assessment, when contextualising cyber defence ambitions within the EU Global Strategy, the CDPF notes the importance of capabilities in securing 'the EU's strategic role and its capacity to act autonomously'. Accordingly, '[T]hese goals require more cooperation in capability development, promoting the effectiveness and interoperability of the resulting civilian and military capabilities' [13]. The question becomes: what is the role of cyber defence, in addition and in parallel to, resilience and broader cybersecurity?

For cyber defence to have politico-strategic value for the EU, it needs to be aligned with Europe's existing political arrangements and military operational mechanisms, and properly situated in broader European security aspirations. In some aspects, it is already being demonstrated that cyber defence has become an important element in the broader system of crisis management and defence industrial cooperation. Corresponding measures taken under the Permanent Structured Cooperation initiative are telling in this respect: the Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security project and

[10] On how current European national cybersecurity strategies have addressed threats and the role of the defence sector, see for example the Dutch (*National Cyber Security Agenda*, Ministry of Justice and Security, 2018), Estonian (*Cybersecurity Strategy 2019-2022*, Ministry of Economic Affairs and Communication), Portuguese (*National Strategy for Cyberspace Security 2019-2023*, Resolution of the Council of Ministers No. 92/2019) and Spanish (*National Cybersecurity Strategy*, National Security Council, 2019) ones.

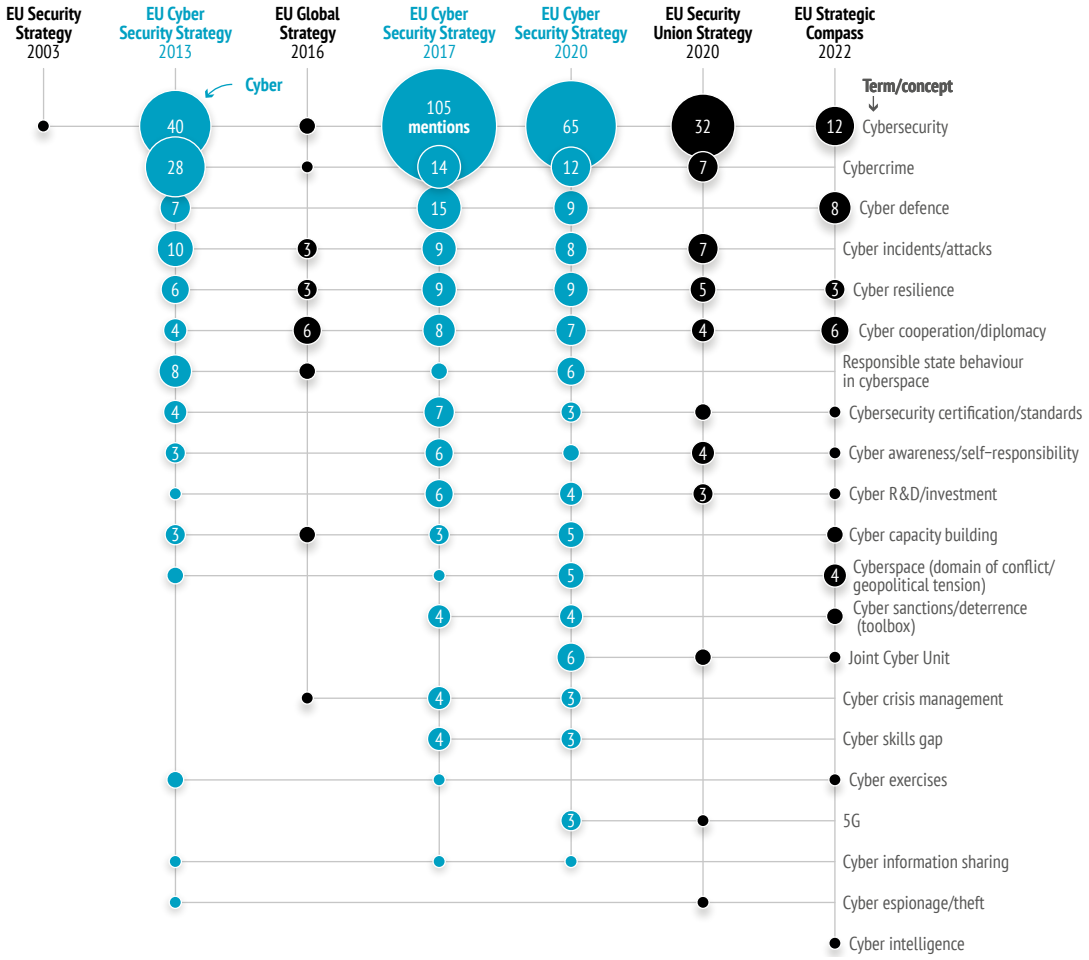
[11] See also Raluca Csernatoni's analysis of the relevant EU policy documents in the chapter 'Future tense: cyber defence and emerging disruptive technologies' in this volume.

[12] 'The EU's cybersecurity strategy for the digital decade', pp. 1-2, op.cit.

[13] 'EU Cyber Defence Policy Framework', op.cit.

Evolution of the EU's cyber vocabulary

Cyber defence has become a recurrent element in the EU's foreign and security strategy, as shown by the number of times related terms and concepts are mentioned in EU security strategy documents



Data: EU strategy documents, 2003–2022

a Cyber Threats and Incident Response Information Sharing Platform[(14)].

The EU's 2020 Cybersecurity Strategy calls for the development of military cyber capabilities. In addition to deliberate emphasis on cyber deterrence, the Strategy encourages the EU and Member States to 'provide further impetus for the development of state-of-the-art cyber defence capabilities through different EU policies and instruments.' This is seen to require 'a strong emphasis on the development and use of key technologies such as AI, encryption and quantum computing.' Moreover, 'the EU should further foster cooperation among Member States on cyber defence research, innovation and capability development, encouraging Member States to make use of the full potential of the Permanent

(14) PESCO Projects, 'Cyber rapid response teams and mutual assistance in cyber security' (https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/); PESCO, 'Cyber threats and incident response information-sharing platform' (https://pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/).

Structured Cooperation (PESCO) and European Defence Fund (EDF)' [15].

However, European cyber defence needs to provide, both *ad hoc* and long-term, more than just cybersecurity or resilience. For sustainable autonomy, the defence sector cannot remain a subsidiary contributor to national cybersecurity – as has tended to be the case so far [16]. Here, the challenge will be to distinguish cyber defence from the IT security of defence organisations, both administratively and financially, and avoid offering defence resources as the first or second answer to the current vacuum of whole-of-government and whole-of-society preparedness to prevent and mitigate cyber incidents.

When compared with the joint military functions of command and control, intelligence, targeting and fires, movement and manoeuvre, protection, and sustainment (logistics) [17], some European cyber defence ambitions start to look more serious and sinister. EU Member States, like several other countries, are developing their own military cyber capabilities. Politically anchored to either national security or collective security within NATO, European governments have allocated taxpayers' money to establishing military cyber commands [18], developing intelligence and offensive cyber operations capabilities and creating cohorts of competent cyber warriors – often without any cyber military doctrine which would establish overall national military guidance and legitimacy. As a result, it is not only rogue or authoritarian states who conduct cyber operations or assume the liberty to do so [19]. Such operational interests drive defence policies to endorse and enable capability development and deployment, without necessarily increasing collective cyber security and defence guarantees.

It is not only rogue or authoritarian states who conduct cyber operations or assume the liberty to do so.

It is also obvious that the importance of cyber operations in and to military operations as well as in information, influence and intelligence activities and civilian projection of state power, is increasing. This raises serious questions for European defence policy – what are the expected benefits of cyber operations, the parameters of conducting them, and applicable collective rules of engagement? Moreover, as the EU Member States' security and defence policy orientations and practices differ, there may exist a legitimacy gap between justifiable technocratic ambitions and Member States' similarly understandable political preferences. The considerations of different Member States merit deeper analysis; for example, while Estonia established a Defence Forces Cyber Command whose remit also includes handling ICT matters for the Defence Ministry, Germany's cyber command became a dedicated operational command, and Finland has chosen not to opt for a command, at least before doctrinal and organisational cyber capacity has been further developed [20].

The relationship and respective tasks and responsibilities between Member States, the EU and NATO also require further clarification. A recent framework for countering hybrid threats underlines that while a stronger and more

[15] 'The EU's cybersecurity strategy for the digital decade', op.cit., p. 17.

[16] Most national cybersecurity strategies do not address the role of the defence sector or defence forces at all. When the relationship is recognised, it is usually, and logically, civilian- and cybersecurity-centric.

[17] See, for example, Joint Chiefs of Staff, *Cyberspace Operations* (JP 3-12), 22 October 2018 (https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150).

[18] Pernik, P., *Preparing for Cyber Conflict: Case studies of cyber command*, International Centre for Defence and Security, Tallinn, 2018 (https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf).

[19] See, for example, 'U.S. Cyberforce was deployed to Estonia to hunt for Russian hackers', *The New York Times*, 3 December 2020; and 'Dutch intelligence first to alert U.S. about Russian hack of Democratic Party', *NOS*, 25 January 2018.

[20] Discussions with respective national authorities.

capable EU in the field of security and defence will contribute positively to global and transatlantic security, it remains complementary not only to Member States but also to NATO, which remains the foundation of collective defence for its members [21]. What this means for EU cyber defence and cyber defence policy is still to be decided.

It is also essential to consider more broadly where EU and Member State cyber defence decisions and trends are taking European defence. The European Parliament resolution on the state of EU cyber defence capabilities is politically ambitious. Here, the Parliament has noticed the 'continuous growth in malicious cyber operations' conducted by state and non-state actors and 'stresses the urgent need to develop and strengthen both common and the Member State cyber defence capabilities'. Broadening the defence ambitions of the Union, the resolution underlines 'that a common cyber defence policy and a substantial EU level cooperation on generating common, and also better, cyber defence capability are core elements for the development of a deepened and enhanced European Defence Union' [22].

CONSIDERATIONS FOR A SUSTAINABLE EUROPEAN CYBER DEFENCE

Aligning European cyber defence with other European defence instruments requires placing the cyber defence requirements and measures into the bigger picture of threats and challenges that the EU, EU Member States and their partners are facing.

The problems of cybersecurity flirting with defence are threefold. Threat assessments provide no real basis to conclude that cyber operations have the potential, let alone are likely, to become profoundly violent and destructive. Firstly, defence proper with the capability to employ violent and destructive military force can easily be diluted if optimised in the context of largely non-military cyber operations. This already happened for most Western countries when a flurry of crisis management operations was launched and 'the war on terrorism' was at its height. Secondly, defence, with its inherently military attributes and functions, will inevitably militarise cybersecurity. Although some might favour military-grade cyber operations, cybersecurity and its twin sister, resilience, benefit from their civilian rather than military, cooperative rather than secretive or adversarial and societal rather than executive nature [23]. Combating cybercrime is a civilian function. Similarly attribution and attribution policies should be left to (superior) civilian agencies and authorities. Finally, few Europeans or Member States advocate for the common destiny of a defence union; we, the Europeans, seem to prefer national defence – or a collective defence arrangement within NATO.

In addition, the proposed policies and measures need to be analysed against existing policies and solutions. Europe cannot afford duplication of efforts, not between the EU and NATO and certainly not between military and civilian authorities. Ultimately, European

(21) 'Council conclusions on a Framework for a coordinated EU response to hybrid campaigns', op.cit**.,** para 2.

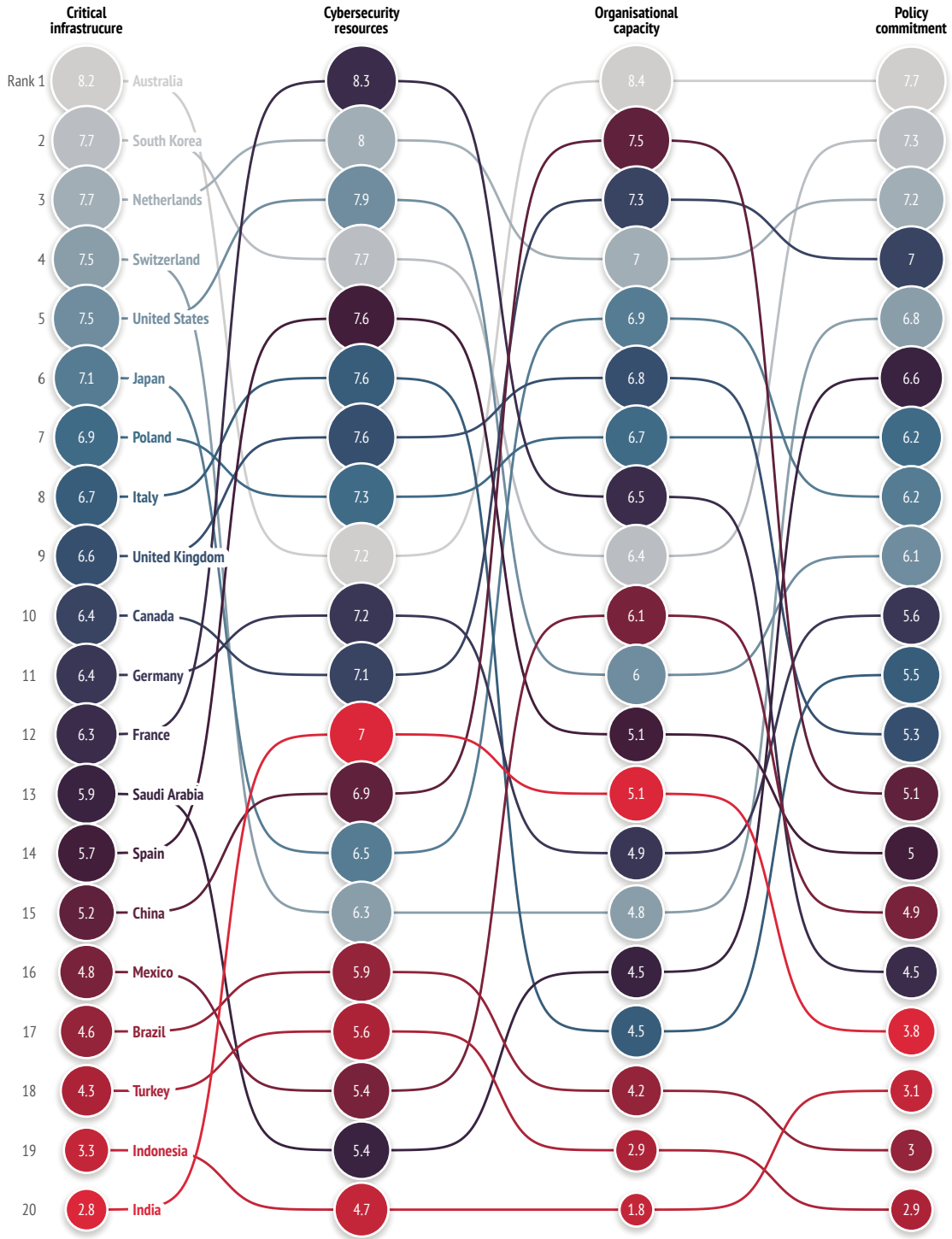
(22) European Parliament, 'European Parliament resolution of 7 October 2021 on the state of EU cyber defence capabilities', 2020/2256, 7 October 2021 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0412&from=EN). Ideationally the notion of a European Defence Union rests on the concept of a European Defence Community of the early 1950s. Politically it is anchored to recent pronouncements by the European Commission, e.g. Commission President Jean-Claude Juncker's State of the Union Address, September 2017 (https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165).

(23) For those interested in foundational considerations on the role of the armed forces in a society (the United States), see Huntington, S., *The Soldier and the State*, Belknap Press of Harvard University Press, Cambridge, 1957 and Janowitz, M., *The Professional Soldier*, Free Press, Glencoe, 1957.

Cyber Defence Index

2022/23

The Cyber Defence Index measures the degree to which 20 of the world's major economies have adopted technology practices that improve resilience to cyberattacks and how well governments and policy frameworks promote secure digital transactions.



Data: MIT, *The Cyber Defense Index 2022/23*, 2022

politicians and senior officials have to be able to explain how European cyber defence policy and capabilities add distinct value to Europe and European security, cybersecurity and resilience. Indeed, the majority of European defence forces are not in a position to conduct sustainable cyber operations, whether in terms of possessing the requisite resources and skills or from a political, legal, doctrinal or organisational point of view. European states and defence sectors have been keen to adopt ICTs, increase connectivity and the flow of digitalised information, but operationally there is a long way to go[(24)].

Cyber military capabilities do fit well in national cybersecurity portfolios. Military communication systems are often deployable and robust and secured; military personnel are known to be adept at solving problems in a mission-oriented manner, and military network and signal intelligence capabilities can support other national intelligence authorities. However, 'the military', the core capacity to seize, control and destroy, is very rarely a useable political tool. The EU should not try to solve global world order or cyber normative problems by resorting to a military approach. Military means are also most unsuitable for solving domestic, societal and technical cyber-digital issues. It is therefore noteworthy that the measures the EU has taken to strengthen cybersecurity in 2020-2022 primarily focus on resilience and cybersecurity proper[(25)].

The current direction of EU cyber defence policy expands the executive branch of power. The inclusion of defence, both as a notion and a sector, into European cybersecurity echoes the concerns about the 'military-industrial complex' described by President Eisenhower in his farewell address of 1961[(26)]. If the weapons industry of the 1950s and 1960s was able to shape American defence and military policy, the new cybersecurity policy and capability industry has no less potential for influence. Proactive defence involves transfer of authority to the executive branch and the creation of new mandates. The 'contract state', founded on the Treaties and the rule of law, should therefore seek to implement strong political control to avoid unnecessary securitisation and militarisation of information technology and cyber development policies.

The majority of European defence forces are not in a position to conduct sustainable cyber operations.

Maybe it is a characteristic European trait to keep high ambitions alive while implementing more modest, acceptable and feasible, objectives? The EU's currently overly ambiguous and ambitious cyber defence policy is however likely to deepen global antagonism and undermine regional stability, if not international peace. What is of particular concern is the EU establishment and some Member States eagerly pursuing cyber military capabilities while globally such a course is being considered problematic. European cyber defence policy and tangible measures taken to implement it need to provide clear and compelling political value for the EU as an international actor and enhance the Union's ability to address actual security and defence needs.

(24) Smeets, M., *No Shortcuts: Why states struggle to develop a military cyber-force,* Hurst Publishers, London, 2022.

(25) Council of the European Union, 'Cybersecurity: How the EU tackles cyber threats. Timeline – cybersecurity' (https://www.consilium.europa.eu/en/policies/cybersecurity/timeline-cybersecurity/).

(26) US National Archives, 'President Dwight D. Eisenhower's Farewell Address', 1961 (https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address).

CHAPTER 3

SYNTAX: SUBJECTS AND OBJECTS IN ACTIVE CYBER DEFENCE

by
MATTHIAS SCHULZE

INTRODUCTION

It is common wisdom that cyber operations often do not entail repercussions for the attackers, which is part of the reason why ransomware has become one of the most lucrative criminal business models in recent years. Attribution and international law enforcement collaboration problems make it hard to extradite hackers based in foreign countries. To solve this problem, some states are seeking to engage in active cyber defence. Instead of relying on passive perimeter defences like firewalls and intrusion detection systems, they want to adopt a more offensive posture.

There is no agreed-upon definition of active cyber defence and it can have various purposes and goals. Penetration testing of an organisation's own networks, takeover of botnets and open source intelligence generation in the Darknet and hacker forums are all forms of active measures that serve a defensive purpose, which does not necessary require hacking into foreign systems. Cyber operations can also serve the purpose of active defence: one goal could be to tactically disrupt ongoing cyber operations at the source, in adversary networks. Another goal could be to 'hunt forward' in allied networks for signs of malicious activities and use this knowledge to bolster one's own defences. Another goal could be to create deterrence by threat of punishment. The logic goes like this: an attacker will think twice if there are consequences to be expected in the form of a counter cyberattack. Since raising IT-security and building society-wide cyber resilience is a complex, costly and time-consuming endeavour, active cyber defence is sometimes heralded as the panacea.

As the EU is pondering the next step in its cyber sanctions regime and trying to define its cyber deterrence posture, it is worthwhile asking whether active cyber defence or its conceptual successor, known as 'persistent engagement', can be an appropriate strategy for the EU. This chapter compares the US and EU approaches to active cyber defence. It focuses on the goals, the required means and the linkage with other cyber policy issues such as international norms development. Unfortunately, the success of active defence is mixed and persistent engagement has high operational requirements in terms of intelligence sharing. As a deterrent, its effectiveness is severely limited.

A SHORT HISTORY OF ACTIVE DEFENCE

In 2012, President Obama issued Presidential Policy Directive 20 in an attempt to establish an active cyber defence policy for the United States [1]. The directive allowed US intelligence agencies to conduct offensive cyber operations to produce effects outside of US networks, like disrupting enemy command and control systems, and to protect against 'imminent threats'. These cyber operations required high-level presidential approval [2].

In the years that followed the creation of an active cyber defence policy, the US fell victim to a series of high-profile cyber operations: the Sony Pictures hack in 2014, the Office of Personnel Management breach in 2015, the Shadow Brokers episode in 2016, WannaCry, NotPetya (both 2017) and more. Critics argue that active cyber defence did little to stop these attacks or even to deter Russian influence operations during the 2016 presidential election. Some argue the failure was due to Barack Obama's reluctance to employ active defence out of fear of escalation: the US as a vulnerable high-tech nation has more to lose in a tit-for-tat cyber escalation than others [3]. Others attribute the failure of active defence to prevent these incidents to bureaucratic constraints and lengthy approval processes [4].

Meanwhile, US Cybercommand was learning its first practical lessons with cyber operations by actively disrupting the digital networks of the so-called Islamic State in Iraq and Syria (ISIS) [5]. This turned out to be a cat and mouse game: ISIS was very quick in rebuilding its IT infrastructure after it was disabled by US Cybercommand cyber operations. The lesson learned from this was that *ad hoc* cyberattacks are futile against agile and resilient adversaries that can quickly rebuild infrastructure. In the end, a continuous engagement was necessary to effectively shut down ISIS digital infrastructure. The lesson learned was that *ad hoc* active defence is inefficient in a high-speed, high-volume and high-velocity strategic environment where cumulative attacks unfold in continuous campaigns, targeting multiple organisations over a long period of time. In combination with lessons learned from cyber interactions with Russia, China, Iran and North Korea, the United States scrapped its active cyber defence policy in 2018 under the Trump presidency and replaced it with a new strategic vision: persistent engagement and defending forward.

GOALS OF PERSISTENT ENGAGEMENT

The vision is based on an understanding of cyber-conflict as a low-intensity conflict or strategic competition below the threshold of an armed conflict and not as an outright cyber-war above the said threshold [6]. The new strategy was built on the premise that the cyber environment is dramatically different compared to the conventional or the nuclear domain. The interconnectedness of cyberspace

(1) Presidential Policy Directive 20, PDD-20, reproduced in 'Obama tells intelligence chiefs to draw up cyber target list – full document text', 7 June 2013 (https://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text).

(2) Raymond, A.K., 'Trump makes it easier for the military to launch cyberattacks', *Intelligencer*, 16 August 2018 (https://nymag.com/intelligencer/2018/08/trump-makes-it-easier-for-the-u-s-to-launch-cyber-attacks.html).

(3) Sanger, D., *The Perfect Weapon: War, sabotage and fear in the cyber age*, Crown Publishers, London, 2018, p.9.

(4) Geller, E., 'Trump scraps Obama rules on cyberattacks, giving military freer hand', *Politico*, 16 August 2018 (https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095).

(5) Temple-Raston, D., 'How the US hacked ISIS', NPR, 26 September 2019 (https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis).

(6) Lindsay, J.R., 'Stuxnet and the limits of cyber warfare', *Security Studies*, Vol. 22, No 3, 2013, pp. 365–404.

creates constant contact of actors in a network of networks that transcends national boundaries. At the same time, vulnerable IT systems control many resources of state power and harbour useful strategic information. Thus, exploiting these infrastructures and extracting information cumulatively creates strategic advantages in the form of technical and military superiority [(7)]. This implies that security concepts inherited from the Cold War such as coercion or deterrence by punishment no longer work.

The goal of the US vision is to achieve 'superiority through persistence' that 'maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they manoeuvre' [(8)]. First, it recognises that cyber defence and offense are logically intertwined: knowing how to hack into foreign networks and learning from adversary behaviour is also useful for defence. That is why persistent engagement employs active threat hunting methods that are traditionally used to identify and pursue attackers deeply burrowed within one's *own* network, externally in foreign networks. Knowledge gained is then communicated to defenders to enable them to anticipate and mitigate current attack campaigns by adversaries more swiftly.

The US as a vulnerable high-tech nation has more to lose in a tit-for-tat cyber escalation than others.

Second, persistent engagement has a twofold temporal dimension: instead of passively waiting to be attacked at one's own perimeter, persistent engagement has a pre-emptive logic built-in. It tries to stop hostile cyber activity before it materialises in US perimeters and networks. This is based on the 'assume breach' paradigm of information security: the attacker will always get through and it is incredibly hard to keep an APT outside of a network. Thus, the partner concept of 'defending forward' tries to turn this dynamic upside down by putting pressure on the attacker in bringing the 'battle' to the adversary by disrupting its operational infrastructure which is likely hosted in foreign countries. Defend forward tries to actively contest adversaries by disrupting their cyber operation's infrastructure, e.g. command and control servers, to steer malware and infected devices before, or during, ongoing attacks. It is designed as a tactical counter-force capability and not as a strategic counter-value capability that targets strategic sources of national power like critical infrastructures. The cyber operation against the Russian Internet Research Agency to conduct cyber-enabled influence operations during the US mid-term elections in 2018 serves as an illustrative example here [(9)]. But since cyber-infrastructure is often redundant and resilient, meaning it can be rebuilt quickly and cheaply, it requires a *continuous* contestation. This is the second temporal factor: in principle, persistent engagement operations have no end. They are ongoing and indefinite. [(10)]

Third, there is an element of cost imposition. The idea is that disrupting adversary command and control servers will introduce friction into adversary cyber operations. This is done by burning adversary malware by reporting it to anti-virus vendors or by finding and

(7) Harknett, R. J., and Smeets, M., 'Cyber campaigns and strategic outcomes', *Journal of Strategic Studies*, 2020, pp.1-34 (https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354).

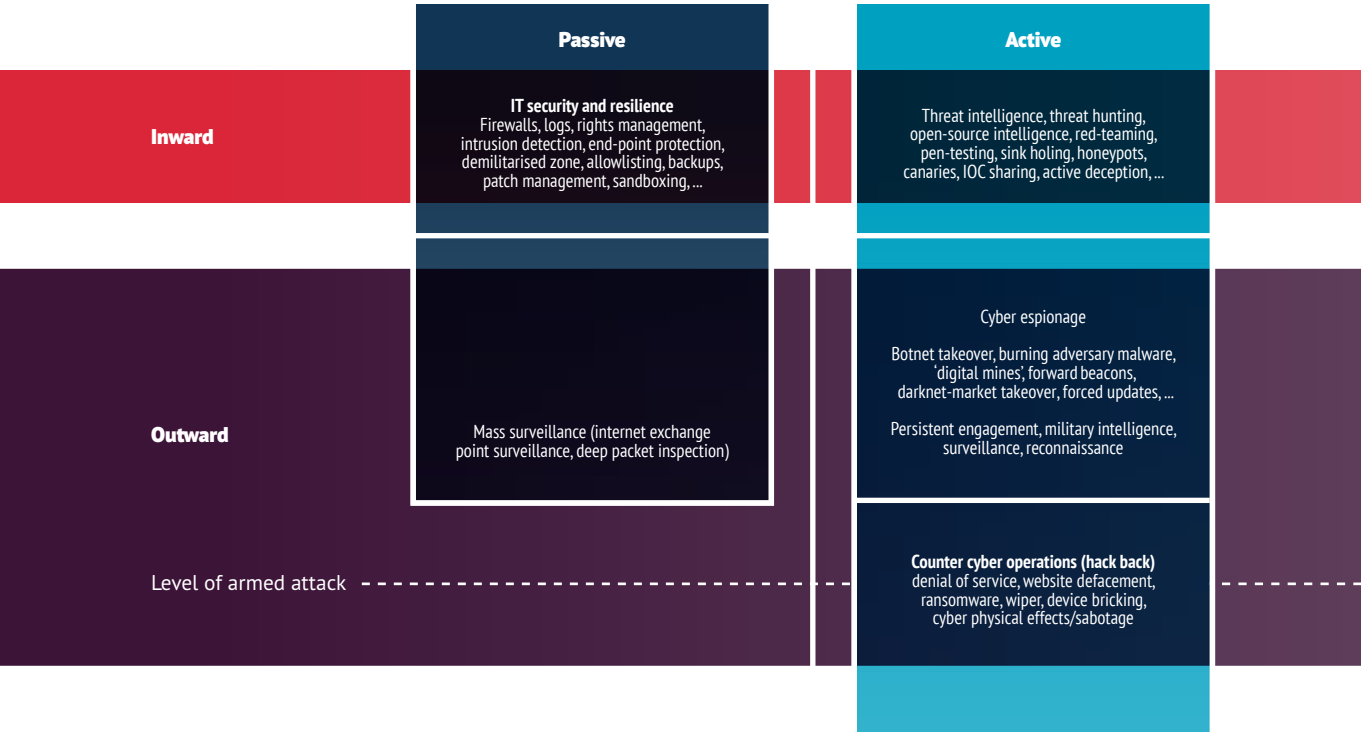
(8) Department of Defense, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command' (https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.)

(9) Nakashima, E., 'US Cyber Command operation disrupted internet access of Russian troll factory on day of 2018 midterms', *The Washington Post*, 26 February 2019 (https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html).

(10) Schneider, J., 'Persistent engagement: Foundation, evolution and evaluation of a strategy', Lawfare Blog, 10 May 2019 (https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy).

States' use of cyber tools

Active cyber defence may sometimes reach the level of an armed attack and result in conflict escalation



reporting zero-day vulnerabilities that serve as the basis for exploits disclosed to software manufacturers which then can develop a patch to deny this attack vector. Another method would be to lock adversary administrators out of their systems by altering passwords. The idea is to make adversary operations slower, more complex, more costly, and more uncertain regarding their outcome and effectiveness. If a vulnerability is burned through a patch, an attack campaign has to be redesigned to accommodate that loss. Attackers will have to replace disabled attack infrastructures, spend additional resources to find new vulnerabilities, and spend more time developing new malware. Persistent engagement requires cyber-adversaries to invest more time and money in protecting their attack-infrastructure, otherwise they might lose it. The hope is that in the long run attackers will shift more resources to their own defences and thus have less resources available to invest in their offense. In principle, this could result in fewer cyber operations being directed at the United States.

