Politeja
No. 4(79), 2022, pp. 111-129
https://doi.org/10.12797/Politeja.19.2022.79.07

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

CYBER PEARL HARBOR IS NOT COMING

US POLITICS BETWEEN WAR AND PEACE

ABSTRACT In 2012, the US Defense Secretary Leon E. Panetta warned against an inevitable 'cyber-Pearl Harbor', an attack that would cause physical destruction and loss of life. Even though the darkest scenarios have not come true, his words shaped the perception of conflicts in cyberspace.[1] Recently, between the cyberwar and cyberpeace, states started recognizing a grey zone area – aggressive and offensive actions below the threshold of armed aggression that enable gaining strategic advantage. The aim of the article is to describe and discuss the change in the American approach to managing conflicts in the cyberspace. The focus will be on describing the current state of the concept of the grey zone in the US strategic documents, as well as the premises for forecasting the development of the grey zone in the future.

Keywords: cybersecurity, cyber Pearl Harbor, USA, cyberwar

[1] S. Gordon, E. Rosenbach, "America's Cyber-Reckoning: How to Fix a Failing Strategy", *Foreign Affairs*, vol. 101, no. 1 (2022), pp. 10-20.

INTRODUCTION

Following the 9/11 attacks, government security specialists have long predicted an inevitable 'Cyber 9/11' or a 'Cyber Pearl Harbor', a devastating digital attack on critical national infrastructure. Even though the darkest scenarios have not come true, these warnings shaped the perception of conflicts in cyberspace where the only alternative to cyberwar is cyberpeace.[2] However, cyberwar and cyberpeace, although polar opposites, are not binary. An expanse called the grey zone lies between them. Governments, businesses, and citizens face pervasive and unrelenting cyberthreats that would have been hard to imagine a decade ago.

This new paradigm shift in planning future conflicts is reflected in US strategic documents (e.g., *National Security Strategy*, 2017; *DoD Cyber Strategy*, 2018; *National Cyber Strategy*, 2018). All of them state that the US is entering a stage of intense strategic competition in cyberspace, recognizing China and Russia as the most advanced challengers,[3] where the rivalry will take place primarily below the threshold of aggression that would force an armed reaction. Now, the possibility of winning a conflict in peacetime is also pursued through gradual and methodical 'salami tactics', that is, successively achieving a set of political interests. Moreover, according to the Atlantic Council report published in December 2021, the purpose of US strategy should not be *to play Go better, but rather to build a new game and force China and Russia to play the United States' game*.[4] Therefore, aggressive and offensive grey zone activities, which are the actions below the threshold of armed aggression referring to the entire spectrum of possible actions, not only those in cyberspace, are recognized as means for gaining strategic advantage and enhancing the role of US global leadership.

It is argued throughout this article that states are capable – thanks to their activities in the grey zone, especially in its cyber component – to achieve strategic goals effectively, targeting social, economic, and political security, as well as the cohesion of the state, at lower cost than through the use of kinetic conflict. Deterring grey zone tactics in cyberspace poses unique strategic challenges to current US foreign policy, which should work to ensure that the US is in control of key escalation decisions. Taking all the above mentioned into consideration, it is assumed that the decade-old assumptions of a cyber Pearl Harbor[5] were exaggerated. Consequently, states, especially technologically advanced ones, such as the USA, will increasingly use techniques from

[2] Ibid.

[3] C.G. Starling et al., *Seizing the Advantage: A Vision for the Next US National Defense Strategy*, Washington, DC 2021.

[4] Ibid., p. 20.

[5] E. Nakashima, "Cyberattack on Mideast Energy Firms Was Biggest Yet, Panetta Says", *The Washington Post*, 11 October 2012, at https://www.washingtonpost.com/world/national-security/cyberattack-on-mideast-energy-firms-was-biggest-yet-panetta-says/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html, 29 August 2022.

the cyber and non-cyber grey area to achieve their political goals without risking conflict escalation.

The aim of this article is to describe the change of the American approach to conflict management in the grey zone. The focus will be on describing the current state of the concept of the grey zone in US strategic documents, as well as the premises for forecasting the development of the grey zone in the future. An initial analysis of the grey zone activities of the US and its rivals allowed for the adoption of the following research hypotheses: (H1) the grey zone makes it possible to achieve political goals more effectively and at lower cost than through the use of kinetic conflict; (H2) activities in the grey zone may provide a strategic advantage over the opponent, without risking the escalation of the conflict to the level of kinetic aggression; (H3) despite growing activity in building a strategy for operating in the grey zone, the United States still lags behind in this respect. Therefore, responding to new competition below the threshold of aggression with China and Russia, the US government needs to take more definite actions in the grey zone.

This paper will proceed as follows: the first section defines the term 'grey zone' and explains its importance, with special emphasis on cyber tools in this area, to provide the theoretical framework for further considerations. The second section describes the US's strategic goals and tactics in the grey zone, drawing an overall picture of the American shift in cybersecurity policy since Donald Trump's presidency. The third part deals with the problem of competition between great powers in the grey zone.

GREY ZONE AND CYBER GREY ZONE

'Grey zone' activities of a state are not a new concept. Most generally, they refer to situations in which states intentionally make their hostile activities difficult to interpret on the basis of international law in order to impede the international community in assigning responsibility to a wrongdoer.[6] Due to the ambiguity of the actions taken and the hidden targets of the attacker, it is difficult to consider specific grey zone activities in terms of the international law concepts of the 'use of force' and 'aggression'. In other words, grey zone activities are a type of phenomenon that fulfils neither the definition of 'war' nor of 'peace'. They are conducted in ambiguous ways, using information operations, political coercion, economic coercion, cyber operations, proxy support, and provocation by state-controlled forces to such a degree that the actor or intent are veiled.

