Politeja
Nr 5(92), 2024, s. 281-309
https://doi.org/10.12797/Politeja.21.2024.92.13

Dominika DZIWISZ
Jagiellonian University in Kraków
dominika.dziwisz@uj.edu.pl

RETHINKING FUTURE CONFLICTS

THE CYBER GREY ZONE FROM THE RUSSIAN PERSPECTIVE[1]

ABSTRACT: This article examines the concept of the 'grey zone' in international conflict, with a particular focus on its application in cyberspace. The grey zone refers to non-conventional strategies employed by states to achieve strategic objectives without escalating to overt warfare. The study highlights the evolving nature of grey-zone activities, driven by technological advancements and increasing reliance on cyberspace, which has introduced novel vulnerabilities and opportunities for state actors.

Adopting a neoclassical realist framework, the article argues that the unique characteristics of cyberspace – its borderless nature, lack of territorial constraints, and difficulties in attribution – render it an attractive domain for conducting grey-zone operations. By minimizing the risk of escalation while maximizing strategic impact, state actors can pursue their objectives with relative impunity.

Through a critical analysis of scholarly literature, public reports, and governmental sources, this study identifies the strategic assumptions underpinning Russia's cyber operations and assesses their effectiveness in achieving specific policy goals. The findings suggest that while Russia's cyber activities reflect a sophisticated understanding of the grey zone, the escalation to conventional warfare in 2022 indicates a failure to meet objectives solely through ambiguous actions.

Keywords: cyberwar, Russia-Ukraine war, information warfare, grey zone

[1] The publication has been supported by a grant from the Faculty of International and Political Studies under the Strategic Programme Excellence Initiative at Jagiellonian University.

INTRODUCTION

In 1948, the American diplomat George Kennan cautioned against the rise of 'political warfare', which he characterised as *the utilisation of every available method by a nation, excluding war, to accomplish its national goals*.[2] Subsequent scholars coined various terms for this concept – e.g., 'unpeace',[3] 'grey zone' between war and peace (the most popular one),[4] 'non-war military activities',[5] 'warfare during peacetime',[6] 'subliminal aggression', 'persistent (cyberspace) confrontation', 'indirect war'[7] or 'non-war', yet they all essentially encompass a range of diplomatic, informational, economic and military non-conventional strategies employed by states to attain their aims without reaching the point of outright warfare.[8] Professor of International Law, Rosa Brooks, wrote that in the grey zone, *we do not know what counts as 'armed conflict' or 'the use of force'... we're no longer even sure what counts as a weapon*.[9] Additionally, over the past few decades, technological advancements have progressively shifted grey-zone challenges from being uncommon to becoming the standard. The growing interconnectivity worldwide has introduced fresh vulnerabilities for both states and non-state actors, amplified by our increasing reliance on cyberspace. Thus, gaining the ability to conduct offensive cyber operations below the threshold of aggression may bring exceptional benefits from cyberspace as an operational domain. At the same time, cyber operations in the grey zone – where the principles and rules of international law are difficult to enforce – are

2 S. Lucas, K. Mistry, "Illusions of Coherence: George F. Kennan, U.S. Strategy and Political Warfare in the Early Cold War, 1946-1950," *Diplomatic History*, vol. 33, no. 1 (2009), pp. 39-66.

3 S. Zilincik, I. Duyvesteyn, "Strategic Studies and Cyber Warfare," *Journal of Strategic Studies*, vol. 46, no. 4 (2023), pp. 836-857.

4 L.J. Morris et al., "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War", *RAND Corporation*, 27 June 2019, at https://www.rand.org/pubs/research_reports/RR2942.html, 19 XI 2023; G. Popp, S. Canna, "The Characterization and Conditions of the Gray Zone: A Virtual Think Tank Analysis (ViTTa)," *NSI*, January 2017, at https://nsiteam.com/social/the-characterization-and-conditions-of-the-gray-zone-a-virtual-think-tank-analysis-vitta/, 19 XI 2023.

5 Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 2020, at https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF, 20 XI 2023.

6 S. Takashi, *Increasingly Complex and Sophisticated 'Hybrid Warfare' during Peacetime: Japan's Comprehensive Response and the Japan-US Response*, Nakasone Peace Institute 2020, at https://www.npi.or.jp/en/research/NPI_Research_Note_20201005.pdf, 22 XI 2023; J.R. Van de Velde, "Make Cyberspace Great Again Too!," *RealClearDefense*, 23 July 2018, at https://www.realcleardefense.com/articles/2018/07/23/make_cyberspace_great_again_too_113634.html, 20 XI 2023.

7 M. Galeotti, "The 'Gerasimov-Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, 6 July 2014, at https://inmoscowsshadows.wordpress.com/2014/07/06/ the-gerasimov-doctrine-and-russian-nonlinear-war/, 22 XI 2023.

8 Ibid.

9 R. Brooks, "Rule of Law in the Gray Zone," *Modern War Institute at West Point*, 7 February 2018, at https://mwi.usma.edu/rule-law-gray-zone/, 15 XII 2023.

subject to competing interpretations.[10] For this reason, numerous countries have centred their national security and defence strategies on positioning campaigns within the ambiguous territory between peace and war.[11]

The starting point of this article are the findings published on the first day [sic] of the Russian kinetic aggression in Ukraine by the International Institute for Strategic Studies (IISS).[12] The report constitutes a comparative analysis of offensive cyber operations by the United States, Russia and China. According to the United States' assessment, it affirms that the country is effectively structured for exerting power within cyberspace. Moreover, it is well-equipped organisationally to carry out operations in the cyber domain. In contrast, China has shown an interest in projecting power through cyberspace for social and political purposes – especially concerning Taiwan – but so far these operations appear to have been mainly for nuisance effect. In terms of their offensive cyber capabilities, China's armed forces are at a far earlier stage of maturity compared with those of Russia and the U.S. By contrast, Russia has a solid knowledge foundation for both cyber-sabotage and cyber-influence operations but has been constrained by resource availability and relatively narrow transformations within the relevant agencies. There is one common point for Russia, the USA and China: low confidence (at the political level) that cyber campaigns could achieve a strategic effect. However, after over two years since the war began and observing Ukraine's utilisation of cyberspace, one might question whether Russia is an exception and possesses a strong comprehension of leveraging cyberspace for strategic goals, albeit with a different approach than that of Western countries.

International conflicts arise from contradictory interests that accumulate over time, and a well-managed conflict in a grey zone should be able to produce strategic outcomes. However, in the case of the Russia-Ukraine conflict, it has gone well beyond the grey zone. The fact that Russia felt the need to use overt, large-scale conventional force in Ukraine since 24 February 2022 – despite years of operating there in the grey zone – may demonstrate that this ambiguous use of force in Ukraine failed to achieve its intended objectives.[13] Similarly, it prompts consideration of whether Russia diverges

[10] M.N. Schmitt, "Gray Zones in the International Law of Cyberspace," *The Yale Journal of International Law Online*, vol. 42, no.2 (2017), pp. 1-21, at https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf, 22 XI 2023; J. Matisek, "From Little Green Men to Little Blue Helmets: Imagining the Future of Russian Aggression – And what to Do about it," *Modern War Institute at West Point*, 11 February 2021, at https://mwi.westpoint.edu/from-little-green-men-to-little-blue-helmets-imagining-the-future-of-russian-aggression-and-what-to-do-about-it/, 22 XI 2023.

[11] L.J. Morris et al., "Gaining Competitive Advantage in the Gray Zone..."; L.R. Sheppard et al., "By Other Means Part I: Campaigning in the Gray Zone," *CSIS*, 8 July 2019, at https://www.csis.org/analysis/othermeans-part-i-campaigning-gray-zone, 22 XI 2023.

[12] G. Austin, K. Lin Ten, M. Sharma, "Great-Power Offensive Cyber Campaigns: Experiments in Strategy," *IISS*, 24 February 2022, at https://www.iiss.org/en/research-paper/2022/02/great-power-offensive-cyber-campaigns/, 22 XI 2023.

[13] R.S. Cohen, "Has the War in Ukraine Damaged Russia's Gray Zone Capabilities?," *RAND Corporation*, 22 June 2022, at https://www.rand.org/pubs/commentary/2022/06/has-the-war-in-ukraine-

from the norm within the IISS research findings, indicating a competent mastery of utilising cyberspace for strategic aims but potentially employing a divergent approach in contrast to Western nations' interpretations.

Subsequently, the main goal of the article is to answer three fundamental questions. Firstly, what were the objectives behind Russia's utilisation of the (cyber) grey zone? Secondly, to what extent do Western experts possess a holistic comprehension of Russia's utilisation of cyberspace? Thirdly, could Russian activities in the cyber grey zone between 2014 and 2020 be considered as crossing the line of aggression under international law? To answer the above questions, a detailed analysis of assumptions and predictions regarding the significance of utilising the cyber grey zone for strategic objectives was conducted. For the study, a registry and database were established, encompassing scholarly articles, public literature and reports from official think tanks and governmental sources, focusing on the strategic utilisation of cyberspace by the Russian Federation. The paper adopts an essay format, employing a comprehensive analysis of these sources conducted through critical analysis methodology.

