Ádám Farkas* – László Vikman**

# Information Operations as a Question of Law and Cyber Sovereignty

## Abstract

The transmission of information content in the digital space, or its restriction, obstruction or distortion, is an extraordinary tool in the information age. States can be targets of information operations, regardless of their political system. For this reason, the ability and capacity to counter operations in the information space are fundamental issues for any state with a modern defence system. Information operations are, therefore, a necessary tool for the self-defence of sovereign states in the 21st century. However, the question arises as to what legal and institutional framework can provide an appropriate basis for information operations in such a way that the framework does not react to *ad hoc* events but ensures a systemic response in the long term while upholding the fundamental values of the state. The paper aims to contribute to understanding this problem by reviewing different nation-state solutions and providing a conceptual framework that synthesises legal, political, military and intelligence aspects.

**Keywords:** information operations, influence, cyber sovereignty, resilience, cognitive warfare

## I Introduction

Technological developments in recent decades, such as the virtually limitless possibilities for communication, the continuity and speed of information flows and globalisation, have changed how individuals and society live their daily lives. Adapting to this has also been a major challenge for states in terms of interpersonal, economic and administrative relations. The security challenge is even greater. Both the legislature and the executive have a major

* Dr Ádám Farkas PhD, Senior Research Fellow, Széchenyi István University – Ludovika University of Public Service. ORCID iD: 0000-0003-2918-5267.

** Dr László Vikman, Assistant Researcher, Ludovika University of Public Service. ORCID iD: 0009-0002-1202-5769.

role to play in establishing and operating the appropriate regulatory framework. The fourth generation of warfare[1] is intrinsically linked to this accelerated and globalised system, as already evidenced by several international and non-international armed conflicts in the 21st century, as well as local conflicts, especially the Russo-Ukrainian war. However, beyond the dimension of statehood, the defence and security institutions of states must also reckon with the rise of non-state actors. One of the most striking novelties of hybrid scenarios is precisely the info-communication environment and its social, economic, political – and therefore security – embeddedness. However, this extends beyond the scope of warfare according to a much broader understanding of complex security and involves sub-threshold military operations and non-military operations.

Effective responses to contemporary defence and security challenges – mostly national security, military and law enforcement, but also affecting all segments of public administration – require an operational framework that is both adaptable to the specificities of the hybrid environment and provides the necessary guarantees. This is not a regulatory and operational challenge that can be solved by a targeted amendment to the law or by regulating specific issues that have been identified as priorities and otherwise maintaining the old ways of doing things. A change of mindset is needed. Another important specificity is that, given the nature of the challenges and threats, NATO allies, the EU and national regulation can only work effectively together. The concept of information operations (info ops) is, of course, not new in this context. However, its content and correlations, not least its scope, seem to be entering an era of deepening. It could be said that an 'information operations explosion' is taking place,[2] which is increasing the importance of the information space both for warfare and for influence and intervention outside it.

A legal-regulatory approach to this issue is of paramount importance for the rule of law, maintaining the values of the international community and operating within the rules and concerning the need for effective, systematic and consistent protection and action in the information space.[3] It is important, however, to put the issue under the spotlight of legal analysis in its own right, separately from fourth-generation warfare and hybrid threats,

---

1 For more details, see William S. Lind, Gregory A. Thiele, *4th Generation Warfare Handbook* (Castalia House 2015); William S. Lind, 'Understanding Fourth Generation War' (2004) (September-October) Military Review 12–16.

2 Mike Chapple, David Seidl, Cyberwarfare: *Information Operations in a Connected World.* (Jones & Bartlett Learning 2023, Burlington); Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Praeger 2017, Santa Barbara), DOI: https://doi.org/10.5040/9798400636431; Katharina Ludwig and others, 'Divided by the Algorithm? The (Limited) Effects of Content- and Sentiment-Based News Recommendation on Affective, Ideological, and Perceived Polarization' (2023) 41 (6) Social Science Computer Review 2188–2210, DOI: https://doi.org/10.1177/08944393221149290

3 Talita Dias, 'Limits on Information Operations Under International Law' in T. Jancárková and others (eds), *15th International Conference on Cyber Conflict: Meeting Reality* (CCDCOE 2023, Tallin) 345–363; Tsvetelina van Benthem, Talita Dias, Duncan B. Hollis, 'Information Operations under International Law' (2023) 55 Vanderbilt Law Review.

and to make it the subject of more intensive investigation beyond pre-existing studies.[4] It should be seen that this phenomenon of change also has implications for state and legal theory, whether in relation to the idea of cyber sovereignty[5] or the cyberfare state. The validation of the latter phenomena could significantly impact the design of more concrete state responses and the developments needed to shape them, as could the new meaning of information superiority.[6]