The literature on this subject is rich in terms describing actions below the threshold of armed aggression, referring to the entire spectrum of possible actions, for example,

[6] A. Kleczkowska, "Explaining the Meaning of 'Grey Zones' in Public International Law Based on the Example of the Conflict in Ukraine", *Contemporary Central & East European Law*, no. 1(133) (2019), p. 76.

the *grey zone between war and peace*,[7] *non-war military activities*,[8] *unpeace*,[9] *warfare during peacetime*,[10] *subliminal aggression*,[11] or *persistent cyberspace confrontation*.[12] The broad and exhaustive definition of the 'grey zone' is that offered by the RAND Corporation, explaining it as *an operational space between peace and war, involving coercive actions to change the* status quo *below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events*.[13] The definition highlights three main features of grey zone activities. Firstly, the goal of all activities is to avoid open conflict and serious clashes. Secondly, the definition underlines the incremental nature of actions taken, which prevents the determination of the conflict threshold. And lastly, the problem with assigning responsibility for an attack is even more prominent due to its greater anonymity, which makes it possible to hide the source of the attack, or at least raise doubts about it. Such tactics delay or block the attacked country's response. In this sense, the Crimea operation in 2014, when Russia sent professional soldiers in Russian-style combat uniforms but without identifying insignia (i.e., 'little green men') to conduct the hostile operation, is a striking exemplification of this definition. Russia firmly denied any Russian soldiers were involved in Crimea and claimed they were 'local self-defense units', only to admit later that the Russian Army was there indeed.[14]

It is worth noting that the concept of grey zone conflict differs from the concept of hybrid conflict (also referred to as **hybrid warfare**). The latter was developed in

[7] G. Popp, S. Canna, *The Characterization and Conditions of the Gray Zone. A Virtual Think Tank Analysis (ViTTa)*, Boston, MA 2016, at http://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTTa-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf, 11 February 2022; L.J. Morris et al., *Gaining Competitive Advantage in the Gray Zone. Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica, CA 2019.

[8] United States Department of Defense, *Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress*, at https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF, 9 February 2022.

[9] L. Kello, *The Virtual Weapon and International Order*, New Haven 2017.

[10] S. Takashi, "Maritime Security Study Group Research Progress Report. Increasingly Complex and Sophisticated 'Hybrid Warfare' during Peacetime: Japan's Comprehensive Response and the Japan-US Response", *NPI Research Note*, 11 September 2020, at http://www.iips.org/en/research/NPI_Research_Note_20201005.pdf, 20 October 2021; J. van de Velde, "Make Cyberspace Great Again Too!", Real Clear Defence, 23 July 2018, at https://www.realcleardefense.com/articles/2018/07/23/make_cyberspace_great_again_too_113634.html, 3 February 2022.

[11] „Agresja podprogowa" [subliminal agression], in National Security Bureau, "(Mini)słownik BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa", at https://docplayer.pl/21264635-Mini-slownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, 20 February 2022.

[12] G. Casey, "Remarks at the National Press Club", U.S. Army, 14 August 2007, at https://www.army.mil/article/4436/aug_14_2007_remarks_at_the_national_press_club, 10 January 2022.

[13] L.J. Morris et al., *Gaining Competitive Advantage...*, p. 8.

[14] S. Pifer, "Crimea: Six Years after Illegal Annexation", The Brookings Institution, 10 March 2020, at https://www.brookings.edu/blog/order-from-chaos/2020/03/17/crimea-six-years-after-illegal-annexation/, 3 March 2022.

American military strategic studies by the US Marine Corps Lieutenant Colonel Frank G. Hoffman in 2006 and was driven by an awareness of the increasing complexity of conflicts, in terms of the number and kinds of belligerents and the tools available for them, in which the US and its allies have been involved with since the 9/11 attacks.[15] The concept of hybrid warfare is understood as the space-time coexistence of several different generations of wars, which intersect, interpenetrate, and confront each other on the battlefield or in operations other than war, and which rely on a combination of both kinetic and non-military tools.[16] However, the grey zone which encompasses defensive and offensive activities, may involve only unconventional techniques, that is, cyber operations, facilitating a situational ambiguity which states use to their advantage.[17] In contrast to hybrid warfare, actions taken in the grey zone of a conflict do not clearly cross the threshold of war, which is due to the ambiguity of international law and the ambiguity of actions and attack attribution. Therefore, grey zone operations *are aimed at undermining the security of the target state but without triggering active armed conflict*.[18]

Considering that there is always a risk of escalating a grey zone conflict to a conventional conflict, as the links between the perceived effects and the threats are loose and may be different for each country,[19] to some extent managing conflict and maintaining it at the desired level is possible.[20] Grey zone activities are approached with an effect-based logic.[21] This means that the key issue in determining how a country will respond to an attack is the effect of such an event.[22] And the cause may be completely irrelevant. Any serious attacks can be interpreted as 'armed aggression' and justify the use of force in self-defense.[23] An example is the tense situation between China, the US, and the countries involved in territorial disputes in the South China Sea. If the tensions

[15] D. Belo, D. Carment, *Grey-Zone Conflict: Implications for Conflict Management*, Calgary 2019.

[16] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, VA 2007.

[17] D. Belo, D. Carment, *Grey-Zone Conflict...*

[18] C.G. Starling et al., *Seizing the Advantage...*

[19] M.C. Libicki, *Crisis and Escalation in Cyberspace*, Santa Monica, CA 2012.

[20] It is worth mentioning that in many studies escalation is described as an 'escalation ladder' of changes in conflict intensity. However, a new approach, which characterizes cyber escalation as a lattice, has been offered by Martin C. Libicki and Olesya Tkacheva. They argue that in *cyberspace the distinction between the escalatory and de-escalatory use of cyber capabilities is less straightforward* [...] *allowing horizontal spill over to other domains as well as vertical movement that corresponds to greater intensity of conflict*. M.C. Libicki, O. Tkacheva, "Cyberspace Escalation: Ladders or Lattices?", in A. Ertan et al. (eds), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn 2020, pp. 60-73, at https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf, 10 January 2022.

