CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Criminology on the fringes of war
Authors	Kaucz, Błażej
Publication date	2025-08-27
Original Citation	Kaucz, B 2025, Criminology on the fringes of war. in B Kaucz (ed.), Polish Contributions to Criminology. Springer Science + Business Media, pp. 213-241. https://doi.org/10.1007/978-3-031-94142-9_8
Type of publication	Book chapter
Link to publisher's version	https://www.scopus.com/pages/publications/105022324285 - 10.1007/978-3-031-94142-9_8
Rights	© 2025 The Editor and The Author, under exclusive license to Springer Nature Switzerland AG. This is an Accepted Manuscript version of the following work: Błażej Kaucz, Criminology on the Fringes of War, 2025, Palgrave Macmillan, Cham. This version of the manuscript has been accepted for publication, after final editorial and peer review (where applicable) is complete, but is not the Version of Record and does not reflect post-acceptance improvements (such as copyediting or typesetting), or any corrections. The final authenticated version is available online at: https://doi.org/10.1007/978-3-031-94142-9_8. Use of this Accepted Manuscript version is subject to the publisher's Accepted Manuscript terms of use: https://www.springernature.com/gp/open-research/policies/accepted-manuscript-terms
Download date	2026-11-06 16:04:30
Item downloaded from	https://hdl.handle.net/10468/19548



University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Błażej Kaucz

CHAPTER VIII

Criminology on the Fringes of War

Abstract

This chapter offers a criminological perspective on the peripheral effects of war. The idea behind this chapter is not to take away attention from important subjects, like genocide, but rather to highlight other impactful matters related to war and its consequences (i.e., the misplacement of people). Some of these might potentially be applicable to other countries bordering conflict zones. Of importance was the examination of both the direct and indirect impacts of the war on society. This chapter focuses on the complex and often ambiguous nature of crime and security issues that arise in the broader context of war beyond direct combat activities. This highlights the need to understand and address these issues to fully grasp the impact of war on societies and individuals. To this end, it offers real-world scenarios rooted in Poland to illustrate how conflicts spill over into neighbouring regions while especially considering human and citizen rights violations, hybrid warfare, global surveillance, the infosphere, domestic and foreign interferences, shadow economies, surveillance architecture, safeguarding rights, new war geographies, financial tactics, cyberwarfare, new warfare means, and grey zones.

Keywords: Poland, Fringes, War, Criminology, Conflict

Introduction

Poland, at the time of writing this chapter, remains in a liminal space (Szakolczai 2000, 2017; Turner 1995) suspended somewhere between peace and war. A fully fledged war is happening at its doorsteps. Since Ukraine was invaded by Russia on the 24th February 2022, the country that shares a border with Poland has been in a state of war. Poland's other neighbouring state, Belarus, supports this invasion of its next-door country in various forms. This war, from both a geopolitical and social point of view, is intricate to say the least. Poland

is not formally a part of that conflict but sided with Ukraine[1]. The atrocities of war cannot be compared with anything happening on the fringes of warzones or countries involved in conflict. However, this is not the focus of this chapter. Its aim is to shed more light on the problems faced by countries that share a border with another country subjected to a fully-fledged military conflict.

In general, this chapter offers a criminological perspective on war's peripheral effect of war on societies, particularly focusing on Poland's experience with the ongoing conflict in Ukraine. The idea behind this chapter is not to take away attention from important subjects, like genocide, but rather to highlight other impactful matters related to war and its consequences (i.e., the misplacement of people, including academics). Some of these might be potentially applicable to other countries bordering conflict zones. It is crucial to emphasise the significance of examining both the direct and indirect impacts of war on societies and, as a result, the idea for this chapter was born.

Why should we discuss war in the criminological debate? Following the calls issued separately by Ruth Jamieson (1998), Josh R. Klein (2016), and Ross McGarry together with Sandra Walklate (2015), criminological inquiry is being placed on the subject of war and war-related matters. Any conflict and wars, especially incite mass violence, with many victims experiencing suffering, which likely results in long-term trauma. Criminology has made some contributions to the way we understand the direct impact of war on societies in pre-war, war, and post-war conditions. This highlights the significance of engaging in conversation on the various impacts of war on Poland and other bordering countries and on the societal impact of the fringe effects of warts.