These kinds of theoretical questions significantly broaden the horizon of response. Without a broader spectrum of interpretation and, with it, planning, organisation and action, not only may the effectiveness of active operations be called into question, but the lack of adequate situational awareness and the reduced effectiveness of defence mechanisms may result in a serious disadvantage in terms of responding to counter-actions. A purely technical approach and the adaptation of old cognitive schemas and various rules to a new technical environment may easily lead to maladaptive solutions. In view of this, it is necessary to consider the possible legal responses to information operations within a complex framework. This framework must take into account sovereignty issues, defence-security specificities, the functioning of information operations and the structure of law as a system. All of this must be integrated into the very complex matrix of resilience in the context of social justice since the main impact of information operations is on society, whether the operation is military, intelligence or other.

Our main hypothesis is that legal responses to information operations should be adapted to complex security environment and that the different solutions should be linked to each other and then to the issue of resilience. To support this, we draw on literature, policy, strategic and regulatory sources, with the aim of identifying general lines of action for adequate protection against information operations. This may form the basis for further research on the topic.

Our analysis proceeds using three main sections. First, we review some of the main contexts of information operations. We use three subsections to increase understanding of the military-security perspective, and we outline the definitions of NATO on the matter and the always-evolving conceptualisation of these activities, the most state-of-the-art

---

4 See, for example: Oxford Institute ELAC, 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' <https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities> accessed 15 October 2024; Eian Katz, 'Information Operations in International Humanitarian and Criminal Law: Reflections on the Oxford Statement' <http://opiniojuris.org/2021/07/22/information-operations-in-international-humanitarian-and-criminal-law-reflections-on-the-oxford-statement/> accessed 15 October 2024; Waseem Ahmad Qureshi, 'Information Warfare, International Law, and the Changing Battlefield' (2020) 43 (4) Fordham International Law Journal 901–937.

5 Sean S. Costigan, 'Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty' (2021) 20 (2) Connections QJ 9–13, DOI: https://doi.org/10.11610/Connections.20.2.01

6 Ádám Farkas, 'The Status and Role of Law and Regulation in the 21st-Century Hybrid Security Environment' (2022) 11 (2) Acta Universitatis Sapientiae, Legal Studies 113–124.

of which is cognitive warfare. In the following subsection, we briefly review the elusive approach to sovereignty in cyberspace, which will be difficult to capture (with significant consequences) due to the current rather diverse state practices and which, precisely because of these diverging interests, is not expected in the near future. We conclude the first chapter by presenting a proposal for a specific set of criteria to be followed in the context of the state regulation of information operations. In the second main section, we argue that, in addition to legislative and administrative instruments and hard state responses, individual and group-level resilience, which is increasingly important in security matters, must also play a role in countering the activities of counter-acting actors in the cognitive space. In the concluding reflections in the summarising third main section, we argue first and foremost that, in addition to identifying possible regulatory directions and pursuing a comprehensive analysis, efforts are needed to embed this in a comprehensive view of resilience.

With our article, we aim to stimulate professional dialogue and debate that, through a multidisciplinary approach but grounded on the basis of positive law, can develop definitions, frameworks, control and governance mechanisms that will allow states to guarantee a high level of national security proportionate to the threat while respecting fundamental human rights.

## II Contexts for Information Operations

The importance of the information operations environment is due to the prominent role that info-communication has attained among the civilian population. Thus, the importance of cooperation with civilians regarding military and non-military threats has been enhanced. This, in turn, has increased the weight of the cognitive orientation on the military side concerning the technological approach to information operations. The phenomenon of 'sub-threshold' crises resulting from hybrid threats (in which, in addition to the military element's embeddedness in the population, cooperation with administrative, law enforcement and national security actors and the strengthening of state and civilian resilience play a prominent role), also has a bearing in this direction. In this context, it is also worth taking into account that the legal aspects of active and passive (operational) activities in the information space, including counter-actions, share the fate of other legal issues related to hybrid threats and new forms of warfare.[7] The character of 'sub-threshold' and non-purely military response phenomena clearly implies the application of a different

[7] See for more details: Aurel Sari, *Blurred Lines: Hybrid Threats and the Politics of International Law* (European Centre of Excellence for Countering Hybrid Threats 2018, Helsinki); Aurel Sari, 'Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats' 1/2019 Exeter Centre for International Law Working Paper, DOI: https://doi.org/10.2139/ssrn.3315682; Aurel Sari, 'Hybrid Warfare, Law and the Fulda Gap' in Christopher Ford, Winston Williams (eds), *Complex Battle Spaces* (Oxford University Press 2019, Oxford) 161–190, DOI: https://doi.org/10.1093/oso/9780190915360.003.0006

legal regime, both in the nation-state and international context, which, if left unimproved, may even impact the legitimacy of action.[8]

