Non-War Activities in Cyberspace as a Factor Driving the Process of De-Bordering

Dziwisz, Dominika

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Dziwisz, D. (2022). Non-War Activities in Cyberspace as a Factor Driving the Process of De-Bordering. *Politics and Governance*, *10*(2), 293-302. https://doi.org/10.17645/pag.v10i2.5015

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2022, Volume 10, Issue 2, Pages 293–302
https://doi.org/10.17645/pag.v10i2.5015

Article

Non-War Activities in Cyberspace as a Factor Driving the Process of De-Bordering

Dominika Dziwisz

Institute of Political Science and International Relations, Jagiellonian University, Poland; dominika.dziwisz@uj.edu.pl

Submitted: 29 October 2021 | Accepted: 8 April 2022 | Published: 15 June 2022

Abstract
Whereas war is the continuation of politics by other means, a new space between diplomacy and open conflict is now becoming available for state and non-state actors, tempting them with the promise of achieving a strategic advantage over an opponent without risking the escalation of the conflict to the level of kinetic aggression. From that perspective, the ongoing shift of states and societies into cyberspace is becoming extremely interesting. As it blurs national borders, it offers an excellent dimension in which to exercise non-war activities, enabling reduction of kinetic aggression in the three basic dimensions of warfare (land, air, and sea) and providing new means of reaching one's political objectives. The aim of this article is twofold. Firstly, it discusses the changing nature of borders and examines the impact of non-war doctrine on the functions played by national borders. Secondly, it analyzes how states utilize these activities to achieve political goals and gain strategic advantage over opponents, as well as to what extent they foster de-bordering.

Keywords
borders; cybersecurity; de-bordering; grey-zone conflict; non-war; re-bordering

Issue
This article is part of the issue "Re-Visioning Borders: Europe and Beyond" edited by Artur Gruszczak (Jagiellonian University) and Roderick Parkes (German Council on Foreign Relations).

1. Introduction

The last 50 years have been marked by rapid technological progress in the fields of automation, computerization, and digitalization. Nevertheless, during the last several months that already high pace of change has accelerated by at least an order of magnitude. The Covid-19 pandemic has not only driven development of many innovative technologies but has also turned out to be a catalyst for the adoption of new solutions in society. It will undoubtedly also have a profound impact on the future of international conflicts. Society's shift online means that cyberspace has become an even more significant dimension of how foreign states and non-state organizations exert influence.

The basic research assumption of this article is that due to the specific features of cyberspace, like its borderlessness, a-territoriality, and attack attribution difficulty, its importance for state competition is constantly growing. Especially attractive are activities in a non-war area that lie between peaceful cooperation and open conflict. They enable reducing kinetic aggression in the three basic dimensions of warfare: on land, in the air, and at sea. As a result, these activities are a factor in diminishing the importance of the traditional, geographical boundaries that were designed to protect against traditional threats. This means that states may deliberately keep their activities below the threshold, which, if exceeded, would force the use of an armed response. In this scenario, the escalation of conflict means the escalation of activities in cyberspace, where traditionally understood boundaries do not exist. The kinetic forces remain at bay. This path gives time for the necessary negotiations before states move to pursuing their policies by other means.

As the jurist and political theorist Carl Schmitt argues, international law arises directly from changing perceptions about how political legitimacy is tied to geography

(Schmitt, 2003). However, the advent of cyberspace has caused shifts in the traditional understanding of geography and traditional borders defined as lines separating physical spaces. Therefore, the methodology of this article will be similar to Michael Reisman's hermeneutic approach to international incidents in which "the formal sources of law have genuine significance or are merely a facade concealing raw and ephemeral political calculations [that] can only be assessed when you have seen how they fared in a particular incident" (Reisman, 2014, p. 5). Thus, in this article the selected case studies will discuss transnational incidents and examine how activities in cyberspace change the meaning of the national borders.

This article proposes using neoclassical realism theory, the most recent strand of realism. This theoretical approach aims at examining both structural factors of state behavior and domestic level variables (so-called intervening variables), e.g., the perceptions and misperceptions of decision makers or strategic culture, which shape all aspects of state responses (Ripsman et al., 2016). Neoclassical realism theorists seek to analyze individual state behaviors, e.g., military doctrine force posture, alliance preferences, or foreign economic policy, by studying the model's variables (Taliaferro, 2000–2001, p. 135).

Neoclassical realists agree with structural realists that states construct their foreign security policies balancing the threats and opportunities that arise in the international system. Also, since the primary purpose of a state is to ensure its own survival, it wants to minimize the risk of endangering its own existence. Consequently, any opportunity to limit the risks to state survival in the case of an unforeseen development of events is desirable. This contributes to the attractiveness of non-war activities in that they enable pursuing states' goals while avoiding openly aggressive actions and clear attack attribution, which implies lower risks for states' security.

In the adopted analysis model, the dependent variable is the degree of implementation of a state's goals, e.g., destabilizing a rival country or slowing down/delaying an opponent's military research program. The means used to achieve these goals were considered an independent variable in the study. Whereas the intervening variable is the level of risk to state security while achieving the assumed goals.

This article will proceed as follows: The second section discusses the changing nature of borders and their diminishing importance in the era of cyberspace's ubiquity. The third section defines the term "non-war activities in cyberspace" to provide the theoretical framework for the case studies analyzed in the subsequent part. Consequently, the fourth part draws an overall picture of the impact of non-war doctrine on the functions played by national borders. The examples of non-war activities in cyberspace will be discussed to analyze how states apply these activities to achieve a strategic advantage over an opponent and to what extent they foster de-bordering.