Fourth, persistent engagement is proposed as an alternative way to create new cyber norms. The originators of the idea argue that constant interaction between attackers and defenders will create an 'agreed competition' below the threshold of armed conflict [(11)]. This is an alternative for managing escalation (the other alternative being deterrence by punishment). It is not a contractual arrangement but rather a set of *de facto* norms and red lines that develop

(11) Fischerkeller, M.P. and Harknett, R.J, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation*, Institute for Defense Analyses, 2018, p. 5 (https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx).

out of practice, through attacker and defender behaviour over time. During their engagement, cyber operators will tacitly bargain with one another and in the course of repeated interactions agree on certain implicit rules of engagement, for example not risking escalation into the kinetic or conventional domain [12]. This is akin to the tacit gentlemen's agreements between intelligence agencies during the Cold War not to pursue certain practices. The hope is that norms and agreements on the operational level between cyber operators spill over and shape behaviour on the strategic level between states (bottom-up instead of top-down as with the UN GGE). One hope is that states 'recognize a firebreak between cyber operations and other more conventional means of conflict' [13]. The other hope is that agreed competition replaces the current *de facto* norm of a free-for-all cyberspace in which states can act with relative impunity [14].

THE QUESTION OF DETERRENCE

Since the EU is currently in the process of further defining its cyber deterrence posture it is worthwhile asking whether persistent engagement can contribute to cyber deterrence. The Department of Defense (DoD) vision maintains that persistent engagement contributes to strategic deterrence by punishment and that it can deter aggression by influencing the decision calculus of adversaries. It does not explicitly state how. Some commentators argue that persistent engagement was born out of the realisation that cyber deterrence by punishment strategies, i.e. retaliating against cyberattacks with active cyber defence to achieve strategic effects, *is not a credible strategy* [15]. This implies different organisational understandings of the concept: the State Department and parts of the US Department of Defense believe in cyber deterrence by punishment, while the operational level at US Cybercommand has less faith in the concept.

The idea of deterrence by punishment is to avoid direct contact and confrontation between two parties, with one side threatening the use of force and signalling its intent to use it, once a certain threshold or red line is crossed. Successful deterrence is defined by the absence of unwanted behaviour. Historically, these red lines have been based on geography, i.e. crossing of borders, or based on effects, i.e. the prohibition to use chemical or nuclear weapons. Some commentators argue that deterrence by punishment in cyberspace (but not necessarily in the other domains of war) is flawed because (a) the environment is shaped by constant contact and continuous activity and not by the absence of it; (b) a deterrence posture based on territorial boundaries and Westphalian concepts of sovereignty makes no sense in an interconnected network of networks where every node can communicate with one another; (c) the majority of cyber operations intentionally stay below the threshold of armed attacks and feature characteristics of subversion, espionage and tactical (not strategic) sabotage. In cyberspace, the multitude of non-state actors and proxies makes deterrence by punishment an unfeasible option to counter most malign

(12) Fischerkeller, M.P. and Harknett, R.J., 'Persistent engagement and tacit bargaining: A path toward constructing norms in cyberspace', Lawfare Blog, 9 November 2018 (https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace).

(13) Schneider, J., 'Persistent engagement: Foundation, evolution and evaluation of a strategy', Lawfare Blog, 10 May 2019 (https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy).

(14) Harknett, R., 'United States Cyber Command's new vision: What it entails and why it matters', Lawfare Blog, 23 March 2018 (https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters).

(15) Fischerkeller, M.P. and Harknett, R.J, 'Deterrence is not a credible strategy for cyberspace', *Orbis*, Vol. 61, No 3, 2017, pp. 381–393.

cyber activity, at least below the threshold of armed attacks [16].

To this it may be replied that cyber-deterrence by punishment has still a role to play for cyber defence as there is an indication that high-level deterrence above the threshold of armed attacks is indeed working [17]. High-level destructive or disruptive cyberattacks against strategic targets on a massive scale, and with critical effects comparable to that of an armed attack, rarely happen, if at all. One reason might be self-restraint due to fear of unwanted escalation [18]. Due to the interconnected nature of cyberspace, attackers cannot be sure what type of cascading or blowback effects might happen. This acts as a restraint for attackers or alternatively as 'deterrence by entanglement' [19]. Yet, it is hard to deter lower level or sub-threshold cyber activity like subversion, cyber espionage, and cybercrime especially if non-state actors are involved.

COMPARING THE EU AND US APPROACHES

It is therefore clear that the EU's strategic approach to cyberspace is in stark contrast to the vision of persistent engagement. The goal of EU cyber diplomacy is 'to prevent, deter and respond to malicious cyber activities directed against the EU or its member states' [20]. The EU tries to achieve this through multiple instruments of soft and normative power: e.g. international law, cyber sanctions, cyber norms and confidence-building measures and law enforcement.

Persistent engagement involves more of a cyber hard power approach. From a persistent engagement perspective, the EU is stuck in the old conceptual thinking of cyber warfare, which focuses on cyberattacks rather than armed attacks as its primary threat model. The EU tries to support abstract, diplomatic norms of responsible state behaviour that have little to do with the operational reality and *de facto* norms of behaviour among cyber operators. The current EU cybersecurity posture is based on a logic of response: reacting to cyber operations through diplomatic means and law enforcement that kicks in *after* the fact [21]. Because attribution capabilities vary across EU Member States, the process of technical, legal and, finally, political attribution (naming and shaming) and imposition of cyber sanctions, is rather slow [22]. The EU assumes that soft power instruments in the cyber toolbox are sufficient to change the cost/benefit calculus of potential attackers. It seems unlikely that even the sharpest tool in the box, restrictive measures, will impose meaningful costs on adversaries [23]. The same is true for current EU law enforcement efforts. Although Europol is quite capable in dismantling botnets and darknet markets, the operational impact tends to be short-lived as new alternatives pop up almost immediately.

[16] Schulze, M., 'Cyber deterrence is overrated', German Institute for International and Security Affairs, SWP Comment 2019/C34, 21 August 2019 (https://www.swp-berlin.org/publikation/cyber-deterrence-is-overrated).

[17] Lin, H. and Smeets, M., 'What is absent from the U.S. Cyber Command "Vision"', Lawfare Blog, 3 May 2018 (https://www.lawfareblog.com/what-absent-us-cyber-command-vision.)

[18] Valeriano, B., Jensen, B.M. and Maness, R.C., *Cyber Strategy: The evolving character of power and coercion*, Oxford University Press, New York, 2018.

[19] Nye, J.S., 'Deterrence and dissuasion in cyberspace', *International Security*, Vol. 41, No 3, 2017, pp. 44–71.

[20] Council of the European Union, 'EU imposes the first ever sanctions against cyber-attacks', 30 July 2022 (https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/).

[21] Nakasone, P., 'A Cyber Force for persistent operations', *Joint Forces Quarterly*, No 92, 2019, pp. 10–14.

[22] Schulze, M. and Bendiek, A., 'Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW', SWP Research Paper 2021/ RP 11, 16 December 2021 (https://www.swp-berlin.org/publications/products/research_papers/2021RP11_EU_CyberSanctions.pdf).

[23] Soesanto, S., 'Europe has no strategy on cyber sanctions', Lawfare Blog, 20 November 2020 (https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions).

In principle, there are even sharper tools in the EU cyber toolbox, namely launching countermeasures (once attribution is successful or a failure of due diligence by another state can be demonstrated) or, at the extreme end, the activation of the EU's solidarity clause once a cyber operation reaches the threshold of an armed attack. This is analogous to NATO's invocation of Article 5 if a cyberattack reaches the scale and intensity of an armed attack. If counter cyberattacks were to play a part in that in the future, the model would likely be akin to the active cyber defence policy and culture of restraint developed under the Obama administration. The problem with this approach is that it is designed to deter significant, high-level cyber operations above the threshold of armed attacks, but it does not address the below-threshold espionage and sabotage activity. For persistent engagement, reacting to high-level cyber operations with counter operations is insufficient as multiple, insignificant cumulative cyberattacks can collectively be as catastrophic [(24)]. Right now the EU is operating in a strategic vacuum: it is unclear how EU active cyber defence could complement diplomatic means in the toolbox targeting these low-level activities without invoking the solidarity clause, which is not warranted in response to below-threshold cyber-activities [(25)].

TENSIONS BETWEEN THE APPROACHES

The competing approaches between the EU and the United States are likely to create tensions in the future. Defending forward might include effects operations in allied networks on EU territory. The only known precedent is a case where US Cybercommand wiped propaganda material from a server in Germany [(26)]. The German government was notified but did not have a say in the matter, which caused minor diplomatic tensions. This brings up the question of notification requirements before US Cybercommand disrupts a server on allied territory. This is related to an ongoing discussion in international law, whether persistent engagement operations below the threshold of armed attacks in foreign networks are akin to espionage operations and thus not illegal, or whether they have more military characteristics and constitute a violation of the sovereignty principle. [(27)] Some EU Member States like the Netherlands argue that persistent engagement might constitute a violation of sovereignty. The United States has not published its own assessment on the sovereignty matter. It could be that a majority of EU Member States come to the conclusion that persistent engagement is incompatible with international law and thus with the rules-based order in cyberspace which the EU promotes. Whatever the final verdict, taking down a system in allied territory via a cyber operation without notification or consent of another ally might undermine trust. In the worst case, this could affect an ongoing law enforcement or intelligence operation already being conducted on

(24) Goldman, E. O., 'From reaction to action: Adopting a competitive posture in Cyber Diplomacy', *Texas National Security Review*, Vol. 3, No 4, 2020, p. 94 (http://dx.doi.org/10.26153/tsw/10950).

(25) Liebetrau, T., 'Cyber conflict short of war: A European strategic vacuum', *European Security*, February 2022, pp. 1–20 (https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2031991).

(26) Smeets, M., 'U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and intelligence collection', *Intelligence and National Security*, Vol. 35, No 3, 2020, pp. 444–453.

(27) Chesney, R., 'Title 10 and Title 50 issues When computer network operations impact third countries', Lawfare Blog, 12 April 2018 (https://www.lawfareblog.com/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries).

the computer system that is disrupted by this persistent engagement activity.

To avoid tensions like this, the idea of collective persistent engagement has been mooted, i.e. including allies in the process to increase the punch of the strategy [28]. The EU or other NATO states are obvious candidates, as they too start to build up military cybercommands. Burden-sharing could compensate the costs of the US approach which is quite broad and lacks meaningful prioritisation of which adversary (China, Russia, North Korea, Iran), to contest [29]. In the end, it boils down to the number of personnel: how many persistent engagers can actively contest which number of adversary cyber teams? If there are more attackers than persistent engagers (and when non-state hackers are included this is likely to be the case), the chances are that adversaries will slip through and outmanoeuvre these forces, as was the case with Solar Winds [30]. Therefore, permanent investment and more attack teams are required to tighten the net around adversary activity. Including allies in some form of burden-sharing might be a plausible solution to this numbers game.

However, the operational requirements of collective persistent engagement are complex. First, the EU does not have a single coordination structure like US Cybercommand. Persistent engagement works because of the tightly-knit connection between intelligence gathering, military cyber operations and intelligence sharing with the private sector. This is best done in a joint planning process between intelligence and military entities in order not to accidentally burn espionage assets due to a failed persistent engagement operation. In the EU, military and intelligence agencies are usually separated and operate under different legal regimes, reducing their operational effectiveness for persistent engagement. An integrated military and intelligence unit, tasked with persistent cyber operations in foreign networks, coordinated at the EU level has currently no legal basis (Art. 4(2) Treaty on the European Union). And then there is the classic reluctance of states' governments to outsource national sovereign powers to the EU as well as to agree to cyber intelligence sharing between intelligence agencies [31]. Additionally, the more actors are involved, the more complex a bureaucratic coordination process becomes. This creates the challenge to maintain the necessary secrecy for collective persistent engagement operations in order not lose assets. All of this hampers the operationalisation of a collective persistent engagement process in the EU. If the EU were to actively engage in cyber defence or persistent engagement, it would require a unanimous vote by the Member States within the framework of the CSDP.

Second, tacit bargaining requires a uniform actor that shares the tacit behavioural knowledge and interprets it with a common lens. Developing behavioural norms of agreed competition in a multi-stakeholder setting with different countries and respective strategic cultures and thus diverse threat interpretations, is more difficult. Different EU Member States are likely to draw different conclusions from persistent engagements on what norms of appropriate state behaviour are indeed tacitly agreed upon.

Third, there is also the risk that these tacit norms of agreed competition, and the explicitly discussed norms of the UN GGE which the EU promotes, are not necessarily compatible with one another: the UN GGE norms speak of not harming critical infrastructures or not

(28) Manantan, M., 'The missing pieces of the US Cyber Strategy of "Persistent Engagement"', *The Diplomat*, 28 April 2021 (https://thediplomat.com/2021/04/the-missing-pieces-of-the-us-cyber-strategy-of-persistent-engagement/).

(29) Lin, H. and Smeets, M., 'What is absent from the U.S. Cyber Command "vision"', Lawfare Blog, 3 May 2018 (https://www.lawfareblog.com/what-absent-us-cyber-command-vision.)

(30) Harknett, R., 'SolarWinds: The need for Persistent Engagement', Lawfare Blog, 23 December 2020 (https://www.lawfareblog.com/solarwinds-need-persistent-engagement).

(31) Seyfried, P., 'A European intelligence service? Potentials and limits of intelligence cooperation at EU level', Federal Academy for Security Policy, Working Paper No. 20/ 2017 (https://www.baks.bund.de/sites/baks010/files/working_paper_2017_20.pdf).

harming emergency response teams. But these norms have been caught in the crosshairs recently: Moscow accused Washington of attacking critical infrastructures in Russia to 'defend forward' [32]. US Cybercommand also indicated that it was active against Russian networks in support of Ukraine in the ongoing war [33]. If the EU were to join collective persistent engagement, it might undermine its stance as a normative cyberpower. It is also conceivable that malign cyber operators will outmanoeuvre US persistent engagement efforts by intentionally launching their attacks from their own or even remote-controlled third-party critical infrastructures in the hope that this might provide some sort of 'human' shield, because the United States and its allies will not attack these systems.

These tensions between tacit and explicit UN GGE norms are highly likely to continue. Behaviou r becomes normalised if it goes uncontested. Currently, internet control and surveillance, systemic privacy violations, interference in domestic discourses, and economic and political espionage are *de facto* behavioural norms of cyberspace [34]. It is hard to see how the Solar Winds hack represents any form of agreed competition or norms of practice, even though it was 'just' large-scale espionage (unless the United States had a similar, large-scale operation in place as one commentator has speculated) [35]. The United States in the past did not agree that intellectual property theft and cyber espionage carried out for economic reasons are valid forms of inter-state competition and does not interpret Solar Winds as agreed, but rather as 'egregious' cyber-behaviour [36].

Lastly, persistent engagement might create a conflict for the EU in terms of its goals and aspirations. The EU strategy aims for stability and de-escalation in cyberspace. Although the somewhat 'hawkish' proponents of persistent engagement argue that the strategy is intended to be de-escalatory and thus creates stability in the long run, others warn that this causal mechanism is speculative and that there is escalatory potential, especially given ongoing geopolitical tensions [37]. Escalation is in the eye of the beholder as there is always room for misinterpretation of adversary intent. There are some indications that Russia and China are ramping up their cyber offensive capabilities, to counter the United States' persistent engagement strategy. This could create an endless cycle as persistent engagement currently has no clear indicators of success or failure, signalling when persistent operations should end because there is no further need to engage [38].

It is conceivable that the US will push for collective persistent engagement either via NATO or via the EU.

[32] Sanger, D., and Perlroth, N., 'U.S. escalates online attacks on Russia's power grid', *The New York Times*, 15 June 2019 (https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html).

[33] Greig, J., 'Cyber Command chief stands by comments on "offensive" operations against Russia', *The Record by Recorded Future*, 19 July 2022 (https://therecord.media/cyber-command-chief-stands-by-comments-on-offensive-operations-against-russia/).

[34] Goldman, E. O., 'From reaction to action: Adopting a competitive posture in cyber diplomacy', *Texas National Security Review*, Vol. 3, No. 4, 2020, p. 94 (http://dx.doi.org/10.26153/tsw/10950).

[35] Schneier, B., 'Russia's SolarWinds Attack', Schneier on Security Blog, December 2020 (https://www.schneier.com/blog/archives/2020/12/russias-solarwinds-attack.html).

[36] Miller, J. and Pollard, N., 'Persistent Engagement, agreed competition and deterrence in cyberspace', Lawfare Blog, 30 April 2019 (https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace).

[37] Healey, J. and Jervis, R., 'The escalation inversion and other oddities of situational cyber stability', *Texas National Security Review*, Vol. 3, No 4, 2020 (http://dx.doi.org/10.26153/tsw/10962).

[38] Healey, J., 'Memo to POTUS: Responding to cyber attacks and PPD-20', *The Cypher Brief*, 24 May 2018 (https://www.thecipherbrief.com/column_article/memo-potus-responding-cyber-attacks-ppd-20).

CONCLUSION

The EU and the United States operate under a different conceptual understanding of cyber conflict. The United States, like China and Russia, subscribes to the premise of continuous cyber conflict and strategic competition below the threshold of armed conflict. The EU approach is predicated on a responsive rather than persistent posture: it will react (albeit slowly) to significant cyberattacks *post hoc*. The more severe the malicious activity, the more severe the diplomatic response in the cyber diplomacy toolbox. The hope is that this will somehow create strategic deterrence of below-threshold activity. There is little indication that this approach is successful. However, persistent engagement is currently incompatible with the EU's understanding of a rule-based international order and its general notion of stability in cyberspace, which means less, and not more, continuous cyber operations. However, the EU must position itself *vis-à-vis* persistent engagement. US demands to operate in allied networks will grow and continue to produce diplomatic tensions. It is also conceivable that the United States will push for collective persistent engagement, either via NATO or via the EU. US Cybercommand has deployed persistent engagement and hunt forward operations in Ukrainian networks to unmask Russian APT activity and to share knowledge about their tools, tactics and procedures with the Ukrainian authorities and the US private sector in order to prepare for future attacks [(39)]. There are indications that these hunt forward operations somewhat helped to prevent large-scale attacks against industrial control systems, that might lead to power outages [(40)]. So persistent engagement is likely to remain the favoured approach.

Although not without risks, a coordinated or even shared approach between the EU and the United States to persistent engagement appears preferable to another alternative: the EU adopting its own notion of persistent engagement under the guise of 'strategic autonomy' without including the United States. An EU-only persistent engagement strategy could likewise imply EU cyber operations in US networks, for example to trace the Solar Winds hackers which used US servers as jump-off points. This would raise the spectre of cyber instability and hence needs to be averted. To avoid this, memoranda of understanding on offensive cyber operations in allied networks should be developed, either via NATO or via EU mechanisms [(41)]. This should include a common notification requirement for operations in allied networks and efficient, secure communication channels between EU and US cyber forces. Another idea is to grant transit rights for other networks. Considering the operational obstacles, it is more likely that the EU might adopt an active cyber defence stance in the near future. As this chapter has demonstrated, this might have limited effectiveness against agile adversaries.

(39) Matishak, M., 'Cyber Command Chief: U.S. has "stepped up" to protect Ukraine's networks', *The Record by Recorded Future*, 5 April 2022 (https://therecord.media/cyber-command-chief-u-s-has-stepped-up-to-protect-ukraines-networks/).

(40) Lemos, R., 'Early discovery of pipedream malware a success story for industrial security', Dark Reading, 22 April 2022 (https://www.darkreading.com/vulnerabilities-threats/pipedream-response-shows-best-case-for-industrial-security).

(41) Smeets, M., 'U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection', *Intelligence and National Security*, Vol. 35, No 3, 2020, pp. 444-453 (https://doi.org/10.1080/02684527.2020.1729316).

CHAPTER 4

AFFIRMATION AND NEGATION: THE CHALLENGE OF ATTRIBUTION

by
AUDE GÉRY

INTRODUCTION

On 18 January 2019, the French Minister of the Armed Forces, Florence Parly, introduced the French Military Cyber Strategy. In her speech, not only did she mention an operation attributed to Turla, a threat actor known to be associated with the Russian Federal Security Service (FSB), but she also repeated several times that France had the capacity to identify perpetrators and that it would not hesitate to use its cyber capabilities to retaliate. Both elements of her speech illustrate the role of attribution in military cyber operations and the role of the armed forces in attribution.

Attribution is one of the most complex and contentious issues in the domain of cybersecurity and cyber policy and there is a rich body of academic and policy literature on the subject. It is also one of these polyvalent words that encompasses many different meanings. The goal of this chapter is not to recapitulate everything that has already been written on attribution. Yet it is important to recall that there are three different kinds of attribution (technical attribution, political attribution and legal attribution), that they can be conveyed through different means (security alerts, official statements, regulatory and legal documents) [(1)], that they can designate different types of entities (individuals, threat actors, companies, states, etc) [(2)] and that they serve different purposes (enforcement, defence, deterrence, constitution of norms) [(3)]. Finally, attribution denotes both the result of an investigation to identify the perpetrator and a process [(4)].

This brief summary of the different facets of attribution sets the scene for analysing attribution in the military context. It also indicates that, depending on the precise meaning of the

(1) Eichensehr, K., 'The law and politics of cyberattack attribution', UCLA School of Law, *Public Law Research Paper*, No 19, 2020.

(2) Steffens T., *Attribution of Advanced Persistent Threats: How to identify the actors behind cyber-espionage*, Springer, Berlin, 2020.

(3) Hollis D., and Finnemore, M., 'Beyond naming and shaming: Accusations and international law in cybersecurity', *E.J.I.L.*, Vol. 31, No 3, 2020, pp. 969-1003.

(4) Rid, T. and Buchanan, B., 'Attributing cyber attacks', *Journal of Strategic Studies*, Vol. 38, No 1-2, 2015, pp. 4-37.

term, the military might play a specific role in the EU's cyber defence. This chapter starts by analysing the specific role of the armed forces in these different types of attribution. It then proceeds with an analysis of the role of attribution in military cyber operations followed by an overview of the role of the armed forces in attribution.

THE ROLE OF ATTRIBUTION IN MILITARY CYBER DEFENCE

Depending on the type of attribution and the goal pursued, attribution can play different roles in the context of military cyber operations: it is an important tool in supporting military cyber defence; it can be a legal prerequisite before conducting cyber operations; and finally the fog of attribution can be leveraged as an operational advantage.

Attribution as a component of military cyber defence

Different types of attribution can play different roles for military cyber defence, understood as the technical, organisational, legal and human measures and capacities put in place to protect and defend the networks and information systems of an organisation. Firstly, *technical attribution* of cyber operations to threat actors, which is part of cyber threat intelligence, can be useful to predict, detect and defend against cyberattacks. Although 'in the IT-security community there is the often-repeated mantra that it is irrelevant who is behind an attack because IT-security measures are always the same, irrespective of the origin of the perpetrators', [(5)] it is nevertheless true that 'knowing whether and which APT groups target a certain industry sector can provide information which security measures are to be prioritized' [(6)]. Indeed, the process of technical attribution provides insights into the threat actors, their tactics, techniques and procedures, knowledge that can be useful both to adapt the tools used to detect intrusions and to shorten incident response times. From the perspective of military cyber defence, this shows that technical attribution is part of the threat assessment conducted by military forces to protect their networks.

Secondly, *political and/or legal attribution* helps evaluate the threat from a political perspective, in order to decide on its characterisation in the context of foreign policy and defence and to define the appropriate response, both at the level of the armed forces and of the government as a whole. As a consequence, political and/or legal attribution can be the first step towards the conduct of (cyber) operations by the armed forces if a decision is taken to retaliate.

Attribution as a constraint for military cyber operations

Attribution can be seen as a constraint for military cyber operations for several reasons. Firstly, the lawfulness of certain cyber operations can be dependent upon attribution. This means that the ability of the armed forces to react (lawfully) might be limited by a lack of attribution. Secondly, the fact that attribution tends to be a time-consuming process might be at odds with the need to react quickly, again limiting a state's ability to react.

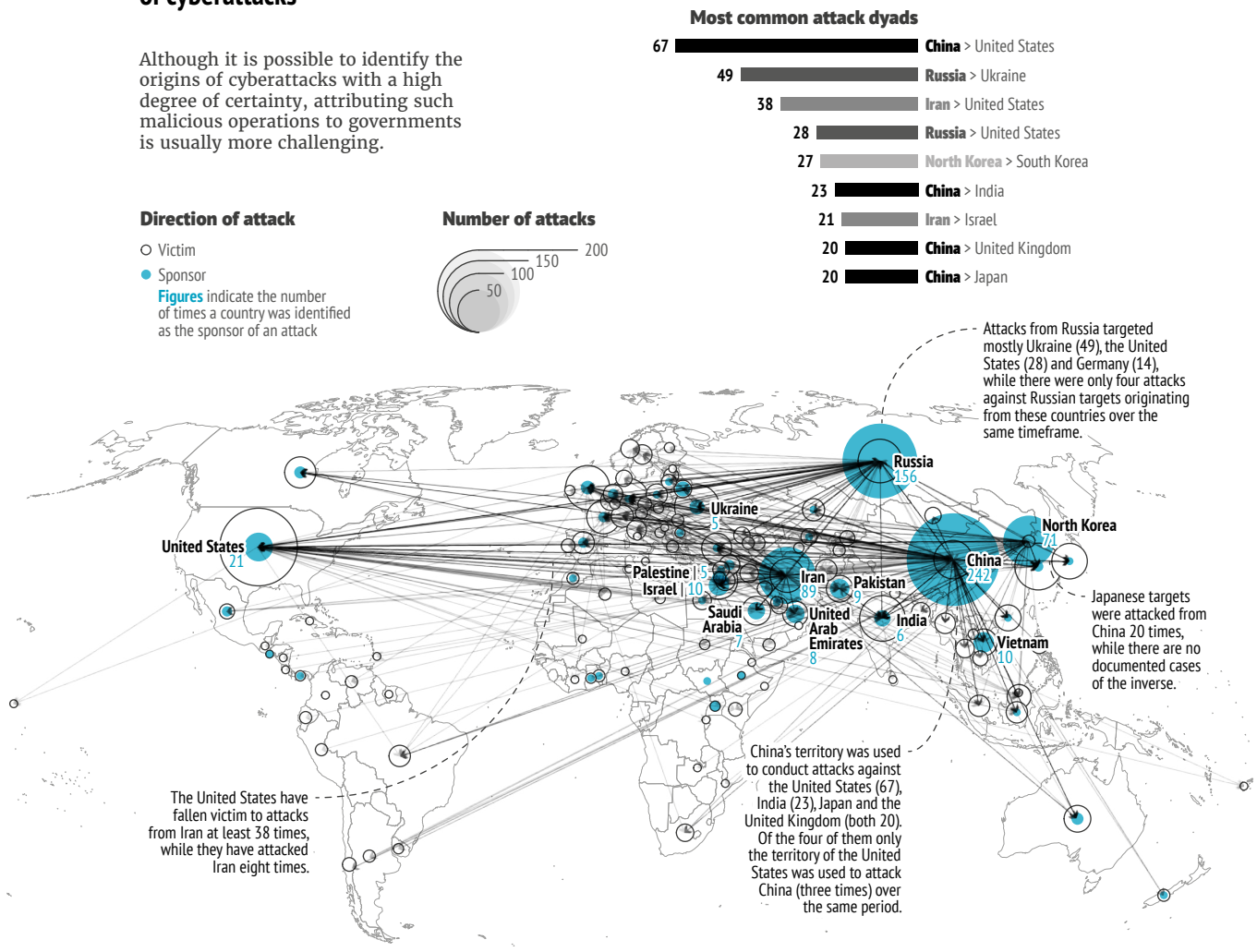
Legal attribution has important repercussions for the conduct of cyberoperations. The EU and most of its Member States have affirmed

(5) *Attribution of Advanced Persistent Threats: How to identify the actors behind cyber-espionage*, op. cit., pp. 24-25.

(6) Ibid.

Origins and targets of cyberattacks

Although it is possible to identify the origins of cyberattacks with a high degree of certainty, attributing such malicious operations to governments is usually more challenging.