In the matter of war, combatants themselves have not only sought a fire-and-brimstone approach since the beginning of history, but in order to conserve physical resources, conserve reserves and maintain high levels of capabilities before (or instead of) actual kinetic confrontations, the winning by decisive superiority without battle through deception, deterrence, the winning of hearts and minds, or the breaking of will with dominant manoeuvring has always been of great value, as Sun-tzu points out in his work The Art of War: 'supreme excellence consists in breaking the enemy's resistance without fighting'.

It took quite a long time to proceed from the less formalised use of scaremongering, propaganda, censorship and then the gradually more sophisticated and targeted use of psychology in pre-20th century conflicts to the total state control of the media in the Second World War, especially associated with the Third Reich and under Goebbels. In terms of media, the era of radio and TV, which revolutionised mass communication, was overtaken first by the explosive parallel development of telecommunications and mobile communications and then by the Internet, which by the 21st century had made entirely new forms of communication and platforms available in real-time, providing a space and a forum for communicators with a wide variety of goals, motivations and skills.

The definition and precise content of information operations are also changing and constantly evolving, and therefore, sometimes as vague or blurred as the activity itself. It follows that their classification, regulation and general analysis are also not simple and straightforward. However, in order to define the theoretical framework for this article, it is necessary to provide some relatively widely accepted starting points so that the details and specifications can be presented from common ground.

As a starting point, an accepted but somewhat understandably military-oriented definition of information operations according to NATO Policy is 'a staff function to analyze, plan, assess and integrate Information Activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives'.[9]

Cyberspace is perhaps the most dominant medium for information operations because of the extent of its use and its role in everyday life in entertainment, information, work and

---

[8] This is perfectly reflected in the issue of 'lawfare' and legal vulnerability, which makes the inadequacies and shortcomings of state regulation and competing instruments of international law an effective tool for both state and non-state actors. On the subject: Charles J. Dunlap Jr. 'Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts' <https://people.duke.edu/~pfeaver/dunlap.pdf> accessed 15 October 2024; Rode F. Kittrie *Lawfare. Law as a Weapon of War* (Oxford University Press 2016, Oxford), DOI: https://doi.org/10.1093/acprof:oso/9780190263577.001.0001; Sascha Dov Bachmann, Andres B. Munoz Mosquerra 'Lawfare and hybrid warfare – how Russia is using the law as a weapon' (2015) (102) Journal of the Society for Advanced Legal Studies 25–28, DOI: https://doi.org/10.14296/ac.v2015i102.2433

[9] NATO MC 0422 – NATO Military Policy for Information Operations, 2012. 2, <https://shorturl.at/6LTOw> accessed 15 October 2024.

access to government and commercial services. Accordingly, the academic approach has developed the concept of cyber-enabled infoops as a subcategory. According to Herbert Lin and Jackie Kerr,[10] 'information/influence warfare and manipulation (IIWAM) is the deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes'.

Cognitive warfare as a new approach can be deemed a 'unification theory' concerning the matter because, as Cornelis van der Klaauw writes, 'Cognitive warfare is a structured and well[-]considered approach to target[ing] the human cognition of individuals, groups and societies in a way that affects their decision-making processes and ultimately their behaviour'.[11] This involves all means and methods, psychological or technological, that are suitable for changing the behaviour, emotion and thought processes of the targeted individual, group or population by affecting the subconscious mind. A more concentrated approach comes from Francois du Cluzel: 'the art of using technologies to alter the cognition of human targets, most often without their knowledge and consent'.[12] This definition, being narrower, clearly focuses on the technical means and the human brain as a target. To present a broader overview, we try to outline the main elements of these concepts and focus on some of the most important stages of development of the last decade.

## 1 NATO and Info Ops

Countering adversarial information operations, disinformation campaigns and malicious propaganda connected to diverse hybrid threats is a core allied task.[13] Article 3 of the Washington Treaty is the 'highest' point of reference and the foundation of the resilience principle, which has been of rising importance, especially since the Crimean aggression, the meddling with democratic processes and the disinformation campaigns related to the global COVID pandemic. Article 3 states: 'In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.' The Strengthened Resilience Commitment[14] in 2021 and the Strategic

[10] Herbert Lin, Jackie Kerr, 'On Cyber-Enabled Information/Influence Warfare and Manipulation' in Paul Cornish (ed), *The Oxford Handbook of Cyber Security* (Oxford University Press 2021, Oxford) 251–272, DOI: https://doi.org/10.1093/oxfordhb/9780198800682.013.15

[11] Cornelis van der Klaauw, 'Cognitive Warfare, The 21st Century Game-Changer' (2023) (39) The Three Swords 97–101.