2. Cyberspace as a New Frontier for National Security

Since the Peace of Westphalia, state borders—lines separating physical spaces—have been an important security element delimiting the scope of territorial jurisdiction of the authorities, creating a barrier against external threats, and regulating the international movement of people and goods. As Spruyt states: "Borders enabled sovereigns to specify limits to their authority and also precisely specify who their subjects were" (Spruyt, 1996, p. 21). In this Westphalian style, territorial borders are constructed and reconstructed in the search for control and power (Newman & Passi, 2001). Therefore, border control has become a core activity for states (Anderson, 1996, as cited in Andreas, 2003, p. 1).

At the beginning of the 1990s, a change in the meaning of territorial borders was distinctly indicated by former Israeli prime minister Shimon Peres, who said that in a world where missiles can precisely hit a target thousands of miles away, the existence of clearly located land borders does not matter much (Rose, 1994). It was a message that the state-centric approach of traditional realists, in which sovereignty, territoriality, and state boundaries were accepted as obvious and existing features, was in question (Luke, 1993, as cited in Newman & Passi, 1998; Shapiro & Alker, 1996). Agnew called this traditional way of reasoning a territorial trap (Agnew, 1994). He intended to draw attention to the fact that by concentrating on this kind of thinking, which emphasizes the importance of territorial states, we avoid analyzing the influence of power in alternative spatial configurations. In other words, the "territorial trap" amounts to the "freezing of geography" in which power and action belong only to the territorial state, at the expense of engaging many geographic areas, scales, and complexities of policies and political actions around the world (Agnew, 2010, as cited in Ashraf, 2015, p. 55). From that moment on, international security, freed from its former close ties to geographical territory, was extended to new areas and forms. As David Newman argues, classical bordering based on the Westphalian assumption of the necessity to delineate and control borders, accepting exclusive state sovereignty, had to change—adapting to the new meaning of borders as contact zones (Newman, 2003).

Globalization processes and increasing interdependence, catalyzed by the development of modern information technologies, and above all Western European and North American experiences, i.e., opening markets and lifting trade barriers, have unsealed national borders. The third industrial revolution, powered by furtherance in fields like computer science and biotechnology, entails a transition for advanced industrial nations from an economy based on natural resources and physical inputs to one based on intellectual assets. Therefore, the advent of the knowledge economy implies the lessened significance of deposits of natural resources and industrial regions, which, in consequence, implies the dwindling

relevance of national borders. Capturing a piece of land in the 21st century brings incomparably lower benefits than a century or two ago. Thus, here is another powerful force diminishing the importance of physical borders.

Such a process of losing territorial anchorage is framed within the concept of de-bordering. First coined by Albert and Broch (Senhardt, 2013), de-bordering can be explained as an increasing permeability of state territorial borders, together with the decreased ability of states to close themselves off from all kinds of cross-border activities (Senhardt, 2013). In other words, de-bordering means "the functional change of borders, the loss of importance of their territorial anchoring and—as a consequence—the decoupling of (functional) system borders and territorial borders" (Bonacker, 2007, as cited in Senhardt, 2013).

Even though some idealistic globalization literature assumes a "borderless" world or the "eclipse of the state," it can be noted that states are currently dealing with the simultaneously existing processes of closing and opening. On the one hand, borders have been opened to the passage of capital and commodities under the banner of neoliberalism (Gregory, 2011, p. 242), and on the other, there have been attempts by states to seal their borders (caused by, e.g., the migration crisis or the threat of terrorist attack), walling practices along state borders (e.g., at the borders of the US and Mexico or Israel and Palestine), and other barriers to mobility (e.g., stopping the movement of migrants over the border Poland shares with Belarus in 2021). The most recent manifestation of re-bordering is an effect of the Covid-19 pandemic. Many governments have decided to seal their borders by intensification of border controls, or even outright closure to protect against the spread of the virus. Megoran is of the opinion that it is naïve to think that Covid-19 "borders on steroids" and migration regimes will simply dematerialize when the pandemic is defeated (Megoran, 2021).

Therefore, the creation of border control mechanisms is an outcome of these two tendencies—both the desire for border opening and to control migration (Van der Wusten, 2002, as cited in Newman, 2003). Especially after the devastating terrorist attacks on September 11, the need to seal borders, "re-bordering," returned with doubled strength and the voices for open borders were muted (Andreas, 2002; Newman, 2006; Rumford, 2006). Also, the securitization of state borders has shifted academic interest to the issues of strengthening border control, surveillance, crime prevention, or even the militarization of borders (Gruszczak, 2018, p. 25). Therefore, one may assume that territoriality and state borders have not yet lost their meaning and that the process of reinforcing national lines is still in progress.

Taking into consideration all that has been mentioned above, one can draw two simple conclusions. Firstly, de-bordering and re-bordering processes are largely intertwined (Senhardt, 2013, p. 29). Herzog and Sohn articulate that bordering cannot be analyzed as an "either/or" binary condition. Particularly, bordering is "an inherently co-mingled process, whereby institutional, economic and socio-cultural behaviors simultaneously embrace both elements of rebordering and debordering" (Herzog & Sohn, 2019, p. 195). In fact, these two dynamics collide, confront their contrasting goals, influence each other, and co-mingle. Secondly, despite theories regarding the diminished importance of territorial borders and against the state-centric understanding of borders (Newman & Passi, 2001), state governments are pushing back against the consequences of such ideas. Attempts are being made to conduct cyberspace territorialization, which consists firstly in "the application of territorial notions of international law to persons, activities, and objects existing or operating in or through cyberspace and, secondly, in states asserting their sovereignty in cyberspace by creating national cyberspace zones" (Tsagourias, 2018). Creating cyberspace zones, that is, cutting a state off from the global Internet and building a national one, is probably the most radical way of asserting sovereignty in cyberspace (Tsagourias, 2018). In the case of the national internet, the borders of the national network overlap with state territorial borders. This concept was implemented, e.g., in Iran (Halal internet) and in North Korea (Kwangmyong internet), but such ideas are also being aggressively developed in Russia (RuNet).