The Fringes of War

One such example is the contemporary situation in Poland. The Polish state is not directly involved in or a party to military conflict. Nonetheless, it is involved in supporting Ukraine, its next-door neighbour, which was invaded by Russia (partly in 2014 and on a full scale in 2022). This means that the conflict is seeping into Poland in some ways, which is not always the most expected. This prompts us to consider why criminology should engage in such a conflict. Criminological inquiry should not be limited to examining only the direct and

[1] The various reasons for this are beyond the scope of this chapter. However, Poland also experienced the effects of that conflict, like other countries, in the form of additional price inflation and an influx of people fleeing the war.

indirect consequences of war on the affected populations. Some compelling reasons for criminology to engage with this assessment of conflicts include the intensification of surveillance, the rise in militarisation (and militarism), the complexities of hybrid warfare, and the interplay between surveillance and hybrid warfare as mechanisms of social control, addressing both internal and external threats to safety.

In most circumstances, war leads to restraining civil rights in some way, for example, when new surveillance efforts are employed. This can happen in response to external interference in internal matters, or can only be portrayed as such a response to foreign interventions when the rationale for it might lie elsewhere. In both cases, this leads to a restraint of personal freedoms in the face of (portrayed or real) security threats (Buzan, Wæver, and Wilde 1998; Kaucz 2022; Kraska 2007). The 21st century has brought about a new means of waging wars (or crime-inducing in other states). The case of Poland is interesting, as many war-related processes occur within its boundaries, and wide-ranging ripples of war are becoming visible there as well. It is not a battlefield, but somehow it witnesses many war repercussions that deserve more attention. We should be looking at conflicts more broadly in terms of their wide-ranging consequences beyond the boundaries of the states involved.

Regarding the military conflict taking place in Ukrainian soil, several states supported the conflict on both sides. It appears that Russia's threat of potentially targeting other states if it wins this conflict is becoming more prominent. Consequently, many European states (including some of the Nordic and Baltic states) were involved in it indirectly by supporting firearms, weaponry, military, non-military equipment, and intel to Ukraine. Geographically distant states, such as the USA and the UK[2], also partook in offering training, support, and military equipment to Ukraine. Russia is supported, for example, directly by Iran (i.e., Iranian Shahed drones are used by Russia to attack Ukrainian cities) and North Korea, which supplies its soldiers, and indirectly by China in various forms.

Increased Militarisation (and Militarism)

[2] It is worth noting that after the dissolution of the USSR, Ukraine became the third largest holder of nuclear weapons that it inherited from the Soviet bloc. Ukraine was safekeeping this stock of missiles; however, operationally, Russia was still under its control. In 1994, Ukraine agreed to transfer these back to Russia, which, together with the United States and the United Kingdom, became the signatories of the Memorandum (United Nations 1994). It was agreed as part of that document that Ukrainian independence would be upheld as a result of the transfer of nuclear weapons. Parties agreed "to respect the independence and sovereignty and the existing borders of Ukraine" (ibid.:169).

With military conflicts at one's doorsteps, many military values are becoming more pronounced and incorporated into the everyday lives of citizens (Kaucz 2022). Narratives tied to militarism (military ideology or military influence) and militarisation (socio-political processes that perpetuate militarism)(Enloe 2004; Shaw 2012; Uyangoda 2005) are increasingly appearing in the public sphere and consciousness. One of the signs of these processes taking place in Poland are soaring military expenses at the state level[3]. Even the growing presence of military elements or the absence of opposing principles or narratives in the public domain has the potential to transform visuality into a structure of social power (Brown 2017:10) and to influence public opinion. Thus, visual criminology also plays a role in employing criminological imagination and inquiry into military absence or presence in the public space.