[12] Francois du Cluzel, 'Cognitive Warfare, a Battle for the Brain' (2022) NATO ACT, STO Meeting Proceedings Paper <https://www.sto.nato.int/publications/STO%2520Meeting%2520Proceedings/STO-MP-HFM-334/%24MP-HFM-334-KN3.pdf> accessed 15 October 2024.

[13] Suzanne Waldman, Sean Havel, 'Launching Narrative into the Information Battlefield' (2022) 2 (21) Connections QJ 111–122, DOI: https://doi.org/10.11610/Connections.21.2.08

[14] NATO, Strengthened Resilience Commitment <https://www.nato.int/cps/en/natohq/official_texts_185340.htm?selectedLocale=en> accessed 15 October 2024.

Concept of 2022[15] both include marked disinformation campaigns and the coercive use of information tactics as hybrid threats, which are to be dealt with on a national and alliance level as well. Member states and the Alliance must be able to prepare for, detect, assess these and deter or defend against their use. For guidance on information operations activity areas, see paragraph 13 of MC 0422.[16]

Building upon the strategic-level alliance documents, the practical guidance on how to achieve the strategic goals is regulated on the doctrinal level. The Allied Joint Doctrine for Information Operations AJP-10.1[17] is fairly new; it was published in January 2023. The doctrine states the following ground principles for executing info ops: Comprehensive understanding, Narrative-led, Effects-focused, Integrated, Agility, Centralized planning and decentralized execution and Assessment. Information Operations staff work directly together with Strategic Communications[18] and NATO Communication Capabilities groups, namely Psychological Operations[19] and Military Public Affairs. Additional capabilities that can contribute to an info ops campaign are cyberspace operations, electromagnetic warfare, civil-military cooperation, physical destruction (kinetic force), operations security and deception, information assurance and emerging and disruptive technologies.

An overview of the above elements is necessary for assessing the principles, approaches and tools that may emerge in the context of info ops, whether defensive or active. It is also important to assess our own theoretical frameworks, thus creating a basis for comparison with the ideas of our counterparts and for outside-the-box innovations that may emerge.

## 2 Information/Influence Warfare and Manipulation

Herbert Lin's term was developed to describe the rising importance of information warfare as a form of confrontation to which liberal democracies are particularly vulnerable and are not particularly potent compared to usually authoritarian adversaries who specialise in this form of conflict and use free speech and freedom of ideas as a weakness. Lin also pointed out

15 NATO, NATO 2022 Strategic Concept <https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf> accessed 15 October 2024.

16 NATO MC 0422 2012.

17 AJP-10.1, 26.

18 Military Committee (MC) 0628, NATO Military Policy on Strategic Communications: 'in the NATO military context, the integration of communication capabilities and the information staff function with other military activities, in order to understand and shape the information environment, in support of NATO strategic aims and objectives'.

19 Allied Joint Publication (AJP)-3.10.1, Allied Joint Doctrine for Psychological 2 AJP-10.1 31 Edition A Version 1 + UK national elements Operations and MC 0402, NATO Military Policy on Psychological Operations: 'planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives'.

the doctrinal confusion in an article[20] in 2020. Reference to 'Information Warfare' appeared first in 1992 in a US Department of Defense (DOD) directive and later in 1996 in a doctrine. This changed to 'Information Operations' in 1998. Influence Operations was not a DOD term; it appeared in a study by the RAND Corporation in 2009. Psychological operations are a key component of information operations, but this has a deeper history. Last, the concept of 'Cyberspace Operations' was introduced in 2013. All these involve very similar key components and important overlaps, not just from the public viewpoint but in terms of political leadership and other military and defence functions. As Lin states,[21] 'Using these same terms differently in different contexts is likely to create conceptual confusion that in turn can also result in [the] misallocation and misalignment of resources and capabilities.'

## 3 Cognitive Warfare

As a next evolutionary step, NATO is developing the idea of Cognitive Warfare. Leading researchers Bernard Claverie and Francois du Cluzel have published many papers[22] on this new concept, going as far as to claim that human cognition is the sixth domain of warfare (after land, sea, air, space and cyber). With rapid advances in the fields of nanotechnology, biotechnology, information technology and cognitive sciences, the misuse of knowledge about the functions of the human brain is a rapidly growing risk. It brings with it a new (third) dimension of warfare, the cognitive space, in addition to the physical and informational.