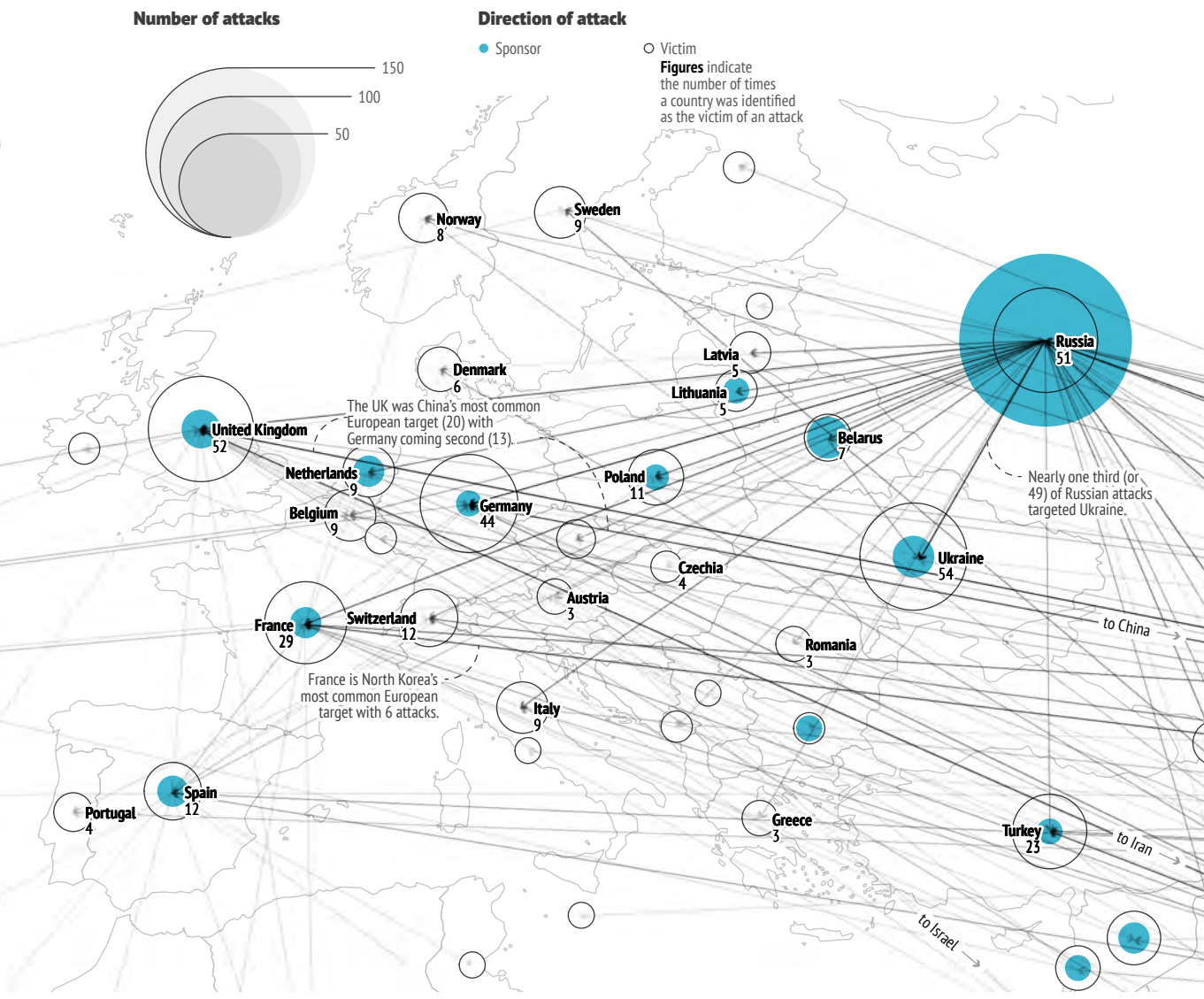


Data: CFR, *Cyber Operations Tracker*, 2022

their commitment to existing rules and principles of international law. Complying with international law means that, under some circumstances, states will have to abide by the rules of attribution of the law of state's responsibility or proceed to the identification of the attacker before acting. The goal of international humanitarian law (IHL) is to regulate the conduct of hostilities and protect civilians during armed conflicts. One of the cardinal principles of humanitarian law is the principle of distinction [7] which distinguishes between combatants and non-combatants, civilian objects and military targets and only allows attacks against combatants and military targets. People who are not combatants are civilians; yet they may decide to take up arms against a belligerent. In order to take this situation into account, article 51(3) of the Additional Protocol I to the Geneva Conventions states that 'civilians shall enjoy the protection afforded by this Section, unless and for such time as they

(7) International Court of Justice, *Legality of the threat or use of nuclear weapons*, Advisory Opinion, *ICJ Report 1996*, 8 July 1996, p. 257, para. 78 (https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf).

European targets of cyberattacks



Data: CFR, *Cyber Operations Tracker*, 2022

take a direct part in hostilities' [8]. Moreover, 'under IHL, the concept of direct participation in hostilities refers to conduct which, if carried out by civilians, suspends their protection against the dangers arising from military operations' [9]. As a result, parties to an international armed conflict can, in accordance with international law, conduct attacks against such persons. Analysing the conditions under which a person can be considered as directly participating in hostilities and the problems that arise when their intervention

(8) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

(9) Melzer, N., *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, International Committee of the Red Cross (ICRC), 2020, p. 12.

takes the form of cyber operations is outside the scope of this article [10]. But from the perspective of attribution, the implementation of this rule of international law will require a state to identify the perpetrator of a cyber operation before proceeding to a legal assessment to determine whether or not the conditions of the qualification of direct participation in hostilities are met and if it can act against the identified perpetrator. Here, legal attribution thus appears as a constraint for military operations, cyber or not.

Another dimension of *legal attribution* as a constraint for military cyber operations is related to the determination of whether or not a state, including its armed forces, can implement countermeasures in reaction to an internationally wrongful act. The issue at stake here is the nature and scale of the reaction of the armed forces. When targeted by a cyber operation, a state has several options to react. The reaction is determined by both political motives and the legal qualification of the cyber operation. The *Articles on Responsibility of States Internationally Wrongful Acts* [11] drafted by the International Law Commission lay out the conditions under which a state's responsibility can be engaged and sets out the content of international responsibility and the legal framework to actually engage a state's international responsibility. Among other things, it dedicates a chapter to countermeasures, that is measures that would normally be unlawful under international law but that become lawful because taken by the injured state in reaction to an internationally wrongful act, that is an action or omission that is attributable to a state under international law and that constitutes a breach of an international obligation of the state [12]. Therefore, the injured state will have to *legally attribute* the cyber operation and qualify it in order to determine whether or not it can implement countermeasures. It should be noted that not all reactions require attribution. Measures of retorsion (i.e. acts that do not violate international law) can be used to react to unfriendly acts, that is acts that do not violate any international obligation. In this case, there is no requirement of legal attribution. Considering the state of uncertainty regarding the interpretation of international law, the requirement of attribution will thus be debatable. As explained by one law professor, 'in short, where states disagree about whether a particular action violates international law, they will also disagree about whether countermeasures are available and thus about whether attribution is required' [13], thus impacting the type of operations that might be conducted by the armed forces.

Along with impacting the lawfulness of military cyber operations, the fact that attribution tends to be a time-consuming process might be at odds with the flexibility that armed forces might need to react to threats. This was particularly well noted by the Department of Defense General Counsel Paul Ney Jr in a speech delivered at the US Cyber Command Legal Conference:

> *'In a particular case it may be unclear whether a particular malicious cyber activity violates international law. And, in other circumstances, it may not be apparent that the act is internationally wrongful and attributable to a state within the timeframe in which the DoD must respond to mitigate the threat. In these circumstances, which we believe are common, countermeasures would not be available'* [14].

Depending on the context in which armed forces may be acting and the rules of international law that apply, their actions might

(10) Schmitt, M. N. and Vihul, L. (eds.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, pp. 428-432, 'Rule 97'.

(11) International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts*, 2001.

(12) Ibid., Article 2.

(13) Eichensehr, K., 'Cyberattack attribution as empowerment and constraint', *Aegis Paper* No 2101, Hoover Institution Essay, 2021, p. 5 (https://www.hoover.org/sites/default/files/research/docs/eichensehr_webreadypdf.pdf).

(14) Ney Jr, P., 'DoD General Counsel Remarks at U.S. Cyber Command Legal Conference', 2 March 2020 (https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/).

be constrained by an obligation to legally attribute a cyber intrusion or attack. This requirement might sometimes be problematic considering the pace of military operations. Indeed, if *legal attribution* is required, the *process of attribution* might limit the ability of military forces to react, thus leaving a state with fewer options to act. But the difficulty in technically, politically and legally attributing a cyber operation might also be an advantage from an operational perspective.

The fog of attribution as an operational advantage

Depending on the type of attribution that is sought, the difficulties will be more or less important [(15)], even if they should not be overestimated as states' capabilities to identify the perpetrators increase. Yet the fog of attribution can constitute an operational advantage, both from the perspective of the attacker and the victim. States conducting cyber operations can leverage this situation, especially in the case of operations conducted by intelligence services. Deniability can indeed provide operational advantages: collecting information without the victim knowing it, producing effects without bearing the consequences, etc. But unlike intelligence services that have more room for manoeuvre and may benefit more from the fog of attribution, it should be noted that the armed forces must be ready to take responsibility for their operations, thus limiting this operational advantage. For the victim as well, there might be operational advantages in not letting the attacker know that they have been identified, i.e. to collect information about them for example.

To sum up, different types of attribution can have different functions for the armed forces, depending on the goal pursued. For the EU, this means that technical attribution can be part of the threat assessment made by technical and military organs but also that its external actions conducted through national capacities will be constrained, at the national level, by attribution. The different functions highlighted here are not all specific to military cyber defence. For example, technical attribution is a process done by other agencies – including civilian ones – and the fog of attribution is shared with intelligence services. Other categories of attribution are more specific. This is particularly the case with legal attribution and the conduct of operations against civilians directly participating in hostilities. This contrasts with the key role of the military in attribution.

THE ROLE OF ARMED FORCES IN THE PROCESS OF ATTRIBUTION

The role of the armed forces is not limited to the military sphere when it comes to attribution. Indeed, their expertise is also of great importance for civilian cyber defence. But their role is not limited to the identification of the perpetrator as they can also be involved in the responses adopted by a state in reaction to a cyber operation.

The armed forces as an attribution player in the identification process

When protecting their networks and collecting intelligence, armed forces will collect indicators of compromise, that is 'technical characteristic[s] that – if found in system or network

(15) Bartholomew, B. and Guerrero-Saade, J-A, 'Wave your false flags! Deception tactics muddying attribution in targeted attacks', Virus Bulletin Conference, Denver, 5-7 October 2016, p. 11; Tsagourias, N. and Farrell, M., 'Cyber attribution: Technical and legal approaches and challenges', *E.J.I.L*, Vol. 31, 2020, pp. 941-967.

logs – is evidence for malicious activities'[16], information about the tactics, techniques and procedures of attackers drawn from the analysis of past and ongoing cyber operations, data about the attack infrastructure used by attackers or any other technical data relevant for investigating a cyber incident. But the type of data that armed forces can gather and present in the attribution process – *the identification of the attacker* – goes beyond technical indicators. Their knowledge of the international environment and of the actors involved in international conflicts is also a valuable source of information to help understand the geopolitical context: who has interests in the targeted region? Who are the actors there[17]? What are the conflicts? Finally, intelligence collected by the military – or intelligence services (including military ones) – gleaned from human intelligence or general signals intelligence[18] is also key to identify the perpetrators and/or the beneficiary of a cyber operation, that is to move from strict technical attribution to *political attribution* and *legal attribution*. The collection of elements of proof will thus be of interest to more actors than just the armed forces themselves, making them a key player in the attribution process. But this situation is not without difficulties.

Because different governmental agencies can collect technical indicators, the process of attribution will require cooperation[19]. The issue of cooperation is of utmost importance to ensure adequate security and an appropriate response. But such cooperation is constrained by objective and subjective limitations. Objective obstacles to technically, politically and legally attributing a cyber operation lie in the legal framework surrounding information sharing, the level of classification associated with the information, the way such information must be dealt with considering the operational security framework or the origin of the information (for example, if it comes from a third party that did not authorise disclosure to another one[20]). Sometimes, not revealing the needed information is also a prerequisite to preserve the secrecy of ongoing cyber operations. Subjective obstacles are mainly about trust between the collecting party and the receiving one. Mention should also be made of the diverging interests between the parties involved in the attribution process[21].

These restrictions may even be more difficult to overcome if the receiving party is another state, an international organisation or a private actor. The context of the European Union is a good example of the challenges of information sharing for attribution. Within the EU, several institutions and agencies are involved in the cyber defence of the Union and its Member States. Despite the implementation of several initiatives at the civilian (i.e. the CERT-EU which is a permanent structure for

(16) *Attribution of Advanced Persistent Threats: How to identify the actors behind cyber-espionage*, op. cit., p. 27.

(17) For example, the conflict in Ukraine has moved to cyberspace, leading to accusations against Russia that it is one of the main attackers considering its interests in the region.

(18) For example, the Sony Pictures hack of 2014 is known to have been a cyber operation conducted by North Korea, an attribution that is believed to have been made thanks to intelligence collected by the United States: Sanger, D.E. and Fackler, M., 'N.S.A. breached North Korean networks before Sony attack, officials say', *The New York Times*, 18 January 2015 (https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html).

(19) For example, the *Strategic Review of Cyber Defence* published by France in February 2018 identifies six missions for cyber defence, one of them being attribution. It identifies several agencies, both civilian and military, in charge of this mission and calls for cooperation between them: France, Secrétariat général de la Défense et de la Sécurité nationale, *Strategic Review of Cyber Defence*, February 2018, p. 51 (http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf?bcsi_scan_858c91d0398e8bd7=0&bcsi_scan_filename=20180206-np-revue-cyber-public-v3.3-publication.pdf). The EU Cyber Defence Policy Framework also lists several examples of such collaborations: Council of the European Union, 'EU Cyber Defence Policy Framework (as updated in 2018)', 14413/18, 19 November 2018 (https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf).

(20) This problem often arises when EU Member States collaborate or in the context of EU-NATO collaboration on cyber defence issues.

(21) Bradshaw, S., 'Combatting cyber threats: CSIRTs and fostering international cooperation on cybersecurity', Global Commission on Internet Governance and Chatham House, *Paper Series* No 23, December 2015, p. 14 (https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf).

the EU institutions, agencies and bodies [22]) and military levels (i.e. the Cyber Threats and Incident Response Information Sharing Platform, which 'aims to help mitigate these risks by focusing on the sharing of cyber threat intelligence through a networked Member State platform, with the aim of strengthening nations' cyber defence capabilities' [23]), lack of cooperation leads to a situation where the EU does not have a collective situational awareness of cyber threats [24].

Yet, information sharing for attribution, through *technical and political attribution*, might be a requirement for the EU to implement several mechanisms. In the case of sanctions applied through the EU Cyber Toolbox, *attribution to an individual or an entity* (a physical or moral person) is necessary. And as a matter of the rule of law, sanctions can be contested before the EU Court of Justice. Even if special rules of procedures can be implemented in case of information that could harm the security of the Union or its Member States, [25] this could limit a state's willingness to share information obtained by its military apparatus. In 2017, the Council of the European Union stressed 'that a particularly serious cyber incident or crisis could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause and/or Mutual Assistance Clause' [26]. There is little doubt that if a Member State were to invoke one of these two clauses, other Member States would request information about the perpetrator of the cyber incident, requiring information sharing, including at the military level. Armed forces are thus important players in the attribution game. Their influence extends beyond their traditional perimeters and impacts the EU. But it is also true in the reaction phase of attribution. In that sense, the meeting of the heads of Member States' cyber commands during the French presidency of the Council of the EU illustrates well how deeper cooperation could be institutionalised at the highest operational level.

Armed forces as an attribution player in the response phase

As a process, attribution does not stop at the identification of the perpetrator and/or beneficiary of a cyber operation. A victim state can decide to react to a cyber operation. One way to do so is denounce the operation. As experts have noted, attribution as a process also includes communicating about the perpetrator and/or beneficiary [27].

Armed forces are thus important players in the attribution game.

Communication can involve information sharing on technical attribution and political/legal attribution to partners, specific communities and/or the general public. A study of the public attributions made by states shows that the armed forces play only a marginal role in the communication phase since most of the *public attributions* do not come from them. However, they can still be involved. For example, in the United States, CYBERCOM shares

(22) More recently the Commission has announced the creation of a joint cyber unit to strengthen cooperation among Member States and EU institutions. European Commission, 'Joint Cyber Unit', 23 June 2021 (https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088).

(23) PESCO Projects, 'Cyber threats and incident response information sharing platform' (https://pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/).

(24) European Commission, Joint Communication to the European Parliament and the Council, 'The EU's Cybersecurity Strategy for the Digital Decade', Join (2020) 18 final, 16 December 2020, p. 3 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN).

(25) 'Space Exploration. Mapping the EU's cyber sanctions regime', in Pawlak, P. and Biersteker, T. (eds.), *Chaillot Paper* No 155, 'Guardian of the Galaxy: EU cyber sanctions and norms in cyberspace', EUISS, October 2019, p. 38.

(26) Council of the European Union, Council Conclusions on the Joint Communication to the European Parliament and the Council, 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', 14435/17, 20 November 2017, para. 32 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en).

(27) 'Attributing cyber attacks', op. cit.

malware samples that it believes to be used by state-sponsored hackers [28]. In France, the Minister of the Armed Forces was the first one to publicly attribute an intrusion set associated with a threat actor linked to a state [29]. The involvement of armed forces in *public technical attribution* carries an important political dimension considering their role in a state's national security. Although their role seems rather limited, it should not be underestimated.

The reaction to a cyber operation might not be limited to public statements but may also include the conduct of (cyber) operations in return. Here, military forces can be involved in the conduct of cyber operations or other types of operations as measures of retorsion or countermeasures. One could imagine that if a cyber operation were to cross the armed attack threshold, the armed forces would undoubtedly be involved in the reaction, whether it be cyber or kinetic. Interestingly, traditionally, they were not much involved in states' reaction to unfriendly acts or internationally wrongful acts. The dawn of cyber operations has changed the game and led the military to play a bigger role in a state's response to cyber operations [30].

Threats are shared by all actors, and better coordination including at the EU level will benefit Member States.

CONCLUSION

The different components of attribution have different relationships with military cyber defence. Technical attribution is an important component of cyber defence. Legal attribution can be a constraint for military cyber operations. And the fog of attribution can be leveraged as an operational advantage to conduct cyber operations. But the role of attribution in military cyber defence is as important as the role of the armed forces in the big game of attribution. Depending on the type of attribution and the timing, their role will vary and be more or less unique within a state's organisational architecture compared to other agencies. Armed forces are an indispensable player in the process of attribution. They collect data through multiple sources that can be of help to identify the perpetrator and/or beneficiary of a cyber operation. They can also be involved in a state's political response through the conduct of cyber operations in reaction to unfriendly acts or internationally wrongful acts, whether these take the form of cyberattacks or not.

If the EU wants to build a solid cyber defence, both at the military and civilian level, it will not be able to do so without involving the armed forces from EU Member States and framing collaboration in the attribution of cyberattacks. As already explained, for the EU to effectively implement its defence and foreign policy, such cooperation is required. The EU is also involved in different civil and military operations across the world. To ensure their security and integrity, they need to be protected, including in cyberspace. The revision of the concept framework for EU-led military operations and missions, which includes the military vision and strategy on cyberspace as a domain of operations, will thus need to take into account the different facets of attribution to determine how they participate in the EU's strategy. While Member States need to strengthen their collaboration on attribution in order for the EU to implement its strategy, Member States will

[28] See for example, Cimpanu, C., 'US Cyber Command exposes new Russian malware', *ZDNet*, 1 November 2020 (https://www.zdnet.com/article/us-cyber-command-exposes-new-russian-malware/).

[29] Desforges, A. and Géry, A., 'France doesn't do public attribution of cyberattacks. But it gets close', *Lawfare*, 3 September 2021 (https://www.lawfareblog.com/france-doesnt-do-public-attribution-cyberattacks-it-gets-close).

[30] A good example of this, although outside the scope of this chapter, is the takedown of the Trickbot botnet by the US CyberCom in 2020: Chesney, R., 'Persistently engaging TrickBot: USCYBERCOM takes on a notorious botnet', *Lawfare*, 12 October 2020 (https://www.lawfareblog.com/persistently-engaging-trickbot-uscybercom-takes-notorious-botnet).

also benefit from the strengthening of European military cyber defence. Threats are shared by all actors, and better coordination including at the EU level will benefit Member States. But more importantly, better resilience across the EU will require strong coordination between all agencies from the EU and Member States, a cooperation that needs to move beyond the traditional civil/military distinction. As this chapter has demonstrated, all actors will benefit from the knowledge of others, and cyber resilience cannot be achieved without the involvement of the armed forces.

CHAPTER 5

MORPHOLOGY: CYBER ESPIONAGE AND DEFENCE

by
FRANÇOIS DELERUE

INTRODUCTION

Conventional military activities are often dependent on intelligence gathering activities, notably to assess the forces and capabilities of other actors and infer their intentions [(1)]. Yet espionage activities are often treated separately, especially in the cyber realm. The dawn of ICTs created new opportunities and radically transformed espionage activities. The most notable evolution that accompanied the technological revolution concerns intelligence gathering methods, shifting notably from human intelligence (HUMINT) as a main method to signal intelligence (SIGINT) and cyber intelligence (CYBINT).

The transformation of espionage has resulted in new challenges. Cyberspace has broadened the scope and scale of espionage, making it possible to spy on almost everybody from a remote location and gain access to an unprecedented amount of information, including trade or military secrets. In 2009, for instance, Chinese hackers were accused of having hacked into computer systems related to the development of the Joint Strike Fighter programme and of having downloaded terabytes of data [(2)]. At the same time, the sheer amount of data that may be accessed and collected challenges the processing and storage capacities of intelligence services. In other words, the problem is no longer the access to the information but the identification of the relevant information within the large volume of data collected.

As a consequence, the demarcation line between espionage activities and other military activities in cyberspace tends to become blurred in most circumstances. In recent years, the EU has positioned itself as a leading international actor on cybersecurity issues and has developed its own way to address cyber threats, notably with the adoption of the EU Cyber Diplomacy Toolbox. The objective of this chapter is to question the relevance of the demarcation line between espionage activities and other military activities in cyberspace. In this context, this chapter and the different questions it raises aim at contributing to the debate on how the EU and its Member States should apprehend and react to alleged state-sponsored cyber espionage campaigns.

(1) Libicki, M. C., 'Drawing inferences from cyber espionage' in Minárik, T., Jakschis, R. and Lindström, L. (eds), *2018 10th International Conference on Cyber Conflict - CyCon X: Maximising Effects*, NATO CCDCOE Publications, 2018.

(2) Gorman, S., Cole, A. and Dreazen, Y., 'Computer spies breach fighter-jet project', *The Wall Street Journal*, 21 April 2009 (https://www.wsj.com/articles/SB124027491029837401).

DEFINING CYBER ESPIONAGE

Cyber espionage may be defined as the unauthorised access and collection of confidential information [3]. According to the *Tallinn Manual 2.0*, it can be defined as the 'use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information' [4].

Cyber espionage activities are generally distinguished in two categories: on the one hand, political cyber espionage; on the other hand, economic cyber espionage. In 2015, the United States and China adopted a Cyber Agreement, through which they agreed 'that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors' [5]. In other words, these two countries agreed on refraining from economic cyber espionage, but not from political espionage, which is generally perceived as acceptable and an inevitable part of international relations.

The Covid-19 pandemic has highlighted how the distinction between economic and political espionage might sometimes be blurred.

Cyber espionage activities associated with military activities generally fall in the first category of political espionage. Yet, it is important to note that political intelligence gathering activities are also used by some states and other actors in support of the military industrial economy. It has been asserted, for instance, that the hacking of the US Joint Strike Fighter programme mentioned in the introduction may have contributed to the development of its own jet fighter programme by the state behind the data theft [6]. Similarly, the Covid-19 pandemic has highlighted how the distinction between economic and political espionage might sometimes be blurred. The health crisis has been marked by cyber espionage campaigns against individuals and institutions rendered more vulnerable due to the recourse to telework, institutions involved in the management of the crisis as well as research institutions engaged in the development of a vaccine [7]. These intelligence gathering activities, and in particular those related to the vaccine race, may be conducted with a political and an economic objective at the same time.

The past decade has witnessed accusations of large-scale political cyber espionage campaigns, notably conducted by US intelligence agencies against their competitors as well as their allies. The main case remains the 'Snowden revelations', which started in 2013 with the publication by a group of international media outlets of documents collected by Edward Snowden [8]. More recently, on 30 May 2021, the Danish public service radio and television broadcasting company DR released a report on how the United States National Security Agency (NSA) collaborated with the

(3) 'Drawing inferences from cyber espionage', op. cit., p.111; Buchan, R., *Cyber Espionage and International Law*, Bloomsbury Publishing, 2018, p.2.

(4) Schmitt, M., and Vihul, L., (eds), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edition, Cambridge University Press, Cambridge, 2017, p. 168, para. 2.

(5) United States, The White House, Office of the Press Secretary, 'Fact Sheet: President Xi Jinping's State Visit to the United States', 25 September 2015 (https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states).

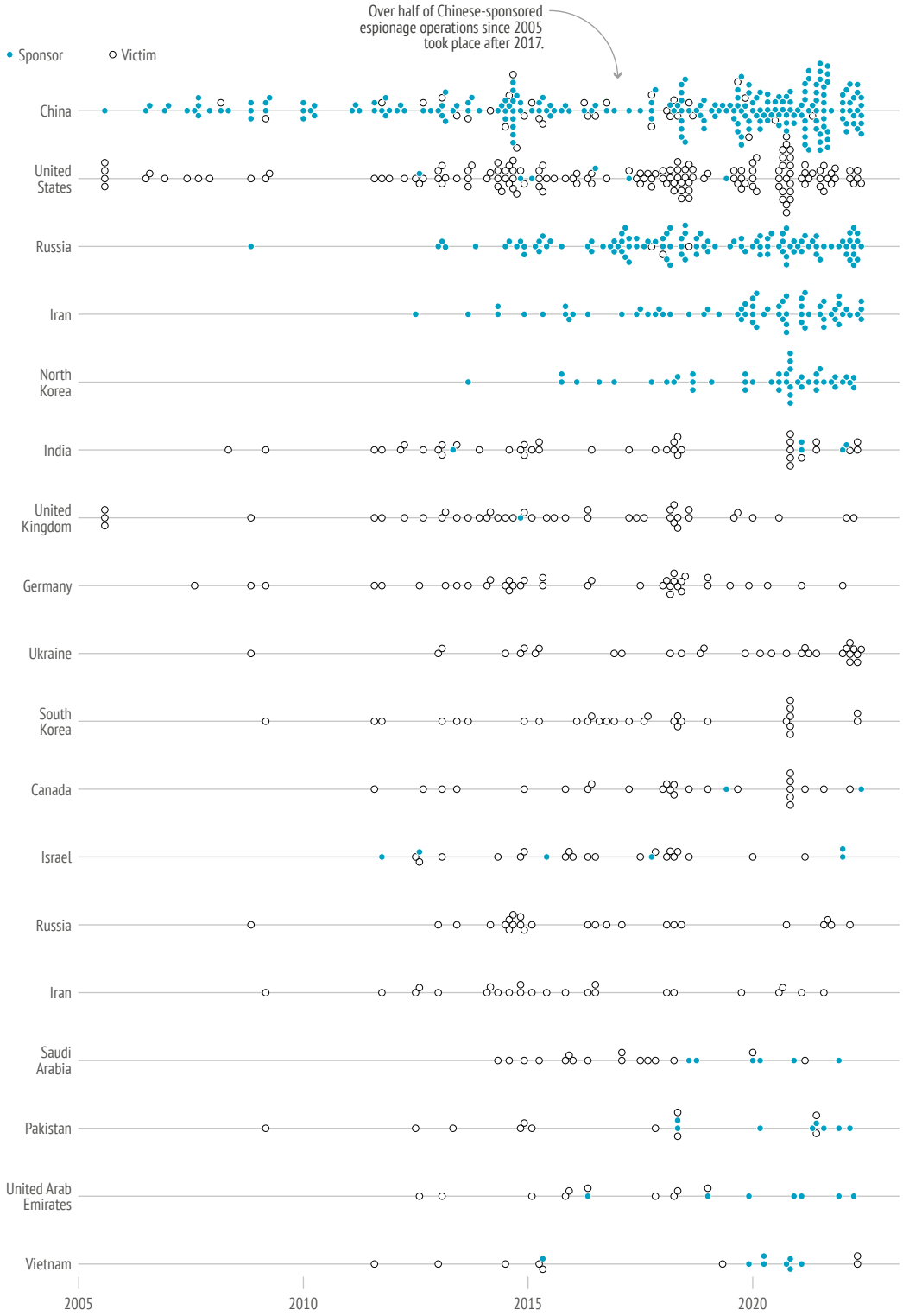
(6) Alexander, D., 'Theft of F-35 design data Is helping U.S. adversaries - Pentagon', Reuters, 19 June 2013 (https://www.reuters.com/article/usa-fighter-hacking-idUSL2N0EV0T320130619).

(7) See, for instance: UK NCSC, 'Advisory: APT29 Targets Covid-19 vaccine development', United Kingdom's National Cyber Security Centre, 2020 (https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf).

(8) See, for instance, 'The NSA Files', *The Guardian* (https://www.theguardian.com/us-news/the-nsa-files).

Sponsors and victims of cyber espionage

Sponsors are hardly ever the victims



Data: CFR, Cyber Operations Tracker, 2022

Danish military intelligence services (*Forsvarets Efterretningstjeneste*) to collect data from internet cables transiting through Danish territory to spy on various European officials, including Angela Merkel [9]. The United States is not the only state believed to be conducting cyber espionage activities against its allies; a document belonging to the Communications Security Establishment Canada (CSEC) and published as part of the Snowden leaks in 2013 attributed 'with moderate certainty' the spyware named *Babar* or *Snowglobe* to a French intelligence service [10].

These few examples show very different methods of data collection. On the one hand, the monitoring of data transiting into cables and computer systems located on the territory of the spying state. On the other hand, the unauthorised access to computer systems belonging to another actor. This chapter focuses predominantly on the latter form.

The perpetrators of cyber espionage

Spying has also always existed and contributed to military activities. States have always spied on each other, whether allies or competitors, notably to estimate the capabilities of the other side and infer its intentions. During an armed conflict, the information collected through various types of intelligence gathering activities have often played an important role both at the preparatory stage and during the conduct of hostilities. Interestingly, espionage activities have often been treated as distinct activities because of their covert nature. This is also true in cyberspace. Espionage activities are generally distinguished from military activities according to two alternative criteria: the identity of the perpetrating institution and the purpose of the activity.

Cyber espionage activities are generally conducted by intelligence gathering agencies. There is a presumption that because they are conducted by an institution tasked with intelligence gathering, these activities are intelligence activities. Yet, cyber offensive activities are also sometimes part of the mandate of these intelligence gathering agencies. In France, for instance, certain cyber offensive capabilities and cyber intelligence gathering are both part of the respective mandates of the COMCYBER and intelligence agencies, such as the DGSE (*Direction générale de la Sécurité extérieure* – the French foreign intelligence agency) [11]. A similar situation exists in other countries, such as the United States regarding the mandate of the US CYBERCOM [12]. In other words, the demarcation lines between intelligence gathering and offensive activities tend to become blurred in cyberspace.

Cyber espionage and the purpose of a cyber operation

The nature and purpose of cyber operations are also used to distinguish cyber espionage from other forms of cyber activities, notably in policy and strategic documents. In the United

[9] Fastrup, N. and Quass, L., 'Forsvarets Efterretningstjeneste lod USA spionere mod Angela Merkel, franske, norske og svenske toppolitikere gennem danske internetkabler', *DR.dk*, 30 May 2021 (https://www.dr.dk/nyheder/indland/forsvarets-efterretningstjeneste-lod-usa-spionere-mod-angela-merkel-franske-norske).

[10] CSEC CNT/Cyber CI, 'Snowglobe: From discovery to attribution', Communications Security Establishment Canada, published by Spiegel 2011 as part of the Snowden documents. See the discussion in: Delerue, F., *Cyber Operations and International Law*, Cambridge University Press, 2020, pp. 81–82.