Considering the proliferation of military-related information in the public sphere, information about the military-industrial complex has entered the public sphere more often than ever before into the public sphere in Poland (and elsewhere). This includes, for example, information about military purchases, plans to consider the relevancy of specific equipment in the context of the ongoing war efforts in Ukraine, the long-term consequences to the Polish Army, information about what equipment is being supplied to Ukraine, military strategies and training, considerations in relation to the reintroduction of military conscription, the size and strengths of the army, the role and training of paramilitary organisations, and the specifications of specific military equipment (and its overall role in the Polish military).

With the increasing levels of weapons acquired by the Polish people[4], information about military, military, or military-like equipment that can be purchased by civilians is more visible in the media. It is also one of the signs that militarisation is seeping into public consciousness as an increasing number of individuals consider applying for a firearm permit comparable to any other period after 1989. Increasing militarisation can potentially lead to an abuse of power

[3] The Polish budget for defence in 2025 is planned at PLN 186.6 billions, which corresponds to 4.7 percent of GDP, compared to PLN 137 billions assigned for military expenditure in 2023 and PLN 158,8 billions in 2024 (Polish Press Agency 2024).

[4] The number of people obtaining a firearms permit for a given purpose was 224,651 (in 2019), 286,751 (in 2022), and 323,983 (in 2023), an increase of 37,232 (or 11,50%) year-on-year between 2022 and 2023 and 69,34% increase between 2019 and 2023. The number of firearms registered by firearms permit holders was 551,410 (in 2019), 760,218 (in 2022) and 843,755 (in 2023), an increase of 83,537 (or 9.90%) year-on-year between 2022 and 2023 and a 65,35% increase between 2019 and 2023 (Policja 2024).

since the state is acquiring more equipment and know-how that might be used to control not only the forces outside of the state but also its own citizens (Kaucz 2022).

The growing production of weaponry and dual-use (civil-military) equipment should also be of concern to the public and criminology as an academic discipline. The invasion of Ukraine by Russia (and later the conflict in Israel) ramped up arms production globally. This can also potentially translate into the employment of some of these military technologies and equipment for civilian use as part of the state's surveillance apparatus. The dual use of specific technologies or equipment depends on their application, either internally or externally. For example, Armin Krishnan (2015) recognises that drones can be used differently in these circumstances for the purpose of the "security applications (surveillance) and for unconventional warfare[5] (targeted killings)" (ibid.:13). Also, the same techniques and equipment that are being employed against proxy forces in the hybrid warfare can be used against internal actors who have nothing to do with hybrid wars. Kevin D. Haggerty and Richard V. Ericson (2019) think that the modern military focuses more on using advanced technology for computing, visualisation, and communication. For example, satellites are significant "enablers for military operations in all other domains of warfare: land, sea, air and cyber" (Krishnan 2015:15). Satellites are important as a source of intel but also as a potential source of information needed to wage wars (both in the physical sphere and the infosphere). The same technology that is being used for surveillance to tackle potential internal threats can be used externally to destabilise other states and achieve specific foreign intelligence, surveillance, or intel targets.

This division of internal and external sources of threat loses importance when different lenses are applied. In the context of the militarisation of outer space, this dichotomy is unimportant. This is because global actors have very little incentive to make any differentiation whatsoever as the only important matter is to achieve their greater goals, which might sometimes require local intervention and other times externally. Again, this is because the military importance of outer space relates to the achievement of specific goals that are not necessarily related to a specific state. However, goals can be set by specific country-oriented

[5] One notable example of unconventional warfare that many will recognise involves the suspicious deaths of prominent individuals in recent years. These incidents often include deaths under questionable circumstances involving Russian state agents or company representatives tied to key industries or sectors of the economy that are responsible for strategic resources.

actors, but even in those instances, they can decide to achieve them notwithstanding country boundaries.