The foundational premise of this article posits that the ever-increasing significance of state competition stems from the distinct characteristics of cyberspace, such as its borderless nature, lack of territorial constraints and challenges in attributing attacks. Therefore, the article advocates for the application of neoclassical realism theory, which represents the latest iteration within the realism framework. Neoclassical realists acknowledge that states shape their foreign security strategies by weighing the challenges and advantages stemming from the global system. Given a state's fundamental aim of ensuring its survival, minimising risks to its existence is paramount.[14] Therefore, any chance to mitigate threats to state survival amid unforeseen circumstances is appealing. This underscores the attractiveness of grey-zone activities, as they facilitate the pursuit of state objectives without overtly aggressive actions or clear attribution of attacks, thereby reducing security risks for states.

There is considerable controversy and debate regarding the comprehension of the grey zone today, specifically concerning the definition of its boundaries, its association with related concepts commonly used interchangeably and its diverse historical practices in recent decades, as well as the ongoing evolution of its application. Therefore, the first section defines the term 'grey zone' with a special focus on grey-zone activities in cyberspace to provide the theoretical framework for the analysed case studies. Consequently, the second section juxtaposes the concept of 'cyber grey zone' with the 'use of force' in cyberspace. An attempt is made to describe specific and universally applicable criteria for evaluating the level of aggression in cyberspace. The third part presents an overall picture of the Russian assumptions regarding the use of cyberspace in Ukraine. The question is posed as to whether Russian actions in the grey zone could be classified as aggression under international law. Therefore, specific operations in the cyber grey

damaged-russias-gray-zone-capabilities.html, 22 XI 2023.

14 N.M. Ripsman, J.W. Taliaferro, S.E. Lobell, *Neoclassical Realist Theory of International Politics*, Oxford 2016.

zone are discussed, categorised into cyber technical operations and cyber psychological operations.

DEFINING THE (CYBER) GREY ZONE

The inception of the term 'grey zone' can be traced back to the 2010 *Quadrennial Defense Review* (QDR).[15] However, the concept of engaging below the threshold of aggression is not a recent development. Throughout history, both states and non-state entities have utilised grey-zone tactics – notably during the Cold War – ranging from influencing elections to supporting insurgencies by state-sponsored rebels. Nonetheless, the analysis of Russian actions in Ukraine since at least 2014 suggests that the conflict in the grey zone represents a recognisable and intentional strategy of actions, indicating a growing and noteworthy occurrence.

Despite some critics asserting that grey-zone activities are merely a repetition of terms like hybrid warfare, fifth-generation warfare, proxy warfare, unconventional warfare and irregular warfare,[16] the core argument in the article stands on the premise that 'grey zone' is not merely a trendy term, but constitutes a unique sphere. While it is true that much of what is now termed the grey zone is not entirely novel,[17] the broader range of tools available today – such as sophisticated and aggressive informational campaigns or cyber-attacks – enables more effective outcomes in the non-war domain. Additionally, economic interdependence fosters an aversion to war and a preference for actions below the threshold of aggression.

The grey zone represents the sphere where the distinction between war and peace becomes indiscernible due to the ambiguity surrounding the employed tactics. The term 'grey zone' is primarily used within the realm of politics, lacking universally binding definitions grounded in international practice and law. Hence, it necessitates referencing and aligning with the concepts of 'use of force' and 'aggression', which hold clear definitions under international law, signifying *the use of armed force by a state or a group of states against the territorial sovereignty or political independence of another*

[15] F. G. Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," *The Heritage Foundation*, 5 October 2015, at https://www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protracted-gray, 22 X 2023.

[16] T.M. Azad, M.W. Haider, M. Sadiq, "Understanding Gray Zone Warfare from Multiple Perspectives," *World Affairs*, vol. 186, no. 1 (2023), p. 85.

[17] A. Elkus, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," *War on the Rocks*, 15 December 2015, at https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/, 22 XI 2023.

state.[18] Essentially, the grey zone constitutes a phenomenon defined by the absence of war, yet it does not meet the criteria for either 'war' or 'peace'.[19]

It is not surprising that there is no agreement on 'grey zone' terminology. John Arquilla even highlights that *the aggressors see no grey zone 'between war and peace'. They see all as war; so must we*.[20] However, the fact is that despite sidestepping traditional military conflicts, the aggressor actively participates in a grey-zone conflict. Each opponent approaches this conflict uniquely, yet collectively they contribute to an ongoing grey--zone war that continuously challenges the attacked country. The strategies and actions used in the realm between peace and war are deliberately unclear, designed to avoid easy classification, which – in turn – hinders effective responses.

Irrespective of the terminology used, an increasing volume of research delineates a comparable range of occurrences, encompassing the following:

a) Strategical gradualism

Hostile actions within the grey zone increasingly resemble a form of low-level conflict between entities, where the conventional understanding of what constitutes unacceptable aggressive behaviour becomes considerably murkier. These actions can range from non-intrusive activities like information gathering or propaganda, to more invasive acts such as cyber-attacks on critical infrastructure facilities. Without proper management, there is potential for these activities to escalate into traditional interstate conflicts. Conversely, well-handled situations might confine these activities to subtle manoeuvres, strategically kept by the aggressor below the distinct threshold marking open warfare. Moreover, it is essential to recognise that the connections between perceived effects and threats vary and are not universally applicable across countries. In alignment with the fundamental principles of realism, it is anticipated that there is a discernible rationale in the conduct of states.

Although it is challenging to establish exact and universally applicable criteria, grey--zone tactics mainly aim to evade situations that could lead to escalation.[21] Therefore, grey-zone activities *unfold gradually over time rather than involving bold, all-encompassing actions to achieve objectives in one step. By stretching aggressive moves over years or even decades, such 'salami tactics' provide less basis for decisive responses – and, thus, less ability to make unambiguous deterrent threats in advance*.[22] As indicated in the RAND

[18] UN General Assembly, "Definition of Aggression," *Refworld*, 14 December 1974, at https://www.refworld.org/docid/3b00f1c57c.html, 22 XI 2023.

[19] D. Dziwisz, "Non-War Activities in Cyberspace as a Factor Driving the Process of De-Bordering," *Politics and Governance*, vol. 10. no. 2 (2022), pp. 293-302.

[20] J. Arquilla, "Perils of the Gray Zone: Paradigms Lost, Paradoxes Regained," *National Defense University Press*, 9 May 2018, at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983610/perils-of-the-gray-zone-paradigms-lost-paradoxes-regained/, 24 XI 2023.

[21] L.R. Sheppard et al., "By Other Means Part I...".

[22] L.J. Morris et al., "Gaining Competitive...".

report: *Russian actions in Ukraine have stretched this definitional aspect to its breaking point, essentially crossing the threshold into conventional war*.[23] Consequently, as Michael J. Mazarr emphasises in his monograph, patience serves as a vital element in remaining beneath the threshold of aggression: *Patience is more important than rushing, if the risk is triggering a massively disproportionate reaction. As Russia discovered when moving on from Crimea to Ukraine proper, the cardinal sin in gray zone campaigns is becoming too ambitious. Once a campaign has triggered a disproportionate response, the advantage of the gray zone realm has been lost, and the risks of escalation grow*.[24] This, in fact, resulted in an escalation in Ukraine on 24 February 2022, potentially indicating that Russia had run out of patience in pursuing its strategic goals within the grey zone.

Not many researchers, among them J. Andres Gannon, Erik Gartzke, Jon Lindsay and Peter Schram, accurately diagnosed Russia's plans in their article from January 2022, recognising that the conflict in the grey zone was not the panacea for Russia's aspirations as most experts had envisioned.[25] Moreover, Russian efforts in the grey zone yielded an effect contrary to their intentions. Since 2014, Ukrainian military capabilities have significantly improved due to better equipment, training and substantial experience. Additionally, Russian cyber-attacks had little impact on events on the battlefield. Furthermore, NATO has been invigorated with a sense of purpose not seen since the Cold War. Therefore, Russia was left with either accepting the loss of influence in Ukraine, maintaining its subversive activities to save face temporarily or initiating a military intervention.

In the new era of strategic rivalry, conventional ideas about escalation (e.g., the 44-rung 'escalation ladder' by Herman Kahn) which imply straightforward and somewhat foreseeable progressions from minor crises to complete nuclear conflict will be less certain. Rebecca Hersmann rightly observes that: *The blurring of conflict across sub--conventional, conventional, and strategic levels as well as the proliferation of actors across that landscape challenge this conceptualisation of escalation and call into question its utility. Rather than progressing (more or less) stepwise, with clear thresholds between behavior that would elicit a conventional or nuclear response, crisis or conflict between nuclear-armed adversaries in this new environment is far more complex and unpredictable*.[26] The concepts of conflict escalation that worked during the Cold War, in a less predictable security environment where escalation paths are less foreseeable, Hersmann suggests replacing with the concept of a 'wormhole' dynamic. *Holes may suddenly open in the fabric of deterrence through which competing states could inadvertently enter and suddenly traverse between sub-conventional and strategic levels of conflict in accelerated and decidedly*

[23] Ibid.

[24] M.J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Carlisle 2015.

[25] J.A. Gannon et al., "Why Did Russia Escalate Its Gray Zone Conflict in Ukraine?," *Lawfare*, 16 January 2022, at https://www.lawfaremedia.org/article/why-did-russia-escalate-its-gray-zone-conflict-ukraine, 22 XI 2023.