[21] H. Farrell, Ch.L. Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine", *Journal of Cybersecurity*, vol. 3, no. 1 (2017), pp. 7-17.

[22] W.A. Owens, K.W. Dam, H.S. Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, DC 2009, pp. 356-368.

[23] M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Tallinn 2017.

resulting from these disputes escalated to the point of risking a kinetic conflict, then, for example, any serious cyber incident, such as a DDoS attack on critical infrastructure, could be interpreted by one of the participants in the conflict as an *opening shot*, leading to the outbreak of war.[24] Therefore, the strategy responding to the grey zone aggression must *balance the risk of escalation with the reality that, to be effective, countering grey zone aggression demands some degree of risk tolerance*.[25] Also, states need to ensure that the implemented grey zone tactics help to keep the key escalation decision on their side.[26]

Although the 'grey zone' reflects an age-old approach, its contemporary uses, most profoundly in cyberspace, offer a wide range of new applications. Cyber operations have been conducted as a part of ongoing conflicts; however, the vast majority of them are taking place in the grey zone, making it possible to achieve political goals more effectively and at lower costs than through the use of kinetic conflict. Therefore, grey zone cyber activities may allow for a strategic advantage over an opponent, without seriously risking the escalation of the conflict to the level of military aggression. This is due to the specific features of cyberspace, like its borderlessness, aterritoriality, and difficulty of attack attribution. The latter makes the grey zone an especially attractive environment for competition between states. Without proper attribution, accountability within the international space cannot be guaranteed. As Rid and Buchanan articulate, despite the increasing advancement in tracking cyberattacks, source determination is still a slow, multi-step process that rarely provides certainty as to the source of an attack.[27] Due to the lack of a single standardized attribution methodology,[28] achieving an 'almost certain' or 'nearly certain' analytic assessment is almost impossible, and uncertainty regarding the origin of an attack can only be minimized. This is corroborated by the 2018 Office of the Director of National Intelligence (ODNI) "Guide to Cyber Attribution",[29] which states that *no simple technical process or automated solution for determining responsibility for cyber operations exists. The painstaking work in many cases requires weeks or months of analyzing intelligence and forensics to assess culpability. In some instances, the* [intelligence community] *can establish cyber attribution within hours of an incident, but the accuracy and confidence of the attribution will vary depending on available data*.[30] This is in line with the results of a recently published analysis of more than 200 cybersecurity incidents related to

[24] M.C. Libicki, *Crisis and Escalation...*

[25] L.J. Morris et al., *Gaining Competitive Advantage...*

[26] R.W. Maass, "Salami Tactics: Faits Accomplis and International Expansion in the Shadow of Major War", *Texas National Security Review*, vol. 5, no. 1 (Winter 2021-2022).

[27] T. Rid, B. Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies*, vol. 38, no. 1-2 (2015), pp. 4-37.

[28] J.S. Davis II et al., *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monica, CA 2017.

[29] Office of the Director of National Intelligence, "A Guide to Cyber Attribution", 14 September 2018, at https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf, 2 February 2022.

[30] Ibid.

the activities of nation states since 2009.[31] Every other attack was conducted using simple scripts that can be easily purchased on the darknet. For an additional 20%, attackers applied slightly more advanced, custom-made cyber-weapons that exploit known vulnerabilities. The remaining 30% of the analyzed cases involved the use of sophisticated tools, difficult to backtrack and examine. They leave behind very few clues for investigators and are virtually impossible to attribute, if applied properly.

AMERICAN (CYBER) GREY ZONE STRATEGY

The American awareness of and preparations for the new challenges of strategic competition, which largely occurs below the threshold of armed conflict, is growing. However, it is just an early stage of recognizing how grey zone competitors operate. The 2017 National Security Strategy (*National Security Strategy*, 2017), the 2018 Department of Defense Cyber Strategy (*DoD Cyber Strategy*, 2018) and the National Cyber Strategy (*National Cyber Strategy*, 2018) all say that the US is entering a stage of intense strategic competition in the cyber grey zone, with Russia and China being its biggest rivals. Also, numerous statements by senior US officials clearly show the rivalry will take place primarily below the threshold of aggression that would force an armed reaction.[32] This is a completely new understanding of conflict by the US authorities, because traditionally, risks were considered mainly in categories of losing a kinetic conflict. Now, the possibility of winning a conflict in peacetime is also considered through the aforementioned 'salami tactics'. At this point in time, the US *has the capability to be a formidable and effective grey zone actor but does not yet have a plan to employ or integrate its capabilities to achieve its objectives*.[33] A promising step towards creating such a plan is *The Interim National Security Strategic Guidance* that sheds light on the strategic risks that grey zone threats pose to the United States. According to Biden's strategic assumptions, focusing on where and how grey zone competition is unfolding, the US needs to develop capabilities to better compete and deter grey zone actions, taking a more active posture to maintain US influence.[34]

This shift in thinking about conflict is particularly evident in the new vision of US-CYBERCOM.[35] It presents a detailed action plan to keep the US ahead in cyberspace.

[31] M. McGuire, "Nation States, Cyberconflict and the Web of Profit", HP Development Company, 2021, at https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf, 8 February 2022.

[32] L.J. Morris et al., *Gaining Competitive Advantage...*

[33] J. Schaus, "Competing in the Gray Zone", Center for Strategic and International Studies, 24 October 2018, at https://www.csis.org/analysis/competing-gray-zone-0, 20 February 2022.

[34] The White House, *The Interim National Security Strategic Guidance*, March 2021, at https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf, 20 February 2022.

[35] United States Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, April 2018, at https://www.cybercom.mil/Portals/56/Documents/US CYBERCOM%20Vision%20April%202018.pdf, 1 December 2022.