Another example of trying to establish digital boundaries coinciding with state territorial borders is enforcing state laws in cyberspace in order to exercise their normative jurisdictions (Desforges & Géry, 2022). Specifically, when governments try to connect a cyber event to their territory by referring to the physical location of information technology (IT) infrastructure (Internet cables, servers, etc.), individuals, or entities within their territory, the problem of determining the appropriate jurisdiction arise. A good example of a situation of jurisdictional conflict is that of the Clarifying Lawful Overseas Use of Data (CLOUD) Act (U.S. Department of Justice, 2018), a new digital data acquisition model for investigating the most serious crimes (e.g., acts of terrorism or child pornography). The CLOUD outlines the terms on which law enforcement authorities may access digital data collected by Internet service providers and located in foreign jurisdictions other than the seat of the issuing authority. The CLOUD mandates every US firm to disclose data hosted on their servers, wherever in the world these servers may be located. Since its signature in 2018, the document has been criticized mostly due to concerns regarding its threat to the sovereignty of other states.

However, except for radical solutions like the national internet of authoritarian regimes, state borders, both geographic and normative, may only partially help national security in cyberspace. In fact, the Internet is a "battleground of control" by national governments to only a small extent. The process of de-bordering is especially evident in cyberspace.

Whereas historically, every crime or threat to state security was physically linked to traditional state borders, currently, any form of hostile activity can at least be facilitated by the cyber component. Some crimes, like large-scale theft of personal data, wouldn't be even possible before the advent of cyberweapons. Without a doubt, cyber threats have radically changed the border security landscape, blurring traditional ideas about borders. This detachment from traditional concepts of borders encourages states to shift to cyberspace which gives them a wide range of tools for achieving political goals, especially in the information field (e.g., social media and digital propaganda), without the necessity of engaging military capabilities in direct confrontation (Morris et al., 2019). For adversaries who want to make strategic gains without reaching the conflict threshold laid down in Article 5 of the Washington Treaty (NATO), the anonymity of cyberspace and attribution dilemmas drive activities in the non-war area.

Although state governments try to articulate their territory in cyberspace, e.g., by introducing censorship and control over the Internet, filtering, and surveillance, they should avoid the simplified analogy between cyberspace and traditional national territory. Despite the fact that cyberspace is not limited by borders in the same way as territorial spaces, from a realistic perspective, state governments often mistakenly perceive the Internet as an extension of existing state territory (Manjikian, 2010). Cyberwar and other malicious activities in cyberspace ignore traditional territorial boundaries, since states solve conflicts using technology, bypassing territory. Therefore, all boundaries in cyberspace are artificial and can be likened to fortifications painted with easily washable chalk on the ground.

3. War and Non-War Activities in Cyberspace

During the NATO summit in Warsaw in 2016, it was stated that defense of cyberspace was one of the basic tasks of NATO's collective defense. Consequently, cyberspace was recognized as an area of military operations. However, while war is a legally, morally, and strategically exceptional condition, most cyberattacks are non-military activities that fall under the general category of "grand strategy" (Lonsdale, 2019). Thus, "cyberwar" does not fit within the traditional and legally defined concept of "war" (or the more commonly used term "armed conflict"), which refers to situations where "there is use of armed forces or prolonged armed violence between states and organized armed groups or between such groups within the territory of a single country" (*Prosecutor v. Dusko Tadic*, 1995, § 70).

Cyberwar is full of ambiguities and therefore there are doubts as to whether cyberattacks can be classified as war at all. It is difficult to assess the effectiveness of the weapon used before or even after its use, to determine the time needed to recover from the attack, and whether the selected line of attack can be continued. In case of cyberwar, one cannot be sure whether a failure of a given part of the system caused by an attack will not lead to damage to other parts of the system (cascading failure). It is almost impossible to predict the actions of the other side and third parties. However, the overriding challenge in cyberconflicts is establishing attribution for cyber operations.

As shown in a recent analysis of more than 200 cybersecurity incidents related to the activities of nation states since 2009 (McGuire, 2021), half of them concerned low-budget, simple tools that can be easily purchased on the darknet, while an additional 20 percent involved more sophisticated custom-made weapons. However, a further 30 percent were of uncertain, or unattributable origin. If the latter are used correctly, in most cases the attackers won't provide investigators with enough evidence to prove the source of the attack.

There are many factors that may enable attack attribution (Davis II et al., 2017), including: (a) technical indicators, such as network analysis and inspection of the log files of software programs and processes executed on the victim's computer systems, and of the networks used by the victim through third-party service providers; (b) political indicators, consisting of the political context in which an incident takes place and the relevant motives of capable parties (*cui bono*); and (c) all-source intelligence indicators, including sophisticated capabilities available to very few countries. For example, the theory that the Stuxnet worm that caused physical damage to Iranian centrifuges was built in American–Israeli cooperation, is based on a complex set of indicators. The technical ones include, e.g., a text string that suggests that the attackers named their project Myrtus, which was an allusion to the Hebrew word for Esther (Markoff & Sanger, 2010), circumstantial evidence of Israeli involvement in Stuxnet's code construction. Moreover, Israel has its own *style points*, and in the case of Stuxnet, they used not one, but two stolen certificates, four zero-day vulnerabilities, and included hints in the code (Singer, 2015). There were also political indicators, including, e.g., the fact that degrading the Iranian nuclear program would be beneficial to US and Israeli interests, and Israel felt threatened by Iran's growing nuclear program (De Falco, 2012). Stuxnet's attribution was declared thanks to independent research and off-the-record conversations conducted by David Sanger. Later, independent researchers also presented attribution findings and evidence in a variety of other informal ways, e.g., through blogs and social media posts (Davis II et al., 2017, p. 18).