[26] R. Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review*, vol. 3, no. 3 (2020), pp. 90-109.

non-linear ways.[27] The concept of escalation wormholes aids in comprehending and delineating numerous escalation patterns observed within the grey zone. Particularly, in the era of technological innovations, disinformation and weaponised social media, traditional linear concepts of conflict escalation diminish in significance when analysing contemporary international conflicts.

b) Revisionist powers as the main grey-zone actors

As Michael J. Mazarr writes, *If world politics were composed solely of status-quo powers, there would be little engine of gray zone conflict*.[28] Hence, discussions about grey-zone conflicts should centre on revisionist powers such as Russia, Iran or China, which possess the capacity to challenge the global order.[29] Their motivations of the revisionist powers are the same as in the physical world: *Russia acts because it lost, China because it is behind, Iran because it is revolutionary, North Korea because it is starving [...]*.[30] States striving to revise the existing order are usually those that have augmented their power, perceiving the current global order as inherently unjust. Revisionists seek to change the distribution of goods (for example, territory) among the great powers in international relations, whereas status-quo states prefer maintaining the existing state of affairs, which sparks balancing behaviour that mitigates their threat.[31] For revisionist states, *staying in place is not the primary goal [...]. They want to increase, not just preserve, their core values and to improve their position in the system*.[32] Furthermore, revisionist powers seek to alter the international system to elevate their own position rather than dismantle the existing global order. Consequently, their interests and objectives within these revisionist endeavours are limited.[33] In the case of China, it possesses both the motivation and the capability to modify the established order; Russia, as a dissatisfied power, boasts more limited capabilities yet remains steadfast in its pursuit to recalibrate the existing framework, while Iran seeks to boost its influence in the Middle East and beyond and reject

27 Ibid.

28 M.J. Mazarr, *Mastering the Gray Zone...*, p. 10.

29 J.E. Hayes, "Beyond the Gray Zone: Special Operations in Multidomain Battle," *National Defense University Press*, 5 November 2018, at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1681855/beyond-the-gray-zone-special-operations-in-multidomain-battle/, 25 XI 2023; J.J. Wirtz, "Life in the 'Gray Zone': Observations for Contemporary Strategists," *Defense & Security Analysis*, vol. 33, no. 2 (2017), pp. 106-114.

30 J. Healey, *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities*, United States House of Representatives, 1 March 2017, at https://nsarchive.gwu.edu/sites/default/files/documents/3515025/Document-11-Jason-Healey-Columbia-University.pdf, 19 XI 2023.

31 J.W. Davidson, "The Roots of Revisionism: Fascist Italy, 1922-39," *Security Studies*, vol. 11, no. 4 (2002), pp. 125-126.

32 R. Schweller, "Bandwagoning for Profit: Bringing the Revisionist State back in," *International Security*, vol. 19, no. 1 (1994), p. 87.

33 M.J. Mazarr, *Mastering the Gray Zone...*, p. 21.

the U.S.-led world. In the realm of territory, China has erected new land formations in the South China Sea, whereas Russia has intervened in Ukraine. Simultaneously, leaders from China, Russia and Iran have voiced grievances about what they perceive as an unfair set of norms favouring the United States and its allies and partners.[34] Therefore, grey-zone tactics aim to secure these advantages without escalating into open warfare, without crossing established boundaries and thereby without subjecting the practitioner to the consequences and risks that such escalation could entail.[35]

c) Unconventional (cyber) tools

Grey-zone strategies encompass the utilisation of unconventional methods and tactics, such as propaganda, economic coercion, cyber-attacks and leveraging non-state actors (e.g., technology enterprises, private military companies, groups of activists, hacking groups), as well as supporting proxy fighters and gradual military expansion. These approaches steer clear of overt state-level aggression while pursuing strategic objectives. Moreover, a crucial aspect is that an effective grey zone strategy hinges on amalgamating these methods and tactics within a unified campaign to yield a cumulative strategic impact. Failing this integration, these measures are unlikely to achieve anything beyond mere tactical objectives.[36]

Cyberspace is a critical enabler of grey-zone activities that aim to intensify the fog and uncertainty by inducing confusion and interrupting essential services. Characteristic features of cyberspace, such as the attribution problem, a-territoriality, uncertainty and the failure of a given part of the system caused by an attack not leading to damage to other parts of the system (cascading failure), or the difficulty in predicting the actions of the other side and third parties, may be perceived by states more as an opportunity than a risk. This perception can lead to efforts to coerce, acquire influence, shape the perceptions and political decisions of large numbers of individuals or destabilise key countries and regions. Numerous statements from state officials, such as U.S. defence representatives, make it clear that competition is expected to play out primarily below the threshold of major war.[37]

It is worth noting that the indisputable benefits of cyber operations in a conflict that remains below the threshold of aggression lose their significance once the conflict becomes 'hot'. Most of the aforementioned advantages of utilising cyberspace diminish

[34] M. Green et al., *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Center for Strategic and International Studies 2017, at https://www.jstor.org/stable/pdf/resrep23165.6.pdf?refreqid=fastly-default%3A50890b0403d6b04aa66c62c040096d4a&ab_segments=&origin=&initiator=&acceptTC=1, 12 XII 2023.

[35] H. Brands, "Paradoxes of the Gray Zone," *Foreign Policy Research Institute*, 5 February 2016, at https://www.fpri.org/article/2016/02/paradoxes-gray-zone/, 12 XII 2023.

[36] R. Lazović, "Ambiguous Approach – All Shades of Gray," *Cyber, Intelligence, and Security*, vol. 4, no. 1 (2020), pp. 41-57.

[37] L. Morris et al.,"Gaining Competitive...".

when both sides are engaged in physical confrontation. Primarily, in an open conflict situation, attributing an attack becomes obvious because the attacker's intentions are clear. Additionally, disrupting the enemy's information exchange becomes more effectively achievable, for instance, through missile attacks on elements of information infrastructure. Furthermore, the advantage of a-territoriality in the grey zone loses its significance when it is possible to target kinetic objectives across the enemy's entire territory (as the Russians do by attacking targets in Ukraine).[38]

d) Ambiguity

General Valery Gerasimov, Russian Chief of the General Staff, is credited with formulating the 'Gerasimov Doctrine', a comprehensive governmental strategy that integrates both hard and soft power across diverse domains. The utilisation of a broad spectrum of tools aims to cripple a society within a short span of days or weeks. In the opening paragraph, he observes, *In the twenty-first century, we have observed a tendency towards the blurring of lines between states of war and peace. Wars are no longer declared and, once begun, follow an unfamiliar pattern*.[39] The essence of modern warfare lies in blurring boundaries and embracing ambiguity. By creating the desired level of uncertainty and engaging in minor hostilities, foreign observers remain unsure about what future developments might hold. While inherent uncertainty characterises all conflicts and ambiguity is not a novel notion, grey-zone campaigns intentionally embrace ambiguity to disrupt an opponent's strategic assessments and render their decision-making process paralysed. Ambiguity can arise concerning four fundamental aspects of conflict interaction: the parties engaged in the conflict, their activities, potential results and the information accessible to those involved.[40] As a consequence of a skilfully orchestrated grey-zone campaign, an actor deliberately remains ambiguous regarding a policy, aiming to maintain a balance of interests and preserve flexibility in available options. The objective is to compel the opponent to factor in uncertainty about the actor's intentions, capabilities and potential actions within their strategic considerations.

[38] D. Dziwisz, B. Sajduk, "Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę «specjalnej operacji wojskowej»," in A. Gruszczak (ed.), *The War Must Go On: Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski*, Kraków 2023.

[39] V. Gerasimov, "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review*, January-February 2016, at https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf, 10 VII 2023.

[40] R. Lazović, "Ambiguous Approach...," p. 53.

CROSSING THE RED LINE – THE USE OF FORCE IN CYBERSPACE

As previously discussed, establishing precise and universally applicable criteria for assessing the threshold of aggression is challenging. Hostile activities in cyberspace increasingly resemble a type of low-level interstate conflict, where the normative boundaries defining unacceptable aggressive behaviour become less evident. They range from non-invasive actions like information gathering or propagandising to invasive ones like disrupting government websites or disabling civilian data systems. This progression has the potential to elevate cyber-attacks into conventional interstate conflicts if not appropriately handled. Conversely, with proper management, these activities might remain below the relatively clear threshold of traditional open warfare, existing as subtler engagements orchestrated by the attacking party.[41]

Nevertheless, while *war* exists within a legally, morally and strategically unique realm, most cyber-attacks represent non-military actions falling under the broader umbrella of *grand strategy*.[42] Consequently, the term *cyberwar* does not align with the conventional and legally defined concept of *war* (or the commonly employed term *armed conflict*), which typically denotes scenarios involving *the use of armed forces or sustained armed violence between states and organised armed groups or among such groups within a single nation's territory*.[43] Due to the inherent ambiguities within cyber warfare, as previously mentioned, there remains uncertainty regarding the classification of cyber-attacks as acts of force. Hence, there is a need to juxtapose the concept of 'cyber grey zone' with the 'use of force in cyberspace'.

The term 'use of force', as defined by the UN Charter, goes beyond 'war' and 'armed conflict'. In Article 2, Point 4, the Charter prohibits the use of force against the territorial integrity or political independence of any state or in any other manner inconsistent with the principles of the United Nations.[44] However, the subject of the applicability of this provision in cyberspace raises a lot of controversy. The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) experts in Tallinn argued that: *The mere fact that a computer [...] is used during an operation has no bearing on whether that operation amounts to a 'using force'. Similarly, it has no bearing on whether a state may use force in self-defence*.[45] This prohibition applies to '*any use of force, regardless of the weapons*

[41] S. Watts et al., "Understanding Conflict Trends: A Review of the Social Science Literature on the Causes of Conflict," *RAND Corporation*, 12 September 2017, at https://www.rand.org/pubs/research_reports/RR1063z1.html, 9 I 2023.