[11] France (SGDSN), 'Stratégie nationale de la cyberdéfense [*Revue stratégique de cyberdéfense*]', Secrétariat général de la défense et de la sécurité nationale & Economica, 2018 (http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/); Ministère des Armées, COMCYBER, 'Éléments publics de doctrine militaire de lutte informatique offensive', 2019 (https://www.defense.gouv.fr/sites/default/files/ema/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf).

[12] United States, Department of Defense, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command', 2018 (https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010).

States Department of Defense (DoD) *Dictionary of Military Terms and Associated Terms*, [13] for instance, there is a broad category of 'cyber operations', formerly referred to as 'computer network operations (CNO)' [14]. Until November 2012, CNO were described as comprised of computer network attack (CNA), computer network defence (CND) and computer network exploitation (CNE) operations, the latter corresponding to cyber espionage activities which are thus considered separately from cyber operations having a different purpose. This terminology was abandoned in 2012 with the adoption of DoD Joint Publications 3-0 and 3-13 [15] replacing CNO by 'Cyber Operations' [16]. The former category of CNA has been replaced by 'cyberspace attack', defined as 'actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires' [17]. Cyberespionage, formerly referred to as CNE, is not referred to as 'cyberspace exploitation', which is defined as 'actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations' [18]. It can be observed that that the distinction would appear to be determined by the objective of the activities undertaken. 'Cyberattacks' are generally likely to be destructive by nature while 'cyber espionage activities' aim at intelligence gathering. This distinction is relevant and applicable in some cases, but not in all cases. As mentioned in the definition of cyberspace exploitation in the *DoD Dictionary*, cyber espionage activities may also constitute preparatory actions for a cyberattack, thus blurring the line between the two.

The SolarWinds case offers an interesting illustration. In December 2020, it was reported that a group of Russian hackers, allegedly linked to the Russian Foreign Intelligence Service (SVR), hacked into the software Orion produced by SolarWinds to penetrate the computer systems of its end users, including several US governmental agencies [19]. As pointed out by Jack Goldsmith, this seems to have been purely a cyber espionage campaign in which state-backed hackers penetrated computer systems to access and steal data [20]. This case led to numerous comments and speculations on the motivations and objectives of the perpetrators as well as how the United States should react to this cyber espionage campaign [21]. Yevgeny Vindman, a former deputy legal adviser on the White House National Security Council, notably wrote in the *Lawfare* blog:

> *'The attackers' access allowed them free and persistent entry into systems, to steal data and deliver a latent but as yet unutilized ability to alter data or execute destructive attacks. [...] In SolarWinds, the espionage and operational access of the "hands on keyboard" cyberattack are intertwined. The vulnerabilities are present and continuing on an unprecedented scale, even if currently latent. Consequently, a U.S.*

(13) United States, Department of Defense, *DOD Dictionary of Military and Associated Terms*, 2021.

(14) Ibid, p. 55.

(15) United States, Department of Defense, 'Joint Publication 3-0 (Incorporating Change 1 of 22 October 2018)', 2017-2018; United States, Department of Defense, 'Joint Publication 3-13 (Incorporating Change 1 of 20 November 2014)', 2012-2014.

(16) *DOD Dictionary of Military and Associated Terms*, op. cit., p. 55.

(17) Ibid.

(18) Ibid.

(19) Sanger, D. S., Perlroth, N. and Schmitt, E., 'Scope of Russian hacking becomes clear: Multiple U.S. agencies were hit', *The New York Times*, 14 December 2020 (https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html).

(20) Goldsmith, J., 'Self-delusion on the Russia hack', *The Dispatch*, 18 December 2020 (https://thedispatch.com/p/self-delusion-on-the-russia-hack).

(21) See, for instance, Bossert, T. P., 'I Was the Homeland Security adviser to Trump. we're being hacked', *The New York Times*, 16 December 2020 (https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html); Vindman, Y., 'Is the SolarWinds cyberattack an act of war? It is, if the United States says it is', *Lawfare*, 26 January 2021 (https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it).

> *response to this attack should be understood as self-defense to an attack in progress.'* [22]

In other words, because the activities conducted to access and steal data may also constitute the first step of a destructive cyber operation, he considers that it should be treated as an ongoing destructive cyber operation.

Vindman's legal assessment of the case may be challenged, in particular regarding whether the SolarWinds case meets the criteria for an armed attack that would allow the United States to invoke their right of self-defence. Yet his approach on the demarcation between cyber espionage and a destructive cyber operation is interesting. Indeed, it has been observed that 'a successful cyberattack requires a vulnerability, access to that vulnerability, and a payload to be executed. A [cyber espionage activity] requires the same three things – and the only technological difference is in the payload to be executed' [23].

The SolarWinds hack is generally considered as a cyber espionage campaign. In practical terms, the cyber operation that was carried out appears very similar to some operations conducted by the United States Cyber Command as part of the implementation of the 'defend forward' cyber strategy aiming at deterring other states from conducting malicious cyber activities against the United States. In 2019, for instance, the *New York Times* reported that the US Cyber Command hacked into the computer systems running the Russian power grid as preparatory measures for potential further actions [24].

These examples demonstrate the difficulty for the victim, when identifying that another actor is currently present in its computer systems, to ascertain whether it is an attempt to access and steal data, and thus only a cyber espionage operation, or the preparatory phase of a destructive cyber operation.

It is also conceivable that in some cases, the responsible actor is also collecting information to decide on their next step and thus may have not yet decided whether their intelligence gathering operation will be turned into a more aggressive and destructive one. The hacking during the 2016 US presidential elections and the 2017 French presidential elections offer an illustration of this point. In case of an unauthorised access into the computer systems of a political party – a textbook example of a political cyber espionage activity – it might be impossible to tell whether the perpetrator's objective is only to access this data or if there is a further objective, and thus another possibly more consequential action to come. Depending on the nature of the stolen data, the perpetrator may decide to leak it online, use it to blackmail the concerned party or even conduct a harmful cyber operation.

As these examples illustrate, in numerous cases of unauthorised access to computer systems, it might be impossible for the targeted actor to determine the motives of the perpetrator and thus whether it is a cyber espionage operation or another type of cyber operation. It might thus be preferable for the targeted actor to treat them similarly, regardless of their potential purpose.

THE CONSEQUENCES OF THE DISTINCTION

The distinction between cyber espionage and other forms of cyber operations has various consequences, notably from the point of

[22] See, for instance, Vindman, 'Is the SolarWinds cyberattack an act of war?', op.cit.

[23] Owens, W. A., Dam, K. W. and Lin, H. S., (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Research Council, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, 2009, p. 150 (http://www.nap.edu/catalog/12651/technology-policy-law-and-ethics-regarding-us-acquisition-and-use-of-cyberattack-capabilities).

[24] Sanger, D. S. and Perlroth, N., 'U.S. escalates online attacks on Russia's power grid', *The New York Times*, 15 June 2019 (https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html).

view of the legal assessment of the activities concerned [25].

In 2019, the French Ministry of the Armed Forces released a document entitled *International Law Applied to Operations in Cyberspace* in which it is notably specified that 'This document does not contain any specific analysis or treatment of cyberespionage' [26]. This clarification implies that for the authors of the document, cyberespionage might deserve a specific treatment under international law in comparison to other types of cyber operations.

It is generally accepted that a conventional military activity, including when taking the form of a cyber operation, may constitute an internationally wrongful act, such as a violation of territorial sovereignty or an armed attack. There is some debate on the specific interpretation of existing rules and principles of international law regarding specific types of military activities [27], but this is a different question. Concerning intelligence gathering activities, in contrast, a debate has developed on whether the fact that they are conducted for the purpose of espionage would constitute a circumstance excluding the wrongfulness of these acts. While most of the literature considers that espionage activities may constitute internationally wrongful acts, a vocal minority advocates for the opposite view and considers that espionage activities should always be considered as lawful. This debate also exists in cyberspace, notably among the group of experts who authored the *Tallinn Manual 2.0*. In the *Tallinn Manual 2.0*, cyberespionage activities are treated separately from other types of state-conducted or state-sponsored cyber operations. In the first part dedicated to 'General international law and cyberspace' [28], there is a fifth section titled 'Cyber operations not *per se* regulated by international law' comprised of two rules, one dedicated to peacetime cyberspace espionage (Rule 32) and the other to cyber operations by non-state actors (Rule 33) [29]. Thus, the structure of the *Tallinn Manual 2.0* shows that for its authors, these cyber operations are different from the rest. Secondly, while Rule 32 restates the traditional and majority view on the lawfulness of espionage, 'although peacetime cyber espionage by States does not *per se* violate international law, the method by which it is carried out might do so'; [30] the commentary to this Rule tends to be less definitive notably while discussing hypothetical examples [31].

These observations show the consequences of the distinction on the perception of certain cyber operations and thus how it might affect the reaction of the concerned state.

---

(25) On cyber espionage and international law, see generally: Lubin, A., 'The Liberty to Spy', *Harvard International Law Journal*, Vol. 61, 2020, p.185; *Cyber Espionage and International Law*, op. cit.; *The Tallinn Manual 2.0*, op. cit., pp. 168–174; see also: Lafouasse, F., *L'espionnage dans le droit international*, Nouveau monde, Paris, 2012; Baker, C. D., 'Tolerance of international espionage: A functional approach', *American University International Law Review*, Vol. 19, 2004, 1091.

(26) Ministère des Armées, France, 'International law applied to operations in cyberspace', 2019, p. 4, footnote 2. Interestingly, this mention is not present in the document with the same title submitted by France in 2021 to the United Nations Open-Ended Working Group on security of and in the use of information and communications technologies: France, 'International law applied to operations in cyberspace', 2021 (https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf).

(27) See, for instance, the discussion in Corten, O., *The Law against War: The prohibition on the use of force in contemporary international law*, Hart, 2012.

(28) *The Tallinn Manual 2.0*, op. cit., pp. 9–176.

(29) Ibid, pp. 168–176.

(30) Ibid, p. 168, Rule 32.

(31) See the discussion in: *Cyber Operations and International Law,* op. cit., pp. 193–197.

GOING BEYOND THE DISTINCTION IN A EUROPEAN APPROACH

The present chapter has questioned the demarcation between cyber espionage activities and other forms of cyber operations from the point of view of a reacting institution. In doing so, it has highlighted how such a distinction might be a bit artificial in numerous cases, if not impossible. These questionings and observations are of importance for the EU and its Member States regarding two main situations. On the one hand, these issues should be considered in the elaboration of cybersecurity and cyber defence policy as well as for the implementation of the EU Cyber Diplomacy Toolbox. In assessing cyber operations and possible reactions, should the EU and its Member States distinguish those conducted by intelligence agencies or those having an espionage purpose from other forms of cyber operations? The observations made in this chapter tend to advocate for a negative answer. That being said, the identity of the perpetrator, their relationship with a sponsoring state, the purpose, and the consequences of the cyber operations concerned are relevant factors to be assessed in determining a potential reaction. Yet the argument developed in this chapter is that this assessment should not be based on an artificial demarcation but should rather focus on the concrete facts of the case in question. Beyond the question of the assessment and reaction, it is also a question for the communication of the EU and its Member States. In communicating on the facts and in reacting publicly, it may not be relevant to dissociate cyberespionage activities from other types of cyber operations as labelling them in this way tends to be perceived by some actors and commentators as excusing the unfriendliness, if not the wrongfulness, of the concerned behaviours. On the other hand, concerning the actual practice of the Member States of the EU when it comes to cyber espionage, some Member States may be conducting or involved in cyberespionage activities against other Member States, as shown by the 2021 Danish example. This observation raises questions on how to approach such activities in the context of the relationship of the responsible state with other Member States and the EU in general. More generally, reflecting on the demarcation between cyberespionage activities and other forms of cyber operations may be relevant for the cybersecurity policies and strategies of the EU and its Member States. Moreover, these different questions and observations might also constitute an interesting axe of reflection for the Intelligence College in Europe, created in 2021 by 21 Member States of the EU together with Norway and the United Kingdom [(32)], notably on how to apprehend the cyber dimension of espionage as well as to assess the relationship between cyber espionage activities and other forms of cyber operations. The observations made in this chapter demonstrate that in these documents it may not always be desirable to refer to such a distinction, as it may have important political and legal implications.

(32) The 23 signatories are: Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Italia, Latvia, Lithuania, Malta, the Netherlands, Norway, Portugal, Romania, Slovenia, Spain, Sweden, United Kingdom. 'Letter of Intent concerning the development of the Intelligence College in Europe', February 2020 (https://www.intelligence-college-europe.org/wp-content/uploads/2020/03/LoI-English.pdf).

CHAPTER 6

GRAMMAR: RULES IN A CYBER CONFLICT

by
KUBO MAČÁK AND LAURENT GISEL

INTRODUCTION

Today, the use of cyber operations during armed conflicts is a manifest reality. While only a few states have publicly acknowledged engaging in such operations, an increasing number of states are developing military cyber capabilities, and their use is likely to increase in the future. The international community recognises that just like any other means and methods of warfare, cyber operations may seriously affect civilian infrastructure and thus result in 'devastating humanitarian consequences' [(1)].

These words of caution are supported by the growing evidence of serious cyber incidents over the past few years (primarily occurring outside armed conflicts), including cyber operations against hospitals, water and electrical infrastructure, and nuclear and petrochemical facilities, that are of particular concern [(2)]. The increasing use of military cyber capabilities and the related humanitarian concerns underscore the urgency of reaching shared understandings on the legal constraints that apply to the use of cyber operations during armed conflicts. That is the focus of the present chapter [(3)].

The chapter sets the scene by defining the notion of cyber operations during armed conflicts and by presenting an overview of the current military use of cyber operations and their potential human cost. It then discusses the threshold question of *whether* international humanitarian law (IHL) applies to cyber operations and zooms in on three specific issues related to how IHL principles and rules apply to cyber operations during armed conflict. The chapter concludes by emphasising

(1) United Nations General Assembly, 'Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/75/816, 18 March 2021 (hereafter OEWG report), p. 17, para. 18 (https://undocs.org/A/75/816).

(2) Mačák, K. and Lawson, E., 'Avoiding civilian harm during military cyber operations: six key takeaways', Humanitarian Law and Policy Blog, 15 June 2021 (https://blogs.icrc.org/law-and-policy/2021/06/15/avoiding-civilian-harm-military-cyber-operations/).

(3) Although written in a personal capacity, the chapter is informed by and builds on previous public positioning by the International Committee of the Red Cross (ICRC) on these matters. See, in particular, ICRC, 'International humanitarian law and cyber operations during armed conflicts: ICRC position paper', November 2019 (hereafter ICRC position paper); see also Gisel, L., Rodenhäuser, T., and Dörmann, K., 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts', *International Review of the Red Cross*, Vol. 102, No 913, 2020, pp. 287–334 (https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/abs/twenty-years-on-international-humanitarian-law-and-the-protection-of-civilians-against-the-effects-of-cyber-operations-during-armed-conflicts/BE68981904487F07B9919836B78B6DAD).

the importance of states formulating national positions on the application of international law, including IHL, to cyber operations.

CYBERSPACE AND CYBER OPERATIONS: SETTING THE SCENE

IHL does not contain a definition of cyber operations, cyber warfare or cyber war, and neither do other fields of international law. Definitions used by states range from those that narrowly focus on the use of cyber capabilities to achieve goals in cyberspace [(4)] to broader approaches that refer instead to information war and define this notion in a manner that includes at least some aspects of what is often understood as cyber warfare [(5)]. The International Committee of the Red Cross (ICRC) understands cyber operations during armed conflict as 'operations against a computer system or network, or another connected device, through a data stream, when used as means or method of warfare in the context of an armed conflict' [(6)].

The potential human cost of cyber operations must not be neglected.

In recent years, societies have become largely dependent on ICTs, a process that has been accelerated by the ongoing Covid-19 pandemic. While there are numerous benefits and opportunities offered by growing interconnectivity, increased dependency also implies increased vulnerability. Whereas the emergent proliferation of cyber tools and their use as a means or method of warfare may offer belligerents the possibility of achieving their objectives without necessarily causing direct harm to civilians or physical damage to civilian infrastructure, the potential human cost of cyber operations must not be neglected.

By means of cyber operations, processes controlled by computer systems can be triggered, altered, or otherwise manipulated and essential civilian data, including medical data, can be tampered with, with the potential to entail significant harmful effects for civilians. Moreover, cyber operations can harm infrastructure in at least two ways. First, they can affect the delivery of essential services to civilians, as has been shown with cyber operations against electrical grids, water supply facilities, or the healthcare sector. Second, they can cause physical damage, as was the case with the Stuxnet attack against a nuclear enrichment facility in Iran in 2010, and an attack on a German steel mill in 2014 [(7)].

These risks are compounded by the interconnectivity that characterises cyberspace, which means that whatever has an interface with the internet can be affected by cyber operations conducted from anywhere in the world. A cyber operation against a specific system may have repercussions on various other systems, regardless of where those systems are located. Cyber operations conducted over recent years – primarily outside armed conflicts – have shown that malware can spread instantly around the globe

(4) See e.g. United States Department of Defense, *DOD Dictionary of Military and Associated Terms*, January 2021, p. 55 (https://irp.fas.org/doddir/dod/dictionary.pdf).

(5) See e.g. Ministry of Defence of the Russian Federation, 'Russian Federation Armed Forces' Information Space Activities Concept', undated (https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle).

(6) 'ICRC position paper', op.cit., p. 3, fn. 1.

(7) See ICRC, 'The potential human cost of cyber operations', May 2019 (https://www.icrc.org/en/document/potential-human-cost-cyber-operations).

and affect civilian infrastructure and the provision of essential services [8]. There is a real risk that cyber tools – either deliberately or by mistake – may cause large-scale harm and damage to critical civilian infrastructure, such as essential industries, telecommunications, transport, governmental and financial systems. As one cybersecurity expert put it recently, such military operations constitute a 'humanitarian crisis in the making' [9].

The characteristics of cyberspace raise other concerns as well. For example, cyber operations entail a risk of escalation and related human harm for the simple reason that it may be difficult for the targeted party to know whether the attacker's aim is intelligence collection or more harmful effects. The target may thereby react with greater force than necessary out of anticipation of a worst-case scenario, leading to 'unexpected escalation of competition and conflict' [10].

Cyber tools also proliferate in a unique manner. Once used, they can be repurposed or reengineered and thus widely used by actors other than the one that had developed or used them initially. A further concern is the difficulty to reliably attribute cyber operations, which hampers the identification of the authors of such operations and holding them accountable, as well as the determination of the applicable legal framework [11]. The perception that it will be easier to deny responsibility for such operations may also weaken the taboo against their use – and may make actors less scrupulous about using them in violation of international law [12].

Overall, these concerns underscore the need to understand the potential harmful impact of cyber operations on the civilian population and, accordingly, the protection afforded to civilians and civilian infrastructure by the applicable international law.

APPLICATION OF IHL TO CYBER OPERATIONS

States have repeatedly reaffirmed that international law is applicable to the use of ICTs, most recently in last year's reports of the UN Open-Ended Working Group (OEWG) [13] and the UN Group of Governmental Experts (GGE) [14]. The GGE report also explicitly referred to international humanitarian law in the cyber context (a historical first for UN-based processes), noting that this branch of international law 'applies only in situations of armed conflict' [15]. Commentators have interpreted this reference as amounting to a consensus

[8] Examples include the malware CrashOverride, the ransomware WannaCry, the wiper program NotPetya, and the malware Triton. CrashOverride affected the provision of electricity in Ukraine; WannaCry affected hospitals in several countries; NotPetya affected a very large number of businesses; Triton was aimed at disrupting industrial control systems, and was reportedly used in attacks against Saudi Arabian petrochemical plants. For some discussion, see Gisel, L. and Olejnik, L., 'The potential human cost of cyber operations: starting the conversation', Humanitarian Law and Policy Blog, 14 November 2018 (https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/).

[9] Caltagirone, S., 'Industrial cyber attacks: A humanitarian crisis in the making', Humanitarian Law and Policy Blog, 3 December 2019 (https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/).

[10] ICRC, 'Avoiding civilian harm from military cyber operations during armed conflicts', 2021, p. 12 (https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations).

[11] See ICRC, 'International humanitarian law and the challenges of contemporary armed conflicts', 2011, p. 37; 'Twenty years on', op.cit., pp. 309-310.

[12] ICRC position paper, op.cit., p. 8.

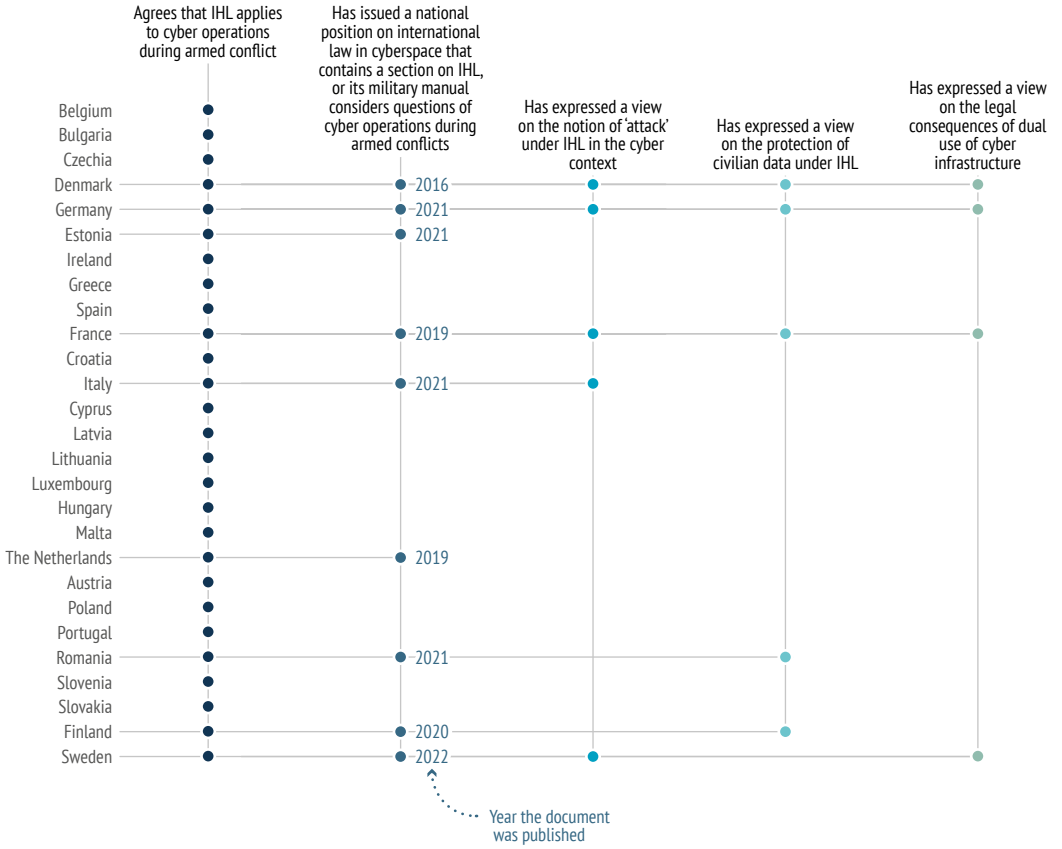
[13] OEWG report, p. 10, para. 34.

[14] United Nations General Assembly, 'Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security', UN Doc. A/76/135, 14 July 2021 (hereafter GGE 2021 report), p. 18, para. 71(f) (https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf).

[15] Ibid.

Application of IHL to cyber operations during armed conflict

EU Member States' views



among the participating states on the applicability of IHL to cyber operations [16].

In our view, there is no question that IHL applies to, and therefore limits, cyber operations during armed conflict – just as it regulates the use of any other weapon, means and methods of warfare in an armed conflict, whether new or old. In doing so, IHL seeks to minimise the humanitarian consequences of armed conflict, whether caused by kinetic or cyber means. This holds true whether cyberspace is considered as a new domain of warfare similar to air, land, sea and outer space; a different type of domain because it is man-made while the former are natural; or not a domain as such. [17]

In line with this view, an increasing number of states and international organisations have

[16] See, e.g., Schmitt, M., 'The sixth United Nations GGE and International Law in cyberspace', *Just Security*, 10 June 2021 (https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/); Ponta, A., 'Responsible state behavior in cyberspace: Two new Reports from parallel UN processes', *ASIL Insight*, 30 July 2021 (https://www.asil.org/insights/volume/25/issue/14); Osula, A.-M., 'In search of a coherent international approach to governing technologies', *ORF Digital Frontiers*, 17 October 2021 (https://www.orfonline.org/expert-speak/international-approach-to-governing-technologies/).

[17] 'International humanitarian law and the challenges of contemporary armed conflicts', op.cit., p. 40; see also Schmitt, M. N. and Vihul, L. (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd edition, Cambridge University Press, Cambridge, 2017 (hereafter *Tallinn Manual 2.0*), p. 375, Rule 80.

publicly asserted that IHL applies to cyber operations during armed conflict [18]. There is also a consensus on this point among all EU Member States [19]. At the same time, some states have expressed opposition to the militarisation of cyberspace or a cyber arms race and have expressed concerns regarding a possible legitimisation of the use of military cyber operations [20]. While these are important considerations, they are not necessarily incompatible with the application of IHL to cyber operations during armed conflict.

In particular, acknowledging that IHL applies to cyber operations during armed conflict is not an encouragement to militarise cyberspace and should not be understood as legitimising cyber-warfare [21]. As underscored in the 2021 GGE report, 'recalling [IHL] principles by no means legitimizes or encourages conflict' [22]. In fact, IHL imposes substantial limits on the militarisation of cyberspace by prohibiting the development of military cyber capabilities that would violate IHL [23].

Finally, it must be noted that any use of force by states – cyber or kinetic – remains governed by the Charter of the United Nations and the relevant rules of customary international law, in particular the prohibition against the use of force [24]. International disputes must be settled by peaceful means [25], as recently reaffirmed in the cyber context in both the OEWG and the GGE processes [26].

SPECIFIC CHALLENGES

While affirming that IHL applies to cyber operations in armed conflict is an essential first step to avoid or minimise the potential human suffering that cyber operations might cause, it is equally important for states to work towards common understandings of how IHL principles and rules apply to the specific nature of cyber operations [27]. In the present section, we emphasise three key challenges in this area [28].

(18) See e.g. Council of the EU, 'Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy – Joint communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', *11357/13*, 25 June 2013, para. 6 (https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/137602.pdf); NATO, 'Wales Summit Declaration (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales)', 5 September 2014, para. 72 (https://www.nato.int/cps/en/natohq/official_texts_112964.htm).

(19) See e.g. EU, 'Joint comments from the EU and its Member States on the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security', May 2020, para. 10 (https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf).

(20) See e.g. the submissions of China, Cuba, Iran, Nicaragua, or Russia on the initial pre-draft of the OEWG report (www.un.org/disarmament/open-ended-working-group/).

(21) ICRC position paper, op.cit., pp. 4–5.

(22) GGE 2021 report, op.cit., p. 18, para 71(f) *in fine* (noting that 'recalling [IHL] principles by no means legitimizes or encourages conflict').

(23) For example, IHL prohibits the development of cyber capabilities that would qualify as weapons and would be indiscriminate by nature or would be of a nature to cause superfluous injury or unnecessary suffering. See e.g. Henckaerts, J.-M. and Doswald-Beck, L. (eds.), *Customary International Humanitarian Law, Vol. 1: Rules*, Cambridge University Press, Cambridge, 2005 (hereafter *ICRC Customary Law Study*), Rules 70, 71 (https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul).

(24) UN Charter, Article 2(4).

(25) UN Charter, Articles 2(3) and 33.

(26) OEWG Report, op.cit., p. 10, para. 35; GGE 2021 Report, op.cit, p. 17, para 70.

(27) GGE 2021 Report, op.cit., p. 17, para 71.

(28) For further analysis of the relationship between international law and military cyber operations, see Mačák, K., 'Unblurring the lines: military cyber operations and international law', *Journal of Cyber Policy*, Vol. 6, No 3, 2021, pp. 411–428 (https://www.tandfonline.com/doi/full/10.1080/23738871.2021.2014919).

Cyber operations and the notion of 'attack' under IHL

The question of whether or not an operation amounts to an 'attack' as defined in IHL is essential for the application of many of the rules deriving from the principles of distinction, proportionality and precaution, which afford important protection to civilians and civilian objects [29]. Concretely, rules such as the prohibition on attacks against civilians and civilian objects, the prohibition on indiscriminate and disproportionate attacks, and the obligation to take all feasible precautions to avoid or at least reduce incidental harm to civilians and damage to civilian objects when carrying out an attack apply to those operations that qualify as 'attacks' as defined in IHL. The question of how widely or narrowly the notion of 'attack' is interpreted with regard to cyber operations is therefore essential for the applicability of these rules and the protection they afford to civilians and civilian infrastructure.

Article 49 of the 1977 Additional Protocol I defines attacks as 'acts of violence against the adversary, whether in offence or in defence'. It is well established that the notion of violence in this definition can refer to either the means of warfare or their effects, meaning that an operation generating violent effects can qualify as an attack even if the means used to bring about those effects are not violent as such [30].

It is also widely accepted that cyber operations expected to cause death, injury or physical damage constitute attacks under IHL [31]. Some states, including Denmark, Finland, New Zealand, Norway, Switzerland, or the United States, have clarified that this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack [32], for example the death of patients in intensive-care units caused by a cyber operation on an electricity network that results in cutting off a hospital's electricity supply – a view shared by the ICRC [33].

Beyond this, cyber operations that significantly disrupt essential services without necessarily causing physical damage – such as those that would incapacitate banking or communications networks – constitute one of the most important risks that cyber operations raise for civilians. Diverging views exist, however, on whether a cyber operation that results in a loss of functionality without causing physical damage qualifies as an attack as defined in IHL.

In the ICRC's view, during an armed conflict an operation designed to disable a computer or a computer network constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means. Indeed, if the notion of attack is interpreted as only referring to operations that cause death, injury or physical damage, a cyber operation that is directed at making a civilian network (such as electricity, banking, or communications)

(29) The notion of attack under IHL, defined in Art. 49 of the 1977 First Additional Protocol, is different from and should not be confused with the notion of 'armed attack' under Article 51 of the UN Charter, which belongs to the realm of *jus ad bellum*. To affirm that a specific cyber operation, or a type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.