The development of the new concept is such a major objective that the First NATO scientific meeting on Cognitive Warfare was held in France in June 2021.

## 4 Some Thoughts About Cyber Sovereignty

The legal assessment of sovereignty is not only closely linked to cyberspace operations in the narrow sense but also to information and cognitive warfare; since the primary tool and theatre of these operations in the 21st century is cyberspace, it is clear that the issue of sovereignty is also of vital importance for states in their own national information spaces.

Sovereignty is an ancient legal principle aligned with territoriality that guarantees peaceful coexistence through mutual recognition between states.[23] In modern international

---

[20] Herbert Lin, 'Doctrinal Confusion and Cultural Dysfunction in DoD Regarding Information Operations, Cyber Operations, and Related Concepts' (2020) 5 (2) The Cyber Defense Review 89–108.

[21] Lin (n 20) 100.

[22] Bernard Claverie, Francois du Cluzel, 'The Cognitive Warfare Concept' (2023) NATO ACT <https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf> accessed 15 October 2024.

[23] Dieter Grimm, *Sovereignty – The Origin and Future of a Political and Legal Concept* (Columbia University Press 2015); Lucie Kadlecová, *Cyber Sovereignty – The Future of Governance in Cyberspace* (Stanford University Press 2024).

law, the definition set out in the *Las Palmas Case* of 1928[24] is taken as the authoritative one: '[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.' The state has the capacity to exercise power independently inside its borders; in relations extending outside the state, nations have the right to self-determination and to act without external coercion and international law respects this.

Over the past millennia, this approach has helped establish the jurisdiction of states involved in a given matter in a significant number of cases and determine the legal status of parties in a given situation. However, in cyberspace, the cross-border services and the technical solutions that allow anonymity make it far from easy to apply this principle and, in some cases, to enforce and recognise it,[25] even though sovereignty as a core principle has been considered valid in relation to cyberspace by several international organisations and national declarations on the legal regime applicable to cyberspace.

Although Hungary has not yet issued a comprehensive national position[26] on the legal framework for cyberspace, the concept is reflected in several strategies and laws. The legal definition of cyberspace in Hungary is currently: 'the part of the electronic information systems of the global cyberspace that are located in Hungary and the social and economic processes that take place in Hungary or are directed to Hungary or involve Hungary, which are represented by data and information through the electronic systems of the global cyberspace'.[27] Obviously, at least four or five elements of this sentence may overlap with other states' similar national definitions of cyberspace, especially since there are several competing approaches to the interpretation of the violation of sovereignty in cyberspace.

The more defensive view is that its violation is a breach of a substantive primary rule of international law and constitutes an internationally wrongful act. Regarding the more permissive approach, sovereignty is merely a principle of international law; cyber operations cannot violate sovereignty as a rule of international law, although they may constitute prohibited interventions, use of force or other internationally wrongful acts.

According to the assessment prevailing in NATO member- and friendly states, the principles of international conventions, customary law and customary international law remain valid and applicable in cyberspace. The Tallinn Manual,[28] which contains five main rules for the interpretation of sovereignty in cyberspace, is the practical embodiment and

---

[24] *Island of Palmas Case* (United States v The Netherlands), Permanent Court of Arbitration, 2 U.N. Reports of International Arbitral Awards 829 (1928).

[25] Gergely Gosztonyi, *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices* (Springer 2023, Cham) 157–165, DOI: https://doi.org/10.1007/978-3-031-46529-1_11

[26] For national positions, see <https://cyberlaw.ccdcoe.org/wiki/Sovereignty#cite_note-1> accessed 15 October 2024.

[27] Act 50 of 2013 on electronic information security in public and local government bodies, § 1(1)35.

[28] Michael N. Schmitt (ed), *Tallinn Manual 2.0,* (Cambridge University Press 2017, Cambridge) DOI: https://doi.org/10.1017/9781316822524

professional guide to this. Using another approach, a new set of international conventions based on international consensus that respects existing international legal rules and goes beyond multiple interpretations based on analogies could indeed be a forward-looking and useful solution to the legal problems of cyberspace. Preparatory work on this has been ongoing for some time in the framework of the UN Open-Ended Working Group on Information and Communication Technologies (OEWG), which currently has a mandate until 2025. However, increasing multipolar competition is also present in the OEWG, and national positions are far from converging.[29]

According to Aleksi Kajander,[30] the principle of sovereignty and its implications for cyberspace remained a contested issue in the sessions in 2023, and the publishing of detailed national positions on international law and cyberspace, which was encouraged by numerous states at the OEWG, is a crucial step towards creating a common understanding of how pre-existing international law applies in cyberspace and what gaps exist because recognition of the existence of state positions reduces the possibility of unfounded claims based on 'majority positions'.