Intensifying Surveillance, Espionage, and AI

The spectacle of war, as it is sometimes portrayed in the media, or even the threat of a looming military conflict, can support efforts to increase surveillance. This can also lead to building and reinforcing the acceptance of such increased surveillance as a source of reassurance that the state is in control of these situations and protects its citizens. States and non-state entities (which might be supported by governments) can escalate the use of direct and indirect tools of social control to drive their own agenda in the public sphere. While tapping into some of these countrywide narratives, these actors can use existing narrations devised by other internal (politically driven) factors or local actors (for example, a right-wing party wanting to control the opposition and the overall population). As a result, the efforts of external actors might be attributed to internal actors and pass nearly unnoticed, as the source of these narratives might be misunderstood and considered less of a direct threat.

Surveillance as a tool of social control resides on the other side of the spectrum of the spectacle of war where, as a result of these situations (where external actors intervene in internal politics), state officials can try to subdue their own citizens. This can result in actions employing surveillance tactics that can lead to further decreases in the freedom of citizens, which might have nothing to do with any war efforts. In these instances, states can employ more sophisticated surveillance technologies, including spyware software. Citizens and their rights are at stake, and Poland has become one of the prime examples where the government (between 2015 and 2023) used such technology against its own citizens and in some cases against their political opponents. In publicly known cases, the software known as Pegasus[6] (owned by NSO Group Technologies, an Israeli cyber-intelligence company), which is capable of remotely surveilling mobile phones, was used to intercept information stored on the mobile phones of specific individuals. One such example, which happened in 2019, was related to the head of the campaign run by the largest opposition party. This person's mobile phone was accessed several dozen times during the weeks leading to parliamentary elections (Amnesty International 2022). The use of such technology was apparently sanctioned by the Polish court, under what it looked like a false premise. It is one of the examples when state agencies (but the

[6] In that specific case, Pegasus software was used to monitor citizens' activities. The software itself was purchased using funds allocated to help victims of the crimes.

same applies to private companies) can be gathering data for intel purposes (through the so-called backdoor in software) or thanks to what is known as open source intelligence (OSINT) software, which helps collect resources and publicly available information. The Polish government seemed to have access to at least four different spying programmes in the last few years, namely, Galileo, Pegasus, Predator, and Hermes[7].

Another technology can potentially have socially disruptive characteristics. It seems that artificial intelligence (AI), understood as a system or algorithm capable of performing tasks that normally require human intelligence (Lee 2022), is a double-edged sword that can pose a risk to the privacy of both individuals and societies[8]; however, it can be a useful tool for states to protect themselves from internal and external interference[9]. That is, with increasing levels of routine surveillance entering the daily lives of citizens, for example, any changes in satellite imagery over time can be used to make specific decisions about state interventions. The same capability can be used to determine whether illegal buildings or structures were built without permission or if illegal dumping of waste to rivers, land, or forests occurred. This is one of the problems faced when attempting to critically assess the role of any new technology. It is very difficult to distinguish between social control instruments (used internally towards one's own citizens) and hybrid wars (which are actions employed towards citizens by other actors, including states). Artificial intelligence, especially in its generative form, such as large language models (since it can easily generate content, ideas, and patterns), has the potential to generate information that can effectively influence opinions or decision-makers and aid efforts in spreading propaganda. For the same reasons, AI can also be used to generate deep fakes[10] from photographs and videos. In these instances, media might also play a role, especially when sparking social and moral panics (Cohen 2002; Horsley 2017).

In democratic countries, one of the very few strategies to counterbalance the asymmetry of powers between the government and citizens and redress the ever-present gaze of government officials is to start observing in accordance with the synopticon tactic. In the synopticon, locals observed globals. According to Zygmunt Bauman (Bauman 2001; Bauman

[7] There is also the Hermes' equivalent, Maltego, is also a less sophisticated version of Hermes.

[8] Armin Krishnan (2015) uses the term "the dataveillance of populations" which is a form of the intrusive surveillance technology used to persistently monitor citizens' activity and gather information to be able to influence their lives.

[9] A discussion about the bias that is replicated based on the content that the algorithm was fed initially and other issues related to AI are beyond the scope of this publication.