(30) Droege, C., 'Get off my cloud: Cyber warfare, International Humanitarian Law, and the protection of civilians', *International Review of the Red Cross*, Vol. 94, No 886, 2012, p. 557 (https://international-review.icrc.org/articles/get-my-cloud-cyber-warfare-international-humanitarian-law-and-protection-civilians); Boothby, W. H., *The Law of Targeting*, Oxford University Press, Oxford, 2012, p. 384; 'Twenty years on', op.cit., p. 312.

(31) 'International humanitarian law and the challenges of contemporary armed conflicts', op.cit., pp. 41–42; *Tallinn Manual 2.0*, op.cit., p. 415, Rule 92.

(32) Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 2016, p. 677 (when discussing computer network attacks); Finland, *International Law and cyberspace: Finland's national positions*, 2020, p. 7; New Zealand, *Manual of Armed Forces Law*, 2nd edition, 2017, Vol. 4, para. 8.10.22; Norway, *Manual i krigens folkerett*, 2013, para. 9.54; Switzerland, 'Switzerland's position paper on the application of international law in cyberspace: Annex UN GGE 2019/2021', 27 May 2021, p. 10; United States, 'United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014–15)', p. 6 and from a practical perspective *Joint Publication 3-12 (R) 'Cyberspace operations'*, 5 February 2013, p. IV-4.

(33) ICRC position paper, op.cit., p. 7.

dysfunctional, or is expected to cause such an effect incidentally, might not be covered by essential IHL rules protecting the civilian population and civilian objects. Such an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities [34].

Because cyber operations can significantly disrupt essential services without necessarily causing physical damage, this question constitutes one of the most critical debates for the protection of civilians against the effects of cyber operations. For the moment, opinions vary among the states that have taken public positions. States that subscribe to the broader view that includes loss of functionality under the notion of 'attack' include Ecuador, France, Germany, Guatemala, Italy, Japan, or New Zealand [35]. States that take the narrower view that requires physical damage include Denmark, Israel, or Peru [36].

Finally, IHL remains relevant also to those cyber operations that do not qualify as 'attacks'. On the one hand, some rules apply to a broader range of conduct described in IHL as 'military operations'. This is the case, for example, with the obligation that 'in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects' [37]. This obligation requires all those involved in military operations to continuously bear in mind the effects of military operations on the civilian population, civilians and civilian objects, to take steps to reduce such effects as much as possible, and to seek to avoid any unnecessary effects [38]. Its applicability to cyber operations has been expressly reaffirmed by several states, including Finland, France, or Germany [39].

On the other hand, some rules of IHL afford specific protection to certain categories of persons and objects that goes beyond the protection against attacks [40]. For example, IHL specifically makes it illegal 'to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population' [41]. The explicit mention of 'rendering useless' must be understood as covering a broader

(34) ICRC position paper, op.cit., pp. 7–8; for more details, see 'Twenty years on', op.cit., pp. 312–316.

(35) Ecuador, 'Verbal Note 4-2 186/2019 from the Permanent Mission of Ecuador to the OAS' (28 June 2019), cited in Organization of American states (OAS), *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, OAS Doc. CJI/doc. 615/20 rev.1, 7 August 2020, para. 32 (https://www.oas.org/en/sla/iajc/docs/themes_recently_concluded_International_law_State_cyber_operations_FINAL_REPORT.pdf); France, Ministère des Armées, 'International Law applied to operations in cyberspace', 2019, p. 13; Ministry of Foreign Affairs of Germany, 'On the application of International Law in cyberspace Position Paper', March 2021, p. 9; Guatemala, 'Note Of. 4VM.200-2019/GJL/lr/bm, from Mr. Gabriel Juárez Lucas, Fourth Vice Minister of the Interior Ministry of the Republic of Guatemala to Luis Toro Utillano, Technical Secretariat, Inter-American Juridical Committee (14 June 2019), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, op.cit.; Italy, 'Italian Position Paper on 'International Law and Cyberspace'', 2021, pp. 9–10; Japan, Ministry of Foreign Affairs of Japan, 'Basic position of the Government of Japan on International Law applicable to cyber operations', May 2021, p. 7; Department of the Prime Minister and Cabinet, New Zealand, 'The application of International Law to state activity in cyberspace', 1 December 2020, para. 25.

(36) Ministry of Defence of Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 2016, pp. 290–291; Schöndorf, R., 'Israel's perspective on key legal and practical issues concerning the application of International Law to cyber operations', *International Law Studies*, Vol. 97, 2021, pp. 395–406, at p. 400; Peru, Response Submitted by Peru to the Questionnaire on the Application of International Law in OAS Member States in the Cyber Context (June 2019), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, op.cit., para. 31.

(37) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I), Art. 57(1); *ICRC Customary Law Study*, op.cit., Rule 15.

(38) See e.g. United Kingdom, Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict*, 2004, para. 5.32.1; *Tallinn Manual 2.0*, op.cit., para. 4 of the commentary on Rule 114; Oeter, S., 'Methods of Combat', in Fleck, D. (ed.), *The Handbook of International Humanitarian Law*, 4th edition, Oxford University Press, Oxford, 2021, p. 215; Neuman, N., 'A precautionary tale: The theory and practice of precautions in attack', *Israel Yearbook on Human Rights*, Vol. 48, 2018, pp. 28–29.

(39) Finland, 'International law and cyberspace: Finland's national positions', 2020, p. 7; France, Ministère des Armées, 'International Law applied to operations in cyberspace', 2019, p. 15; Germany, 'On the application of International Law in cyberspace: Position paper', March 2021, p. 9.

(40) See 'Twenty years on', op.cit., pp. 322–329; see also Federal department of Foreign Affairs, Switzerland, 'Switzerland's position paper on the application of international law in cyberspace: Annex UN GGE 2019/2021', 27 May 2021, p. 10.

(41) AP I, Art. 54(2); Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II), Art. 14; *ICRC Customary Law Study*, op.cit., Rule 54.

range of operations that may impact these goods, beyond attacks or destruction [42]. Accordingly, cyber operations that are designed, or can be expected, to disable indispensable objects or facilities such as drinking water installations are prohibited, irrespective of whether they qualify as attacks. IHL also requires respecting and protecting medical and humanitarian personnel and facilities – again a protection that goes beyond the protection against attack [43], as does the obligation to take constant care in the conduct of military operations [44].

The protection afforded to civilian electronic data under IHL

Essential civilian data – such as medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records – constitutes an essential component of digitalised societies. Such data is key to the functioning of most aspects of civilian life, be it at individual or societal level. Deleting or tampering with essential civilian data can quickly bring government services and private businesses to a complete standstill and such operations could therefore cause more harm to civilians than the destruction of physical objects.

With regard to data belonging to certain categories of objects that enjoy specific protection under IHL, the protective rules are comprehensive. In particular, the obligations to respect and protect medical facilities [45] and humanitarian relief operations [46] must be understood as extending to medical data belonging to those facilities and data of humanitarian organisations that are essential for their operations [47]. Similarly, deleting or otherwise tampering with data in a manner that renders useless objects indispensable to the survival of the civilian population, such as drinking water installations and irrigation systems, is prohibited [48].

Still, it is important to clarify the extent to which civilian data is protected by the existing general rules on the conduct of hostilities. In particular, debate has arisen on whether data constitutes objects as understood under IHL, in which case cyber operations against data (such as deleting data) would be notably governed by the principles of distinction, proportionality and precaution and the protection they afford to civilian objects [49].

Experts hold different views on whether data qualifies as an object for the purposes of the IHL rules on the conduct of hostilities. One view, held by the majority of experts involved in the Tallinn Manual process, is that the ordinary meaning of the term 'object' cannot be interpreted as including data because objects

[42] 'Twenty years on', op.cit., p. 327; *Tallinn Manual 2.0*, op.cit., paragraph 6 of the commentary on Rule 141.

[43] 'Twenty years on', op.cit., pp 328–329; *Tallinn Manual 2.0*, op. cit., paragraph 5 of the commentary on Rule 131; see also Rodenhäuser, T., 'Hacking humanitarians? IHL and the protection of humanitarian organizations against cyber operations', *EJIL:Talk!*, 16 March 2020 (https://www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/); Mačák, K., Gisel, L., and Rodenhäuser, T., 'Cyber attacks against hospitals and the Covid-19 pandemic: How strong are international law protections?', *Just Security*, 27 March 2020 (https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/).

[44] 'Twenty years on', op.cit., pp 323–324; *Tallinn Manual 2.0*, op.cit., Rule 114.

[45] See, for instance, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Art. 19; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Art. 12; Convention (IV) relative to the Protection of Civilian Persons in Time of War, Art. 18; AP I, Art. 12; AP II, Art. 11; *ICRC Customary Law Study*, op.cit., Rules 25, 28, 29.

[46] See e.g. AP I, Arts 70(4), 71(2); *ICRC Customary Law Study*, op.cit., Rules 31 and 32.

[47] See 'Twenty years on', op.cit., pp. 327–328; *Tallinn Manual 2.0*, op.cit., para. 3 of the commentary on Rule 132.

[48] AP I, Art. 54; AP II, Art. 14; *ICRC Customary Law Study*, op.cit., Rule 54.

[49] See also 'Unblurring the lines: military cyber operations and international law', op.cit., pp. 421–422.

are material, visible and tangible [50]. Some states, including Denmark, Chile, or Israel, also subscribe to this view [51].

By contrast, others have argued that either all or some types of data should be considered as objects under IHL. One view, taken by several states – including Finland, Germany, Norway, and Romania – is that the protection of civilian objects extends to civilian data [52]. This implies that all data constitutes an object for the purposes of IHL. This interpretation is supported by the 'modern meaning' of the notion of objects in today's society as well as by the object and purpose of the relevant IHL rules [53]. It is also consistent with the traditional understanding of the notion of 'object' under IHL, which is broader than the ordinary meaning of the word and encompasses also locations and animals [54]. Another approach, thus far endorsed by one state, France, is to consider content data as protected under the principle of distinction, leaving aside the issue of whether other types of data (such as code) formally qualify as objects or not [55].

Except for some specific military networks, cyberspace is predominantly used for civilian purposes.

While the question of whether and to what extent civilian data constitutes a civilian object remains unresolved, the assertion that deleting or tampering with such essential civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the objective and purpose of IHL. Logically, the replacement of paper files and documents with digital files in the form of data should not diminish the protection that IHL affords to them [56]. In essence, excluding essential civilian data from the protection afforded by IHL to civilian objects would result in a significant protection gap.

The military use of cyberspace and the effect on its civilian character

In order to protect critical civilian infrastructure that relies on cyberspace, it is also crucial to protect the infrastructure of

[50] See *Tallinn Manual 2.0*, op.cit., para. 6 of the commentary on Rule 100. The experts relied on the 1987 ICRC Commentary which notes that objects are material, visible and tangible; this explanation in the Commentary however, aimed at distinguishing objects from concepts such as 'aim' or 'purpose', not at differentiating between tangible and intangible goods, and therefore cannot be seen as determinative for the debate on data (see 'Twenty years on', op.cit., p. 318).

[51] *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, op.cit., p. 292; Chile, Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire (14 January 2020), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, op.cit., para. 36; 'Israel's perspective on key legal and practical issues concerning the application of international law to cyber operations', op.cit., p. 401.

[52] 'International law and cyberspace: Finland's national positions', op.cit., 2020, p. 7; Germany, 'On the application of International Law in cyberspace: Position Paper', op.cit., p. 8; Norway, *Manual i krigens folkerett*, 2013, para. 9.58; Romania, 'National contribution on the subject of how international law applies to the use of information and communications technologies by States' in United Nations General Assembly, 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266', UN Doc. A/76/136, 13 July 2021, p. 78.

[53] Mačák, K., 'Military objectives 2.0: The case for interpreting computer data as objects under International Humanitarian Law', *Israel Law Review*, Vol. 48, No 1, 2015, p. 80 (https://www.cambridge.org/core/journals/israel-law-review/article/abs/military-objectives-20-the-case-for-interpreting-computer-data-as-objects-under-international-humanitarian-law/9DD4F5EBF48CF8C665F7B5E27049E3F7); see also McLaughlin, R., 'Data as a military objective', Australian Institute of International Affairs, 20 September 2018 (https://www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/).

[54] 'Twenty years on', op. cit., p. 319.

[55] France, 'International Law applied to operations in cyberspace,' op.cit., p. 14. For the view that, conversely, operational-level data (i.e., code) may qualify as an object, see Harrison Dinniss, H.A, 'The nature of objects: Targeting networks and the challenge of defining cyber military objectives', *Israel Law Review*, Vol. 48, No 1, 2015, pp. 39–54 (https://www.cambridge.org/core/journals/israel-law-review/article/abs/nature-of-objects-targeting-networks-and-the-challenge-of-defining-cyber-military-objectives/A0E60CDE115C4EACB3D8F7F1305D94F5).

[56] 'International humanitarian law and the challenges of contemporary armed conflicts', op.cit., p. 28.

cyberspace itself. The challenge lies, however, in the interconnectedness of civilian and military networks.

Except for some specific military networks, cyberspace is predominantly used for civilian purposes. Furthermore, military networks may rely on civilian cyber infrastructure, such as undersea fibre-optic cables, satellites, routers or nodes. Conversely, civilian vehicles, shipping and air traffic controls increasingly rely on navigation satellite systems that may also be used by the armed forces. Civilian logistical supply chains and essential civilian services use the same web and communication networks through which some military communications pass. In other words, except for certain networks that are specifically dedicated to military use, it is to a large extent impossible to differentiate between purely civilian and purely military cyber infrastructures [(57)].

Under IHL, attacks must be strictly limited to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage [(58)]. All objects which are not military objectives under this definition are civilian objects under IHL and must not be made the object of an attack or of reprisals [(59)]. In case of doubt as to whether an object that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, it must be presumed to remain protected as a civilian object [(60)].

It is traditionally understood that an object may become a military objective when its use for military purposes is such that it fulfils the definition of military objective even if it is simultaneously used for civilian purposes (such objects are sometimes referred to as 'dual-use objects') [(61)]. However, a wide interpretation of this rule could lead to the conclusion that many objects forming part of cyberspace infrastructure would constitute military objectives and would therefore not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ever-increasing civilian reliance on cyberspace [(62)].

The applicable rules provide some important safeguards in this respect. Firstly, as noted earlier, IHL requires that the target's destruction or neutralisation must offer a 'definite military advantage' in the circumstances ruling at the time [(63)]. However, because cyberspace is designed with a high level of redundancy, one of its characteristics is the ability to immediately reroute data traffic. This inbuilt resilience must be considered by those who are planning or deciding upon an attack [(64)]. If – because of this resilience – a given cyber operation was expected to only offer 'potential or indeterminate advantages' to the attacker [(65)], its target would remain a civilian object, and thus protected from attack [(66)].

(57) 'Twenty years on', op. cit., pp. 320–322.

(58) AP I, Art. 52(2); *ICRC Customary Law Study*, op.cit., Rules 7–8.

(59) AP I, Art. 52(1); *ICRC Customary Law Study*, op.cit., Rule 9.

(60) AP I, Art. 52(3); 1996 Amended Protocol II to the Convention on Certain Conventional Weapons, Art. 3(8)(a); see also *ICRC Customary Law Study*, op.cit., Rule 10, commentary pp. 35–36.

(61) See e.g. *ICRC Customary Law Study*, op.cit., Rule 10, commentary p. 32; *Tallinn Manual 2.0*, op.cit., para. 1 of the commentary on Rule 101.

(62) 'Twenty years on', op. cit., p. 321.

(63) AP I, Art. 52(2); *ICRC Customary Law Study*, op.cit., Rule 8.

(64) 'International humanitarian law and the challenges of contemporary armed conflicts', op.cit., p. 42.

(65) See Sandoz, Y., Swinarski, C. and Zimmerman, B. (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva, 1987, p. 636 para. 2024 ('it is not legitimate to launch an attack which only offers potential or indeterminate advantages').

(66) 'Twenty years on', op. cit., p. 321.

Secondly, even if certain parts of cyberspace infrastructure qualify as military objectives during armed conflicts, any attack against them remains governed by the prohibition of indiscriminate attacks [67] and the rules of proportionality [68] and precaution in attacks [69]. Precisely because civilian and military networks are often highly interconnected, assessing the expected incidental civilian harm of any cyber operation is critical to ensuring that the civilian population is protected against its effects [70]. For example, attacks against root servers or submarine data cables would raise concerns under the prohibition of indiscriminate attacks because of the difficulty of limiting the effects of such attacks, as required by IHL [71].

CONCLUSION

This chapter has provided an overview of some of the rules that apply to, and thus limit, the use of cyber operations during armed conflicts. It has also shown that certain legal questions – such as the exact interpretation of the IHL notions of attacks and objects – remain unsettled for the time being. It should thus be welcomed that states, including several European ones, have started issuing national positions on the application and interpretation of international law, including IHL, to cyber operations. After all, only if states make their views known will it be possible to assess whether the law, as applied and interpreted in the cyber context, sufficiently addresses the humanitarian concerns associated with the use of cyber operations.

This is the case irrespective of whether a given state is developing military cyber capabilities or whether it is, or expects to be, involved in armed conflicts. All states have the duty to ensure respect for IHL and, therefore, they all share an interest in maintaining this body of law effective and able to respond to modern challenges. In addition, from a more pragmatic perspective, the interconnectivity of cyberspace means that the effects of cyber operations conducted by some states during armed conflicts may well cause harm to civilians and civilian populations in otherwise uninvolved states located on the other side of the globe, which therefore have an interest that the protections that IHL affords are upheld with regard to cyber operations.

Therefore, the present circumstances present a prime opportunity for states who have not yet issued such national positions to consider doing so. At the time of writing, only around twenty such positions have been published worldwide [72], which means that new ones not only contribute to the consolidation of international law in the area, but they may also influence other states both at the regional and the global level [73]. In the European context, the process can be streamlined and accelerated if the EU develops a shared position on the application of international law in cyberspace, as recommended by the 2020 EU Cybersecurity Strategy [74] and endorsed by the 2022 Council

[67] AP I, Art. 51(4); *ICRC Customary Law Study*, op.cit, Rules 11–12.

[68] AP I, Arts 51(5)(b) and 57; *ICRC Customary Law Study*, op.cit., Rule 14.

[69] AP I, Art. 57; *ICRC Customary Law Study*, op.cit., Rules 15–21.

[70] See ICRC position paper, op.cit., p. 7.

[71] AP I, Art. 51(4)(c); *ICRC Customary Law Study*, op.cit., Rule 12(c).

[72] For a full overview, see Cyber Law Toolkit, 'National Positions' (https://cyberlaw.ccdcoe.org/wiki/Category:National_position).

[73] See Mačák, K., 'From cyber norms to cyber rules: Re-engaging states as law-makers', *Leiden Journal of International Law*, Vol. 30, No 4, 2017, pp.896–898 (https://doi.org/10.1017/S0922156517000358).

[74] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, 'The EU's Cybersecurity Strategy for the Digital Decade', JOIN(2020) 18 final, 16 December 2020, p. 20 (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0). On the EU's approach to promoting compliance with IHL, see also Council of the EU, 'Updated European Union Guidelines on promoting compliance with international humanitarian law (IHL)', 2009/C 303/06, 15 December 2009 (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0).

Conclusions on the development of the EU's cyber posture [(75)]. In our view, any such new statements should reaffirm the applicability of IHL to the use of cyber operations during armed conflict – recalling, as noted earlier, that doing so does not legitimise conflict or encourage militarisation – and then address the key interpretive challenges posed by the development of cyber capabilities.

Overall, the development of such positions should be informed by an in-depth understanding of the relevant technological developments, the potential human cost they may entail, and the protection afforded by existing law. In this respect, it is imperative that interpretations of IHL with regard to novel issues do not decrease the level of protection developed in traditional contexts. Instead, states and international organisations should be guided by the object and purpose of this body of law, i.e., to restrict the use of means and methods of warfare in order to protect civilians and civilian objects against the effects of hostilities. In the cyber context, that includes in particular interpreting the law so as to preserve civilian infrastructure from significant disruption and to protect civilian data.

(75) Council of the European Union, 'Council Conclusions on the development of the European Union's cyber posture', 9364/22, 23 May 2022, paras 25 and 30 (https://www.consilium.europa.eu/media/56358/st09364-en22.pdf).

CHAPTER 7

DIALECTS: COLLECTIVE CYBER DEFENCE IN THE EU AND NATO

by
PETER B.M.J. PIJPERS, HANS BODDENS HOSANG AND PAUL A.L. DUCHEINE

INTRODUCTION

Collective defence is the cornerstone of the North Atlantic defence system, in which the European partners rely heavily on the (nuclear) deterrence assets of the United States. The solidarity in this system has been relatively one-sided. Given the US shift to the Pacific [(1)], in a geopolitical context where threats against the core values of the EU remain acute or have even magnified [(2)], the European Union is pursuing increased strategic autonomy [(3)].

The EU nowadays has a clause for mutual defence similar to NATO's Article 5, replacing the somewhat obsolete collective defence system of the Western European Union (WEU) [(4)]. So far, both NATO's Article 5 and the EU's mutual defence clause have been invoked only once, in the latter case by France in search of political rather than military support [(5)]. Though the collective defence systems of both the EU and NATO are built on the customary international law standard regarding the right of self-defence [(6)], the wording and the scope of the clauses differ. Whereas NATO is confined to the military sphere and a nascent diplomatic role, to the EU all instruments of power – such as the economy, diplomacy, information, culture, knowledge [(7)] – are available.

(1) Manyin, M.E. et al, 'Pivot to the Pacific? The Obama Administration's "rebalancing" toward Asia', CRS Report for Congress, 2012 (https://sgp.fas.org/crs/natsec/R42448.pdf).

(2) NATO, 'Madrid Summit Declaration 29 June 2022', NATO Press Release. Bullet 3, 29 June 2022 (https://www.nato.int/cps/en/natohq/official_texts_196951.htm); Johnson, R., 'The first phase of the Russian invasion of Ukraine 2022', Changing Character of War Centre, Oxford, 2022.

(3) Sari, A., 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', *10 Harvard National Security Journal*, 2019, p. 408; EU High Representative for Foreign Affairs and Security Policy, 'Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy', 2016 (https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf).

(4) Boddens Hosang, J.F.R. and Ducheine, P.A.L, 'Implementing Article 42.7 of the Treaty on European Union: Legal foundations for multual defence in the face of modern threats', ACIL, 2020, pp. 3-4 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748392).

(5) Bakker, A. et al., 'The EU's mutual assistance clause' in *Spearheading European Defence: Employing the Lisbon Treaty for a stronger CSDP,* Clingendael Institute, 2016 (https://www.clingendael.org/sites/default/files/2016-02/Report_Spearheading_European_Defence.pdf).

(6) As laid down in Article 51 of the Charter of the United Nations.

(7) Ducheine, P.A.L. and Pijpers, P. B.M.J., 'The missing component in deterrence theory: The legal framework' in Osinga, F.P.B. and Sweijs, T. (eds), *Deterrence in the 21st Century – Insights from Theory and Practice* Springer, 2021, pp. 481-482.

The differences between the EU and NATO collective defence systems come into sharper focus with regard to their ability to cope with threats emerging from cyber operations. In cyberspace, state and non-state actors can operate on a near equal footing; moreover, although prone to generate strife and even conflict, activities in cyberspace predominantly fall below the threshold of the use of force, hence outside the classic military remit.

The problem that emerges is that cyberattacks (below the level of force) and collective defence systems (against an armed attack) appear to be mutually exclusive. Is collective cyber defence an oxymoron or should the mechanism be revisited, embracing a broader vision of collective defence? And if so, given the fact that the EU has a wide array of instruments of power at its disposal (from diplomatic measures via economic sanctions and financial fines to legal retorsions) would this then also imply that the EU is better equipped to provide a security umbrella against modern cyber threats?

This chapter aims to offer a strategic and legal perspective on collective defence against cyberattacks in an EU and NATO context. In order to assess whether the EU is better equipped than NATO to provide a collective defence system against cyberattacks, first various types of cyberattacks including their core attributes will be described. Next, a comparative overview of the NATO and EU collective defence systems is presented. In the following section the attributes of cyberattacks are cross-referenced with the collective defence systems to see what gaps remain. In the final section some concluding reflections are provided and an answer to whether or not the EU is suited to provide a collective cyber defence system.

ON CYBER OPERATIONS

Collective defence is associated with armed attack in the traditional land, sea or maritime domains. Cyberattacks differ from traditional kinetic attacks in several ways. To put the differences into context a short description of cyberspace and the various categories of malicious cyber operations is provided in this section.

Cyberspace is a domain in which activities are performed and carried out, similar to the land, sea, space or air domains [(8)]. Therefore, cyberspace is not an instrument or a weapon as such, but rather 'an enabling environment that allows actors to transmit information to large audiences at low cost, near instantaneously, through multiple distribution points, across borders and with heightened opportunities for anonymity' [(9)]. Cyberspace is an operational domain contained within the information environment. The information environment entails three conceptual dimensions: the cognitive, virtual and physical [(10)]. These can in turn be subdivided into seven layers as depicted in the diagram opposite.

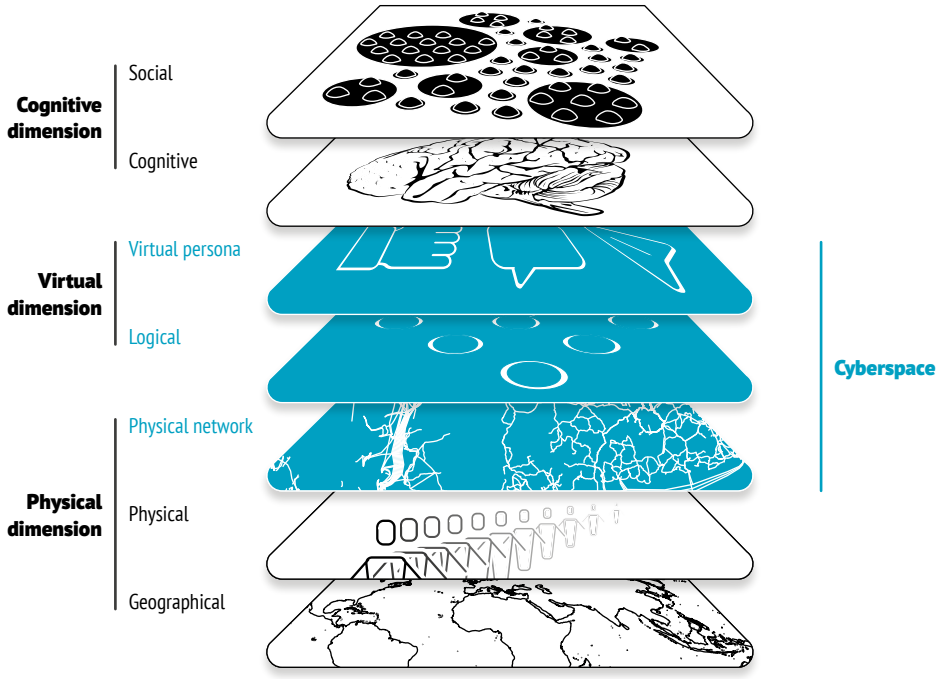
For the purpose of this chapter, the scope of cyberspace consists of three layers: (i) the physical network layer of the computers,

(8) Heintschel von Heinegg, W., 'Territorial sovereignty and neutrality in cyberspace', US Naval War College, *International Law Studies*, Vol. 89, 2013, p. 123; Nye, J. S. Jnr, 'Cyber Power', Harvard Kennedy School, Belfer Centre for Science and International Affairs, May 2010, p.7 (https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf); Delerue, F., 'Reinterpretation or contestation of International Law in cyberspace?', *Israel Law Review*, Vol. 52, No 3, November 2019, pp. 304-305.

(9) Lin, H.S. and Kerr, J., 'On cyber-enabled information warfare and information operations', in Cornish, P. (ed.), *Oxford Handbook of Cybersecurity*, 2021, pp. 262–265; Jensen, E., 'Cyber sovereignty: The way ahead', *Texas International Law Journal*, Vol. 50, No 2, 2015, p. 275, p. 279.

(10) Ducheine, P.A.L., van Haaster, J. and van Harskamp, R., 'Manoeuvring and generating effects in the information environment' in Ducheine, P.A.L and Osinga, F.P.B (eds.), *Winning Without Killing: the strategic and operational utility of non-kinetic capabilities in crisis - NL ARMS 2017*, 2017, pp. 5-7; CJCS, 'Information Operations - Joint Publication 3-13', Washington D.C., 2014, p. I.1.

The infomation environment and cyberspace



Data: Data: Ducheine, P.A.L. et al (eds.), *Winning Without Killing: the strategic and operational utility of non-kinetic capabilities in crisis*, 2017; van Haaster, J., *On Cyber: The utility of military cyber operations during armed conflict*, 2018.

cables and hubs, i.e. the hardware storing data and making the transfer of data possible; (ii) the logical layer of data, software applications and protocols [11]; and (iii) the cyber-persona layer which consists of virtualised representations of entities or groups and enables them to access the logical layer and hardware, and thus to interact in cyberspace (*inter alia* on the internet and social media).

With the inception of cyberspace three new layers have been introduced for human communication, commerce but also conflict as we have seen with the 2010 Stuxnet attack [12], the hack-and-release activities during the 2016 US presidential election [13], or more recently the SolarWinds hack compromising critical infrastructure [14], affecting the cognitive and physical layers of the information environment [15].

Activities in cyberspace can be divided into so-called 'hard' and 'soft' cyber operations [16]. Hard cyber operations are cyber-related

[11] The internet entails the physical network layer and the logical layer. See *On Cyber*, op.cit., pp. 136-137.

[12] Lindsay, J.R., 'Stuxnet and the limits of cyber warfare', *Security Studies*, Vol. 22, 2013, pp. 378-389, p. 365,

[13] Office of the Director of National Intelligence, 'Assessing Russian activities and intentions in recent US elections', Washington, 2017 (https://www.dni.gov/files/documents/ICA_2017_01.pdf).

[14] Singh, P., 'SolarWinds: Cyber strategists are back to the drawing board', *Hindustan Times*, 27 December 2020 (https://www.hindustantimes.com/analysis/solarwinds-cyber-strategists-are-back-to-the-drawing-board/story-L5QunVMY7vRa04isQlT1QL.html).

[15] Betz, D.J. and Stevens, T., 'Power and Cyberspace', *Adelphi Series*, Vol. 51, No 424, 2011, p. 35, p. 41.