According to this document, the Department of Defense is taking a more decisive approach to protecting American networks, which is a significant difference from the previous way of thinking about the nation's cybersecurity. It acknowledges the fact that most cyber operations are deliberately below the threshold of 'armed aggression' and that cyberspace is an area of constant competition. In this 'new normality', opponents expand their influence without resorting to physical aggression, that is, they provoke and intimidate without fear of legal or military consequences. In addition, the Department of Defense questions the effectiveness of passive deterrence in cyberspace.[36] Consequently, USCYBERCOM will prioritize offensive actions to challenge the enemy's capabilities through continuous, integrated operations. Such constant activity forces opponents to first reduce the scale, and thus – the effects, of their malicious actions – because it is impossible to stop or prevent all undesirable acts; and second, to shift resources to limit and defend against the US attacks.

In particular, this new strategic approach is evident in the new concept of 'persistent engagement'. As explained in the USCYBERCOM strategic vision: *Superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver. It describes how we operate – maneuvering seamlessly between defense and offense across the interconnected battlespace. It describes where we operate – globally, as close as possible to adversaries and their operations. It describes when we operate – continuously, shaping the battlespace. It describes why we operate – to create operational advantage for us while denying the same to our adversaries*.[37] In other words, the approach to securing US national interests through *persistent engagement* means that the US seeks to anticipate and exploit its opponents' weaknesses, while undermining their offensive capabilities. The United States will consistently confront its opponents in cyberspace, rather than waiting for them to attack US networks. This is also an announcement that USCYBERCOM will be everywhere, all the time and in all ways, continually monitoring foreign networks for malicious activities. Therefore, the United States must adopt the concept of 'victory in a time of peace'.[38] This means that US activities will focus primarily on offensive actions that cannot be called 'war', but which involve violating the sovereignty and interests of other states.

Persistent engagement is the 'strategic umbrella' underneath which the 'defend forward' concept exists, that is, defense going beyond only American networks and fighting threats before they reach the USA.[39] The Department of Defense's cyberstrategy articulated a clear confirmation of the continuation of the 'offensive step forward' in

[36] United States Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, 11 February 2022.

[37] United States Cyber Command, *Achieve and Maintain…*

[38] J. van de Velde, "Make Cyberspace…".

[39] J.G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy", Lawfare, 10 May 2019, at https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy, 13 February 2022.

cyberspace operations. As explained: *Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins*.[40] Previously, it was thought that opponents were too often dealt with inside of US networks, rather than being stopped from entering them. Therefore, the new approach allows USCYBERCOM to leave the Department of Defense networks and to attack opponents in their own networks. The DoD cyberstrategy concludes that since US cyber forces are in *persistent engagement* with adversaries, then it is imperative for them to *defend forward* and to *continuously contest* opponents.[41] Defend forward is the clearest manifestation of the fact that the US recognizes that cyber threats *do not merely take the form of discrete events but are also continuous operations that must be defended against in real time*.[42]

Both *persistent engagement* and *defend forward* is a rejection of the strategy promoted by Barack Obama in which cyberspace was treated as a common good.[43] Deterrence in cyberspace has been recognized as pointless and unreliable, and therefore, a more aggressive approach to defending one's own networks is a better alternative to Obama's restraint. It can be assumed that the consequences of the new US cybersecurity policy may be twofold. Either, thanks to operations in cyberspace, it is possible to limit kinetic activities in the three basic dimensions of warfare, that is, keeping them below the threshold which, if exceeded, would necessitate an armed response, or the US 'pre-emptive defense' will meet a resolute, kinetic response from a hostile country. However, the big data analyses, survey experiments, and war games indicate that escalation to armed conflict is fairly impossible, as the *individuals feel differently about cyberspace than other means of competition or conflict – a conclusion that largely supports the ideas behind persistent engagement*.[44] However, the Department of Defense should put more work into understanding what types of attack targets or outcomes may inadvertently lead to an escalation of a conflict beyond cyberspace. This will require significant investment in technical solutions and acquiring cyber talents.

As the Biden administration prepares to release its National Defense Strategy, in 2019 the US Joint Chiefs (JCS) introduced the concept of the *competition continuum* which *describes a world of enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict*.[45] In other words, waiting for

[40] United States Cyber Command, *Achieve and Maintain...*, p. 6.

[41] J. Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace", *Journal of Cybersecurity*, vol. 5, no. 1 (2019).

[42] J. Kosseff, "The Contours of 'Defend Forward' Under International Law", 11th International Conference on Cyber Conflict (CyCon), Tallinn 2019, p. 4, at https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf, 2 March 2022.

[43] The White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, May 2011, at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 20 February 2022.

[44] J.G. Schneider, "Persistent Engagement...".

[45] JCS, *Joint Doctrine Note 1-19. Competition Continuum*, Washington, DC, 3 June 2019, at https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf, 3 March 2022.

a response to an event after it has occurred is too late. Forces must be constantly engaged in activities against enemies to contest their activities and gather the appropriate intelligence and access in the event of an escalating circumstance.[46] However, while today the DoD is comfortable deterring and preparing for conventional conflict, it is much less experienced in competing in the grey zone. As the recent Atlantic Council report states, *this needs to change*[47] as the US has no desire for war. Therefore, if the DoD underinvests in developing below-threshold conflict capabilities, then it may lose a strategic advantage over its rivals. In other words, *resourcing below-threshold conflict is key and requires a different approach to the DoD's largely capabilities-based strategy*.[48]

Nowadays, the grey zone is becoming more and more crowded, because countries such as China or Russia more and more often use both cyber and non-cyber tools to overcome the strengths of the USA in global diplomacy, law, and commerce. It is no surprise that this new grey zone competition is tough and unsettling for the United States who used to dominate. Moreover, *competition in the grey zone is an underdeveloped area of US strategy, planning and synchronization of action, despite its wealth of advantages*.[49] Whereas *grey zone actions don't just happen*, and *are not those of tactical commanders freelancing*, they should be purposefully constructed to avoid kinetic clashes.[50]

GREAT POWER GAMES IN A (CYBER) GREY ZONE

A review of the state of the art has shown that competition below the threshold of armed aggression is constantly gaining in importance. The emphasis on activities in the grey zone appears not only in American strategic documents, but also in those of their biggest rivals – Russia and China,[51] as well as in national security strategies of other countries, including Australia, Germany, Great Britain, and Indonesia.