[10] That can include photographs or videos that were edited or created to support specific narratives or generate non-existent events.

and Lyon 2013), the authority of these global figures comes from their distance, making them seem ‘out of this world.’ They are more noticeable than angels ever were, both out of reach, yet always in view. They are seen as superior but serve as role models, admired, and envied like royalties who lead by example rather than by ruling (Mathiesen 1997). However, this is nearly impossible in the Chinese case, as China has its own ever-present surveillance programme known as 'Smart Cities'. China’s ‘Smart Cities' resemble what Felix Guattari has envisaged in “a city where one would be able to leave one's apartment, one's street, one's neighbourhood, thanks to one's (dividual) electronic card that raises a given barrier; but the cart could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person each person's position–licit or illicit–and effects a universal modulation" (Deleuze 1992:7).

How is it connected to Poland and the Polish situation? Since Poland considers itself to be a part of the democratic world, it should offer some level of constraint to its institutions and be in a position to offer protection to its citizens at the personal level from abuses of power (originating from both the outside and inside of that state). Legal safeguards are in place so that any member of the public can ascertain that their rights will be respected and that the powers of the states are curtailed. However, this was not necessarily the case in Poland. The previous Polish government formed by the Law and Justice (PiS) coalition (2015-2023) operated in a manner that was not constrained by this legal principle. It transpired after the turnover of powers to the new government that some of the senior members of the governing party and government were surveilled by their own peers using the same Pegasus software. The internal interference combined with the abuse of the powers, low pay, and demanding working conditions led some service people (in both police and military forces) in Poland to either quit the service or, if they could, retire from it. This could be one of the possible reasons for the drop in the rate of employment in the police force and the increase in the number of vacant posts in the Polish Police force. This, coupled with police militarisation, led to the undermining of the public faith that the police force is capable of performing its duties. The level of the militarisation of the Polish police force is still nowhere near seen elsewhere; however, there are some early signs that the police force in Poland is transforming and adjusting its tactics employed, especially in relation to crowd control measures. Before 2023, some media outlets periodically included accounts of police brutality, particularly during anti-government protests. However, it is nearly impossible to make any binding conclusions based on that one aspect as

an indicator that the police are expanding the use of the enforcement tools utilised, such as in the USA.

Protecting citizens from the abuse of power from outside forces is also challenging. Espionage became more pronounced, and internal affairs became affected. There are accounts of foreign security forces influencing Polish matters. One such example is the account of a judge who fled to Belarus in 2024 to seek asylum. Before that, he presided over judgments relating to matters of state security requiring a high level of clearance when dealing with documents classified as secret. For years, he had access to the state's confidential information, although it is alleged that he was already working for the Belarusian secret service. As a result, these actions have the potential to have a greater impact on Polish society. Another example of interference by Belarus in Polish matters is the case of the Belarusian oppositionist living in Poland. It was purported that covert actions were taken against him in making attempts to portray him as an alcoholic or unstable person. An appearance was created of a car collision that was meant to be of his making to slander him. Some of these actions are claimed to be performed by Belarusian secret service operatives in cooperation with their Russian counterparts.

So, again, why is it relevant to criminology? Actions to destabilise the Polish, or any other, internal situation should be in the scope of criminological interests and enquiry. These situations should push criminologists to exercise their criminological imagination (Yeomans 2019) to better understand the world around us. Similar to previous examples, provocations initiated by one state should be analysed from the perspective of how these actions serve the interests of the state which initiated it. It is important to consider what they aim to achieve through such provocations and the potential effects on the country in which the provocation takes place.

The Expansion of the Grey Zones and Hybrid Warfare

Since the invasion of Ukraine by Russia (as the representation of a conventional conflict), the use of non-conventional approaches, such as hybrid warfare tactics, has remained as strong as ever. It seems that both conventional conflict and hybrid warfare[11] are compatible with and applicable to modern battlefields. This is especially obvious when we consider actions

[11] Other names for hybrid wars are "new wars, fourth generation warfare, compound warfare" (Herța 2017:135) or "as all-out war, terrorism, proxy-war or the other-than-war operations (a euphemism for international policing/enforcement)" (Kambouris 2024:ix), or a version of an unconventional conflict.

against states or non-state actors who are not necessarily actively or openly involved in the conflict. Hybrid warfare tactics are used, for example, against states which are not part of the conflict, but support one side of the conflict. States can be involved as the target of these covert actions and actively pursue their own actions against the other side of the conflict. The situation becomes even more complicated when these phenomena occur in grey zones[12] facilitated by hybrid warfare.