[16] Pijpers, P. B.M.J and Arnold, K.L., 'Conquering the invisible battleground', *Atlantisch Perspectief*, Vol. 4, No 44, 2020, pp. 12-14; Ducheine, P.A.L. and van Haaster, J., 'Fighting power, targeting and cyber operations' International Conference on Cyber Conflict, CYCON 303, 2014, p. 313; Ducheine, P.A.L. and Pijpers, P. B.M.J., 'The notion of cyber operations' in Tsagourias, N. and Buchan, R. (eds), *Research Handbook on International Law and Cyberspace*, 2nd edition, Edward Elgar, 2021.

activities *in* cyberspace such as hacking a computer or disabling, disrupting or destroying software [17] or virtual persona [18]. Hard cyber operations affect cyberspace, while soft cyber operations are cyber-related activities that use cyberspace as a vector. Soft cyber operations use cyberspace as a vector to 'weaponise' the content of a message but also manipulate the source (or outlet) of the message (including via falsifying social media accounts) [19] to influence the cognitive dimension of other actors [20].

Contrary to traditional kinetic attacks, cyberattacks are remotely executed operations that predominantly take place below the threshold of an armed attack as envisioned in Article 51 of the UN Charter [21]. When cyberattacks take place, it is often not the malign act (emplacing malware) that will be noticed, but the effects of it, which may develop (much) later in time [22]. Moreover, given the relatively low costs of entry, attacks may often be perpetrated by non-state actors that may not be under control of a state [23]. Since the impact of cyberattacks, especially in soft cyber operations, is often less tangible, it is generally considered that it is more difficult to attribute the attack to a specific actor [24]. The so-called attribution problem in cyberspace [25] must not be overexaggerated however. The attribution process entails a technical [26], legal and political layer. The layers are not necessarily interrelated, an act can be attributed for political reasons [27] without providing technical evidence [28]. And, finally, even if aggressive acts can be attributed to an actor, an attack carried out in or via the virtual dimension of cyberspace (e.g. related to iCloud services or email-accounts) cannot always be traced to a specific territory, which could have legal implications [29].

(17) Castro, S., 'Towards the development of a rationalist cyber conflict theory', *The Cyber Defense Review*, Vol. 6, No 1, Winter 2021, p. 38 (https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/03_CDR_V6N1_Castro.pdf).

(18) 'Manoeuvring and generating effects in the information environment', op.cit., pp. 2 & 15; Kello, L., *The Virtual Weapon and International Order*, Yale University Press, New Haven, 2017, pp. 51-53; 'Cyber Power', op.cit., p. 6.

(19) Shires, J., 'Hack-and-leak operations: Intrusion and influence in the Gulf', *Journal of Cyber Policy*, Vol. 4, No 2, 2019, p. 240; 'Cyber Power', op.cit., pp. 2 and 5.

(20) Cyber-related influence operations are inherently soft cyber operations. see: Stephens, D., 'Influence operations & international law', *Journal of Information Warfare*, Vol.19, No 4, 2020, p. 2.

(21) Gill, T.G. and Ducheine, P.A.L, 'Anticipatory self-defense in the cyber context', *International Law Studies*, Vol. 89, Naval War College, 2013, p. 459.

(22) Mueller, R.S., 'Report on the investigation into Russian interference in the 2016 presidential election', Volume 1 of II, US Department of Justice, Washington D.C., March 2019, pp. 38-40.

(23) Merrigan, E., 'Blurred lines between state and non-state actors', Council on Foreign Affairs, 2020 (https://www.cfr.org/blog/blurred-lines-between-state-and-non-state-actors).

(24) Finlay, L. and Payne, C., 'The attribution problem and cyber armed attacks', *AJIL Unbound 202*, Vol.113, 2019, pp. 203-205.

(25) Dipert, R.R., 'The ethics of cyberwarfare', *Journal of Military Ethics*, Vol. 9, 2010, p. 385.

(26) Tsagourias, N. and Farrell, M., 'Cyber attribution: Technical and legal approaches and challenges', *European Journal of International Law*, Vol. 31, No 3, 2020, pp. 947-951.

(27) Finnemore, M. and Hollis, D.B., 'Beyond naming and shaming: Accusations and International Law in cybersecurity', *European Journal of International Law*, Vol. 31, No 3, August 2020, pp. 1002-1003.

(28) Some states argue that there is no obligation to disclose the evidence for (political) attribution, see: Eichensehr, K., 'Cyberattack attribution and international law', *Just Security*, 2020 (https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/); Egan, B., 'International Law and stability in cyberspace', *Berkeley Journal of International Law*, Vol. 35, No 1, 2016 (https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf); Ministère des Armées, 'Droit international appliqué aux opérations dans le cyberespace', 2019, pp. 10-11 (https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf).

(29) Pijpers, P. B.M.J. and Van Den Bosch, B.G.L.C, 'The "virtual Eichmann": On sovereignty in cyberspace', ACIL Research Paper 2020-65, December 2020, pp. 19-20 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746843).

COLLECTIVE DEFENCE IN AN EU AND NATO CONTEXT

The right of states to defend themselves against an armed attack is an inherent right deriving from the very nature of statehood [30]. This rule of customary international law is also recognised in Article 51 of the UN Charter [31], and guided by the principles of necessity, proportionality and immediacy [32]. The inherent right of self-defence relates to a response to an (imminent) armed attack, in which case the use of force is permitted, thereby exempting *jus cogens* on the prohibition of the use of force [33], and Article 2(4) of the UN Charter.

The right of self-defence can be exercised individually or collectively as stipulated in NATO's collective defence clause of Article 5 of the North Atlantic Treaty [34], and in the EU's mutual assistance (or mutual defence) clause of Article 42(7) [35] of the Treaty on European Union (TEU). Aside from an assistance clause, the Member States of the EU can also invoke a solidarity clause (Article 222 Treaty on the Functioning of the EU (TFEU) in case of terrorist attacks or natural and man-made disasters [36].

The mutual defence clauses of the EU and NATO both refer to Article 51 of the UN Charter and are similar in intent, although differing in substance. Taking also the EU solidarity clause into account, the differences relate to the activation criterion, the territorial scope and binding nature of the clause, and the arrangements for implementation [37].

The *casus foederis* or the trigger for invoking NATO's Article 5 is an 'armed attack' echoing the words of Article 51 of the UN Charter. The mutual assistance clause of the EU uses the term 'armed aggression' [38]. Despite linguistic differences, the factual differences are marginal. [39] One explanation for the differences is that 'armed aggression' was translated literally from the French version of Article 51 UN Charter, which refers to *agression armée* instead of armed attack [40]. In the view of one expert, this is the narrow interpretation of the activation criterion, equating armed

(30) Boddens Hosang, J.F.R., *Rules of Engagement and the International Law of Military Operations*, Oxford Monographs in International Humanitarian and Criminal Law, Oxford University Press, Oxford, 2020, pp. 51–53.

(31) 'Anticipatory self-defense in the cyber context', op.cit., pp. 441–443.

(32) *Legality of the Threat or Use of Nuclear Weapons – Advisory Opinion of 8 July 1996* [1996], ICJ Reports, Paras 40–42; 'Anticipatory self-defense in the cyber context', pp. 448–452.

(33) *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986], ICJ Reports, Para 190.

(34) 'Article 5: The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. (…).', North Atlantic Treaty, 1949 (https://www.nato.int/cps/en/natolive/official_texts_17120.htm).

(35) Article 42(7): 'If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.' *Consolidated Version of the Treaty on European Union*, *O J* C–326, 2012. (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A12008M042).

(36) NATO could refer to Article 4 when 'territorial integrity, political independence or security of any of the Parties is threatened'. This article will not be dealt with in this chapter since it does not imply collective action of the alliance. See: North Atlantic Treaty, Article 4.

(37) Pawlak, P., 'Cybersecurity and cyberdefence: EU solidarity and mutual defence clauses', EPRS Briefing, June 2015 (https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI(2015)559488_EN.pdf).

(38) Though it is a restatement of the commitments laid down in Article 5 of the Treaty of Brussels that established the Western European Union. See 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', op.cit., p. 433.

(39) 'Implementing Article 42.7 of the Treaty on European Union', op.cit., p. 7.

(40) Perot, E., 'The art of commitments: NATO, the EU, and the interplay between law and politics within Europe's Collective Defence Architecture', *European Security*, Vol. 28, No 1, 2019, pp. 45–46.

aggression to armed attack, while a broader interpretation would give room for providing assistance in a case where unlawful force is used 'that does not reach the gravity threshold of an armed attack' [41]. He argues that it is not likely that the drafters intended to broaden the notion of armed attack, but the possibility must not be discarded completely [42]. This rationale can be supported by arguing that the EU intended to apply alternative collective security mechanisms, by offering the option of assistance based on solidarity in cases other than an armed attack via Article 222 TFEU.

Both NATO and EU mutual defence clauses have a territorial scope [43] and refer to attacks on the territory of the Member States. NATO includes extraterritorial military assets within the region demarcated by Article 6 of the North Atlantic Treaty but excludes overseas territories (e.g. Dutch or French Antilles) [44]. The EU, on the other hand, includes the latter [45]. The EU solidarity clause also relates to territory but to a lesser extent, meaning that the EU could, in reference to Article 222 TFEU, still request assistance for disasters befalling military forces or embassies located outside the EU.

The Member States of NATO and the EU are required to provide support in the event that the collective defence clause is invoked, but the obligatory nature of the clauses differ. While Article 42(7) TEU uses stronger language, it cannot address all Member States equally due to the neutrality of some of them [46]. NATO does not require the Member States to provide aid and assistance 'by all the means in their power' as Article 42(7) requests but asks for such action as the Member States deem necessary. A bigger difference, however, concerns the exact nature of the assistance [47]. In both the EU and NATO, Member States can use all instruments of power to respond, including – but not limited to – the use of force [48]. However, the contribution of NATO Member States is, or can be, substantial in military terms [49], while the EU contribution might not go beyond political and diplomatic support [50].

Invoking Article 222 TFEU in the event of a terrorist attack or a disaster will result in an EU-led and embedded activity [51], while Article 42(7) TEU or Article 5 of the NATO Treaty 'entail direct state-to-state assistance without explicitly mentioning any role for the common EU or NATO institutions as such' [52]. The reason for this is that Articles 42(7) TEU and Article 5 NATO Treaty derive from the inherent right of self-defence, while Article 222 TFEU does not.

---

(41) 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', op.cit., pp. 417-418.

(42) Ibid, p. 419.

(43) 'The art of commitments', op.cit., pp. 49-50.

(44) North Atlantic Treaty, op. cit., Article 6. Although Article 4 of the NATO Treaty has a world-wide scope. Bumgardner, S.L., 'Article 4 of the North Atlantic Treaty', *Emory International Law Review*, Vol. 34, 2019, p. 76.

(45) 'The art of commitments', op.cit., (n 268), p. 49.

(46) 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', op.cit., p. 435.

(47) 'The EU's mutual assistance clause', op.cit., p. 25; 'Implementing Article 42.7 of the Treaty on European Union', op.cit., p. 7.

(48) 'The art of commitments', op.cit., p. 53.

(49) Ibid, p. 51. Moreover, the TEU will not overrule the obligations as laid down in the NATO treaty. Art 42.7 TEU [5] states that 'Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.'

(50) When France invoked Article 42(7) in 2015 it shifted military power from out-of-area operations to mainland France. Other EU Member States have, in response, taken over some of those out-of-area tasks, which could also be valued as an act of solidarity. ECFR, 'Article 42.7: An Explainer', European Council on Foreign Relations, 2015 (cfr.eu/article/commentary_article_427_an_explainer5019/).

(51) Council of the European Union, 'Decision on the arrangements for the implementation by the Union of the solidarity clause', *Official Journal of the European Union*, L 192 53, Article 3 (c) jo Article 5, 2014, pp. 56-57; Article 222 TFEU speaks about 'the Union and its Member States', while Article 42(7) TEU solely addresses the Member States.

(52) 'The art of commitments', op.cit., p. 52.

COLLECTIVE CYBER DEFENCE

The notion of a collective defence system presents challenges and is never free from political considerations. NATO has acted in a collective and concerted manner during many operations since its inception in 1949, and Article 5 was never invoked in the Cold War era. Kinetic operations, and the subsequent use of the collective defence system [53], became even more complex with the rise of terrorism. The attacks by a non-state actor on the Twin Towers and the Pentagon on 11 September 2001 paradoxically triggered the invocation of Article 5 for the first time. The terrorist attacks in Paris on 13 November 2015, which led France to invoke Article 42(7), were also executed by non-state actors [54].

Cyberattacks, making use of the virtual dimension, might prove to be even more challenging to align with the system of collective defence [55]. Not only are non-state actors active in cyberspace, but moreover, cyberattacks predominantly fall below the threshold of the use of force. Two questions must therefore be addressed: can cyberattacks amount to the level of an armed attack, and if not, the subsequent question is whether the collective defence system is applicable to attacks below the threshold of the use of force?'

Armed attacks comprise (i) transnational (ii) use of force, which will have a (iii) substantial impact [56] in terms of (iv) scale and effect [57]. Cyberattacks could amount to the level of an armed attack, if they cause effects 'resulting in physical casualties, substantial physical damage, or such substantial and long-term damage to critical infrastructure that the carrying out of a state's essential functions or its social and political stability are seriously impaired' [58].

Recent cyberattacks have not amounted to the level of use of force (with the possible exception of the 2010 Stuxnet attack) [59], let alone of an armed attack. However, as cyber operations are capable of inflicting crippling effects [60], it is not unlikely that a cyberattack might indeed reach this magnitude [61], and potentially lead to the invocation of current collective defence systems.

Until such a conjuncture, the subsequent question would therefore be if the NATO and EU collective defence systems, including the EU solidarity clause, should, based on state practice and legal opinion, be reinterpreted taking into account the attributes of cyberattacks. Cyber operations are often executed by (elusive) non-state actors, the activities predominantly falling below the theshold of an armed attack, and even below the use of force.

(53) Lanovoy, V., 'The use of force by non-state actors and the limits of attribution of conduct', *European Journal of International Law*, Vol. 28, May 2017, pp. 567-568, p. 563.

(54) 'Article 42.7: An Explainer', op. cit.

(55) See 'Implementing Article 42.7 of the Treaty on European Union', op.cit., pp. 14-15.

(56) Gill, T.D. and Tibori-Szabó, K., 'Twelve key questions on self-defense against non-state actors – and some answers', ACIL, *International Legal Studies*, Vol. 95, 2019, p. 492.

(57) Boothby, W.H. et al, 'When is a cyberattack a use of force or an armed attack?', *Computer*, Vol. 45, 2012, p. 82; *Case concerning military and paramilitary activities in and against Nicaragua*, op. cit., Para 195; 'Implementing Article 42.7 of the Treaty on European Union', op.cit., p. 9; Ducheine, P. A.L., 'Military cyber operations' in Gill, T.D. and Fleck, D. (eds), *The Handbook of the International Law of Military Operations*, 2nd edition, Oxford University Press, Oxford, 2015, pp. 456-475.

(58) 'Anticipatory self-defense in the cyber context', pp. 460-461.

(59) An eloquent analysis can be found in: Efrony, D. and Shany, Y.,'A rule book on the shelf? Tallinn Manual 2.0 on cyber operations and subsequent state practice', *American Journal of International Law*, Vol. 112, No 4, 2018, pp. 594-631. On Stuxnet see: Schmitt, M.N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, Rule 71(10), p. 342; Sanger, D.E., *The Perfect Weapon : War, sabotage, and fear in the cyber age*, Scribe, 2018 (chapter 1).

(60) Referring to recent cyber-attacks and incidents, including SolarWinds, Colonial Pipeline systems and the US executive order in response to that, see: The White House, 'Executive Order on Improving the Nation's Cybersecurity', May 2021 (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/).

(61) For an earlier – more reserved – assessment, see 'Anticipatory self-defense in the cyber context', op.cit., p. 461.

The issue of non-state actors is less problematic. Although Article 51 of the UN Charter (and therefore the derivative Article 5 of the NATO Treaty and Article 42(7) TEU) has been incorporated in treaties regulating state behaviour, this does not impair the inherent or customary international rule of self-defence, also against non-state actors [(62)]. After 9/11, this now also appears to be a common interpretation of Article 51 UN Charter itself [(63)].

The fact that the customary international right of self-defence also applies to armed attacks by non-state actors does not, however, solve the collective cyber defence conundrum. The difficulty lies in the combination of a non-state cyberattack below the threshold of an armed attack, that cannot be attributed to a specific perpetrator, or (territorially) located.

The customary international right to self-defence and hence Article 51 UN Charter, Article 5 NATO Treaty and Article 42(7) TEU, establish the legal basis for responding to armed attacks. The remit could be widened to include 'armed aggression' or even the use of force [(64)]. The United States have, after the *Nicaragua* Case [(65)], refrained from distinguishing between the use of force and an armed attack [(66)], hence, in their view, any form of the use of force can invoke the right of self-defence. However, this legal opinion is not universally held. Using 'armed aggression' instead of 'armed attack' could, liberally reading into the intention of the EU drafters, also stretch the remit of collective defence to include responses to use of force. However, both interpretations will not suffice since a cyberattack could not only fall below the level of armed attack but also below the level of the use of force. Furthermore, from a legal point of view, stretching this standard would be untenable since an armed attack invokes the inherent right of self-defence, while (other) use of force in an interstate setting does not, although the execution of a cyberattack may authorise such responses as countermeasures [(67)] excluding the use of force [(68)]. However, countermeasures are inherently unilateral in the sense that only the injured state (or states) can appeal to them [(69)]; collective countermeasures are not allowed [(70)].

The solidarity clause (Article 222 TFEU) could be used in response to a broader array of attacks, including those below the use of force. Although the solidarity clause is confined to terrorist attacks and natural or man-made disasters, the meaning of disaster is rather broad and includes 'any situation which has or may have a severe impact on people (…)' [(71)]. The 2013 EU Cybersecurity Strategy also alluded to the possibility of invoking Article 222 TFEU in case of a serious cyberattack [(72)].

---

(62) 'Twelve key questions on self-defense against non-state actors – and some answers', op.cit., p. 474.

(63) Ducheine, P.A.L. and Pijpers, P. BMJ., 'The missing component in deterrence theory: The legal framework', ACIL Research Paper 2020-70, 2020., pp. 494-495; 'Implementing Article 42.7 of the Treaty on European Union', op.cit., p. 6.

(64) 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', op.cit., pp. 422-425.

(65) *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op.cit..

(66) Hongju Koh, H., 'International Law in cyberspace', 4854 Faculty Scholarship Series 1, 2012, p. 7; Schmitt, M.N., 'The Defense Department's measured take on International Law in cyberspace', *Just Security,* 11 March 2020 [Section on 'The use of force'] (https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/).

(67) 'The missing component in deterrence theory', op.cit., p. 491.

(68) Article 50 (1) a of the United Nations, 'Responsibility of states for internationally wrongful acts', 2001, II *Yearbook of the International Law Commission* vol II (Part Two).

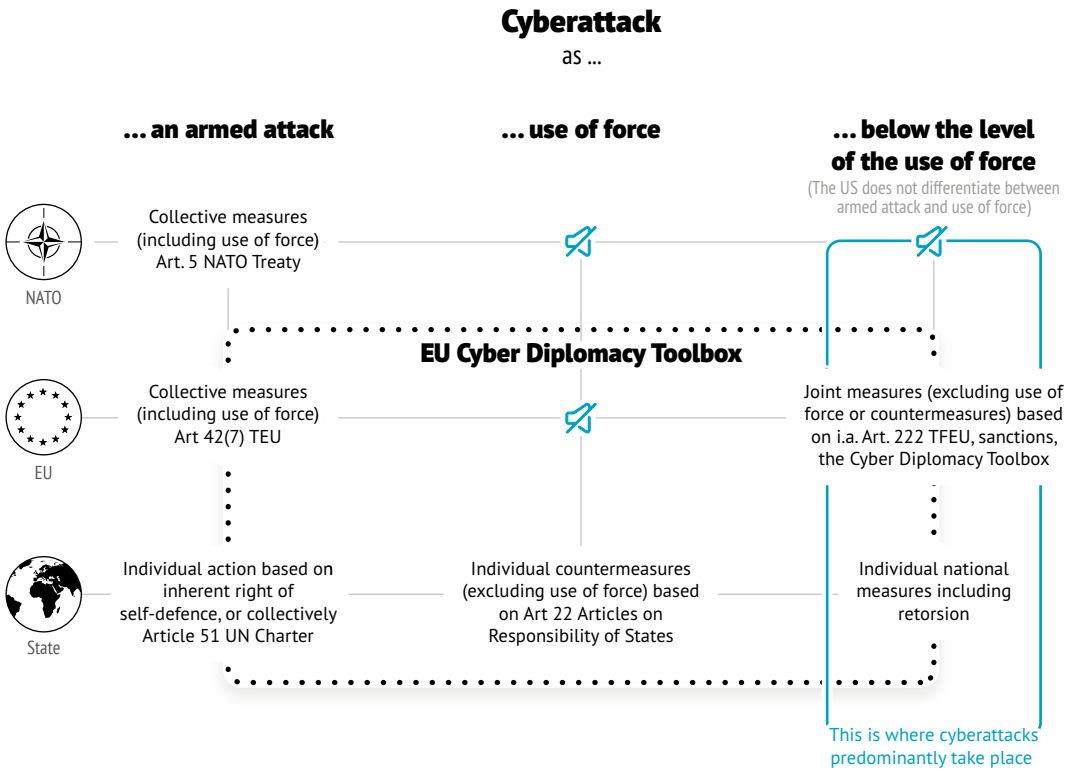
(69) Roguski, P., 'Collective countermeasures in cyberspace – Lex lata, progressive development or a bad idea?', International Conference on Cyber Conflict, CYCON 25, 26-29 May 2020, pp. 27-31.

(70) Delerue, F., *Cyber Operations and International Law*, Cambridge University Press, Cambridge, 2020, p. 232.

(71) Council of the European Union, 'Decision on the arrangements for the implementation by the Union of the solidarity clause', op.cit., Article 3 (a), p, 55; 'Cybersecurity and cyberdefence: EU solidarity and mutual defence clauses', op.cit., p. 4.

(72) European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace', (Join(2013) 1 final), February 2013, p. 19 (https://edps.europa.eu/sites/default/files/publication/13-02-07_communication_join_cyber_sec_en.pdf).

Collective cyber defence and the EU Cyber Diplomacy Toolbox



The EU solidarity clause widens the options to other, more generic collective cybersecurity options than the inherent right of self-defence, individually or collectively, and thus not in response to an armed attack or the use of force. While NATO is able to issue statements regarding unwelcome situations in its territorial perimeter [(73)], it basically lacks instruments of power in the remit below the use of force. This should not be surprising, since this is not NATO's purpose. The opposite applies to the EU. Although the EU has some arrangements regarding responses to an armed attack, the core of its instruments – consistent with the identity of the EU as a soft power – are not related to the use of force. The EU has numerous tools within these instruments of power ranging from restrictive measures (sanctions) [(74)] to recalling diplomats and issuing demarches. In legal terms the responsive measure amounts to retorsions: unfriendly albeit lawful activities [(75)]. It is also in this area (see diagram above) that most cyberattacks take place. To address malign activities in cyberspace, the EU has a joint response mechanism in which Union and Member States' tools

(73) For example: NATO, 'North Atlantic Council Statement following the announcement by the United States of actions with regard to Russia', 15 April 2021 (https://www.nato.int/cps/en/natohq/news_183168.htm#:~:text=Issued%20on%20 15%20April%202021&text=NATO%20Allies%20support%20and%20stand,enhance%20the%20Alliance's%20collective%20 security.)

(74) Title IV, Article 215 on Restrictive Measures, 'Treaty on the Functioning of the European Union', *OJ* C 326, 26 October 2012 (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:FULL:EN:PDF)..

(75) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*., op.cit., Rule 20 (4).

are collected in the so-called cyber diplomacy toolbox [(76)]. Although this toolbox is not a coherent foreign policy instrument but rather a potpourri of options, it demonstrates the potency of a collective cyber defence mechanism against cyberattacks below the use of force [(77)].

REFLECTIONS ON THE ROLE OF THE EU

Is the EU better equipped to provide a collective defence system against cyberattacks than NATO?

It can be assessed that, firstly, cyberattacks predominantly fall below the threshold of the use of force, which implies that collective defence clauses designed for armed attacks are incompatible with most cyberattacks. Secondly, cyberattacks are often executed by non-state actors. Although Article 51 UN Charter was meant to regulate state behaviour, the inherent right of self-defence it reflects is a separate rule of customary international law [(78)]. The latter includes attacks by non-state actors, and after the 9/11 attack Article 51 UN Charter is also commonly interpreted in that sense. Thirdly, the author and the origin of cyberattacks (state or non-state actors) are sometimes difficult to pinpoint, given the time-lapse between the malign cyber-activity and the actual effect of a cyber-attack. Establishing authorship and attributing a cyberattack to an actor or even a state, without conclusive technical and forensic evidence is possible but is a political act. Nevertheless, and although with lower (overt) standards of certainty, attribution is on the rise. Fourthly, since cyberattacks target the cognitive dimension via cyberspace, these attacks seldom have a physical or functional manifestation, making it challenging to conclude that the territory of an EU or NATO Member State is affected.

The EU, as an integrated and political entity, has a broader scope than NATO which can be used to tackle many issues related to cyberattacks. The EU competences coalesce with the attributes of current cyberattacks, especially when related to problems of attribution, the virtual characteristics of the cyberattack, but primarily given the fact that cyberattacks remain below the threshold of the use of force.

In that sense, the EU is better suited to respond to cyberattacks. The EU is able to focus on collective measures below the use of force including diplomatic, economic and other instruments, thereby complementing NATO and not latently competing with it. However, while the current cyber diplomacy toolbox is a welcome first step, it is insufficient as a coherent EU joint response mechanism as it lacks focus. To strengthen EU policy related to a joint response to cyberattacks, the EU response mechanism would need to operate separately from collective responses to armed attacks since the latter are based on the inherent right of self-defence of Member States – individually or collectively. It should also operate autonomously from responses by individual Member States, which include countermeasures against the use of force. Since collective countermeasures by the EU are not allowed, the EU's joint response mechanism against cyberattacks should revolve around lawful but unfriendly retorsions, including collective EU sanctions and issuance of diplomatic statements attributing cyberattacks to alleged perpetrators.

(76) European Union, 'Joint EU diplomatic response to malicious cyber activities ("Cyber Diplomacy Toolbox")', Draft Council Conclusions, 2017; Moret, E. and Pawlak, P., 'The EU Cyber Diplomacy Toolbox: Towards a cyber sanctions regime?', Brief no. 24, European Union Institute for Security Studies, July 2017.

(77) Ivan, P., 'Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox', European Policy Centre, March 2019, pp. 11–12.

(78) 'When is a cyberattack a use of force or an armed attack?', op.cit., p. 83.

CHAPTER 8

FUTURE TENSE: CYBER DEFENCE AND EMERGING DISRUPTIVE TECHNOLOGIES

by
RALUCA CSERNATONI

INTRODUCTION

The growing number of malicious cyber incidents in recent years is a harbinger of a much darker and complicated cyber future. Yet, as the ongoing war in Ukraine confirms, with thousands of Russian-backed cyberattacks being perpetrated every month, it could be argued that the expected dystopian cyber future is already unfolding in the present. Ukraine, a recurrent target of Russian offensive cyber operations at least since 2014, is indeed the 'perfect sandbox for those looking to test new cyberweapons, tactics and tools' [(1)].

Such incidents and tactics open a Pandora's Box of competing geopolitical interests and diverging challenges. Against this backdrop and given the potentially disruptive impact of new technologies in cyberspace, serious security risks driven by malign intent are rapidly proliferating. Global powers across the world, ranging from the United States to the EU to Asia, are shoring up their cybersecurity and cyber defence capabilities and capacities in a race to innovate. In the process, companies, and in particular technological giants and the global telecommunications industry, have been caught up in competing geostrategic interests and a new digital tech 'arms race' rhetoric.

On the one hand, the intrinsically interconnected nature of the global digital world means that it is not simply a matter of applying geopolitical lenses to digital transformation and new tech. On the other hand, geopolitical metaphors are still powerful tools, transforming the digital sphere into a battleground for politics, business, and militarisation. With a complex network of state and non-state actors, cyberspace is indeed blurring the lines between and challenging orthodox understandings of war and peace. This latter interpretation assumes that cyber incidents and threats are moving conflicts into a grey zone [(2)] below the threshold of conventional warfare toward a state of 'unpeace' or mid-spectrum

(1) Cerulus, L., 'How Ukraine became a test bed for cyberweaponry', *Politico*, 14 February 2019 (https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/).

(2) Wirtz, J. J., 'Life in the "Gray Zone": observations for contemporary strategists', *Defense & Security Analysis*, Vol.33, No 2, 2017, pp. 106-114.

rivalry lying below the physically destructive threshold of interstate violence, but whose harmful effects far surpass the tolerable level of peacetime competition [3].

This chapter examines the evolving role of emerging and disruptive technologies (EDTs) in cyber defence. It starts with an overview of different concepts and frameworks used to make sense of the increasing complexity in the relationship between cybersecurity and new technologies. AI and other emerging technologies are already starting to transform how conflicts are fought. The fielding of AI cyber security systems may also lead to new approaches and transformations in cyber system engineering and cyber defence architectures. AI-enhanced cyberattacks, communications jamming, electronic warfare, and other attacks on a system's software will become as important as those that target hardware, if not more so. The chapter then looks at the role of EDTs as an element of the EU's cyber defence and defence policies before concluding with general observations regarding the impact of these developments on the EU's cyber posture.

Cyberspace is blurring the lines between and challenging orthodox understandings of war and peace.

A BRAVE NEW CYBERWORLD

The disruptive impact of new and emerging technologies [4] and an ever-intensifying race to deploy autonomous and intelligent systems result in a paradigmatic transformation regarding armed conflicts. Such technological advancements are seen as critical to dominance in future warfare and for the militaries of tomorrow. Cyberspace has been labelled as the fifth domain [5] and a new theatre for conflict and competition besides land, sea, air and space. It is comprised of three distinctive elements, hardware, software, and information, all three areas susceptible to the transformative influence of emerging and disruptive technologies and their security and defence implications. Related terms such as cybersecurity, cyber resilience, cyber deterrence, and cyber defence have also been used to designate an array of strategies and responses to counter or prevent cyber incidents and attacks in cyberspace.