For example, the Chinese People's Liberation Army divides military operations into two categories: war and non-war.[52] The concept of non-war military activities

[46] J. Gould, M. Pomerleau, "Why the US Should Fight Russia, China in the »Gray Zone«", *Navy Times*, 4 January 2022, at https://www.navytimes.com/information-warfare/2022/01/04/why-the-us-should-fight-russia-china-in-the-gray-zone/?contentFeatureId=f0fmoahPVC2AbfL-2-1-, 2 March 2022.

[47] C.G. Starling et al., *Seizing the Advantage…*

[48] Ibid.

[49] Center for International and Strategic Studies, "Gray Zone Project", at https://www.csis.org/programs/gray-zone-project, 3 March 2022.

[50] P. Layton, "Bringing the Grey Zone into Focus", *The Interpreter*, 22 July 2021, at https://www.lowyinstitute.org/the-interpreter/bringing-grey-zone-focus, 28 February 2022.

[51] F. Gaoyue, J. Char, *Introduction to China's Military Operations Other Than War*, Singapore 2019, at https://www.rsis.edu.sg/wp-content/uploads/2019/02/PR190225_Introduction-to-Chinas-Military-Operations-Other-than-War.pdf, 2 January 2022; Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations*, 11 August 2011, at https://www.hsdl.org/?view&did=685338, 22 September 2021.

[52] United States Department of Defense, *Military and Security Developments…*

(NWMA) is a vast and diverse set of military operations conducted internationally or domestically, covering many areas. China is calibrating its coercive actions so that it does not exceed the threshold of sparking an open conflict with the United States. In other words, they are attacking in cyberspace with varying intensity and duration. Such actions may include threats of violence or the use of low-level force, up to levels approaching war. Non-war operations are seen in the PRC as an effective way to support and protect China's development, as well as a way to expand the global interests of the PRC and gain valuable operational experience. The United Nations maritime entitlements case in the South China Sea in 2013 is probably the best exemplification of a Chinese grey zone campaign. In a meticulously timed sequence, surrounding the islands layer by layer, firstly by sending fishing ships into disputed territory, then fisheries' patrol vessels, then Coast Guard ships and PLA Navy warships, to cut off the island from outside support, China applied a deliberate, gradual pressure which limited the risk of escalation. A few years later, the arsenal of Chinese grey zone tools was enriched with new activities, for example, a systematic cyber and cognitive warfare campaign including espionage, misinformation, and subversive efforts to signal its ability to digitally sabotage. All these activities are operating in conjunction with social media campaigns, radio misdirection, cyber warfare, and GPS interference.[53]

Concepts of the grey zone similar to those in China are also being developed in the Russian Federation. The previous phase of conflict in Ukraine was a testing ground for Russian hostile activities in the grey zone.[54] The hostile activities that took place in Ukraine between 2014 and 24 February 2022 included a hybrid strategy, the basis of which was an ambiguity of actions that lulled western countries into a state of lessened vigilance. As John McLaughlin, the former deputy director of the Central Intelligence Agency (CIA), tweeted: *Putin has choreographed this with the hope that we and the Europeans will debate whether this is an 'invasion' or not. And hoping that throws us enough off balance that he will pay a minimal price for this first slice of salami.*[55] Moscow used conventional forces, but the very 'rules of war' have changed.[56] The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of weapons in their effectiveness.[57] These grey-zone level cybertools, from ongoing mis- and disinformation, informational propaganda, election

[53] P. Layton, "Bringing the Grey Zone...".

[54] M. Smith, "Russia Has Been at War with Ukraine for Years – in Cyberspace", *The Conversation*, 7 February 2022, at https://theconversation.com/russia-has-been-at-war-with-ukraine-for-years-in-cyberspace-176221, 17 February 2022.

[55] J. McLaughlin, Twitter, 22 February 2022, at https://twitter.com/jmclaughlinSAIS/status/1495931329447407621, 25 February 2022.

[56] 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, 22 February 2022.

[57] As Gerasimov explained in his famous speech, in modern conflict, non-military methods are used in a 4:1 ratio to military methods. V. Gerasimov, "The Value of Science...".

interference in 2014,[58] cyberattacks on critical infrastructure in 2015,[59] to a cyberattack that targeted Ukraine's ministries and banks in February 2022,[60] were a form of limited military competition that simmers chronically beyond peace but remains short of full-scale war.[61] Therefore, the Russia-Ukraine conflict until 24 February 2022 was a perfect example of well-tailored salami tactics, offering an attractive option for expansionist powers in the shadow of major war.

It can be noted that the grey zone has been a panacea for Russian aspirations at least since Euromaidan. This was due to the fact that Russia's conventional military power lags behind that of the United States and NATO in size and technological sophistication. As a result, Russians used tools – both military and non-military, which should make it possible to prevent a conflict or deteriorate into further aggression. Moreover, by making the conflict politically ambiguous and by conducting small-scale hostilities, foreign observers were kept uncertain about upcoming developments. Thus, until February 2022, the use of force was calibrated in such a way as to deter opponents from taking further actions. The catalogue of traditional non-military de-escalation tools, used prior to the use of military means – such as economic, information or political pressure – has been successfully expanded to include the tools of cyberspace.

In a recent CSIS report, its experts stated that *leaders in Moscow recognize they are not powerful enough to entirely displace the international order, so they instead seek to disrupt it at every viable opportunity, primarily because they perceive the democratic values espoused by that order as an existential threat*.[62] This turned out to be only half-true as Russia decided that its grey zone strategy was not enough to satisfy its great power aspirations and consequently decided to initiate the military invasion of Ukraine on 24 February 2022. Attacking Ukraine was a clear message to world leaders that what had been the current world order is now officially over. According to some experts, for Russia grey zone conflict was *a second-best option, a half-hearted way of pursuing foreign policy goals while avoiding risky consequences*.[63] However, despite Putin's global

[58] The NATO Cooperative Cyber Defence Centre of Excellence, "Ukrainian Parliamentary Election Interference (2014)", at https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014), 20 January 2022.