However, 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. As Rid and Buchanan articulate, "the process of attribution is not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades" (Rid & Buchanan, 2015). In other words, uncertainty regarding the origin of an attack can be minimized, but the desired high levels of certainty can

rarely be achieved. Despite the common practices and tradecraft that are used by a variety of experts in cyber forensics that shed light on attribution, due to the diversified nature of the attacks there is no single standardized attribution methodology (Davis II et al., 2017). Therefore, the investigative process might be described as "as much an art as a science" (Rid & Buchanan, 2015). Moreover, cyberattribution is not first and foremost a technical problem but a political problem (Rid & Buchanan, 2015).

At the same time, it is worth remembering that not only the attribution problem, but also and most significantly the conditions of conventional military power stopped, e.g., Iran's retaliation against Israel and the US. Assuming that cyberspace is a new, but not entirely separate component of a multi-faceted conflict environment that also includes land, sea, air, and space, from this point of view, cyberwar is more of a description of operational activities than a decisive strategic confrontation (Cornish, 2018). In other words, hostile activities in cyberspace are increasingly likely to be a form of low-level interstate conflict, in which the normative understanding of what constitutes unacceptable, aggressive behavior is much less clear. These activities can be non-invasive, such as gathering information or disseminating propaganda, or invasive, such as disrupting government websites or crippling a civilian data-mining system (SCADA). This has the potential to escalate cyberattacks into conventional interstate conflicts if they are not properly managed. If, on the other hand, they are well-managed, they may be limited to subliminal activities, i.e., maintained by the attacking party at a level below the relatively clearly identifiable threshold of regular open war (Watts et al., 2017). Additionally, it should be taken into account that the links between perceived effects and threats in cyberspace are loose and may be different for each country (Libicki, 2012). In line with the basic assumption of realism, it is expected that there is logic in the behavior of states; therefore, the development of an escalation ladder in the context of cyber activities is possible and necessary, as it will allow for better planning of activities, so as to maintain the desired level.

All things considered, the above-mentioned problems and challenges of cyberwar may be perceived by the states more as an opportunity than a risk by seeking to coerce, acquiring influence within, influencing large numbers of individuals' perceptions and political decisions, or destabilizing key countries and regions. Numerous statements from state officials, e.g., the US defense representatives, make clear that the competition played out primarily below the threshold of major war is mostly expected (Morris et al., 2019).

The term "non-war" is embedded only in the political sense, but there are no binding definitions on the basis of international practice and law. For this reason, it should be examined through the lens of and confronted with the concepts of "use of force" and "aggression," which are well-defined under international law and mean "the use of armed force by a state or a group of states against the territorial sovereignty or political independence of another state" (United Nations, 1974). In other words, non-war is a type of phenomenon that is defined by negating war, while fulfilling neither the definition of "war" nor "peace."

Literature on the subject offers many terms for actions below the threshold of armed aggression and usually refers to the entire spectrum of possible actions, not only those in cyberspace: "grey zone" between war and peace (Morris et al., 2019; Popp & Canna, 2016), "non-war military activities" (Office of the Secretary of Defense, 2020), "unpeace" (Kello, 2017), "warfare during peacetime" (Takashi, 2020; van de Velde, 2018), "subliminal aggression" (National Security Bureau, 2015, as cited in Liedel, 2018, p. 96), or "persistent cyberspace confrontation" (Casey, 2007).

For the purposes of this article, two definitions of actions below the threshold of triggering armed aggression prove to be the most useful. Due to the specificity of the analyzed problem, they will be limited only to activities undertaken in cyberspace.

Lucas Kello defines "unpeace" actions as "mid-spectrum rivalry lying below the physically destructive threshold of interstate violence, but whose harmful effects far surpass the tolerable level of peacetime competition and possibly, even, of war" (Kello, 2017).

A more detailed and exhaustive definition has been proposed by the RAND Corporation, defining the "grey area" 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. (Morris et al., 2019, p. 8)

The above definitions indicate three features of non-war activities: (a) the goal of all activities is to avoid open conflict and serious clashes; (b) the incremental nature of the actions taken, which prevents the determination of the conflict threshold; and (c) the problem with assigning responsibility for an attack 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 order to avoid strong reactions from the attacked state, grey-zone campaigns may be limited to activities that do not threaten vital or existential interests. This harasses the enemy but does not risk attacks on areas that are critical to state security. Thus, the risk of a possible military response from the attacked state is reduced. Campaigns in the grey zone may target specific threats in the target countries, which may lead to dangerous social divisions, prompt economic stagnation, or threaten military capabilities. Also, when analyzing non-war activities, they should always be placed in an international context, i.e., bearing in mind that they are part of the ever-growing

global competition. This is reflected in, e.g., US, Russian, and Chinese strategic documents. Therefore, one should always consider the purpose and effects of a response. Actions taken in the context of the grey zone of one country may set expectations about other problems and fuel international competition.