Irrespective of the conceptual nuances between various terms, cyber issues both in the civil and military domains require comprehensive strategies across various policy fields, as well as increased coordination among international organisations, the military, state and law enforcement agencies, and other private entities. Today, an assortment of malign state and non-state actors perpetrate millions of cyber incidents around the world every day. This complex picture will be further complicated by AI-powered cyberattacks and the increasing availability of AI-based tools. A dangerous and emerging narrative of a so-called 'AI arms race' [6] equally introduces significant challenges and new risks in warfare, putting pressure on governments to cut corners and field powerful, but potentially

[3] Kello, L., 'Cyber legalism: why it fails and what it fails and what to do about it', *Journal of Cybersecurity*, Vol.7, No 1, 2021 (https://doi.org/10.1093/cybsec/tyab014).

[4] Missiroli, A., 'High Tech, Low Take? The strategic impact of disruptive technologies', *CSDS Policy Brief*, March 2021 (https://brussels-school.be/publications/policy-briefs/policy-brief-high-tech-low-take-strategic-impact-disruptive-technologies).

[5] European Defence Agency, 'Cyber Defence', 2021 (https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence).

[6] Csernatoni, R., 'Beyond the hype: The EU and the AI Global "Arms Race"', European Leadership Network, Commentary, 21 August 2019 (https://www.europeanleadershipnetwork.org/commentary/beyond-the-hype-the-eu-and-the-ai-global-arms-race/).

faulty and untested AI-enabled weapons systems, to launch cyberattacks.

What is more, state-led or traditional military approaches to securing and governing cyberspace have often been ineffective at tackling the entire threat landscape spectrum, from ransomware or critical infrastructure attacks, economic or state-sponsored espionage, disinformation and election interference, to physical damage caused to people and objects in the real world. Not particularly helpful is the fact that the term cybersecurity has remained vague and a blanket term, designating both 'the insecurity created by and through cyberspace and [...] the practice or processes to make it more secure' [7]. Cybersecurity encompasses a range of issues, policies, practices, tools, and norms, from fostering freedom and openness, increasing resilience and trust-building, promoting public and private industry collaborations, protecting critical infrastructures and citizens' privacy, combating cybercrime, to spending more on cutting-edge cyber defence technologies. But most importantly, differing visions of cyber warfare, different speeds in innovating or digitalising military forces, and gaps in EDTs-enabled cyber capabilities introduce significant risks and challenges, even among allies, jeopardising both interoperability and technological superiority.

THE TECH FUTURE IS NOW

The past decade has been transformative for technological innovation, signalling what some have labelled as the fourth industrial era [8]. Cyber incidents will follow new technological trends and the roll-out of new technologies. International organisations such as the EU have been faced with the Herculean task of responding to growing transnational cyber threats and the pressing need to invest in cutting-edge technologies and cyber capabilities to stay ahead in the game. Within this context and due to a proliferation of hybrid threats below the threshold of military escalation, the EU has taken steps to foster a strong basis to innovate and create value-added in critical and dual-use technological domains [9]. It comes as no surprise that the EU's Cybersecurity Strategy for the Digital Decade [10] identifies key technologies like AI, encryption, quantum computing, and future generation networks as essential to cybersecurity. It also mentions risks associated with the increased digitalisation of societies and the use of (mass) cyber-surveillance technologies, which generate new threats and the automation and militarisation of cyberspace. In this regard, the EU's Strategic Compass from March 2022 also recognises that in the 'Cyber domain, our forces need to operate in a coordinated, informed and efficient manner. We will therefore develop and make intensive use of new technologies, notably quantum computing, Artificial Intelligence and Big Data, to achieve comparative advantages, including in terms of cyber responsive operations and information superiority' [11].

(7) Cavelty, M. D., 'Cybersecurity', in Collins, A. (ed.), *Contemporary Security Studies*, Oxford University Press, Oxford, 2013, pp. 362-368, p. 363.

(8) Schwab, K., 'The Fourth Industrial Revolution: what it means, how to respond', World Economic Forum, 2016 (https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/).

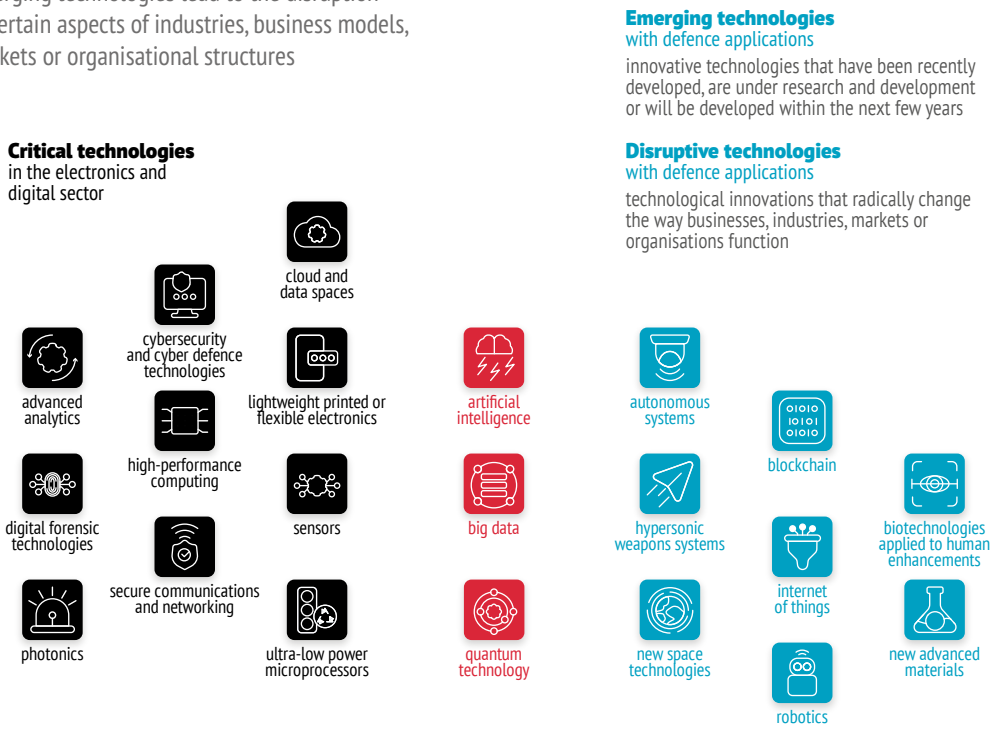
(9) European Commission, 'Action Plan on Synergies between Civil, Defence and Space Industries', COM(2021) 70 final, February 2021 (https://ec.europa.eu/info/files/action-plan-synergies-between-civil-defence-and-space-industries_en).

(10) European Commission, Joint Communication to the European Parliament and the Council, 'The EU's Cybersecurity Strategy for the Digital Decade', 2020 (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0).

(11) European External Action Service, 'A Strategic Compass for Security and Defence', 24 March 2022, p. 46 (https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en).

Technologies

Emerging technologies lead to the disruption of certain aspects of industries, business models, markets or organisational structures



This new technological wave is marked by key advances and fusions in evolving technologies that are increasingly transforming society, security, and (geo)politics. Indeed, emerging and potentially disruptive technologies such as AI, quantum computing, autonomous weapons systems, and future generations of networks are expected to fundamentally transform existing systems of global governance and trigger complex democratic and regulatory debates about their design and deployment in a data driven world. Unprecedented improvements in AI, robotics and so-called 'autonomous' technologies have ushered in an array of pressing questions about their characteristics, research and development (R&D), their legal and moral dimensions, their applications in the military realm, as well as their broader socio-economic and political impact on society, the digital world, and international relations. They are also fuelling a fierce systemic competition to innovate among great powers such as the United States and China, and across Big Tech players, such as American and Chinese tech giants like Google, Apple, Microsoft, Facebook, Baidu, Alibaba, Huawei, and Tencent.

The question remains whether the current 'winner-takes-all' rationale is compatible with the future of a global digital world, with little attention being paid to finding mutually acceptable and feasible short to long-term solutions to de-escalate the current geopolitical rhetoric. These include finding common ground in the promotion of a rules-based focused global governance of cyberspace, the protection of human rights and freedoms, and the responsible development and deployment of EDTs [12] in society more broadly, as well as in sensitive fields such as security and

[12] Ibid.

defence. The EU, as a leading normative and regulatory power, could play a significant role in shifting this increasingly securitised narrative around the technological innovation race. Yet, with its newly-found geopolitical voice in-the-making, and an increasing trend towards militarisation as shown by recent security and defence initiatives [13], the EU has been susceptible to international structural pressures and the evolving digital and tech rivalry between the United States and China.

As a consequence, and with European strategic autonomy in mind, the EU is performing a balancing act between protectionist measures in pursuit of technological sovereignty, increased efforts in defence capability build-up, with the internal and external promotion of a norms-based vision for the future of digital governance, cybersecurity, and the human-centric development of emerging disruptive technologies. There is a growing consensus at the EU-level that in order for the EU to become a credible security provider, it 'must master EDTs for defence applications' [14], in close collaboration with Member States and taking into account activities within NATO. Rapid developments in the field of AI as an all-purpose and enabling technology are already changing the (cyber) threat landscape and the strategic, tactical, and operational environments, involving multiple state and non-state actors across physical and non-physical domains.

DISRUPTIVE TECHNOLOGIES IN CONFLICT

Algorithmic-driven attacks and responses will become faster, more precise, and more disruptive. Hence, as AI and other emerging technologies are increasingly permeating different aspects of social life and cyberspace, the normative and strategic dimension of their European and international governance will equally require further scrutiny. Future and emerging digital technologies introduce formidable conceptual, policy, regulatory, and strategic challenges to expert communities of research and practice, such as policymakers, the military, and the business and tech sectors. Furthermore, as enabling technologies such as AI enter cyberspace and cyber war scenarios, they bring both good and bad news. AI and other emerging technologies are already starting to transform how conflicts are fought. The deployment of AI cybersecurity systems may also lead to new approaches and transformations in cyber system engineering and cyber defence architectures. AI-enhanced cyberattacks, communications jamming, electronic warfare, and other attacks on a system's software will become as important as those that target hardware, if not more so.

For instance, promising advancements in data analytics are likely to become significant in many fields. Certain forms of machine learning (ML) like deep learning (DL) can be used to perform predictive analysis, with AI-based solutions expected to be fielded in critical and strategic fields such as cyber defence, decision-making support, risk management, data correlations, patterns recognition, cyber situational awareness, just to name a few. AI promises to bring both enormous societal and

[13] Csernatoni, R., 'EU security and defense challenges: Toward a European defense Winter?', Carnegie Europe, 11 June 2020 (https://carnegieeurope.eu/2020/06/11/eu-security-and-defense-challenges-toward-european-defense-winter-pub-82032).

[14] European Defence Agency, 'High-level conference on the impact of emerging disruptive technologies on defence', 20 April 2021 (https://eda.europa.eu/news-and-events/news/2021/04/20/high-level-conference-discussed-impact-of-emerging-disruptive-technologies-on-defence).

economic benefits, and huge risks, especially in the case of its military uses. Right now, AI systems are powerful but unreliable, many of them being vulnerable to sophisticated attacks or failing when used outside the environments in which they are trained.

When it comes to the AI and cyber nexus [15], and regarding the AI and ML technologies' potential to bring about a disruptive change in cybersecurity practices and threat intelligence gathering, a paradigmatic shift is indeed expected. It implies an increasing reliance on algorithms, especially when dealing with Big Data, to generate significant input and expert knowledge about cybersecurity threats, by providing new ways of processing and analysing data to detect malicious or anomalous behaviours in real time, instead of testing patterns already provided to algorithms. However, most cybersecurity AI and ML systems will still require humans in the loop for setting and finetuning parameters, but most importantly, to corroborate the algorithms' findings against established social and political norms, or notions of justice or ethics. Equally, AI and ML will bring about critical problems of information, complexity, perception, escalation and ambiguity, as cyber operations will get increasingly smarter and faster all at the same time. This will clearly impact relations in high-level international, diplomatic, and political, as well as cyber strategic interactions.

AI promises to bring both enormous societal and economic benefits, and huge risks.

THE EU'S EMERGING APPROACH

Lately, the EU has been actively focusing on and prioritising the disruptive potential of emerging technologies. As a case in point, the February 2021 European Commission's Action Plan [16] on Synergies between civil, defence and space industries has highlighted the strategic importance of cross-fertilisation between civil-military-space industries in critical technology areas. It covers three priority approaches: firstly, to build new synergies among EU programmes and instruments for disruptive (digital) technologies to find concrete and dual uses across civilian, defence and space industries; secondly, to enable defence and space technologies to find concrete civil application and 'spin-offs'; and thirdly, to 'spin in' and facilitate the use of civil research and innovation into new European security and defence projects. In this respect, in February 2022 the Commission put forward a roadmap on key technologies for security and defence [17], including solutions to boost research, development, and innovation in Europe by reducing strategic dependencies in critical technologies and value chains.

Consequently, against the background of a challenging geopolitical environment, the EU's plans revolve around maintaining its technological innovation edge and supporting the competitiveness of its industrial base across civil-military domains. In this respect, the EU's Multiannual Financial Framework 2021-2027 (MFF) significantly scales up investments in technologies for defence

[15] European Parliamentary Research Service, 'The AI-cyber nexus: mending defences, recasting threats. European Science-Media Hub', 2021 (https://sciencemediahub.eu/2021/07/07/the-ai-cyber-nexus-mending-defences-recasting-threats/).

[16] 'Action Plan on Synergies between Civil, Defence and Space Industries', op.cit.

[17] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; 'Roadmap on critical technologies for security and defence', COM(2022) 61 final, 15 February 2022 (https://ec.europa.eu/info/sites/default/files/com_2022_61_1_en_act_roadmap_security_and_defence.pdf).

or related civilian uses, such as information management, cyber, and space, with relevant MFF programmes tackling research, development, demonstration, prototyping and deployment. In the context of the Commission's Action Plan, critical technological areas are defined as technologies that are relevant across the defence, space, and related civil industries, and contribute 'to Europe's technological sovereignty by reducing risks of overdependence on others.'

Cybersecurity and cyber defence technologies are listed among the key examples under the EU's digital and innovation policy. The Commission also aims to ensure cross-fertilisation across civilian and defence investments and initiatives in cyber, cloud, processors, and quantum technologies. To this end, the Commission will set up the Cybersecurity Competence Centre (CCC) [(18)] and the Network of National Coordination Centres. The CCC will contribute to protecting Europe's economy and society from cyberattacks, by endorsing research and innovation excellence and the competitiveness of EU industry in cybersecurity. The resources for the Centre will come from Digital Europe and Horizon Europe programmes, as well as from Member States. Equally, the Commission is seeking to strengthen synergies, spin-ins and spin-offs between the work of the Centre, the EDF and the EU Space programme on cybersecurity and cyber defence with a view to reducing vulnerabilities and generate efficiencies.

Worth also mentioning is the plan to establish a European-owned space-based global secure communications system, one of the EU flagship projects identified in the Commission's Action Plan aimed at developing a European sovereign infrastructure [(19)]. It will provide access to high-speed connectivity through a multi-orbit space infrastructure, including low earth orbit satellites, and by complementing Galileo/EGNOS and Copernicus as the third EU satellite system. It will leverage and strengthen the role of satellites in the 5G ecosystem, assessing interoperability while also considering the evolution towards upcoming 6G technologies. By integrating quantum encryption technologies, it will ensure highly secured connectivity and communication for governmental and commercial services. For example, it will guarantee better connectivity regarding key infrastructures, in supporting crisis management missions and operations and surveillance practices, and it will also be used for mass-market broadband applications. The end goal with this flagship project is to enable access to high-speed connectivity for everyone in Europe and provide a resilient connectivity system allowing connectivity in times of crises, including in the case of large-scale cyberattacks on the internet.

In line with the above, the 2020 Cybersecurity Strategy recognised that cybersecurity must be integrated with all other EU digital investment initiatives, and particularly in terms of key technologies like AI, encryption, and quantum computing, by using incentives, obligations, and benchmarks. The objective would be to stimulate the growth of the European cybersecurity industry and provide the certainty needed to ease the phasing out of legacy systems. In this respect, the EDF has been singled out in the 2020 Strategy to support European cyber defence solutions, as part of the European Defence Technological and Industrial Base (EDTIB). As an overarching recommendation, the Strategy urges the EU and Member States to provide further impetus for the development of state-of-the-art cyber defence capabilities through different EU policies and instruments, notably via the EU Cyber Defence Policy Framework [(20)], and also by building on

(18) European Commission, 'European Cybersecurity Competence Centre and Network', 2021 (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre).

(19) Airbus, 'European space and digital players to study build of EU's satellite-based connectivity system', 23 December 2020 (https://www.airbus.com/newsroom/press-releases/en/2020/12/european-space-and-digital-players-to-study-build-of-eus-satellitebased-connectivity-system.html).

(20) Council of the European Union, 'EU Cyber Defence Policy Framework (as updated in 2018)' 14413/18, 19 November 2018 (https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf).

the work of the EDA on research and technology road mapping.

This shows that the EU has started to give more teeth to the cyber defence capabilities dimension of its cybersecurity and defence technological and industrial strategies. This is reflected by the recent upswing of EU-led security and defence technological and industrial programmes and an increased focus given to the dual-use and disruptive potential of new and emerging technologies such as AI, including in the areas of cybersecurity and cyber defence. While EU Member States remain responsible for national security and defence, the impact, scale, and transnational nature of (cyber) threats have made a powerful case for EU-level coordinated action and EU-led research and innovation and capability development. This also comes as a consequence of multiple EU-led defence technological and industrial policy initiatives to shore up the EDTIB and in light of increasing funding and a proactive supranational institutionalisation of both security-oriented and defence R&D, as well as in the case of strategic dual-use technologies under the EU's Framework Programmes.

EMERGING DISRUPTIVE TECHNOLOGIES IN THE EU'S DEFENCE POLICY

New and emerging technologies and their impact on geopolitics have also prompted the need for a broader EU reflection on (cyber) security defence matters, more recently embedded in discussions related to European strategic autonomy, technological innovation, and digital sovereignty [(21)]. The result has been a pro-active prioritisation of dual-use research and capability development projects [(22)] under the EU's Framework Programmes, encompassing space, border security, maritime surveillance, drone technologies and cybersecurity; and more recently the launch of the EDF and an EU-led defence research and innovation programme funded for the first time under the EU budget line, and also focusing on future disruptive defence technologies. For instance, in the context of the EU's security research strand in the Horizon 2020, the framework programme has been framed as a timely and targeted financial instrument for encouraging the innovation and development of the industrial and technological resources for cybersecurity. The objective is the development of reliable ICTs solutions that promise the creation of a secure and trustworthy digital environment in the EU and the protection of fundamental rights.

The above also echoes the realisation in high-level European political and policy circles that having an advantage in cutting-edge security technologies and other (digital) technological areas is a defining metric of international influence and sovereignty [(23)]. While recognising the increasing linkages of defence and (cyber) security policies with civilian science, technology, and innovation policies in the EU, it comes as no surprise that the launch of the EDF has been framed as a technological innovation game-changer to boost the EU's excellence and efficiency in defence (digital) technologies. Up to 4 % and 8 % of the Fund's budget is devoted to the development and research of disruptive technologies, i.e. technologies that have the potential to create game-changing innovations. The Fund and its

(21) Csernatoni, R., 'The EU's rise as a defence technological power: From strategic autonomy to technological sovereignty', Carnegie Endowment, 12 August 2021 (https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134).

(22) Csernatoni, R., 'Defending Europe: Dual-use technologies and drone development in the European Union', Focus Paper, No 25, The Centre for Security and Defence Studies, Royal Higher Institute for Defence, September 2016 (https://www.defence-institute.be/wp-content/uploads/2020/04/fp-35.pdf).

(23) 'The EU's rise as a defence technological power: From strategic autonomy to technological sovereignty', op.cit.

precursor programmes, the Preparatory Action for Defence Research (PADR) and the European Defence Industrial Development Programme (EDIDP), have also been referred to as a timely catalyst for European technological innovation [24] given the complexity of emerging risks like cyber-attacks, such incidents making the lines between internal security and external defence increasingly blurred.

Under the EDF precursors programme, the PADR 2019 call selected the project PRIVILEGE [25] – Privacy and homomorphic encryption for artificial intelligence, dedicated to developing AI technologies for encryption of confidential military data. Another PADR project is QUANTAQUEST [26], Quantum Secure Communication and Navigation for European Defence, developing quantum sensing for navigation and timing without relying on Global Navigation Satellite Systems and quantum communication to secure Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). Among the EDIDP 2019 selected projects, the ECYSAP [27] European Cyber Situational Awareness Platform aims at developing and implementing innovative theoretical foundations, methods, research prototypes and their integration towards providing a European operational platform for enabling real-time Cyber Situational Awareness with rapid response defensive capabilities and decision-making support for military end-users. The EDIDP 2019 PANDORA [28] project, Cyber Defence Platform for Real-time Threat Hunting, Incident Response and Information Sharing, aspires to contribute to EU cyber defence capacity building, by designing and implementing an open technical solution for real-time threat hunting and incident response, focusing on endpoint protection, as well as information sharing.

The EU is uniquely positioned to shape the global norms regimes around emerging disruptive technologies.

Overall, the intention is to promote synergies between the EDF and other EU policy areas such as cybersecurity. Due to the widely different levels of cyber defence capabilities and capacities, and the varying speeds at which digital transformation is taking place among the armed forces and military structures of EU Member States, it would indeed make sense to increase joint technological research and innovation and cyber defence cooperation at the EU level. Nevertheless, questions arise concerning the lack of a common (cyber) strategic culture among Member States, the lag in digitalising the militaries of Member States, and how Member States can capitalise on various EU instruments and funding opportunities aimed to boost the research and innovation potential of the EDTIB. In terms of cyber defence capabilities building, there are also the options of the Member States-driven Permanent Structured Cooperation (PESCO), and the European Commission's funding instrument – the EDF with its emphasis on future and disruptive defence technologies. This would indeed require a strong emphasis on the research, development, and use of key emerging technologies such as AI, encryption, and quantum computing. In short, Member States are encouraged to make use of the full potential of PESCO and EDF for collaborative projects. Out of 47 PESCO projects, there are currently 8 cyber-related ones.

[24] Csernatoni, R. and Martins, B.O., 'The European Defence Fund: Key issues and controversies', *PRIO Policy Brief* 3, 2019 (https://www.prio.org/Publications/Publication/?x=11332).

[25] European Commission, 'PRIVILEGE Project - PRIVacy and homomorphIc encryption for artificiaL intelligence' (https://ec.europa.eu/commission/presscorner/api/files/attachment/865750/PADR%20-%20PRIVILEGE.pdf).

[26] 'QUANTAQUEST Project - Quantum Secure Communication and Navigation for European Defence' (https://ec.europa.eu/commission/presscorner/api/files/attachment/865751/PADR%20-%20QUANTAQUEST.pdf).

[27] 'ECYSAP Project - European Cyber Situational Awareness Platform' (https://ec.europa.eu/commission/presscorner/api/files/attachment/865731/EDIDP%20-%20ECYSAP.pdf).

[28] 'PANDORA project - contributing to EU cyber defence capacity building' (https://www.pandora-edidp.eu/).

TOWARDS FUTURE EU CYBER DEFENCE CAPABILITIES

The above initiatives are but a couple of examples of projects crosscutting cyber-related defence and emerging technology fields. They show that there is indeed an interest at the EU-level to lead in the development of future-oriented (cyber) defence capabilities and collaborate in joint research and innovation programmes.

But what does all this really mean for the EU's technological and innovation future and its overall cybersecurity? Are the above capacity and capability-building initiatives when it comes to technological sovereignty, emerging disruptive technologies, and cyber defence really making the EU better equipped to navigate the current geopolitical age of power politics and fierce technological competition? Indeed, technological solutionism, civil-military synergies, and a push to innovate in cutting-edge security and defence technologies seem to be the EU's response to current geopolitical, as well as cybersecurity-related, challenges. Yet, such activism and the quest for European strategic autonomy and technological sovereignty will also require the EU to deploy much greater efforts to align European strategic thinking and political commitments. Political will is also necessary for the EU to assume a leadership role when it comes to the governance of cyberspace, the regulation of emerging disruptive technologies, and to invest in binding legal norms both at home and abroad. In other words, (geo)political thinking begins at home, by bringing together all relevant initiatives and policies to form a coherent and comprehensive external action and strategic outlook. The EU can also best serve its interest by taking leadership in the global development of standards at the international level on cybersecurity, by promoting EU values and priorities when it comes to data protection and human-centric AI legislations, and by advocating for the development of technological standards and best practices in the case of tech applications across the civil-military sectors.

What is more, EU Member States still frame cyber defence via national sovereign interests and their respective strategic cultures. Cyber defence has not been a priority in the framing of the EU's cybersecurity and in the emergence of a European cybersecurity policy field. Only recently the cyber defence component in the EU's approach to cybersecurity has started to become developed, both in terms of its institutional architecture and related to the military dimensions of cyber technologies. On cyber defence-related issues, both defensive and offensive cyber operations rely on the military but mostly on the civilian private sector for the expertise needed to protect critical infrastructures and networks. On top of that, when it comes to EU cyber defence as an emerging EU policy and institutional ecosystem, and as in most high-politics issues related to national security and defence, the topic is certainly a highly sensitive matter. EU-level cooperation in cyber defence is about trust among EU Member States, other partners, and the private sector, as well as the sharing of norms, interests and priorities regarding European cyber issues.

Finally, recent EU efforts to promote innovation in emerging and disruptive technologies in the field of defence, as well as to shield Europe's society and economy from cyber or other evolving threats, are clearly intended to contribute to European digital resilience and strategic autonomy against the backdrop of the current troubled geopolitical climate. The increasing use by the EU of a new language of power, strategy, autonomy, sovereignty and geopolitics around issues related to technology and cyberspace is indicative of a paradigmatic shift in and of itself, which runs counter to long-held understandings concerning the EU's civilian power role on the global stage. This new language is already starting to shape the Union's newly found (geo)political foreign policy aspirations and interests, with the risk that less attention will be given to ethical-regulatory concerns in the global governance of emerging disruptive technologies or cyberspace. In this regard, the EU

should redouble efforts and capitalise on its first-mover advantage to push a new wave of regulations designed to bolster legal certainty and ethical protection for European citizens in a digital era, most notably by safeguarding its agenda-setting in technological standards at the global level. In this regard, the EU is uniquely positioned and has a genuine opportunity to shape the global norms regimes around emerging disruptive technologies, as well as to promote and externalise its vision of a human-centric, ethical, safe, secure and responsible way of driving forward technological innovation.

CONCLUSIONS

RELEARNING THE LANGUAGE OF POWER

by
PATRYK PAWLAK

Rules and vocabulary are elements that set languages apart. But to survive, languages need to evolve over time and adjust to the changing societal context, sometimes incorporating elements of other languages. While some languages hardly ever change and others evolve rapidly, there are also those that die out due to assimilation with more dominant languages.

As this *Chaillot Paper* demonstrates, evolution and survival are also important aspects of the EU's language of power in cyber defence. Much of this process is driven by the EU Member States whose decisions about relinquishing parts of national sovereignty for the sake of closer coordination at EU level or capacity development in defence, including in cyber defence, ultimately impact on what the EU can and cannot do. At the same time, other EU initiatives in this field – such as strengthening cyber resilience, countering cybercrime or promoting responsible state behaviour in cyberspace and safeguarding the open, free, global and secure nature of cyberspace – have advanced at a much faster pace, having no or very limited connection with the EU's cyber defence policy. As a result, the cyber defence component in the EU's cyber posture remains less developed both in terms of its institutional architecture and *vis-à-vis* the military dimensions of cyber technologies, including cyber defence policy in the framework of the CSDP.

The mission for the EU's cyber defence needs to reflect its overall security and foreign policy goals.

The new EU Cyber Defence Policy provides only partial comfort in that respect. Although the document sets out a series of ambitious goals for the EU and the Member States to achieve, it still leaves open many questions about how specifically this will be done. For instance, the planned investment in cyber defence technologies is not bolstered by the commitment of additional funding. Other proposals in the document are also clearly in need of further elaboration and refinement. With this in mind, a critical question to address is the following: how to ensure that the EU's language of power in cyber defence does not become a dying language?

The following sections propose three methods for a successful relearning of the language of power: (i) immersion; (ii) the right learning tools, motivation and will; and (iii) practice.

METHOD 1. IMMERSION IN THE EU'S STRATEGIC CULTURE

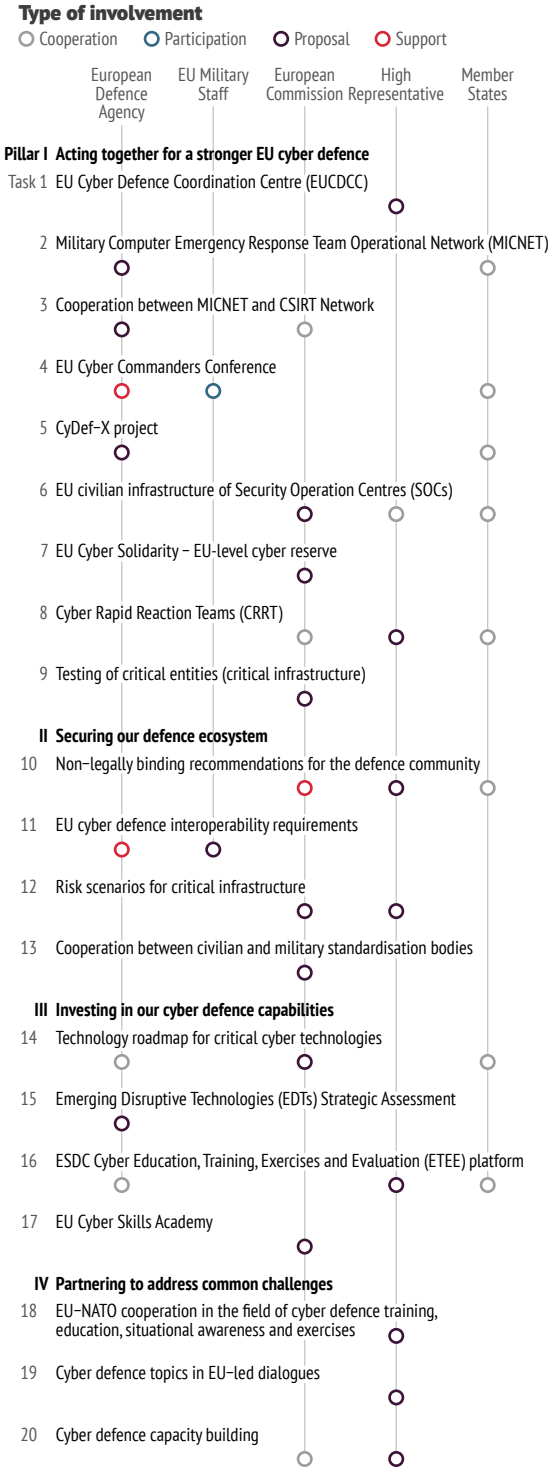
For the EU's cyber defence to be effective, it needs to **become an integral part of the EU's broader security strategy and connect to its overall strategic culture**. It is undeniable that armed forces play an important role in defending European citizens against the consequences of malicious cyber operations.