The growing threats in cyberspace, which are in no small part directly or indirectly attributable to state actors, also have negative effects on global production and trade. It is not surprising that economic operators and the key companies in the tech sector that are primarily affected are also calling for a more secure environment. A good example is Microsoft's Digital Geneva Convention initiative, which encourages states' efforts to strengthen international cybersecurity standards, create new binding rules and protect civilians, similar to the Geneva Conventions.[31]

The tech sector's perspective is relevant because their influence, operation and impact in cyberspace are at least on a level with, and sometimes even above, that of the nation-states that legislate. The phenomenon of techno-polarity[32] describes this opposition, where the arena of competition is cyberspace, data traffic, algorithms and cloud and server environments, not physical space and territory. With the decentralised operations in the cloud, blockchain technology and the possibility of anonymisation, the abuse of AI

[29] Sean S. Costigan, 'Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty' (2021) 20 (2) Connections QJ 9–13, DOI: https://doi.org/10.11610/Connections.20.2.01; Creemers R.J.E.H., 'China's conception of cyber sovereignty: rhetoric and realization' in Dennis Broeders, Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics* (Rowman & Littlefield, 2020) 107–142, DOI: https://doi.org/10.2139/ssrn.3532421

[30] Aleksi Kajander, *A Tale of Two Draft Resolutions: A Report on the Polarising International Law Discussions at the 2023 OEWG Substantive Sessions* (NATO CCDCOE 2023, Tallinn).

[31] Brad Smith, 'The need for a Digital Geneva Convention' (14 February 2017) Microsoft Blog <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention> accessed 15 October 2024.

[32] N/A, 'Cyber Sovereignty' Synergia Foundation, 27 April 2024, <https://www.synergiafoundation.org/insights/analyses-assessments/cyber-sovereignty>

developments may further reduce trust between parties, which may lead to strategies for sourcing from trusted sources that limit free market operations.[33]

Another important issue related to cyber sovereignty in the context of information operations is net neutrality, which directly affects freedom of expression and freedom of information, with proponents arguing for the non-discrimination of network traffic and opponents arguing for security interests from a public perspective and commercial interests from an economic one.[34] The US approach, with its dominant influence over the operation of the Internet, is clearly dominant globally, and it is important to be alert to the decisions taken by the Federal Communications Commission (FCC), the courts and the legislature in favour of net neutrality, which is more likely to be supported under Democratic leadership.[35]

## 5 A Proposal for Regulating Info Ops

The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities[36] can be identified as an international legal professional initiative comparable to the Tallinn Manual. This initiative by the Oxford Institute for Ethics, Law and Armed Conflict aims to establish a 'no-go' list for information operations in the context of human rights protection. The main guidelines set out in the ten rules are that States must refrain from violating the principles of sovereignty and non-intervention and from any propaganda that promotes war, national, racial or religious hatred and discrimination. They must enforce these in their jurisdictions and also refrain from activities that violate the fundamental human rights of individuals within their jurisdiction (including the freedom to seek, receive and impart information).

States must take measures to protect the human rights of individuals within their jurisdiction from violation by information operations. Protective measures should have a legitimate purpose, legality, necessity, and proportionality and not involve discrimination. The regulation of info ops must not unduly restrict human rights, and states must ensure that information and technology companies are able to operate their services consistently in accordance with the human rights of their individual users.

---

33 N/A, 'Cybersecurity in the EU – Member State Implementation of the NIS2 Directive: The Example of the Czech Republic' (July 2023) Morgan Lewis Report 10.

34 Christian Hildebrandt, Lukas Wiewiorra, 'The past, present, and future of (net) neutrality: A state of knowledge review and research agenda' (2024) 39 (1) Journal of Information Technology 167–193, DOI: https://doi.org/10.1177/02683962231170891

35 Tom Wheeler, 'Don't be fooled: Net neutrality is about more than just blocking and throttling' (30 October 2023) Brookings, <https://www.brookings.edu/articles/dont-be-fooled-net-neutrality-is-about-more-than-just-blocking-and-throttling> accessed 15 October 2024.

36 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' <https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities> accessed 15 October 2024.

The conduct of information operations or activities during armed conflict is subject to the applicable rules of international humanitarian law; it prohibits engaging in information operations or activities that amount to international crimes, such as genocide, including direct and public incitement thereto, war crimes and crimes against humanity.