At the very end it must be noted that grey zone conflict can be seen as distinct from hybrid warfare (Belo & Carment, 2019). The concept of hybrid warfare, understood as the space-time coexistence of several different generations of wars that intersect, interpenetrate, and confront each other on the battlefield or in operations other than war, relies on a combination of both kinetic and non-military tools (Hoffman, 2007). However, grey zone conflicts may involve only unconventional techniques, e.g., cyber operations, facilitating a situational ambiguity which states use to their advantage (Belo & Carment, 2019).

4. Testing Non-War in Cyberspace

The development of information technologies and the reduction of their costs has resulted in the saturation of critical systems with modern IT solutions. The possibilities of the modern technologies that have been developed over the last several decades are currently being tested by the most digitally advanced countries. In the military dimension, cyberspace and modern IT solutions are being used by states and non-state actors in new ways. This follows the logic of the RMA (revolution in military affairs) concept (Kamieński, 2009), as technological changes have always shaped the evolution of international security and threatened to upset the balance of power. The key difference is that, today, the pace of these changes is growing exponentially, while the political processes of building resources, drafting legislation, and setting standards in cyberspace all take time (Schjølberg, 2018). The growing dependence on IT services has made cyberspace an entirely new domain for hostile actions. Just as the use of aviation in military operations created the need to defend against attacks from the air, today, IT technologies force states to seek new ways of responding to the threats caused by those technologies. At the same time, we need to remember that traditionally understood, physical boundaries evolved in a world where exerting influence required geographical proximity and all the subjects existed on the same, physical plain. In cyberspace, distance is not measured in kilometers but milliseconds. All publicly available nodes of a network are reachable regardless of physical location, and the people accessing them need no passports.

Activities in cyberspace may facilitate achieving intended effects that had previously been possible only by using kinetic force. As demonstrated above, cyberoperations can seldom be considered armed attacks that warrant an immediate military response by the target. They make it possible to avoid outright military clashes and unambiguous or attributable violations of international law or norms. In neoclassical realist realms, rivals seek ways to achieve relative gains without triggering unnecessary escalation, and without risking liability for the use of force. Moreover, as Fischerkeller and Harknett accurately note, "states are seeking to advance their national interests without recourse to war, thus their interactions in this cyber strategic competitive space are best approached as a form of *tacit agreed competition*" (Fischerkeller & Harknett, 2019, emphasis in original). This doesn't mean that states are explicitly agreeing on illegal behaviors in cyberspace, but rather that they are at the early stages of an agreed to competition, where "mutual understandings of acceptable and unacceptable behaviors are still being developed through competitive interaction" (Fischerkeller & Harknett, 2019).

At the same time, it can be said that in cyberspace the attacking side will usually be a highly developed country. Today's operations in cyberspace result from carefully planned and expertly conducted reconnaissance of targeted objects in order to find the weakest and most appropriate access points. Despite the asymmetric character of cyberweapons, which offers no advantage to highly developed countries, conducting cyberoperations capable of making a strategic impact is complex, expensive, and time consuming. Their complexity is driven by a need to coordinate multiple dependencies, including those outside of cyberspace and often among multiple involved countries. Technical aspects constitute just a small part of such a challenge. This is also why such operations are expensive—the cost goes way beyond personnel payroll, as it involves line items like acquisition of necessary hardware and infiltration of foreign facilities. Given the complexity and cost, it should come as no surprise that strategic-level cyberoperations are not conducted over a weekend. In other words, conducting a successful Distributed Denial of Service (DDoS) attack, stealing an email, or even interfering with critical infrastructure (i.e., carrying out a tactical operation in cyberspace) can be achieved by virtually anyone; successful, large-scale operations that make a strategic-level impact require exponentially more resources. And for these reasons, although aspiring-cyberpowers like North Korea or Iran do possess the capabilities for conducting tactical operations, the ability to carry out cyberoperations that can influence the policy of foreign countries remains in the domain of only the true-cyberpowers, like the US or China.

Following Michael Riesman's approach, let's study two very well documented cases to see how they were resolved and whether the attacks were classified as either border violation or use of force.

A good example of an attack allegedly orchestrated by one of the cyberpowers is an extensive operation carried out by Russian hackers targeting three Ukrainian regional power distribution companies at the end of 2015 that left more than 200,000 inhabitants without power for several hours (Zetter, 2016). The blackout didn't last long as the operators were able to manually

restore power within approximately six hours. However, it caused further difficulties in operating the power plants. The attackers overwrote firmware on critical devices, leaving operators without automated control of power distribution for about a year (Dragos, 2017, as cited in Narayanan et al., 2020). Even after the power supply was restored, workers had to control the breakers manually.

The investigation into the 2015 hacks proved that this operation was carefully planned following months of reconnaissance, studying the networks to launch a perfectly planned and synchronized assault (Zetter, 2016). Even though the Ukrainian intelligence community was certain that the Russian secret services were behind the attack, and security firm experts confirmed that the attacks were carried out by a Russian hacker team known as "Sandworm" (Greenberg, 2017b), there was no evidence to support the claim. However, the fact that the attacks were inspired or organized by Russians might be indicated by the results of an analysis of the scale, goals, and complexity of the entire campaign of attacks against Ukraine. The 2015 cyberspace operation was the result of careful planning and identification of the networks under attack. The complexity and scale of attacks indicate that they were prepared by professionals who could properly gather information, prioritize actions, and distribute tasks among different groups of operators, intelligence analysts, and malware writers. Such large-scale attacks were carried out again in December 2016 and in June 2017 (Dragos, 2017). More importantly, 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 (Greenberg, 2017a).