Even though closer cooperation in cyber defence is mentioned as an objective in the key policy and strategic documents adopted by the EU and the Member States, there is a clear discrepancy between the policy narrative and practice. The EU has been rather hesitant in clearly defining the role of cyber defence in protecting the Union's strategic interests and values – both at home and at the international level. The problem lies in the fact that the majority of the Member States have not elaborated doctrines and strategies for their cyber forces and those who have, have done so independently of the others. Of course, this is not different from military doctrines in general. The second challenge lies in the primarily non-military nature of the EU and its credibility as a military security provider. Despite significant progress made over the past decade regarding defence cooperation at the EU level, there has only been a very modest appreciation of the EU's role as a defence actor. Instead, the EU has been perceived as a normative and soft power that operates through economic, financial and regulatory tools more than with arms. This is also reflected in the often-criticised low levels of defence spending among the EU Member States.

The **mission for the EU's cyber defence** needs to reflect its overall security and foreign policy goals. It should be defined in clear and realistic terms that consider the needs of the EU and its Member States while clearly acknowledging the institutional, legal and political limitations

EU cyber defence policy goals

Who is responsible for the implementation of twenty key commitments?



Data: EEAS, 2022

of the EU's role in this domain. The elements constituting the EU's cyber defence mission might include:

1. **Defending and securing the EU's vital interests from disruptive and destructive attacks, including the CSDP missions and operations**. Ideally, this goal could be supported through a dedicated European Cyber Mission Force that would augment traditional defensive measures and defend priority networks. However, given political and legal questions associated with the establishment of such a Cyber Force under the EU flag, a network of Cyber Commands from the EU Member States could serve as an alternative solution. Such a structure could operate under the EU Military Committee (EUMC) which directs all military activities within the EU framework, in particular the planning and execution of military missions and operations under the CSDP and the development of military capabilities. In addition, it is important that the EU's Cyber Defence Concept duly defines procedures and processes for inclusion of cyber threats and vulnerability analysis in planning of military operations and missions as well as providing a basis for adequate cyber defence capabilities to be made available by Member States or other providers for missions and operations.

2. **Supporting development of ready forces and capabilities to conduct cyber operations.** Although the idea of an EU Cyber Force might prove contentious, in the same way that the idea of establishing a European army has invited controversy, the feasibility of such a proposal might be more realistic, despite its political sensitivity. The challenges that prevent national armies from integrating – those linked to the command structure, strategic enablers and discrepancies in equipment and capabilities that create problems of maintenance and supply – are not necessarily that pronounced in the case of cyber commands and forces. In addition, a deployment of cyber forces to the theatre of a cyber conflict or conflict with a cyber dimension does not create logistical challenges similar to those that beset operations involving boots on the ground. Paradoxically, the same internet connectivity that is a source of vulnerabilities provides benefits for the armed forces: while European armies operate 17 different kinds of tanks, all of them rely on the same internet infrastructure. Also, the legal challenges that would pose a problem for a European army (such as who bears responsibility and is accountable for actions of the troops under the EU flag) do not necessarily exist in the cyber domain since members of the EU Cyber Army would operate from the territory of a Member State and that Member State would be responsible. Another priority is for the Member States to improve the recruitment and retention of a highly skilled workforce. In addition to the existing structures such as PESCO and the EDF, this goal could be supported through the EU research and innovation programme Horizon 2020, in particular the projects focused on developing threat assessment or cyber modelling and simulation capabilities necessary to assess the effectiveness of cyber operations.

3. **Developing options for the EU to shape the conflict environment and control conflict escalation**. When preparing a cyber defence mission and shaping capabilities, it is important to understand that the use of military force should be the option of last resort should other efforts fail. This principle needs to be clearly embedded as part of a cyber defence mission to prioritise de-escalation and conflict prevention and reflect international commitments made by the EU and its Member States, including under the UN framework for responsible state behaviour in cyberspace. To support this goal, Member States could agree or at least exchange information about processes and escalation procedures which would allow the EU to better execute leadership in cyber defence, especially in the context of EU-led operations. As the war in Ukraine has demonstrated once again, this aspect will play an important role in any future conflict where the lines between kinetic and cyber operations are becoming blurred, making the assessment of the conflict environment and control of conflict escalation a

particularly complex exercise. In that sense, strengthening the EU's collective capacity to attribute cyber operations is of paramount importance. Finally, to avoid overreaching and ensure that any military action is linked to desired outcomes [1], the EU needs to clearly answer the question of what constitutes a victory in a cyber war. A victory condition may be preventing future attacks by a specific actor or partial or complete disabling of an aggressor's attack capabilities in case of large-scale conflicts. It is critical that any such decisions are taken in full respect of international humanitarian law.

4. **Forging partnerships with civilian organisations and the private sector** to strengthen resilience and reduce the attack surface across the EU. While the ultimate focus of the cyber forces is the protection of military networks, infrastructure and operations, these functions can hardly be performed without close partnership with civilian structures and the private sector (the section below on method 2 discusses this aspect in more detail). There are two main reasons for this. First, cyber forces cannot defend everyone, everywhere and all the time. Their focus needs to be on the state's most critical networks and assets, in particular those strategic enablers that may affect the capacity of a state to defend itself. Therefore, certain responsibilities for cyber defence need to be undertaken also by civilian organisations, operators of critical infrastructure, etc. In other words, the stronger and more resilient the civilian cyber defence mechanisms are, the more time cyber defence forces will be able to devote to their core mission. In that sense, strengthening cyber resilience across the EU needs to be considered as an important component of the EU's cyber defence posture. This approach is sometimes described as 'deterrence by denial'. In addition, more cyber resilient states and societies are also less likely to overreact and resort to military responses, which significantly reduces the risks of conflict escalation. Second, cyber forces rely on Commercial-off-the-Shelf (COTS) products that facilitate the military's rapid deployment but at the same time increase the risk of compromise in the defence systems. Although the recent focus on certification and accreditation can help to reduce those risks, their full elimination is hardly possible. It is therefore critical that cybersecurity becomes a 'by design' feature in any military planning and capability development rather than an afterthought.

Certain responsibilities for cyber defence need to be undertaken also by civilian organisations.

5. **Building and maintaining international alliances and partnerships to deter malicious actors**. Cyberspace is composed of core national and international infrastructures residing in multiple legal jurisdictions. Clear vision for cooperation – or at least coordination – with international partners is critical in that context for several reasons. First, an armed conflict with a cyber dimension might have regional and global consequences that impact other countries and therefore promoting transparency and sharing information about national doctrines, concepts and structures is important. Second, supporting partners and allies might also be the best method to avoid problems at home due to spill-over effects or escalation. In such cases cooperation to strengthen the cyber defence capacities of partners is one of the possible approaches. Finally, and most importantly, to effectively address threats posed by malicious actors it might be critical to engage with partners in responses across the whole spectrum of response: from law enforcement to diplomatic response and defensive (or offensive) cyber operations.

[1] Colarik, A.M. and Janczewski, L., 'Establishing cyber warfare doctrine', *Journal of Strategic Studies*, Vol. 5, No 1, 2012, pp. 31–48.

METHOD 2: ADEQUATE LEARNING RESOURCES

While a complete immersion in the language and culture is usually the most effective way of learning, it is not always sufficient or possible. This is where access to adequate learning resources and knowledge products becomes critical. In the context of cyber defence this means identifying the best ways to better understand convergence between military and civilian domains to ensure that learning the language of power becomes a whole-of-government effort.

Although the military relies predominantly on the same networks as its civilian counterparts and shares responsibility for protection of the nation's most critical resources, the relationship between civilian and military actors when it comes to cyber defence is yet to be fully understood. One of the key challenges – already identified in the EU's cybersecurity strategy – is that civilian, diplomatic, law enforcement and defence cybersecurity communities do not have a platform to engage in structured cooperation and facilitate operational and technical cooperation. This contributes to limited trust between different communities and affects their willingness to share information or engage in interagency coordination.

What further complicates this situation is the fact that it is still not entirely clear how cyber defence forces and tools fit within the whole-of-government approach at the national and EU level. A complex operational set-up at the EU level regarding who undertakes cyber defence activities [(2)] (i.e. detection, reactions, response) between the EEAS, the Council, the European Commission and other EU bodies and agencies such as ENISA and CERT-EU as well as distribution of competences between the EU and Member States, complicates the task of identifying a decisional centre of gravity when it comes to cyber defence.

There are several steps that the EU and Member States should consider when further elaborating elements of the EU's cyber defence posture:

1. **Improve interoperability between civilian and military actors and instruments**. Interoperability in the context of cyber defence poses a different challenge than traditional defence cooperation. It is primarily about clearly prescribing roles, responsibilities and cooperation mechanisms, where relevant, that enhance synergies between law enforcement, diplomacy and military toolboxes. One of the key challenges in that respect will be to identify thresholds for when civilian defence ends, and military operation begins. Some of the critical questions in that respect include decisions about who has the authority to take decisions, who the relevant stakeholders and partners are, and who takes the ultimate responsibility. Achieving better integration of civilian and military capabilities at the EU's disposal will be impossible without closer cooperation on situational awareness and threat intelligence. In concrete terms, this means improving information sharing among MilCERTs and between MilCERTs and civilian computer security incident response teams (CSIRTs).

2. **Nurture a culture of cybersecurity and ensure greater consideration of cybersecurity across the EU's security and defence policy and capability development**. National defence systems such as military mobility, space capabilities or industrial capacities are increasingly vulnerable to malicious cyber operations. If compromised due to a cyber-attack, their unavailability or destruction could significantly undermine a nation's capability to deploy and execute missions. The increase in cyber espionage operations against military institutions and contractors along the supply chain mean that we

(2) Robinson, N., Walczak, A., Brune, S-C., Esterle, A. and Rodriguez, P., *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)*, Unclassified summary, RAND Europe, 2013 (https://www.rand.org/pubs/research_reports/RR286.html).

are likely to see more activities targeting military institutions and the associated research and private sector. To counter this challenge, there is a clear need for embedding cyber resilience in all stages of military planning. Two aspects are particularly relevant in this context. First, identification and development of defence plans for networks that support key cyber defence missions across the EU and in countries where the EU CSDP missions and operations are currently deployed or planned. Such an exercise is important given that entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded from the scope of new laws such as the revised Network and Information Security Directive (NIS II). Second, strengthening procurement and acquisition standards to better reflect the needs and specificities of the defence institutions and their contractors would contribute to minimising risks across the defence ecosystem. The delivery of technologies and equipment that equip the military to effectively respond to tomorrow's challenges, including the emerging disruptive technologies, could be supported by the European Cybersecurity Research and Competence Centre.

3. **Bridge a strategic gap in the EU's toolbox to meaningfully counter below-threshold activity without escalating to activate the solidarity clause, which might allow cyber operations in foreign networks akin to the persistent engagement model**. The EU's current toolbox should be expanded with new tools. For instance, the United States started the practice of offering bounties for anyone who can provide tips about the whereabouts of foreign cyber-criminals (often aligned with

Main tasks and objectives of cyber forces in EU Member States

Cyber forces are active-duty military organisations that possess the capability and authority to direct and control cyberspace operations for strategic ends

Conduct information operations
Intelligence gathering, intelligence dissemination, and threat collection – including the impact of emerging and disruptive technologies (EDTs).

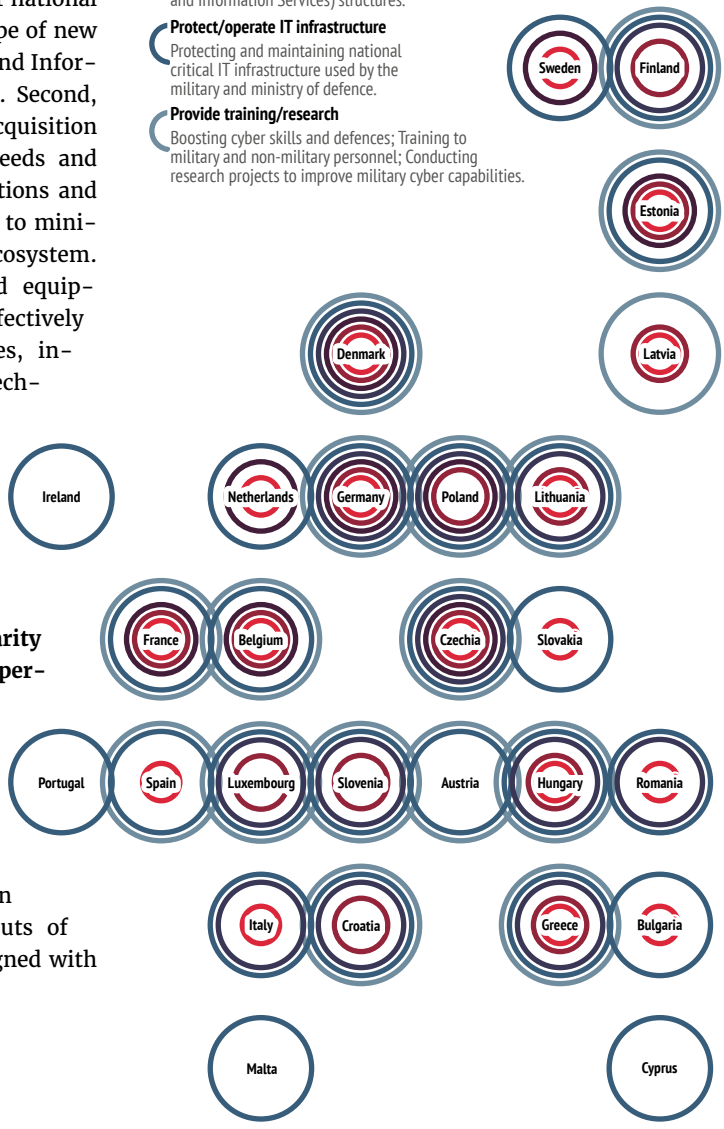
Develop situational awareness/strategy
Developing cyberspace situational awareness; Participating in crafting cyber defence strategies and cyber doctrines.

Offensive capabilities
Explicitly list 'offensive' cyber capabilities within their operational remit.

Identify future IT needs and design/develop CIS
Identifying new IT equipment to support military forces; Contributing to designing CIS (Communications and Information Services) structures.

Protect/operate IT infrastructure
Protecting and maintaining national critical IT infrastructure used by the military and ministry of defence.

Provide training/research
Boosting cyber skills and defences; Training to military and non-military personnel; Conducting research projects to improve military cyber capabilities.



Disclaimer: The information used for this diagram comes from publicly available sources. In the case of Germany, Hungary, France, Latvia, Belgium, Estonia, Slovenia, Finland, Croatia, Lithuania, Denmark, Greece and Czechia this information has been verified formally by the given country. It is possible that in some cases it may not be entirely comprehensive.

their host state).[3] The EU also needs to become more proactive. A logic of response, reacting only to a handful significant cyberattacks, is no longer sufficient. One way to become active is to use 'hunt forward' teams akin to US Cyber Command. These are (military) cyber-units that scout allied networks for signs of malicious activity and share information about adversary tools, tactics and procedures as well as indicators of compromise with cyber-defence actors. There are at least two prerequisites for that: first, EU cyber units need to have the legal rights and the consent from the target organisations to conduct such missions across borders. The EU needs a mechanism for granting this cross-border legal access. Second, information obtained via such hunt forward missions cannot be held secretly but must be shared with relevant stakeholders both nationally and internationally with the purpose of bolstering defences. US Cybercommand created an intelligence sharing hub with the private sector in order to streamline and fast-track sharing of classified indicators of compromise (IoCs). Since Russia, China and North Korea collectively employ tens of thousands of hackers engaged in malicious cyber activities, it makes sense to pool resources on the defender side. The EU should establish a consultation mechanism with US Cyber Command regarding US collective engagement in EU networks and likewise, potentially the other way around. There should be a notification mechanism if the US conducts operations in EU networks or discovers information in adversary networks about foreign actors targeting the EU.

METHOD 3: FIND PARTNERS TO PRACTISE

The final step is to put the language skills into practice. However, finding the right conversation partner is not always an easy task: differences in level, vocabulary or the speed of progress might pose a challenge for even the most devoted partners. A similar challenge is present in the field of cyber defence. Therefore, to become fluent in the language of power in cyber defence, the EU needs to build effective alliances and cooperation mechanisms with its partners globally. The EU needs to better understand how other international players – both friends and enemies – approach cyber defence, what are the possible implications of those approaches for regional and international stability, and most importantly whether those approaches are compatible with the EU's own vision.

Moving forward, the following elements will help the EU to identify suitable conversation partners and define possible strategies to enhance each other's language skills:

1. **Assess the levels of convergence and divergence between the EU's own cyber defence mission and those of its partners and strategic competitors**. Even though the EU indicates that it wants to deter cyberattacks against the targets in its territory, it has approached implementing this strategy differently from its main ally, the United States. While the latter has made it clear that it wishes to 'compete and deter' in cyberspace to advance US interests, the EU's vision is still work in progress. How the EU will progress with implementing its cyber defence mission will be important for assessing whether the vocabulary used by the EU reflects the same meaning as the

(3) US Department of State, 'Reward offers for information to bring darkside information variant co-conspirators to justice', Press Statement, 4 November 2021 (https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/).

language used by its partners or whether maybe it has evolved in a different direction. In other words, deterrence in the EU's language of power may not necessarily reflect the meaning ascribed to it by other countries. This may not be a bad thing since the EU's cyber defence mission should reflect and be immersed in its overall strategic culture and security posture (as explained earlier in the immersion section). Consequently, the EU should promote measures aimed at improving transparency and understanding of national approaches, including through regular contacts between the militaries. In the transatlantic context, such confidence-building mechanisms are part of cooperation within NATO but the EU's goal should also be to gain a better understanding of the positions adopted by other countries, notably China and Iran. Furthermore, the ongoing reflection regarding mutual assistance under Article 42(7) TEU as well as solidarity under Article 222 TFEU provides an opportunity to clarify some of the outstanding issues regarding the EU's collective defence in cyberspace.

2. **Design adequate capacity-building mechanisms for strengthening cyber resilience and cyber defence of partner countries**. To be a good conversation partner, the EU needs to give a new meaning to its capacity building discourse. The response to the war in Ukraine where the European Peace Facility (EPF) was used for the first time to provide military equipment to a partner country is a good illustration of the flexibility that is required. For decades now, the EU has been one of the main providers of cyber-related capacity building focused on countering cybercrime and strengthening cyber resilience through institutional or legislative reforms. But such initiatives have been so far detached from a broader discussion about cyber defence – primarily because such support is funded through the EU's development funding. But as argued earlier, the ambition of the whole-of-government approach cannot deny the role of military actors. As a matter of fact, in some of the countries where the EU provides cyber-assistance, ministries of defence or intelligence agencies play a critical role in securing their nations. However, the engagement on cyber capacity building with armed forces – through for instance Civilian Cyber Missions [4] – should occur while ensuring full respect for human rights and fundamental freedoms of citizens to minimise the risks that capacities provided for defensive purposes are not used in an offensive way against citizens or other countries. The defence consideration for cyber capacity building should be reflected with regard to countries where the EU has ongoing CSDP missions and operations. The reliance on civilian networks and infrastructure in countries where institutional, legal or policy capacities are insufficiently developed increases the risks and vulnerability of the EU's own missions.

3. **Use cyber defence missions to reinforce the UN framework for responsible state behaviour, in particular the application of existing international law in cyberspace**. The EU and its Member States have committed to the implementation of the voluntary norms and principles of responsible state behaviour, the application of existing law in cyberspace (including IHL), and confidence-building measures. Even though the explicit references to armed forces are limited in the text of the GGE reports and OEWG, there is a general understanding that the same rules would apply in times of peace and war. At the same time, even though parts of this framework are of a voluntary nature, states are expected to promote compliance with the agreed provisions and ensure accountability for malicious activities in cyberspace. To support this objective, the EU and its Member States should use all instruments at their disposal, in particular through the Cyber Diplomacy Toolbox.

[4] Pawlak, P., 'What if … the EU launched its first Civilian Cyber Mission?', in Gaub, F. (ed.), 'What if? 14 futures for 2024', *Chaillot Paper* no. 157, EUISS, January 2020 (https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_157.pdf).

ABBREVIATIONS

5G/6G
Fifth/Sixth generation *(of wireless mobile telecommunications technology).*

AI
Artificial Intelligence

APT
Advanced Persistent Threat

CCC
Cybersecurity Competence Centre

CDPF
Cyber Defence Policy Framework

CDRA
Cyber Defence Research Agenda

CERT-EU
Computer emergency response team for the EU institutions, bodies and agencies

CNA
Computer network attack

CND
Computer network defence

CNE
Computer network exploitation

CNO
Computer network operations

COMCYBER
Commander of cyber defence

CSDP
Common Security and Defence Policy

CSEC
Communications Security Establishment Canada

CSIRT
Computer security incident response team

CYBERCOM
Cyber Command

DCR
Declared capabilities rating

DDoS
Distributed denial of service

DoD
Department of Defense

EDA
European Defence Agency

EDF
European Defence Fund

EDIDP
European Defence Industrial Development Programme

EDTIB
European Defence Technological and Industrial Base

EDTs
Emerging and disruptive technologies

EEAS
European External Action Service

EGNOS
European Geostationary Navigation Overlay Service

ENISA
European Union Agency for Network and Information Security

EPF
European Peace Facility

ESDC
European Security and Defence College

EUMC
EU Military Committee

Europol
European Union Agency for Law Enforcement Cooperation

FSB
Federal Security Service (*Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii*)

GCHQ
Government Communications Headquarters

GGE
Group of Governmental Experts

ICRC
International Committee of the Red Cross

ICTs
Information and Communication Technologies

IHL
International Humanitarian Law

IO
Information operations

IoC
Indicator of compromise

IP
Intellectual Property

ISIS
Islamic State in Iraq and Syria

IT
Information Security

MFF
Multiannual Financial Framework

MICNET
Military computer emergency response team operational network

MilCERT
Military computer emergency readiness team

ML
Machine learning

NATO
North Atlantic Treaty Organization

NCIRC
NATO Computer Incident Response Capability

NIS
Network and Information Security Directive

NSA
National Security Agency

OEWG
Open-ended Working Group

OPCW
Organisation for the Prohibition of Chemical Weapons

OSCE
Organization for Security and Co-operation in Europe

OSINT
Open-source intelligence

PADR
Preparatory Action for Defence Research

PCR
Perceived capabilities rating

PESCO
Permanent Structured Cooperation

PLA
People's Liberation Army

R&D
Research and Development

R&T
Research and Technology

SVR
Russian Foreign Intelligence Service (*Sluzhba vneshneĭ razvedki*)

TEU
Treaty on European Union

TFEU
Treaty on the Functioning of the European Union

UN
United Nations

USSR
Union of Soviet Socialist Republics

WIPO
World Intellectual Property Organization

WTO
World Trade Organisation

NOTES ON THE CONTRIBUTORS

Hans Boddens Hosang is senior external researcher with the University of Amsterdam's Center for International Law (ACIL) in the Law of Armed Conflict and Military Operations (LACMO) research programme and external research fellow for Cyber Warfare at the Netherlands Defence Academy. He has published the book *Rules of Engagement and the International Law of Military Operations* (Oxford University Press, 2020).

Raluca Csernatoni is a research fellow on European defence and emerging technologies at Carnegie Europe. She is also a team leader on new technologies for the EU Cyber Direct project. She is currently a guest professor with the Brussels School of Governance and its Centre for Security, Diplomacy and Strategy, at Vrije Universiteit Brussels. She is also visiting faculty on high-tech warfare with the Department of International Relations of Central European University in Vienna, and an associate research expert on *PeaceTech* with the Austrian Centre for Peace.

François Delerue is an Assistant Professor of Law at IE University and a member of the Jean Monnet Centre of Excellence for Law and Automation (Lawtomation). He is also an Associate Fellow of The Hague Program on International Cyber Security (Leiden University) and the GEODE Centre (Paris 8 University). He conducts research on how new technologies challenge international law and international relations. His book *Cyber Operations and International Law* (Cambridge University Press, 2020) was awarded the 2021 Book Prize of the European Society for International Law.

Brigadier-General Paul A.L. Ducheine is the Professor for Cyber Warfare (2015) at the Netherlands Defence Academy. He started his military career in the Engineer Corps (1987). As a Legal Advisor in the Netherlands Army Legal Service, he served at Headquarters 1 (German/Netherlands) Corps, 1 (Netherlands) Division '7 December' and Multinational Division South-West SFOR in Bosnia-Herzegovia. At the University of Amsterdam, he was appointed endowed professor of |Law of Military Cyber Operations in 2014.

Aude Géry holds a doctorate in public international law and is a post-doctoral fellow at GEODE. Her research focuses on the international regulation of the digital space and more specifically on the external legal policies of states, multilateralism in the field of ICTs and the normative stakes of digital instruments. Her thesis, which was awarded the thesis prize of the French branch of the International Law Association, the third thesis prize of the Institut des hautes études de défense nationale (IHEDN) and the special mention of the Léon Bourgeois prize, focused on international law and the fight against the proliferation of digital weapons.

Laurent Gisel is head of the Arms and Conduct of Hostilities Unit at the Legal Division of the International Committee of the Red Cross (ICRC) in Geneva. After having served as Diplomatic Adviser to the ICRC Presidency from 2005 to 2008, he has worked in the ICRC Legal Division in various positions since 2008, including Legal Adviser to Operations, and Senior Legal Adviser and Cyber Team Leader. Between 2013 and 2020, he was the file holder for the rules governing the conduct of hostilities under international humanitarian law, including their application during urban warfare, cyber operations, and outer space operations.

Mika Kerttunen, D.Soc.Sc. (Pol.), LTC (ret. FIA), is Director of the Cyber Policy Institute.

He is Adjunct Professor in military strategy at the Finnish National Defence University, a member of the board of the Swedish Defence University and Visiting Researcher (cyber warfare) at the Stiftung Wissenschaft und Politik (SWP).

Kubo Mačák is a Legal Adviser in the Legal Division of the International Committee of the Red Cross (ICRC), assigned jointly to the Arms and Conduct of Hostilities Unit and the Commentaries Unit. Prior to joining the ICRC in 2019, he worked as an Associate Professor at the University of Exeter in the UK. He is the author of the book *Internationalized Armed Conflicts in International Law* (Oxford University Press, 2018) and of multiple articles in peer-reviewed journals including the *International Review of the Red Cross* and the *Cambridge International Law Journal*. He is also the General Editor of the *Cyber Law Toolkit*, an interactive online resource on the international law of cyber operations.

Antonio Missiroli served as NATO Assistant-Secretary General for Emerging Security Challenges from 2017 to 2020. Previously, he was Director of the EUISS (2012–17), worked at the Bureau of European Policy Advisers of the European Commission (2010–2012), as Director of Studies at the European Policy Centre in Brussels (2005–2010), and as a Senior Research Fellow at the W/EU ISS (1998–2005). He has taught at SAIS Europe in Bologna, the College of Europe in Bruges and Sciences Po in Paris. He holds a PhD in Contemporary History from the Scuola Nonmale Superiore (Pisa) and a Master's degree in International Public Policy from SAIS/Johns Hopkins.

Patryk Pawlak is the EUISS Brussels Executive Officer and leads the Institute's work on cyber and digital issues. He is a project director for the EU Cyber Direct - European Cyber Diplomacy Initiative, an EU-funded multimillion project that supports the EU's engagement on cyber diplomacy and digital policies worldwide. In this capacity, he is also co-editor of the *Directions* Blog on cyber, digital and tech issues. He also has extensive experience in cyber capacity building policy, including as a lead author of the *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building* and a former co-chair of the Advisory Board of the Global Forum on Cyber Expertise. He holds a PhD in political science from the European University Institute in Florence and an MA in European studies from the College of Europe.

Peter B.M.J. Pijpers is an Associate Professor of Cyber Operations at the Faculty of Military Sciences of the Netherlands Defence Academy, and PhD researcher at the University of Amsterdam. Dr Pijpers is a Colonel (GS) in the Netherlands Army and has been deployed four times including to Iraq and Afghanistan. He was seconded to the EU External Action Service from September 2015 to September 2018, and serves as a defence advisor to the EU Delegation for Libya (located in Tunisia). His PhD research was on the applicability of international law to influence operations in cyberspace.

Matthias Schulze is the deputy head at the security division of the German Institute for International and Security Affairs (SWP). His research covers numerous topics within the field of international cybersecurity. He started to focus on the dark side of digitalisation in 2010, exploring topics such as the strategic use of cyber-capabilities in international relations, cyber-conflicts, cyber-espionage, information operations, and cyber-crime.

Eneken Tikk conducts research at the Tallinn University of Technology and the Erik Castrén Institute of Helsinki University. She served as the first Senior Fellow for Cybersecurity at the International Institute for Strategic Studies (IISS) 2011–2016 and directed the ICT4Peace Institute (Switzerland) cyber policy capacity building programme (2014–2020). She has served as adviser to the Estonian Expert in the United Nations Group of Governmental Experts. Her current research focuses on the law and policy of sustainable digitalization and cybersecurity governance.

With cyberspace turning into a battlefield and an arena of strategic competition, the EU has stepped up efforts to define its cyber defence posture. This *Chaillot Paper* examines the evolution of the EU's cyber defence policy and analyses the role of cyber defence within the Union's broader security strategy. In particular, it asks: what is – or should be – the role of armed forces in the event of cyber operations that have large-scale disruptive effects on a country's economy or critical infrastructure? And what rules govern military operations involving cyberspace?

The different perspectives presented in this volume provide EU decision-makers with elements for the comprehensive design and implementation of the EU's cyber defence policy. The volume highlights the key dilemmas linked to when and how defence forces may resort to cyber operations in a time of conflict, regardless of whether deployed for military operations or to protect civilian infrastructure.

European Union Institute for Security Studies

Publications Office of the European Union

ISBN 978-92-9462-143-6
CATALOGUE NUMBER QN-AA-22-004-EN-C