[42] D.J. Lonsdale, "We aren't in a Cyber War – Despite what Britain's Top General Thinks," *The Conversation*, 25 October 2019, at https://theconversation.com/we-arent-in-a-cyber-war-despite-what-britains-top-general-thinks-125578, 18 XII 2023.

[43] Prosecutor v. Dusko Tadic, Case No. IT-94-1-AR-72, *Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction*, 2 X 1995, Par. 70.

[44] "United Nations Charter, Chapter I: Purposes and Principles," Article 2, Point 4, *United Nations*, at https://www.un.org/en/about-us/un-charter/chapter-1, 18 XII 2023.

[45] M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York–Cambridge 2013, p. 45.

employed[46] (also cyber weapons).[47] Therefore, regarding the application of general international law, there is widespread acknowledgment that cyberspace is not devoid of legal regulations; instead, the established principles of international law encompass this realm.[48] Nevertheless, the question persists about the feasibility of implementing these principles in cyberspace. On one front, there is an assertion that applying the tenets of international law is feasible. Indeed, the prevailing stance within the international community indicates an inclination towards extending the application of international law to cyberspace.

However, in practice, the lack of universal definitions and criteria for assessing the degree of cyber threat in a rapidly changing cyber environment makes the use of *ius ad bellum* less clear. Moreover, with the emergence and development of new cyber threats, the practice of states may change the current interpretations of *ius ad bellum*. Reaching an international agreement on the interpretation and enforcement of the law in relation to cyber-attacks might not be an easy task. After all, the UN Charter was drawn up for a different epoch of conflict. Not only are some features of cyberspace activities difficult to interpret by law, but states have divergent strategic interests that will drive their preferred interpretations. Therefore, as Matthew C. Waxman points out, the solution will not be to abandon multilateral legal efforts to regulate cyber-attacks. However, the limitations of these efforts and the implications of the legal proposals should be considered in the context of a broader security strategy.[49]

The experts at CCD COE have taken on the daunting task of resolving issues concerning whether a particular cyber-attack meets the international legal criteria for war. They have addressed this in an extensive publication titled the "Tallinn Manual". The most obvious determining factor for when a cyber-attack violates the prohibition on the use of force under the United Nations Charter is the physical effect of the cyber operation. Typically, the effects-based approach categorises a cyber-attack by assessing its impact severity. If a cyber-attack's consequences match those of a traditional kinetic attack, states might consider treating it similarly and retaliating with force. In other words, if the physical consequences of a cyber-attack resemble the scale of destruction

[46] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons – Advisory Opinion of 8 July 1996*, Para. 39, after: M.N. Schmitt (ed.), *Tallinn Manual...*

[47] Although the Tallinn Manual holds considerable influence in the global arena, it does not possess direct legal authority over nations. Consequently, there is an increasing global momentum, driven by both state and non-state actors, to create a new legally binding agreement called the Digital Geneva Convention. J. Guay, L. Rudnick, "What the Digital Geneva Convention Means for the Future of Humanitarian Action," *UNHCR Innovation*, *The Policy Lab*, 25 June 2017, at https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/, 25 XI 2023; B. Smith, "The Need for a Digital Geneva Convention," *Microsoft*, 14 February 2017, at https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/, 22 XI 2023.

[48] A. Sari, *International Law and Cyber Operations: Current Trends and Developments*, Strasbourg, 24 March 2023, at https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48, 13 XII 2023.

[49] M.C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law*, vol. 36 (2011), p. 425.

caused by dropping a bomb or firing a missile, then such an attack should be considered in the category of the use of force. Clear examples of this are cyber-attacks that cause injury or death to individuals or the destruction or damage of critical infrastructure facilities. Other consequences of a cyber-attack may be more difficult to assess. For instance, some cyber operations lack a kinetic equivalent, leading to continued uncertainty as to whether cases that do not result in physical harm can be deemed the use of force.

Michael Schmitt has introduced a framework based on effects, considering six criteria to ascertain whether a cyber-attack meets the threshold of an armed attack. This approach is widely regarded by scholars as the primary interpretation of the effects-based framework, and the creators of the Tallinn Manual (led by Schmitt) largely embraced this perspective.[50] The first and most important criterion is the 'severity of the attack'. As noted, an attack, including a cyber-attack, that causes physical harm to humans or property will be classified as the use of force. An attack causing mere inconvenience or irritation will not be considered as such. However, it is worth mentioning that certain states assert that sovereignty extends to prohibiting cyber activities that disrupt or render inoperative cyber systems in other states, regardless of any physical damage. A few, like France, Norway and Iran, explain that merely infiltrating national cyber systems, especially those crucial for national security, may cross the threshold of aggression.[51] This stance stems from concerns that infiltrating these systems could form part of shaping future operations, heightening the vulnerability of the targeted state.[52] The second factor is 'immediacy of the attack'. The quicker the consequences of an attack are perceivable, the smaller the chances for a peaceful resolution of the dispute. States perceive greater danger in actions that produce rapid effects than in gradual changes. In other words, it is easier to classify cyber operations as the use of force if they produce immediate results than those achieving the same effect over a longer period, for example, several weeks. The third principle is 'directness' or a cause-and-effect reaction. A cyber operation with a clear link between its cause and immediate effect is more likely to be understood as the use of force. The principle of 'invasiveness' relates to the degree to which a cyber operation disrupts the functioning of the targeted state or its operating systems. The principle stands that the better secured the system is, the more strategic it is for the state and its security. Operations against dot-mil or dot-gov domains will certainly be understood as more invasive than attacks against dot-com domains. Another factor is the 'measurability of the attack's effects'. In the virtual world, the consequences of an attack may be less obvious than in the real world. The easier the consequences are to calculate and identify, the simpler the decision on whether the attack constitutes the

[50] M.N. Schmitt (ed.), *Tallinn Manual...*

[51] *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*, General Assembly, 13 July 2021, at https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf, 13 XII 2023; A. Sari, *International Law and Cyber Operations...*

[52] A. Sari, *International Law and Cyber Operations...*, p. 7.

use of force will be. Determining factors of whether a cyber-attack is the use of force also include: its 'military character', the degree of 'state involvement' in the cyber operation and 'presumptive legitimacy'. The latter of these factors boils down to the idea that actions not prohibited by international law are permissible. For example, international law does not prohibit propaganda, psychological operations, intelligence actions or economic pressure. Any actions falling into these categories are presumed legal and, therefore, there is a lower likelihood that they will be considered the use of force.

In support of his approach, Schmitt contends that nations are inclined to find a balance between *setting the threshold for what constitutes a use of force too high (potentially inviting other states to engage in aggressive conduct without fear of being accused of violating Article 2(4) and setting the threshold too low (limiting one's freedom of action out of fear that seemingly benign conduct will be considered an illegal use of force)*.[53] According to Schmitt, these elements enable states to gauge when a state's behaviour exceeds acceptable limits and transforms into a use of force.

The guidelines crafted by CCD COE experts for evaluating the application of international law norms in cyberspace serve as a crucial point of reference. Nonetheless, when dealing with a significant cyber-attack, it is necessary to scrutinise the precise details of each rule to ascertain their relevance to cyberspace and understand their specific application. As international law professor Aurel Sar rightfully observes: *While some cases are relatively straightforward because the rule in question clearly does or does not apply, in many other cases the application of individual rules is open to reasonable disagreement. This is a source of considerable legal uncertainty*.[54] As highlighted by the UN in 2020, *over a hundred cyber incidents that could undermine international peace and security were identified, posing significant potential for damage and casualties*.[55] Therefore, as it is states that establish international law, the responsibility lies with them to minimise this ambiguity by articulating their understanding of the law.

RUSSIAN (CYBER) GREY-ZONE STRATEGY IN UKRAINE

Russian strategic documents do not refer directly to grey-zone conflict; instead, they frame discussions in the context of war and warfare. Strategic thinking has evolved to embrace a fresh comprehension of warfare, termed by General Valery Gerasimov as 'New Generation Warfare', which, once more, avoids military-induced violence yet is classified as war from the Russian viewpoint.[56] In line with this, Marek Galeotti, an expert on Russian security affairs, asserted that while Gerasimov appeared to employ

[53] N. Simmons, "A Brave New World: Applying International Law of War to Cyber-Attacks," *Journal of Law & Cyber Warfare*, vol. 4, no. 1 (2014), p. 60.

[54] A. Sari, *International Law and Cyber Operations*...

[55] "A New Era of Conflict and Violence," *United Nations*, at https://www.un.org/en/un75/new-era-conflict-and-violence, 14 XII 2023.

[56] V. Gerasimov, "The Value of Science is in the Foresight...".

a defensive narrative by highlighting the necessity to protect Russia from the new form of warfare conducted by the West in the Arab world, he likely intended the opposite – that this was actually the kind of warfare Russia should initiate.[57] Galeotti assumes that: *Presenting the Arab Spring – wrongly – as the result of covert Western operations allows Gerasimov the freedom to talk about what he wants to talk about: how Russia can subvert and destroy states without direct, overt and large-scale military intervention*.[58] In turn, Sergei Chekinov and Sergei Bogdanov categorise a new generation of warfare as comprising opening and closing periods.[59] During the opening phase, employing grey-zone tactics involves deceiving the adversary's political and military leadership regarding the aggressor's intentions. This deception aims to achieve objectives through means like initiating disinformation campaigns, launching cyber-attacks against the enemy's communication systems across all levels of control, engaging in electronic warfare operations, conducting aerospace operations, persistently harassing the enemy with air force actions and deploying high-precision weaponry from diverse platforms. This period allows the aggressor to effectively mislead the opposing country's political and military leaders regarding their intentions, serving as a strategic means to accomplish their goals. The second, closing phase of a new generation of warfare would witness the entry of the attacker's regular ground forces into the target country. Indeed, Russian operations in Ukraine correspond to these stages of conflict.