The Russian–Ukrainian conflict clearly shows that by using grey zone aggression, it is possible for a state to pursue its national interests. Additionally, by creating a new status quo, Russia is successfully lowering the international expectations of its behavior. By making the conflict politically ambiguous and by conducting small-scale hostilities, foreign observers are kept uncertain about upcoming developments. Most importantly, through its activities in cyberspace Russia is creating a "sort of 'digital front line' that reflects the military front line" (Desforges & Géry, 2022). Therefore, one may assume that the main goal of Russians is both to control the network and to bring these territories under Russian influence. All these activities are tied together by Russia's idea of creating a national "sovereign" Internet (RuNet). That being the case, international conflicts can shape the boundaries of cyberspace by modifying existing borders and creating new ones. This leads to the conclusion that setting borders, even as fluid and dynamic as those in cyberspace, is decided by countries that need these borders for certain reasons. And vice versa, in situations where states do not need borders, e.g., for greater freedom of action and anonymity in cyberspace, there will be no such borders.

The most recognized example of effective actions that are below the threshold of armed aggression is the 2010 cyberattack with the computer worm known as Stuxnet on Iranian nuclear installations. It has been called "the world's first digital weapon" (Zetter, 2015), and one of "the most complex threats ever analyzed" (Falliere et al., 2011, p. 2). The attack was a significant event because, for the first time in history, a computer program was used to attack the critical infrastructure elements of a hostile state, causing physical harm. The failure was only discovered after a few days. The Natanz nuclear facility was temporarily shut down, and Iran's attempt to obtain enough highly enriched uranium to build a nuclear weapon was delayed.

There is no definitive evidence of the source of the worm. Although the White House has never issued an official statement, it is suspected, and there is sizable, though inconclusive, evidence that this advanced cyber weapon was created in American–Israeli cooperation. In any event, both countries have never denied the claims that they were involved with Stuxnet's development (De Falco, 2012). Regardless of which country was involved in the construction of Stuxnet, the fact that it required the resources of a nation (Langner, 2010) suggests a new approach to using cyberattacks to achieve national goals. The cost of this operation was comparable to the estimated cost of destroying Iranian facilities using conventional means. However, a conventional operation would have forced Tehran to respond in kind, while the use of malicious software made it possible to avoid an armed conflict (Ashraf, 2015). By analyzing the scale, goals, and complexity of the entire cyberattack campaign, it can be concluded that Stuxnet is a model example of state-sponsored attempts to conduct hostile activities in cyberspace against an enemy state.

Gaining the ability to conduct offensive cyber operations below that conflict level may bring exceptional benefits from cyberspace as an operational domain. Gregory Rattray and Jason Healey argue that: "It may be that the future of cyberconflict is not equivalent to larger, theatre-level warfare but only to select covert attacks which could range across a wide set of goals and targets" (Rattray & Healey, 2010, p. 86). This argument is based, in part, on case studies showing that offensive operations using conventional forces are relatively rare and usually condemned by other states because they are clearly visible, have easy to recognize actors, and inherently carry the risk of escalation. The situation is different with cyber operations in the "grey area of non-war," wherein the principles and rules of international law are difficult to enforce and are subject to competing interpretations (Schmitt, 2017a).

5. Conclusions

Even if certain operations may amount to the use of force, no state or international organization has ever publicly, unequivocally, and explicitly qualified a

cyber operation as the use of force (Delerue, 2020, pp. 273–342). While there is no doubt that the existing norms of international law defining the behavior of states in times of conflict and peace also apply to cyberspace, the borderless nature of cyberspace, its a-territoriality, and the attribution problem mean there is still a question of how the rules of international law should be interpreted (Schmitt, 2013). Unlike physical cyber infrastructure, comprised of tangible elements, from fiber optic cables to cell towers, computers, and servers, "electromagnetic frequencies do not easily fit with a notion of sovereignty that is confined to state borders" (Schmitt, 2017b, p. 14).

The examples of Stuxnet and hacking the Ukrainian power providers have proved the potential of the ambiguity and the effectiveness of cyber operations employed by grey zone adversaries; this potential stands to persist in the future as it has in the recent past. The biggest challenge is that of accountability in cyberspace due to the low confidence in attributing the origin of a given attack (Davis II et al., 2017).

For the attacked state, the lack of attribution is a problem; for the attacking state, it creates new opportunities for action without much fear of the conflict reaching the kinetic phase. Therefore, gaining the ability to conduct strategic offensive cyber operations below the conflict level may bring exceptional benefits from cyberspace as an operational domain. In both examples, (allegedly) Russia and the US/Israel managed to exert a strategic influence over a foreign state without escalating the conflict. Looking through the lens of neoclassical realism theory, avoiding openly aggressive actions and decreasing the probability of attack attribution increase state security. However, to use the full potential of non-war competition to limit confrontation, states need to consider what levels and forms can be tolerated by the attacked state and international opinion. If not assessed properly, the attacking state ends up risking a hybrid "forever war" or a kinetic response.

If Russians were behind the attacks on the Ukrainian power grids, the grey zone technique was a way of expressing dissatisfaction with aspects of the regional power without the risk of being alienated in the international arena and undermining Russia's status as a superpower (Morris et al., 2019). Cyberspace gave the attackers the chance to acquire influence within, and/or destabilize a neighboring country without physical aggression.