[59] 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/, 16 February 2022.

[60] L. Harding et al., "Ukraine Fighting to Stop 'a New Iron Curtain' after Russian Invasion", *The Guardian*, 24 February 2022, at https://www.theguardian.com/world/2022/feb/24/russia-attacks-ukraine-news-vladimir-putin-zelenskiy-russian-invasion, 25 February 2022.

[61] D. Barno, N. Bensahel, "Fighting and Winning in the »Gray Zone«", War on the Rocks, 19 May 2015, at https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/, 13 February 2022.

[62] C.G. Starling et al., *Seizing the Advantage*...

[63] J.A. Gannon et al., "Why Did Russia Escalate Its Gray Zone Conflict in Ukraine?", Lawfare, 16 January 2022, at https://www.lawfareblog.com/why-did-russia-escalate-its-gray-zone-conflict-ukraine, 20 February 2022.

aspirations, the events of the first days of the war (as of 3 March 2022) – the transition to military operations – might be perceived as a bad move. The Russians miscalculated the determination and military preparedness of Ukraine, which markedly improved owing to better weapons, training, significant experience, and massive lethal and non-lethal defensive American aid (the total security assistance the United States has committed to Ukraine in 2021 alone is more than 1 billion USD[64]). Therefore, it can be questioned whether Russia made the right decision to leave the grey zone and start a regular war, since its achievements below the threshold of aggression, mainly via aggressive cyber and information operations, had been significant.[65]

The US National Defense Strategy 2018 reoriented the US focus towards great-power competition. The document highlights *an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations*.[66] Despite the fact that Russia is perceived by the US as a serious source of threats, the US prioritized its efforts to compete with and deter China, which by far is *the most concerning long-term strategic threat*.[67] Beijing is heavily investing in modernizing its military, for example, by building the world's largest navy, and it plans to increase its nuclear warhead stockpile, while Russia is not thought to be powerful enough to displace the international order. While Vladimir Putin's recent invasion of Ukraine has upended assumptions about the sanctity of borders and thrown the world into a whole new situation, the real actions taken in Ukraine depreciate the importance of Russia as a military power. At this point in time, it is not possible to predict how this conflict will end. However, as the main goal for both China and Russia is to weaken the US-led liberal order, there is a risk of the Chinese publicly supporting Russia for the sake of its larger political objectives, making the conflict in Ukraine even more dramatic, and eventually the global order may change.[68]

Both China and Russia have been engaged in competition in the grey zone with the United States for years, albeit in different ways. However, the strategic goals of these states are different. For Beijing, the main goal is to remake the international order with

[64] A.J. Blinken, "Additional Military Assistance for Ukraine", U.S. Department of State, 26 February 2022, at https://www.state.gov/additional-military-assistance-for-ukraine/, 26 February 2022.

[65] Some well-recognized examples of cyberattacks orchestrated by Russian hackers include targeting three Ukrainian regional power distribution companies at the end of 2015, again in December 2016, and once more in June 2017. The blackouts in Ukraine were just one part of a series of events destabilizing practically every sector of Ukraine: the media, finance, transportation, military, politics, and energy. Despite Ukraine being the vastest test ground for Russian grey zone activities, Russian interference in Western democratic countries is also evident. Russian interference in democratic elections, its promotion of mis- and disinformation, cyber propaganda and many more examples prove its engagement in developing grey zone tools.

[66] United States Department of Defense, *The National Defense Strategy (NDS) NDS 2018*.

[67] C.G. Starling et al., *Seizing the Advantage...*

[68] V. Ni, "China Ponders How Russia's Actions in Ukraine Could Reshape World Order", *The Guardian*, 25 February 2022, at https://www.theguardian.com/world/2022/feb/25/china-ponders-how-russia-actions-ukraine-reshape-world-order, 26 February 2022.

China as the preeminent state actor by displacing the US as the world's leading power, while securing the regime internally and preventing other states from interfering in the Indo-Pacific region. Unlike China, which can realistically change the international balance of power, Russia is aware that it cannot accomplish this. However, they want to restore the old spheres of influence, among other things, by fighting democratic values. Despite the methods and tools applied, the grey zone attacks of Russia and China are becoming more and more sophisticated. At the same time, the Department of Defense is not doing enough to compete with the most advanced rivals. Paul Stockton, former Assistant Secretary of Defense for Homeland Defense is of the opinion that the US has *fallen short of accounting for the risk that China and Russia will conduct hybrid warfare-style operations against the United States itself* […]. *I'm not talking about little green men pouring across our borders — that'll never happen — but the use of combined information and cyberattacks to disrupt U.S. defense operations at home*.[69] In just this way, Russian hackers attacked Ukraine, Estonia, Georgia, and the US elections in 2016. Also, that was how China created and fortified artificial island bases in the South China Sea and how Chinese hackers stole billions of dollars in US trade secrets. And they were doing it without much of an effective US response.[70]

CONCLUSIONS

The events following Russian authorization of a *special military operation* in Ukraine on 24 February 24 2022 are an evident proof that cyber Pearl Harbor is not coming. The forces engaged in war on both sides are using cyberspace solely to exert influence and support conventional operations; what denotes this domain is not treated as an entirely separate component of a multi-faceted conflict environment that also includes land, sea, air, and space. Therefore, activities in cyberspace are more likely to be rather a description of operational activities than a decisive strategic confrontation.[71] In other words, it is more likely that the hostile activities in cyberspace and grey zone activities outside of cyberspace will take the form of low-level interstate conflict, in which the normative understanding of what constitutes unacceptable, aggressive behavior is much less clear. This requires actions that are *purposefully constructed to side-step military escalation – crafted as a form of carefully scripted brinkmanship*,[72] which may bring exceptional benefits from the grey zone as an operational domain.