According to J. Andres Gannon, Erik Gartzke, Jon Lindsay and Peter Schram: *Gray zone conflict has not been the panacea for Russia's aspirations that pundits have imagined*,[60] leading the Kremlin to conclude that the only option was to initiate a military campaign. Russia's move from grey-zone operations to kinetic military actions can be attributed not solely to the inefficacy of such measures, but also to Russia's heightened assertiveness in global affairs during the last decade. Vladimir Putin's increasing willingness to take greater risks – especially concerning actions in Russia's immediate vicinity – further explains this shift.[61] This is in line with the 'prospect theory', described by Tor Bukkvoll, which suggests that states fearing losses are more likely to take risky actions than those seeking gains.[62] Thus, one could infer that the concern about conflict escalation did not act as a deterrent for Russian grey-zone activities. It is also possible

[57] A. Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, FIIA Report, vol. 43, Helsinki 2015, p. 49, at https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf, 14 XII 2023.

[58] M. Galeotti, "The 'Gerasimov doctrine'...," after: A. Rácz, *Russia's Hybrid War in Ukraine...*

[59] S.G. Chekinov, S.A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought*, no. 4 (2013), pp. 21, 22; J. Healey, "Preparing for Inevitable Cyber Surprise," *War on the Rocks*, 12 January 2022, at https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/, 13 XII 2023.

[60] J.A. Gannon, E. Gartzke, J. Lindsay, P. Schram, "Why Did Russia Escalate...".

[61] J.J. Driedger, "Risk Acceptance and Offensive War: The Case of Russia under the Putin Regime," *Contemporary Security Policy*, vol. 44, no. 2 (2023), pp. 199-225.

[62] T. Bukkvoll, "Why Putin Went to War: Ideology, Interests and Decision-Making in the Russian Use of Force in Crimea and Donbas," *Contemporary Politics*, vol. 22, no. 3 (2016), pp. 267-282.

that the Russians simply lacked the patience or strategies to keep their activities below the threshold of aggression, hindering the accomplishment of strategic objectives.

To better comprehend the reasons behind exiting the grey zone and the strategic objectives in cyberspace, one must reject the Western perspective on cyber warfare. In this approach, *Cyber war is more about beliefs and data than it is about wresting physical control over objects or destroying material capabilities. Hollywood has gotten cyber war wrong, preferring to imagine a domain in which bits and bytes somehow lead to spectacular explosions. Intellectuals have not done much better*.[63] In Russia, the terms 'cybernetic warfare', 'information warfare' and 'network warfare' carry entirely distinct interpretations.[64] Unlike the Western paradigm that prioritises destructive offensive cyber actions aimed at critical infrastructure, the Russians focus on informational operations.[65]

In Russian strategic documents, references to cyberspace are absent. Instead, Russians refer to the 'information space', which encompasses both computer-based and human information processing, essentially comprising the cognitive domain. Within the realm of 'information space', activities in cyberspace divide into cyber-psychological operations (e.g., aggressive social media campaigns) and cyber-technical operations (targeting critical infrastructure facilities).[66] Furthermore, Russian perspectives consider the separation of actions within the cyber sphere, like processing, attacking, disrupting or stealing information, as artificial. Within this framework, tools such as: *distributed denial of services attacks (DDoS), advanced [cyber] exploitation techniques and Russia Today television are all related tools of information warfare*.[67] To clarify, the concept of 'cyber' as an independent function or domain is not part of the Russian perspective.

A) Cyber-psychological operations

Unlike the Western approach, Russian information warfare extends beyond activities that are limited to or occur just before kinetic warfare. It can be confidently stated that the use of cyber disinformation and propaganda in Russian actions in Ukraine is, as

[63] N. Kostyuk, E. Gartzke, "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," *Texas National Security Review*, vol. 5, no. 3 (2022), pp. 113-126.

[64] J. Darczewska, *The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study*, Warszawa 2014.

[65] K. Giles, A. Seaboyer, *The Russian Information Warfare Construct*, Kingston 2019, at https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf, 31 XII 2024.

[66] T.L. Thomas, "Russian Information Warfare Theory: The Consequences of August 2008," in S. Blank, R. Weitz (eds), *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Carlisle 2010, after: K. Giles, *Handbook of Russian Information Warfare*, Rome 2016, at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf, 12 XII 2023.

[67] D.J. Smith, "How Russia Harnesses Cyberwarfare," *Defense Dossier*, *American Foreign Policy Council*, no. 4 (2012), p. 8, after: K. Giles, *Handbook of Russian...*

Jolanta Darczewska aptly likened it, *an old product in new packaging*.[68] The recently observed Russian information and network warfare should be seen as a long-standing tradition rooted in the evolution of doctrines focused on the active use of intelligence and subversive operations, tracing its origins back to the periods of Tsarist Russia and the Soviet Union. Therefore, the strategies and approaches utilised by Russia are not inherently groundbreaking, despite the advancements in enabling technologies. This is evident in cyber warfare, where the evolution of the internet has expanded the scope and extended the duration of information warfare objectives.[69] Information operations, which encompass electronic warfare, psychological operations (psy-ops) and cyber-warfare, constitute integral components of what Peter Pomerantsev and Michael Weiss have labelled as the Kremlin's 'weaponisation of information'.[70] This concept is progressively used to characterise Gerasimov's 'New Warfare', which involves the deliberate utilisation of information – whether true or false – to accomplish objectives spanning from tactical to strategic, achieved through an active learning process by the targeted entities.[71] This brings the operation into the cognitive domain, where the primary goal is to engage the sentiments and viewpoints of both local and global audiences.

Therefore, despite various theories regarding the reasons for exiting the grey zone and initiating physical aggression, the most plausible explanation appears to be that different objectives were set for the Russian cyber and kinetic invasion. As assessed by Keir Gilles: *the West may be prepared to face 'pure' cyber challenges, but the capabilities and intentions embraced by Russia [...] show that it also needs to be prepared for information war when these are melded with disinformation, subversion, kinetic and EW operations, with highly ambitious aims up to and including regime change in the target state*.[72] Put differently, the cyber dimension may have concentrated on information warfare, whereas the physical aspect targeted territorial acquisition. Accordingly, from the Russian perspective, relying solely on cyberweapons is not sufficient to conquer a nation. Yet, the Russians demonstrate exceptional skill in operating within the information sphere to achieve their political goals.

Hence, in the opening phase of the conflict, the disinformation campaign, ongoing misinformation/disinformation and informational propaganda held particular significance. This was clearly highlighted in the statements of key Russian politicians and military officials before and during the grey-zone phase. That communicated priorities for cyberspace, which were later mirrored in Russian strategic documents and

[68] J. Darczewska, *The Anatomy of Russian Information Warfare...*

[69] A. Foxall, "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain," *Russia Studies Centre Policy Paper*, no. 9 (2016), at https://henryjacksonsociety.org/wp-content/uploads/2016/05/Cyber-FINAL-copy.pdf, 14 XI 2023.

[70] P. Pomerantsev, M. Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, New York 2014, after: A. Foxall, "Putin's Cyberwar...".

[71] F.S. Hansen, "The Weaponization of Information: News from the Cognitive Domain," *Danish Institute for International Studies*, 14 December 2017, at https://www.diis.dk/en/research/the-weaponization-of-information, 18 XII 2023.

[72] K. Giles, *Handbook of Russian...*, p. 13.

implemented in Ukraine from 2014 onwards. Even in the current active conflict phase, experts concur that the 'cyber fire' has yet to generate spectacular breakthroughs on the battlefield.[73] At the same time, very few of the dynamics between cyber and military operations have developed as expected.[74] In addition to the attempts to coordinate cyber and kinetic forces at the beginning of the war, we now observe the independent use of these two Russian capabilities.

B) Cyber-technical operations

As previously noted, Russians categorise activities within the 'information space' into cyber-psychological and cyber-technical operations. The latter covers a wide spectrum of activities aimed at enemy infrastructure. Some experts believe that Russian cyber--technical operations could potentially eliminate the need for military intervention in Ukraine by using cyber-attacks to achieve similar objectives.[75] Other experts believe that operations in cyberspace did not yield the expected results for Russia.[76] Therefore, the substitution strategy proposing that state actions in the grey zone could produce comparable outcomes to kinetic force proved insufficient.[77] However, the discrepancy in positions may stem from the Western misunderstanding of Russian grey-zone warfare, which misinterprets crucial elements of ambiguity and legality.[78]

Between 2014 and February 2022, cyber-attacks conducted by the Russians could be considered hostile acts of aggression against Ukraine. In 2015, a deliberate attack

[73] J.A. Lewis, "Cyber War and Ukraine," *Center for Strategic and International Studies*, 16 June 2022, at https://www.csis.org/analysis/cyber-war-and-ukraine, 19 XI 2023; J. Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," *Carnegie Endowment for International Peace*, 16 December 2022, at https://carnegieendowment.org/2022/12/16/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657, 12 XII 2023; M. Miller, "Russia's Cyberattacks Aim to 'Terrorize' Ukrainians," *Politico*, 11 January 2023, at https://www.politico.com/news/2023/01/11/russias-cyber-attacks-aim-to-terrorize-ukrainians-00077561, 15 XI 2023; M. Willett, "The Cyber Dimension of the Russia–Ukraine War," *Global Politics and Strategy*, vol. 64, no. 5 (2022), pp. 7-26; B. Smith, "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft*, 22 June 2022, at https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/, 10 XI 2023.