If Americans and Israelis were behind the Stuxnet attack, they managed to slow down and delay the Iranian nuclear program. It was also a way to demonstrate the power of the countries in the new competitive domain of cyberspace. Furthermore, it is highly possible that from the very beginning the attackers had assumed that the psychological effects of Stuxnet may be greater and more important than the physical ones. The intent might have been to undermine the Iranian government's trust in its own ability to develop a nuclear weapon. While it can be assumed that the first goals were achieved by the US–Israeli coalition, the psychological effect of the operation likely changed when Iranians realized that they were faced with aggressive foreign adversaries and that burning the centrifuges had not been due to a technical error (Rid, 2013).

As demonstrated above, non-war activities in cyberspace diminish the importance of geographical borders for protecting countries from external influence, and thus can be considered a factor driving the process of de-bordering. The lack of traditionally understood borders in cyberspace favors highly developed countries with developed cyber offensive capabilities. Since cyberspace makes it possible to achieve political goals more cheaply, more efficiently, and without the risk of being exposed to international criticism, the importance of non-war activities will only grow. Given that more and more activities are moving into cyberspace, we can only expect this process to become increasingly visible.

Conflict of Interests

The author declares no conflict of interests.

References

Agnew, J. (1994). The territorial trap: The geographical assumptions of international relations theory. *Review of International Political Economy*, *1*(1), 53–80.

Andreas, P. (2002). The re-bordering of America after 11 September. *The Brown Journal of World Affairs*, *8*(2), 195–202.

Andreas, P. (2003). Redrawing the line: Borders and security in the twenty-first century. *International Security*, *28*(20), 78–111.

Ashraf, C. H. (2015). *The spatiality of power in internet control and cyberwar* [Doctoral thesis, University of California]. UCLA Electronic Theses and Dissertations, https://escholarship.org/uc/item/0w99g31p

Belo, D., & Carment, D. (2019). *Grey-zone conflict: Implications for conflict management*. Canadian Global Affairs Institute.

Casey, G. (2007). *Remarks at the National Press Club* [Speech transcript]. The United States Army. https://www.army.mil/article/4436/aug_14_2007_remarks_at_the_national_press_club

Cornish, P. (2018). *Military operations in cyberspace*. Wilton Park. https://www.wiltonpark.org.uk/wp-content/uploads/2020/09/WP1635-Report.pdf

Davis II, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. (2017). *Stateless attribution: Toward international accountability in cyberspace*. RAND Corporation.

De Falco, M. (2012). *Stuxnet facts report. A technical and strategic analysis*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Delerue, F. (2020). *Cyber operations and international*

law. Cambridge University Press.

Desforges, A., & Géry, A. (2022, January 4). So much for a "world without borders"? Countries are marking their territory in cyberspace. *New Atlanticist*. https://www.atlanticcouncil.org/blogs/new-atlanticist/so-much-for-a-world-without-borders-countries-are-marking-their-territory-in-cyberspace

Dragos. (2017). *CRASHOVERRIDE: Analysis of the threat to electric grid operations*. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

Falliere, N., O Murchu, L., & Chien, E. (2011). *W32. Stuxnet dossier* (Version 1.4). Symantec Security Response.

Fischerkeller, M. P., & Harknett, R. J. (2019, February 19). What is agreed competition in cyberspace? *Lawfare*. https://www.lawfareblog.com/what-agreed-competition-cyberspace

Greenberg, A. (2017a, June 20). How an entire nation became Russia's test lab for cyberwar. *Wired*. https://www.wired.com/story/russian-hackers-attack-ukraine

Greenberg, A. (2017b, July 12). Your guide to Russia's infrastructure hacking teams. Which of Russia's hacking groups is targeting American energy utilities? *Wired*. https://www.wired.com/story/russian-hacking-teams-infrastructure

Gregory, D. (2011). The everywhere war. *The Geographical Journal*, *177*(3), 238–250.

Gruszczak, A. (2018). European borders in turbulent times: The case of the Central Mediterranean "extended borderland." *Politeja*, *5*(50), 23–45.

Herzog, L. A., & Sohn, C. (2019). The co-mingling of bordering dynamics in the San Diego–Tijuana cross-border metropolis. *Territory, Politics, Governance*, *7*(2), 177–199.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.

Kamieński, Ł. (2009). *Technologia i wojna przyszłości: Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych* [Technology and the war of the future: Around the nuclear and informational revolution in military matters]. Wydawnictwo Uniwersytetu Jagiellońskiego.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Langner, R. (2010, September 16). Stuxnet logbook, Sep 16, 2010, 1200 hours MESZ. *OT Base*. https://www.langner.com/2010/09/stuxnet-logbook-sep-16-2010-1200-hours-mesz

Libicki, M. C. (2012). *Crisis and escalation in cyberspace*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf

Liedel, K. (2018). Hybrid threats—How is the security environment in Central and Eastern Europe changing? In P. Piasecka & K. Maniszewska (Eds.), *Security and society in the information age* (pp. 92–100). Collegium Civitas Press. https://doi.org/10.6084/m9.figshare.7454207.v1

Lonsdale, D. J. (2019, October 25). We aren't in a cyber war—Despite what Britain's top general thinks. *The Conversation*. https://theconversation.com/we-arent-in-a-cyber-war-despite-what-britains-top-general-thinks-125578

Manjikian, M. M. (2010). From global village to virtual battlespace: The colonizing of the Internet and the extension of realpolitik. *International Studies Quarterly*, *54*(2), 381–401.

Markoff, J., & Sanger, D. (2010, September 29). In a computer worm, a possible biblical clue. *The New York Times*. https://www.nytimes.com/2010/09/30/world/middleeast/30worm.html

McGuire, M. (2021). *Nation states, cyberconflict and the web of profit*. HP Development Company. https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf

Megoran, N. (2021). Borders on steroids: Open borders in a Covid-19 world? *Political Geography*, *91*(1), Article 102443.