[69] J. Gould, M. Pomerleau, "Why the US Should Fight Russia…".

[70] S.J. Freedberg Jr., "Cyber Warfare in The Grey Zone: Wake Up Washington", Breaking Defense, 9 April 2019, at https://breakingdefense.com/2019/04/cyber-warfare-in-the-grey-zone-wake-up-washington/, 19 February 2022.

[71] *Report: Military Operations in Cyberspace. Wednesday 5-Friday 7 September 2018. WP1635*, Wilton Park, at https://www.wiltonpark.org.uk/wp-content/uploads/2020/09/WP1635-Report.pdf, 23 October 2021.

[72] P. Layton, "Bringing the Grey Zone…".

The global balance of power has changed dramatically in the past two decades. While the US military was focused on the Middle East, two other cyber-powers, Russia and China, focused on great power competition, making huge efforts to develop grey zone capabilities, most significantly those in cyberspace. Although the actions of the US government in recent years have shown the importance of the grey zone, it is widely believed that the US is insufficiently prepared and poorly organized to compete in this space.[73] Joe Biden's recent grey-zone gaffe only highlighted a real dilemma: *no country or alliance has yet mustered an effective strategy for responding to grey-zone aggression*,[74] exposing American unpreparedness for grey-zone confrontation. However, to the surprise of many political commentators, the Biden administration has largely followed Trump's lead, keeping US policy toward its global rivals on a more confrontational level.[75] This was inherited from the previous administration with strategic concepts such as 'defend forward' and 'persistent engagement', and it seems he will actively use them to confirm American domination. Accordingly, as the United States has no desire for war, there is a growing awareness that the DoD needs to compete with China and Russia by engaging in offensive actions in primarily the grey zone by applying strategies that are *joint, combined, and across all domains*.[76]

These efforts, accompanied by heavy investments in below-threshold capabilities, ought to support the US's aspirations of great power competition and focus on countering malign Chinese and Russian activities. Therefore, Biden's long-awaited National Defense Strategy should precisely formulate specific goals, actions, and implementation guidelines to increase the potential of better competing with and deterring grey zone actions. In that sense, the principles from The Interim National Security Strategic Guidance on Competing in the Gray Zone[77] signal that his administration is going to treat this area seriously. That is a good indicator, since regardless of our moral appraisal of this area, the *gray is here to stay*.[78]

[73] L.J. Morris et al., *Gaining Competitive Advantage...*

[74] E. Braw, "Biden's Gray-Zone Gaffe Highlights a Real Dilemma", Defense One, 20 January 2022, at https://www.defenseone.com/ideas/2022/01/bidens-gray-zone-gaffe-highlights-real-dilemma/360982/, 22 February 2022.

[75] J. Rogin, "Biden Doesn't Want to Change China. He Wants to Beat It", *The Washington Post*, 10 February 2022, at https://www.washingtonpost.com/opinions/2022/02/10/biden-china-strategy-competition/, 21 February 2022.

[76] L.J. Morris et al., *Gaining Competitive Advantage...*

[77] The White House, The Interim National Security Strategic Guidance on Competing in the Gray Zone, March 2021, at https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf, 2 December 2022.

[78] K. Bilms, "Gray is Here to Stay: Principles from The Interim National Security Strategic Guidance on Competing in The Gray Zone", Modern War Institute, 25 March 2021, at https://mwi.usma.edu/gray-is-here-to-stay-principles-from-the-interim-national-security-strategic-guidance-on-competing-in-the-gray-zone/, 3 March 2022.

BIBLIOGRAPHY

Barno D., Bensahel N., "Fighting and Winning in the »Gray Zone«", War on the Rocks, 19 May 2015, at https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/.

Belo D., Carment D., *Grey-Zone Conflict: Implications for Conflict Management*, Calgary 2019.

Bilms K., "Gray is Here to Stay: Principles from The Interim National Security Strategic Guidance on Competing in The Gray Zone", Modern War Institute, 25 March 2021, at https://mwi.usma.edu/gray-is-here-to-stay-principles-from-the-interim-national-security-strategic-guidance-on-competing-in-the-gray-zone/.

Blinken A.J., "Additional Military Assistance for Ukraine", U.S. Department of State, 26 February 2022, at https://www.state.gov/additional-military-assistance-for-ukraine/.

Braw E., "Biden's Gray-Zone Gaffe Highlights a Real Dilemma", Defense One, 20 January 2022, at https://www.defenseone.com/ideas/2022/01/bidens-gray-zone-gaffe-highlights-real-dilemma/360982/.

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

Center for International and Strategic Studies, "Gray Zone Project", at https://www.csis.org/programs/gray-zone-project.

Davis II J.S. et al., *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monica, CA 2017, https://doi.org/10.7249/RR2081.

Farrell H., Glaser Ch.L., "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine", *Journal of Cybersecurity*, vol. 3, no. 1 (2017), pp. 7-17, https://doi.org/10.1093/cybsec/tyw015.

Freedberg S.J., "Cyber Warfare in The Grey Zone: Wake Up Washington", Breaking Defense, 9 April 2019, at https://breakingdefense.com/2019/04/cyber-warfare-in-the-grey-zone-wake-up-washington/.

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

Gaoyue F., Char J., *Introduction to China's Military Operations Other Than War*, Singapore 2019, at https://www.rsis.edu.sg/wp-content/uploads/2019/02/PR190225_Introduction-to-Chinas-Military-Operations-Other-than-War.pdf.

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.

Gordon S., Rosenbach E., "America's Cyber-Reckoning: How to Fix a Failing Strategy", *Foreign Affairs*, vol. 101, no. 1 (2022), pp. 10-20.

Gould J., Pomerleau M., "Why the US Should Fight Russia, China in the »Gray Zone«", *Navy Times*, 4 January 2022, at https://www.navytimes.com/information-warfare/2022/01/04/why-the-us-should-fight-russia-china-in-the-gray-zone/?contentFeatureId=f0fmoahPVC2AbfL-2-1-.