[74] N. Kostyuk, E. Gartzke, "Why Cyber Dogs...".

[75] K. Giles, "Putin Does Not Need to Invade Ukraine to Get His Way," *Chatham House*, 10 January 2021, at https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way, 11 XII 2023; D. Cattler, D. Black, "The Myth of the Missing Cyberwar: Russia's Hacking Succeeded in Ukraine – And Poses a Threat Elsewhere, Too," *Foreign Affairs*, 6 April 2022, at https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar, 1 XI 2023.

[76] J.A. Lewis, "Cyber War and Ukraine"; J. Bateman, "Russia's Wartime Cyber Operations in Ukraine..."; M. Miller, "Russia's Cyberattacks...".

[77] N. Kostyuk, E. Gartzke, "Why Cyber Dogs...".

[78] K. Giles et al., "Myths and Misconceptions Around Russian Military Intent," *Chatham House*, 22 September 2022, at https://www.chathamhouse.org/2022/06/myths-and-misconceptions-around-russian-military-intent/myth-1-russia-waging-grey-zone, 1 XII 2023.

targeted the Ukrainian power grid, resulting in more than 230,000 people losing electricity.[79] The Ukrainian intelligence community unequivocally asserted that Russia was behind the attack, although they did not actually present any evidence to support this claim.[80] Multiple control centres were specifically attacked to steal operator credentials, enabling access to the power grid in the Ivano-Frankivsk region. Some areas experienced power outages lasting up to six hours. Concurrently, hackers inundated customer service phone lines with calls to prevent customers from reporting the incident. A similar sequence of events recurred in 2016. Restoring the regular operations of the substations required manual intervention by on-site operators. This involved changing the dispatch control centre from 'automatic' to 'manual mode' due to the hackers infecting the SCADA manufacturer's firmware. Despite the restoration, the affected infrastructures continued to operate under limited capabilities.[81] This assessment of the power grid 2015 hack is reinforced by another aspect of the attack: the hackers had the potential to cause significantly greater damage by physically destroying substation equipment, which would have made restoring power after the blackout considerably more challenging.[82] Therefore, it is possible that, at that time, the Russians only wanted to send another warning signal to Ukraine while still aiming to keep the conflict below the threshold of aggression.

Subsequently, in June 2017, Ukrainian institutions, businesses and services were targeted by the NotPetya malware attack – called *the most devastating cyber-attack in history*.[83] Functioning as ransomware, the virus encrypted the hard drives of the targeted computers and demanded payment in bitcoin. Initially designed to spread within internal networks, likely for a more focused impact, it unexpectedly infected the internal networks of multinational corporations with offices in Ukraine on a global scale. This caused estimated losses surpassing USD 10 billion.[84] Once again, Ukraine has accused Russia multiple times of orchestrating attacks on its computer systems and crucial power infrastructure, which is unsurprising. However, the Kremlin, consistently refuting these allegations, stated that it lacked information about the origin of the global cyber-attack, which also targeted Russian companies such as the oil giant Rosneft

[79] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 23 X 2023.

[80] Ibid.

[81] M. Assante, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," *SANS Institute*, 6 January 2016, at https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/, 25 IX 2023; "Cyber-Attack Against Ukrainian Critical Infrastructure," *Cybersecurity and Infrastructure Security Agency*, 20 July 2021, at https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01, 16 X 2023.

[82] K. Zetter, "Inside the Cunning...".

[83] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 August 2017, at https://www.wired.com/story/notpetya-cyber-attack-ukraine-russia-code-crashed-the-world/, 22 X 2023.

[84] T. Minárik, *NotPetya (2017)*, The NATO Cooperative Cyber Defence Centre of Excellence 2017, at https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017), 11 XI 2023.

and a steelmaker.[85] A statement was made by Kremlin spokesman Dmitry Peskov: *No single entity can effectively combat cyber threats alone, and baseless, broad accusations won't resolve this issue*.[86]

The most severe Russian cyber-attack, occurring one hour before Russian troops crossed the border into Ukraine on 24 February 2022, resulted in a partial interruption of Viasat's KA-SAT consumer satellite broadband service. This impacted several thousand customers in Ukraine and rendered satellite broadband modems inoperable, including those crucially used by the Ukrainian government, as well as tens of thousands of other fixed broadband customers across Europe.[87] Viasat is the most probable case of involvement by Russian cyber forces in coordinated military operations. The breach occurred almost simultaneously with the initial kinetic Russian attacks and could have aided them, worsening what frontline commanders in Kyiv described as a communication-deprived environment that hindered Ukrainian defence around the capital.[88] Opinions on the actual strategic effects of the Viasat attack are divided. Some experts, like Dmitri Alperovitch, referred to it as *perhaps the most strategically impactful cyber operation in wartime history*,[89] while others, like James Lewis, stated that it *ultimately did not provide military advantage to Russia*.[90]

Given the dilemmas concerning the interpretation of cyber-attacks within the realm of international law, it is essential to pose the question: do operations against Ukraine implicate the *ius ad bellum* prohibition on the 'use of force' outlined in Article 2(4) of the UN Charter and customary international law? In other words, it is necessary to assess whether the effects of cyber operations in Ukraine meet the criteria defined in the Tallinn Manual for crossing the threshold of aggression. Michael N. Schmitt's opinion suggests that it did not happen because *it is unlikely that states would consider a short, non-destructive, and non-injurious denial of service operation as qualifying*.[91] According to Ondrej Hamulak and Jozef Valuch, from 2014 until the onset of the kinetic invasion, most cyber operations in Ukraine did not result in destructive impacts on critical infrastructure or in the elimination of war-related equipment.[92] Hence, it can

[85] E. Auchard, J. Stubbs, A. Prentice, "New Computer Virus Spreads from Ukraine to Disrupt World Business," *Reuters*, 29 July 2017, at https://www.reuters.com/article/us-cyber-attack/new-computer-virus-spreads-from-ukraine-to-disrupt-world-business-idUSKBN19I1TD/, 20 XI 2023.

[86] Ibid.

[87] "KA-SAT Network Cyber Attack Overview," *Viasat*, 30 March 2022, at https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview, 20 XI 2023.

[88] J. Bateman, Russia's Wartime Cyber Operations in Ukraine...".

[89] Ibid.

[90] Ibid.

[91] M.N. Schmitt, "Russian Cyber Operations and Ukraine: The Legal Framework," *Lieber Institute West Point*, 16 January 2022, at https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/, 11 XI 2023.

[92] O. Hamulak, J. Valuch, "Cyber Operations During the Conflict in Ukraine and the Role of International Law," in S. Sayapin, E. Tsybulenko (eds), *The Use of Force against Ukraine and International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum*, Hague 2018.

be inferred that these operations were neither prohibited nor did they violate international rules regarding armed conflicts. However, a wholly distinct scenario emerges if these cyber operations were connected to or intertwined with the kinetic war operations, such as those in Crimea. Notably, some states, like Norway and France, assert that sovereignty extends to prohibiting cyber operations, even those causing another state's cyber systems to lose functionality or become inoperable, regardless of whether any physical damage is inflicted. In the examples of cyber-attacks described above, more advanced and harmful techniques than DDoS were employed. Yet, the notable aspect of the Ukraine conflict is not just the abundance of DDoS and other operations typical of the grey zone; it also involves severe mass-destructive or disruptive cyber-attacks.[93] On the other hand, the alignment of cyber operations, excluding the application of force, with international law is a notable aspect. These operations might fall under alternative international legal regulations, such as the prohibition of intervention, which constitutes a component of the principle of sovereign equality among states.[94] This prohibition entails that *all states or groups of states are forbidden from intervening, directly or indirectly, in the internal or external affairs of other states*.[95]

However, Schmitt concludes that "cyber operations at the use of force level attributable to Russia – either because they are conducted by state organs like the GRU or by non-state actors operating pursuant to Russian *instructions or direction or control [...] – would be subsumed within the ongoing use of force violation that began with Russia's 2014 unlawful occupation of Crimea and its actions elsewhere in Ukraine*.[96] Thus, the triggering of Ukraine's right to self-defence resulted from the non-cyber armed attack by Russia against the country. This right remains valid due to the ongoing aggressive occupation of Ukrainian territory and other hostile Russian actions, including cyber operations. *Therefore, whether individual cyber operations or campaigns by Russian intelligence or military organisations, or by non-state hacker groups acting 'on behalf or with the substantial involvement of Russia' [...], rise to the level of an armed attack [...] has no bearing on a Ukrainian response*.[97] Similar views are shared by Professor Aurel Sari, who emphasises that the impact of cyber-attacks on the conflict's course has been limited, offering neither decisive military nor significant political advantages for Russia. Furthermore, many cyber-attacks were not conducted independently but as a supplement to conventional military operations. Consequently, the conduct of cyber operations in and against Ukraine raises a range of legal questions concerning the potential crossing of the threshold of aggression. Hence, it is crucial not to exaggerate their newness and uniqueness. Equally significant is the bidirectional nature of applying established

93 D. Cattler, D. Black, "The Myth of the Missing Cyberwar..."; D. Volz, R. McMillan, "In Ukraine, a «Full-Scale Cyberwar» Emerges," *The Wall Street Journal*, 12 April 2022, at https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203, 11 XI 2023.