Morris, L. J., Mazarr, M. J., Hornung, J. W., Pezard, S., Binnendijk, A., & Kepe, M. (2019). *Gaining competitive advantage in the gray zone: Response options for coercive aggression below the threshold of major war*. RAND Corporation.

Narayanan, A., Welburn, J., Miller, B. M., Li, S. T., & Clark-Ginsberg, A. (2020). *deterring attacks against the power grid: Two approaches for the U.S. Department of Defense*. RAND Corporation.

Newman, D. (2003). On borders and power: A theoretical framework. *Journal of Borderlands Studies*, *18*(1), 13–25.

Newman, D. (2006). Borders and bordering: Towards an interdisciplinary dialogue. *European Journal of Social Theory*, *9*(2), 171–186.

Newman, D., & Passi, A. (1998). Fences and neighbours in the postmodern world: Boundary narratives in political geography. *Progress in Human Geography*, *22*(2), 186–207.

Newman, D., & Passi, A. (2001). Rethinking boundaries in political geography. In M. Antonisch, V. Kolossov, & M. P. Pagnini (Eds.), *Europe between political geography and geopolitics* (pp. 301–316). Societa Geografica Italiana.

Office of the Secretary of Defense. (2020). *Annual report to Congress: Military and security developments involving the People's Republic of China*. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

Popp, G., & Canna, S. (2016). *The characterization and conditions of the gray zone*. NSI. http://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTTa-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf

Prosecutor v. Dusko Tadic, Case No. IT-94-1-AR-72, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction (1995).

Rattray, G., & Healey, J. (2010). Categorizing and understanding offensive cyber capabilities and their use. In National Research Council (Ed.), *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy* (pp. 77–98). The National Academies Press. https://doi.org/10.17226/12997

Reisman, W. (2014). International incidents: Introduction to a new genre in the study of international law. In W. M. Reisman & A. R. Willard (Eds.), *International incidents: The law that counts in world politics* (pp. 3–24). Princeton University Press.

Rid, T. (2013). Cyberwar and peace: Hacking can reduce real-world violence. *Foreign* Affairs, *92*(6), 77–87.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1/2), 4–37.

Ripsman, N. M., Taliaferro, J. W., & Lobell, S. E. (2016). *Neoclassical realist theory of international politics*. Oxford University Press.

Rose, C. (1994, May 18). *The city of Jerusalem; Ehud Ya'ari* [Video]. https://charlierose.com/videos/21722

Rumford, C. (2006). Borders and rebordering. In G. Delanty (Ed.), *Europe and Asia: Towards a new cosmopolitanism* (pp. 181–192). Routledge.

Schjølberg, U. G. (2018, January 30). Poor countries are more vulnerable to cyber attacks. *Norwegian Institute of International Affairs*. https://partner.sciencenorway.no/forskningno-internet-norway/poor-countries-are-more-vulnerable-to-cyber-attacs/1453684

Schmitt, C. (2003). The nomos of the Earth in the international law of the *Jus Publicum Europaeum*. Telos Press Publishing.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Schmitt, M. N. (2017a). Grey zones in the international law of cyberspace. *The Yale Journal of International Law Online*, *42*(2). 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

Schmitt, M. N. (Ed.). (2017b). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Senhardt, B. (2013). Border types and bordering processes. A theoretical approach to the EU/Polish-Ukrainian border as a multi-dimensional phenomenon. In A. Lechevalier & J. Wielgohs (Eds.), *Borders and border regions in Europe: Changes, challenges and chances* (pp. 21–44). transcript.

Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case Western Reserve Journal of International Law*, *47*, 79–86. https://scholarlycommons.law.case.edu/jil/vol47/iss1/10

Spruyt, H. (1996). *The sovereign state and its competitors: An analysis of systems change*. Princeton University Press.

Takashi, S. (2020). *Increasingly complex and sophisticated "hybrid warfare" during peacetime: Japan's comprehensive response and the Japan–US response* (Maritime Security Study Group Research Progress Report). Nakasone Peace Institute. https://www.npi.or.jp/en/research/NPI_Research_Note_20201005.pdf

Taliaferro, J. W. (2000–2001). Security seeking under anarchy: Defensive realism revisited. *International Security*, *25*(3), 128–161.

Tsagourias, N. (2018). Law, borders and the territorialisation of cyberspace. *Indonesian Journal of International Law*, *15*(4), 523–551.

United Nations. (1974). *General Assembly Resolution 3314 (XXIX)*.

U.S. Department of Justice. (2018). *CLOUD Act resources*. https://www.justice.gov/dag/cloudact#:~:text=The%20United%20States%20enacted%20the,crime%20to%20sexual%20exploitation%20of

van de Velde, J. R. (2018, July 23). Make cyberspace great again too! *RealClear Defence*. https://www.realcleardefense.com/articles/2018/07/23/make_cyberspace_great_again_too_113634.html

Watts, S., Kavanagh, J., Frederick, B., Norlen, T. C., O'Mahony, A., Voorhies, P., & Szayna, T. S. (2017). *Understanding conflict trends. A review of the social science literature on the causes of conflict*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1063z1.html

Zetter, K. (2015). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Broadway Books.

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

About the Author

Dominika Dziwisz, PhD, is an assistant professor in the Institute of Political Science and International Relations of the Jagiellonian University in Krakow, Poland. She holds masters' degrees 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 US. 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.