## III Links between Legal Response Options and Resilience

Given the highly complex social, psychological, technological, political, economic and, through them, security implications of the development of info-communications, it is not historically surprising that state and non-state actors alike are seeking to use the achievements associated with this development to advance their own interests *vis-à-vis* others. This leads to a number of novel phenomena ranging from the rivalries of global capitalism to great power competition and crime.[37]

In a changing environment, states, as the organisational system that ensures the orderly coexistence of individuals and their societies, must adapt to change. This implies the development of rules concerning both passive (defensive) and active (advocacy/preventive) state capacities, structures and, in the case of states obeying the rule of law, legal systems. Moreover, this environmental change also sheds new light on the state's self-understanding and the question of sovereignty. Indeed, security awareness, security self-consciousness and consent to state action on the part of individuals and society are essential for effective defence and advocacy in large-scale, networked systems with a high degree of freedom. This can only be guaranteed if resilience is strengthened by treating the state-society system as a whole and by promoting and supporting the security-enhancing potential and awareness of individuals.[38] It is important to stress, however, that without predictable security, individual, social, political and economic confidence is undermined; creative, innovative and productive capacity is reduced, and, ultimately, the degree of freedom is also reduced, which is a clear loss for society as a whole.

It is no coincidence that in many successful model states (such as Switzerland or even Singapore), social and economic productivity is clearly linked to an effective defence-security system and the strengthening of security awareness is based on state and social cooperation. The Nordic and Baltic states' efforts to strengthen security through social cooperation are a similar example.[39] The developmental orientation of NATO and the EU

[37] Benoît Dupont, Thomas Holt, 'The Human Factor of Cybercrime' (2022) 40 (4) Social Science Computer Review 860–864, DOI: https://doi.org/10.1177/08944393211011584

[38] See, for more details: Inez Miyamoto, 'Disinformation: Policy Responses to Building Citizen Resiliency' (2021) 20 (2) Connections QJ 47–55, DOI: https://doi.org/10.11610/Connections.20.2.05; Jim Townsend, Anca Agachi, 'Build Resilience for an Era of Schocks' in Christopher Skabula (ed), *NATO 20/2020. Twenty Bold Ideas to Reimagine the Alliance after the 2020 US Election* (The Atlantic Council 2020, Washington DC).

[39] See, for example: Ieva Bérzina, 'Total defence as a comprehensive approach to national security' in Nora Vanaga, Toms Rostoks (eds), *Deterring Russia in Europe. Defence Strategies for Neighbouring States* (Routledge

(such as the recent legislative results, NIS2 and CER Directives, and the DORA Regulation) in recent years also reflects this trend.

The overall development of information technology, but also of the public services – critical infrastructure – based on the former that underpin the development of a welfare/consumer society, and their becoming a basic necessity has clearly created an extensive, complex, networked and thus multipolar and multi-exposed system in which security cannot be guaranteed by the state alone, at least not without adequate social support, attitudes and security awareness. To think that security can be maintained in this environment by purely state means, by acting 'above' society, is an illusion. However, the idea of self-organisation and self-education at the individual and societal levels that would trigger state action on the grounds that the digital space available to all is also an unrivalled knowledge and organisational base seems equally utopian.

In light of this, we believe that the solution to the challenge lies between the two extremes, where we accept and acknowledge that self-education, self-organisation and security awareness at individual and societal levels have become key but accept and support the modernisation of state capabilities and socio-state cooperation to increase their effectiveness. This could be the real basis for resilience, where – from education and training to the functioning of public administration and defence and security activities – efforts are made to go beyond rigid state-society demarcation in the field of resilience through cooperation.

Resilience has great potential, as it is not only a means of defending oneself but also of defending oneself as an individual, a society and a state. Effectively building resilience also means developing the necessary user, productive, innovative, theoretical-scientific and practical capacities that can boost social and public productivity and security.

However, this requires accepting that the idea, areas and strengthening of resilience must be gradually built into the public and regulatory space and enhanced in the social dimension through the resources and support potential that this offers. This requires:

1. Credible analyses and assessments of related environmental changes and challenges.
2. The credible, well-founded and effective modernisation of public institutions and regulations.
3. Authentic information and communication about security[40] to be separated and compartmentalised as much as possible from domestic and international political competition.
4. Supporting, without controlling, self-organising efforts to promote self-education and security awareness at individual and societal levels.

---

2019, Abingdon) 71–89, DOI: https://doi.org/10.4324/9781351250641-5; James Kennet Wither, 'Back to the future? Nordic total defence concepts' (2020) 20 (1) Defence Studies 61–81, DOI: https://doi.org/10.1080/14702436.2020.1718498

40 Cullen G. Nutt, Reid B.C. Pauly, 'Caught Red-Handed: How States Wield Proof to Coerce Wrongdoers' (2021) 46 (2) International Security 7–50, DOI: https://doi.org/10.1162/isec_a_00421

5. Increased support for innovations that strengthen resilience.
6. Stepping up education and training programmes, supervised and organised by the state, but with ongoing social consultation.