94 O. Hamulak, J. Valuch, "Cyber Operations...".

95 Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment of the Court, No. 86/8, 27 VI 1986.

96 M.N. Schmitt, "Russian Cyber Operations and Ukraine...".

97 Ibid.

international laws to cyberspace: the way states construe and implement these laws in this realm might notably influence their application and interpretation across other domains. Ultimately, grappling with challenging decisions is inevitable, acknowledging that the legal aspect of cyberspace is not solely about rules – it encompasses order and strategic rivalry as well.[98] Therefore, not every kind of aggression should be termed war – it simply means that it is up to the decision-maker to call a war a war. Furthermore, Ukraine initially referred to the conflict in eastern Ukraine as an 'anti-terrorist operation' because this was the main legal framework available for conducting operations without declaring war against Russia.

In fact, the challenge did not lie in identifying the source of these attacks, but rather in the lack of necessary resolve to respond to them. The use of the term 'grey zone' by decision-makers may reflect their reluctance to label certain actions as 'war'. However, this does not imply that all forms of aggression should be classified as war – the decision ultimately rests with those in power. During the ongoing phase of the war, Russia has persisted in utilising cyberspace to carry out operations in the grey zone against countries that support Ukraine. Therefore, it can be anticipated that there will be an escalating intensification of disinformation and intelligence operations. This is supported by the statements of Microsoft specialists, who suggest that Russian hostile activities against Ukraine-supporting countries are predominantly related to intelligence. This includes attempts to obtain knowledge about the logistics of supplying aid to Ukraine, as well as efforts directed at Ukraine-supportive nations – which were not designed to cause harm to systems, but rather to gather information.

Going back to the point, by using the 'taming world opinion strategy', Russians benefitted from the lack of determination of NATO countries. In the grey zone, the Russians carried out cyber-attacks that could be considered hostile aggression against Ukraine. In fact, the problem was not the difficulty of attributing the attacks, but the lack of determination. Therefore, the cyber aspects of the Russia-Ukraine conflict suggest the increased urgency of efforts by states, academics and civil society to clarify legal rules applicable to both high-end and grey-zone-like cyber operations. Hence, the cyber dimensions of the Russia-Ukraine conflict emphasise the growing need for states, scholars and lawyers to expedite efforts in defining legal frameworks that cover both sophisticated high-end and grey-zone-style cyber operations.

CONCLUSIONS

Between 2014 and February 2022, Russia was implementing a grey-zone conflict strategy, which included activities in cyberspace to pressure Kyiv into making concessions. Cyber weapons from the grey zone, including ongoing misinformation and disinformation, informational propaganda, cyber-attacks on critical infrastructure in 2015 and a cyber-attack that targeted Ukraine's ministries and banks in February 2022,

[98] A. Sari, *International Law and Cyber Operations...*

according to many experts, were a form of limited military competition that persisted beyond peace but remained short of full-scale war. The aim of all these activities was to avoid open conflict and serious clashes while simultaneously achieving strategic goals. Therefore, we may conclude that the Russia-Ukraine conflict before 24 February 2022 was a perfect example of 'salami tactics'. The benefits of cyber operations in the grey zone decreased in significance as the conflict escalated. Regardless of the ultimate outcome of the war, Russia will experience military damage and economic decline. This will serve as motivation to resume activities in cyberspace and the grey zone.

Assuming that the Russian cyber grey zone had three fundamental objectives: firstly, creating circumstances that lead to crises – primarily by identifying vulnerabilities in critical infrastructure facilities and launching attacks, such as the 2015 power grid hack, a significant cyber-attack resulting in a widespread power outage in Ukraine; secondly, assessing the response of Western nations to these attacks; thirdly, disseminating misinformation and propaganda. It is equally plausible to assert that all these activities were constrained by the overarching goal of taming world opinion and gradually acclimatising us to the situation in Ukraine. Putin's pre-war tactics can be compared to the parable of the frog in boiling water, where a situation worsens gradually, leading to lethal danger without realisation, until it is too late. Putin skilfully reduced the West's vigilance, and cyber tools proved to be an ideal way to achieve this goal. This is primarily due to three features of cyberspace: the challenge of tracing attacks to their source, the lack of territorial boundaries and the ease of disrupting an adversary's information exchange. To the benefit of the Russians, there is also an issue with defining legal frameworks that cover both sophisticated high-end and grey-zone-style cyber operations. Therefore, Russia was able to exploit the lack of resolve among NATO countries by utilising the 'taming world opinion strategy'. The Russians benefitted from the lack of determination of NATO countries.

While it is crucial to establish legal frameworks encompassing advanced high-end and grey-zone-style cyber operations, the emphasis on determination in countering grey-zone activities could be even more vital in the context of the Russo-Ukrainian conflict. Therefore, regarding the dynamics of the conflict, the grey zone could be characterised as a space where everyone is aware of the adversarial state's actions, yet there is a reluctance or unwillingness to intervene and halt those actions.

BIBLIOGRAPHY

"A New Era of Conflict and Violence," *United Nations*, at https://www.un.org/en/un75/new-era-conflict-and-violence.

Arquilla J., "Perils of the Gray Zone: Paradigms Lost, Paradoxes Regained," *National Defense University Press*, 9 May 2018, at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983610/perils-of-the-gray-zone-paradigms-lost-paradoxes-regained/.

Assante M., "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," *SANS Institute*, 6 January 2016, at https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/.

Auchard E., Stubbs J., Prentice A., "New Computer Virus Spreads from Ukraine to Disrupt World Business," *Reuters*, 29 July 2017, at https://www.reuters.com/article/us-cyber-attack/new-computer-virus-spreads-from-ukraine-to-disrupt-world-business-idUSKBN19I1TD/.

Austin G., Lin Tay K., Sharma M., "Great-Power Offensive Cyber Campaigns: Experiments in Strategy," *IISS*, 24 February 2022, at https://www.iiss.org/en/research-paper/2022/02/great-power-offensive-cyber-campaigns/.

Azad T.M., Haider M.W., Sadiq M., "Understanding Gray Zone Warfare from Multiple Perspectives," *World Affairs*, vol. 186, no. 1 (2023), pp. 81-104, https://doi.org/10.1177/00438200221141101.

Bateman J., "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," *Carnegie Endowment for International Peace*, 16 December 2022, at https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

Brands H., "Paradoxes of the Gray Zone," *Foreign Policy Research Institute*, 5 February 2016, at https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

Brooks R., "Rule of Law in the Gray Zone," *Modern War Institute at West Point*, 7 February 2018, at https://mwi.westpoint.edu/rule-law-gray-zone/.

Bukkvoll T., "Why Putin Went to War: Ideology, Interests and Decision-Making in the Russian Use of Force in Crimea and Donbas," *Contemporary Politics*, vol. 22, no. 3 (2016), pp. 267-282, https://doi.org/10.1080/13569775.2016.1201310.

Casey G., "Aug. 14, 2007 – Remarks at the National Press Club," *U.S. Army*, 15 August 2007, at https://www.army.mil/article/4436/aug_14_2007_remarks_at_the_national_press_club.

Cattler D., Black D., "The Myth of the Missing Cyberwar: Russia's Hacking Succeeded in Ukraine – And Poses a Threat Elsewhere, Too," *Foreign Affairs*, 6 April 2022, at https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar.

Chekinov S.G., Bogdanov S.A., "The Nature and Content of a New-Generation War," *Military Thought*, no. 4 (2013), pp. 12-23.

Cohen R.S., "Has the War in Ukraine Damaged Russia's Gray Zone Capabilities?," *RAND Corporation*, 22 June 2022, at https://www.rand.org/pubs/commentary/2022/06/has-the-war-in-ukraine-damaged-russias-gray-zone-capabilities.html.

"Cyber-Attack Against Ukrainian Critical Infrastructure," *Cybersecurity and Infrastructure Security Agency*, 20 July 2021, at https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

Darczewska J., *The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study*, Warszawa 2014.

Davidson J.W., "The Roots of Revisionism: Fascist Italy, 1922-39," *Security Studies*, vol. 11, no. 4 (2002), pp. 125-159, https://doi.org/10.1080/714005356.

Driedger J.J., "Risk Acceptance and Offensive War: The Case of Russia under the Putin Regime," *Contemporary Security Policy*, vol. 44, no. 2 (2023), pp. 199-225, https://doi.org/10.1080/13523260.2023.2164974.

Dziwisz D., "Non-War Activities in Cyberspace as a Factor Driving the Process of De-Bordering," *Politics and Governance*, vol. 10, no. 2 (2022), pp. 293-302, https://doi.org/10.17645/pag.v10i2.5015.

Dziwisz D., Sajduk B., "Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę «specjalnej operacji wojskowej»," in A. Gruszczak (ed.), *The War Must Go On: Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski*, Kraków 2023, https://doi.org/10.12797/9788381388801.04.

Elkus A., "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," *War on the Rocks*, 15 December 2015, at https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/.

Foxall A., "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain," *Russia Studies Centre Policy Paper*, no. 9 (2016), at https://henryjacksonsociety.org/wp-content/uploads/2016/05/Cyber-FINAL-copy.pdf.

Galeotti M., "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, 6 July 2014, at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Gannon J.A. et al., "Why Did Russia Escalate Its Gray Zone Conflict in Ukraine?," *Lawfare*, 16 January 2022, at https://www.lawfaremedia.org/article/why-did-russia-escalate-its-gray-zone-conflict-ukraine.