Harding L. et al., "Ukraine Fighting to Stop 'a New Iron Curtain' after Russian Invasion", *The Guardian*, 24 February 2022, at https://www.theguardian.com/world/2022/feb/24/russia-attacks-ukraine-news-vladimir-putin-zelenskiy-russian-invasion.

Healey J., "The Implications of Persistent (and Permanent) Engagement in Cyberspace", *Journal of Cybersecurity*, vol. 5, no. 1 (2019), https://doi.org/10.1093/cybsec/tyz008.

Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, VA 2007.

JCS, *Joint Doctrine Note 1-19. Competition Continuum*, Washington, DC, 3 June 2019, at https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf.

Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations*, 11 August 2011, at https://www.hsdl.org/?view&did=685338.

Kello L., *The Virtual Weapon and International Order*, New Haven 2017, https://doi.org/10.2307/j.ctt1trkjd1.

Kleczkowska A., "Explaining the Meaning of 'Grey Zones' in Public International Law Based on the Example of the Conflict in Ukraine", *Contemporary Central & East European Law*, no. 1(133) (2019), pp. 75-93, https://doi.org/10.37232/cceel.2019.07.

Kosseff J., "The Contours of 'Defend Forward' Under International Law", 11th International Conference on Cyber Conflict (CyCon), Tallinn 2019, at https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf.

Layton P., "Bringing the Grey Zone into Focus", *The Interpreter*, 22 July 2021, at https://www.lowyinstitute.org/the-interpreter/bringing-grey-zone-focus.

Libicki M.C., *Crisis and Escalation in Cyberspace*, Santa Monica, CA 2012, https://doi.org/10.7249/MG1215.

Libicki M.C., Tkacheva O., "Cyberspace Escalation: Ladders or Lattices?", in A. Ertan et al. (eds), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn 2020, at https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf.

Maass R.W., "Salami Tactics: Faits Accomplis and International Expansion in the Shadow of Major War", *Texas National Security Review*, vol 5, no. 1 (Winter 2021/2022), https://doi.org/10.15781/eyt5-2k84.

McGuire M., *Nation States, Cyberconflict and the Web of Profit*, HP Development Company, 2021, at https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf.

McLaughlin J., Twitter, 22 February 2022, at https://twitter.com/jmclaughlinSAIS/status/1495931329447407621.

Morris L.J. et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica, CA 2019, https://doi.org/10.7249/RR2942.

Nakashima E., "Cyberattack on Mideast Energy Firms Was Biggest Yet, Panetta Says", *The Washington Post*, 11 October 2012, at https://www.washingtonpost.com/world/national-security/cyberattack-on-mideast-energy-firms-was-biggest-yet-panetta-says/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html.

National Security Bureau, "(Mini)słownik BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa", at https://docplayer.pl/21264635-Mini-slownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html.

Ni V., "China Ponders How Russia's Actions in Ukraine Could Reshape World Order", *The Guardian*, 25 February 2022, at https://www.theguardian.com/world/2022/feb/25/china-ponders-how-russia-actions-ukraine-reshape-world-order.

Office of the Director of National Intelligence, "A Guide to Cyber Attribution", 14 September 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

Owens W.A., Dam K.W., Lin H.S. (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, DC 2009, https://doi.org/10.17226/12651.

Pifer S., "Crimea: Six Years after Illegal Annexation", The Brookings Institution, 10 March 2020, at https://www.brookings.edu/blog/order-from-chaos/2020/03/17/crimea-six-years-after-illegal-annexation/.

Popp G., Canna S., *The Characterization and Conditions of the Gray Zone*, *A Virtual Think Tank Analysis (ViTTa)*, Boston, MA 2016, at http://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTTa-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf.

Report: Military Operations in Cyberspace. Wednesday 5-Friday 7 September 2018. WP1635, Wilton Park, at https://www.wiltonpark.org.uk/wp-content/uploads/2020/09/WP1635-Report.pdf.

Rid T., Buchanan B., "Attributing Cyber Attacks", *Journal of Strategic Studies*, vol. 38, no. 1-2 (2015), pp. 4-37, https://doi.org/10.1080/01402390.2014.977382.

Rogin J., "Biden Doesn't Want to Change China. He Wants to Beat It", *The Washington Post*, 10 February 2022, at https://www.washingtonpost.com/opinions/2022/02/10/biden-china-strategy-competition/.

Schaus J., "Competing in the Gray Zone", Center for Strategic and International Studies, 24 October 2018, at https://www.csis.org/analysis/competing-gray-zone-0.

Schmitt M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Tallinn 2017, https://doi.org/10.1017/9781316822524.

Schneider J.G., "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy", Lawfare, 10 May 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

Smith M., "Russia Has Been at War with Ukraine for Years – In Cyberspace", *The Conversation*, 7 February 2022. https://theconversation.com/russia-has-been-at-war-with-ukraine-for-years-in-cyberspace-176221.

Starling C.G. et al., *Seizing the Advantage: A Vision for the Next US National Defense Strategy*, Washington, DC 2021.

Takashi S., "Maritime Security Study Group Research Progress Report. Increasingly Complex and Sophisticated 'Hybrid Warfare' during Peacetime: Japan's Comprehensive Response and the Japan-US Response", *NPI Research Note*, 11 September 2020, at http://www.iips.org/en/research/NPI_Research_Note_20201005.pdf.

The NATO Cooperative Cyber Defence Centre of Excellence, "Ukrainian Parliamentary Election Interference (2014)", at https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014).

The White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, May 2011, at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

The White House, *The Interim National Security Strategic Guidance*, March 2021, at https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

United States Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, April 2018, at https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

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

United States Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

United States Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America. Sharpening the American Military's Competitive Edge*, at https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

Velde J.R. van de, "Make Cyberspace Great Again Too!", Real Clear Defence, 23 July 2018, at https://www.realcleardefense.com/articles/2018/07/23/make_cyberspace_great_again_too_113634.html.

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/.

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.