Such an approach clearly shows that resilience-building can be approached from at least two angles. The first is associated with NATO's now traditional territorial division.[41] The second is the division into the relevant disciplinary/action dimensions. However, the second approach is also crucial for the effective development, operation and maintenance of the areas of action defined by NATO since it can overcome the *prima facie* obvious but erroneous view that all this can be guaranteed by the state's capabilities, primarily in the areas of defence and related state administration.

The areas of resilience are all those in which social actors are present as both professionals and users/actors. The former's effective provision cannot, therefore, be limited 'only' to the staff (and their awareness) in the public service or the sectors that provide the services in question. In one way or another, society as a whole is directly and indirectly involved through supply chains, public services and the daily activities necessary for a well-ordered life.

Therefore, a key issue for effective development in these areas of resilience is the strengthening of a supportive social environment, which involves education and training, professional cultures/chambers of commerce/training centres, research and development and the sphere of civil society organisations as intermediary environments. In addition, providing and updating the professional and public-regulatory framework within which these areas operate is a perspective that extends beyond the state, as is promoting a social understanding of the anomalies that exist in certain areas based on abuses for the purpose of promoting order and efficiency in society as a whole. In this context, enhancing resilience is therefore not only a task and challenge for the whole of government – ie one that should take effect across the professional-sectoral divide within government – but also for society as a whole, for which the state can provide a framework, targeted support and credible basic information that is acceptable to society at certain points, while only at other points can it be the sole or primary custodian of active action through its defence and security agencies.

## IV Closing Thoughts

Our review of the interpretation, doctrinal background and regulatory issues related to information operations, as well as our focus on cyber sovereignty, has, we believe, established our hypothesis that information operations pose significant regulatory challenges and require systemic renewal in response.

[41] NATO, Resilience, civil preparedness and Article 3 <https://www.nato.int/cps/en/natohq/topics_132722.htm> accessed 15 October 2024.

International attempts to develop positive legal definitions with a view to unifying and defining them are not capable of producing results at the global level in the medium term, given the geostrategic shift towards multipolarity, but this does not mean that efforts at the alliance, EU and national levels to do so are negligible. Moreover, without a clear national position, the national interest cannot be consistently and clearly represented at the international level, and the loss of alliance confidence and credibility in the balance of national security interests must be assessed against sometimes useful ambiguity at the strategic level.

It is self-evident that with such a broad impact mechanism or, rather, matrix, security factors and, to a considerable extent, military aspects will also be present. Clearly, the information space has led to revolutionary developments in non-kinetic modes of warfare, the full horizon of which is perhaps not yet fully appreciated, especially if we look beyond the concept of warfare, which in many respects is considered restrictive, to the whole concept of complex security.[42]

However, it must also be recognised that the information space, and with it, information society, is so multifaceted and complex that its study can only be properly grasped as an intersection of many disciplines and scientific fields. Accordingly, we perceived it as important to take a similar approach in this paper to the interconnections of the information age, particularly concerning the defence and security aspects of the state, paying attention to constitutional, sociological and, to some extent, governance aspects, in addition to the perhaps traditional military/war science approaches.[43]

Perhaps the most striking novelty of the information age is the unprecedented importance of the social milieu in guaranteeing security while the traditional functions of the state are maintained. It should be stressed that the social environment has always been important in warfare and the broader guarantee of order and security, but the technological changes of our time and their natural infiltration into the fabric of society make it difficult or impossible to imagine a security system with a 'state only' or 'social only' emphasis. From this perspective, the information age and information society should, therefore, entail not only the modernisation, networking and complexification of the defence and security structures, instruments and rules of the state but also a significant strengthening of national resilience.

In the context of a mostly legal but multi-disciplinary analysis of information operations, our main proposal is, therefore, to identify possible regulatory directions and to pursue a comprehensive approach while embedding this issue within the framework of resilience. Indeed, the states and societies of the information age interact so closely in the cognitive dimension that it is only in this complex space that the development of appropriate new frameworks and solutions can be properly understood.

---

[42] Risa Brooks, 'Paradoxes of Professionalism: Rethinking Civil-Military Relations in the United States' (2020) 44 (4) International Security 7–44, DOI: https://doi.org/10.1162/ISEC_a_00374

[43] Rachel Tecott Metz, Andrew Halterman, 'The Case for Campaign Analysis: A Method for Studying Military Operations' (2021) 45 (4) International Security 44–83, DOI: https://doi.org/10.1162/isec_a_00408