Gerasimov V., "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review*, January-February 2016, at https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.

Giles K., *Handbook of Russian Information Warfare*, Rome 2016, at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf.

Giles K. et al., "Myths and Misconceptions around Russian Military Intent," *Chatham House*, 22 September 2022, at https://www.chathamhouse.org/2022/06/myths-and-misconceptions-around-russian-military-intent/myth-1-russia-waging-grey-zone.

Giles K., "Putin Does Not Need to Invade Ukraine to Get His Way," *Chatham House*, 10 January 2021, at https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.

Giles K., Seaboyer A., *The Russian Information Warfare Construct*, Kingston 2019, at https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf.

Green M. et al., *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Center for Strategic and International Studies 2017, at https://www.jstor.org/stable/pdf/resrep23165.6.pdf?refreqid=fastly-default%3A50890b0403d6b04aa66c62c040096d4a&ab_segments=&origin=&initiator=&acceptTC=1.

Greenberg A., "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 August 2017, at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Guay J., Rudnick L., "What the Digital Geneva Convention Means for the Future of Humanitarian Action," *UNHCR Innovation*, *The Policy Lab*, 25 June 2017, at https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/.

Hamulak O., Valuch J., "Cyber Operations During the Conflict in Ukraine and the Role of International Law," in S. Sayapin, E. Tsybulenko (eds), *The Use of Force against Ukraine and International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum*, Hague 2018, https://doi.org/10.1007/978-94-6265-222-4_10.

Hansen F.S., "The Weaponization of Information: News from the Cognitive Domain," *Danish Institute for International Studies*, 14 December 2017, at https://www.diis.dk/en/research/the-weaponization-of-information.

Hayes J.E., "Beyond the Gray Zone: Special Operations in Multidomain Battle," *National Defense University Press*, 5 November 2018, at https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-91/jfq-91_60-66_Hayes.pdf?ver=2018-11-06-094122-477.

Healey J., *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities*, United States House of Representatives, 1 March 2017, at https://nsarchive.gwu.edu/sites/default/files/documents/3515025/Document-11-Jason-Healey-Columbia-University.pdf.

Healey J., "Preparing for Inevitable Cyber Surprise," *War on the Rocks*, 12 January 2022, at https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/.

Hersman R., "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review*, vol. 3, no. 3 (2020), pp. 90-109, https://doi.org/10.26153/tsw/10220.

Hoffman F.G., "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," *The Heritage Foundation*, 5 October 2015, at https://www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protracted-gray.

International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons – Advisory Opinion of 8 July 1996*, Para. 39.

"KA-SAT Network Cyber Attack Overview," *Viasat*, 30 March 2022, at https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

Kostyuk N., Gartzke E., "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," *Texas National Security Review*, vol. 5, no. 3 (2022), pp. 113-126, https://doi.org/10.26153/tsw/42073.

Lazović R., "Ambiguous Approach – All Shades of Gray," *Cyber, Intelligence, and Security*, vol. 4, no. 1 (2020), pp. 41-57.

Lewis J.A., "Cyber War and Ukraine," *Center for Strategic and International Studies*, 16 June 2022, at https://www.csis.org/analysis/cyber-war-and-ukraine.

Lonsdale D.J., "We aren't in a Cyber War – Despite what Britain's Top General Thinks," *The Conversation*, 25 October 2019, at https://theconversation.com/we-arent-in-a-cyber-war-despite-what-britains-top-general-thinks-125578.

Lucas S., Mistry K., "Illusions of Coherence: George F. Kennan, U.S. Strategy and Political Warfare in the Early Cold War, 1946-1950," *Diplomatic History*, vol. 33, no. 1 (2009), pp. 39-66, https://doi.org/10.1111/j.1467-7709.2008.00746.x.

Matisek J., "From Little Green Men to Little Blue Helmets: Imagining the Future of Russian Aggression – And what to Do about it," *Modern War Institute at West Point*, 11 February 2021,

at https://mwi.westpoint.edu/from-little-green-men-to-little-blue-helmets-imagining-the-future-of-russian-aggression-and-what-to-do-about-it/.

Mazarr M.J., *Mastering the Gray Zone: Understanding a Changing Era of Conflict,* Carlisle 2015.

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment of the Court, No. 86/8, 27 June 1986.

Miller M., "Russia's Cyberattacks Aim to 'Terrorize' Ukrainians," *Politico*, 11 January 2023, at https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561.

Minárik T., *NotPetya (2017)*, The NATO Cooperative Cyber Defence Centre of Excellence 2017, at https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017).

Morris L.J. et al., "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War," *RAND Corporation*, 27 June 2019, at https://www.rand.org/pubs/research_reports/RR2942.html.

Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 2020, at https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

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, General Assembly, 13 July 2021, at https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

Pomerantsev P., Weiss M., *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, New York 2014.

Popp G., Canna S., "The Characterization and Conditions of the Gray Zone: A Virtual Think Tank Analysis (ViTTa)," *NSI*, January 2017, at https://nsiteam.com/social/the-characterization-and-conditions-of-the-gray-zone-a-virtual-think-tank-analysis-vitta/.

Prosecutor v. Dusko Tadic, Case No. IT-94-1-AR-72, *Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction*, 2 October 1995, par. 70.

Rácz A., *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, FIIA Report, vol. 43, Helsinki 2015, p. 49, at https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf.

Ripsman N.M., Taliaferro J.W., Lobell S.E., *Neoclassical Realist Theory of International Politics*, Oxford 2016, https://doi.org/10.1093/acprof:oso/9780199899234.001.0001.

Sari A., *International Law and Cyber Operations: Current Trends and Developments*, Strasbourg, 24 March 2023, at https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48.

Schmitt M.N., "Russian Cyber Operations and Ukraine: The Legal Framework," *Lieber Institute West Point*, 16 January 2022, at https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/.

Schmitt M.N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York–Cambridge 2013, https://doi.org/10.1017/CBO9781139169288.

Schmitt M.N., "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law Online*, vol. 42, no. 2 (2017), pp. 1-21.

Schweller R., "Bandwagoning for Profit: Bringing the Revisionist State back in," *International Security*, vol. 19, no. 1 (1994), pp. 72-107, https://doi.org/10.2307/2539149.

Sheppard L.R. et al., "By Other Means Part I: Campaigning in the Gray Zone," *CSIS*, 8 July 2019, at https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone.

Simmons N., "A Brave New World: Applying International Law of War to Cyber-Attacks," *Journal of Law & Cyber Warfare*, vol. 4, no. 1 (2014), pp. 42-108.

Smith B., "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft*, 22 June 2022, at https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Smith B., "The Need for a Digital Geneva Convention," *Microsoft*, 14 February 2017, at https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Smith D.J., "How Russia Harnesses Cyberwarfare," *Defense Dossier*, *American Foreign Policy Council*, no. 4 (2012).

Takashi S., *Increasingly Complex and Sophisticated 'Hybrid Warfare' during Peacetime: Japan's Comprehensive Response and the Japan-US Response*, Nakasone Peace Institute 2020, at https://www.npi.or.jp/en/research/NPI_Research_Note_20201005.pdf.

Thomas T.L., "Russian Information Warfare Theory: The Consequences of August 2008," in S. Blank, R. Weitz (eds), *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Carlisle 2010.

"United Nations Charter, Chapter I: Purposes and Principles," *United Nations*, at https://www.un.org/en/about-us/un-charter/chapter-1.

UN General Assembly, "Definition of Aggression," *Refworld*, 14 December 1974, at https://www.refworld.org/docid/3b00f1c57c.html.

Van de Velde J.R., "Make Cyberspace Great Again Too!," *RealClearDefense*, 23 July 2018, at https://www.realcleardefense.com/articles/2018/07/23/make_cyberspace_great_again_too_113634.html.

Volz D., McMillan R., "In Ukraine, a «Full-Scale Cyberwar» Emerges," *The Wall Street Journal*, 12 April 2022, at https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203.

Watts S. et al., "Understanding Conflict Trends: A Review of the Social Science Literature on the Causes of Conflict," *RAND Corporation*, 12 September 2017, at https://www.rand.org/pubs/research_reports/RR1063z1.html.

Waxman M.C., "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law*, vol. 36 (2011), pp. 421-459.

Willett M., "The Cyber Dimension of the Russia–Ukraine War," *Global Politics and Strategy*, vol. 64, no. 5 (2022), pp. 7-26, https://doi.org/10.1080/00396338.2022.2126193.

Wirtz J.J., "Life in the 'Gray Zone': Observations for Contemporary Strategists," *Defense & Security Analysis*, vol. 33, no. 2 (2017), pp. 106-114, https://doi.org/10.1080/14751798.2017.1310702.

Zetter K., "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zilincik S., Duyvesteyn I., "Strategic Studies and Cyber Warfare," *Journal of Strategic Studies*, vol. 46, no. 4 (2023), pp. 836-857, https://doi.org/10.1080/01402390.2023.2174106.

Dominika DZIWISZ – PhD, is an assistant professor in the Institute of Political Science and International Relations of the Jagiellonian University in Kraków, Poland. She holds master's degree both in International Relations as well as Marketing and Management. She received her PhD with distinctions from the Jagiellonian University in 2014. Her PhD research was focused on cybersecurity policy in the USA. This topic, together with critical infrastructure protection and the relationship between Big Data and human rights, to this day remains in the center of her research interests.