Grey zones are spaces between war and peace. These can be engineered by proxy entities (for instance, private military contractors or organised crime groups) and can take, for example, a form of covert combat, intelligence operations, or other illegal activities. Grey zones can be created in preparation for a military conflict or any other active involvement against another state. These might be utilised to decrease another state's ability to wage conventional warfare or cyberwarfare. It can also be used to test the war preparedness of another state. Grey zones have a potential to increase chances of one state to draw another state into the orbit of its influence and to create a dependence on that country. According to Azad et al. (2023), the key characteristics of grey zone warfare include (1) staying below the threshold of conventional war, (2) using non-kinetic means (e.g. information operations, cyber warfare, or guerrilla tactics); (3) creating ambiguity and deniability; and (4) gradually changing the status quo. Grey zone warfare overlaps with hybrid warfare, although it may be used together. These spaces relate to what Herfried Münkler (2005:16) sees as "the de-statization of war". It involves the privatisation of military force, an ambiguous boundary between war and peace, and between state-sanctioned violence and criminal violence. Additionally, it highlights the blurring of internal and external matters as well as the line between commercial activities and the use of force.

As a result, grey zones can be utilised to create a space which will weaken the other side. Still, it can also be time consuming but less costly for those starting it than the conventional conflict. Considering the aforementioned end goal (a debilitation of the abilities of the other side for the sake of it or to lower their abilities to protect themselves ahead of a kinetic conflict), the creation of grey zones varies in effectiveness. One can assume that the mastery of the guerrilla tactics belonging to the realm of grey zones may not be as effective short-term as it was assumed in the first two decades of the twenty-first century. It is especially obvious if we look at it from the Russian perspective by comparing it to conventional conflicts,

[12] Sometimes referred to as gray zones.

while considering territorial gain as the final goal. Following this line of thought, one can assume that Russians lost their patience with that sort of tactic in relation to Ukraine (or just entered another phase of the original plan) and decided to invade it. This assumption is based on the idea that the weakening of Ukrainian economic ties with other countries and disinformation companies was insufficient to achieve their goals for Russia. The unsuccessful attempt to instal a presidential figurehead resulted in failure[13]. However, in this specific case, we can see that the attempt to influence the invaded country and its citizens did not cease after the Russian invasion of Ukraine. It was now meant to be a subsidiary means to achieve Russian goals. The shift from a near primary (the Eastern Ukrainian territories were occupied by Russian-supported military groups since 2014) means of waging wars to a secondary one is obvious. It is possible that the strategy to use the "little green men"[14] was not successful in its implementation in the timeframe provided or perhaps that approach meant to prepare for a kinetic conflict which began in 2022 afterall.

Hybrid Warfare

Hybrid wars transform the way conflicts are waged. There are reasons why hybrid warfare (a form of non-kinetic warfare) should be included in the scope of criminological inquiry. It might seem at first sight that this is more to do with security or critical military studies. Nonetheless, in reality, the fact that the consequences of these actions of hybrid warfare are rooted in contemporary societies should also be considered more broadly by criminologists. According to Manousos E. Kambouris (2024) hybrid warfare has expanded its tactics to include provocation, insurgency, economic warfare, covert operations, proxy warfare, and social destabilisation (by extending its reach into the cyberspace domain[15]). Some other examples of hybrid warfare, as a form of a modern unconventional warfare (Kaucz 2019; Miller 2019), include cyberattacks, economic coercion, propaganda campaigns, election interference, diplomatic manoeuvres, covert local criminal formations, and issuing military threats (Sokoli 2024).

[13] Viktor Yanukovych, the fourth Ukrainian president, was driven out of the country in 2014 as a result of Euromaidan mass protests. Yanukovych was supposedly prepared in 2022 to step back in as the president in case of Ukrainian failure to repel the Russian attack.

[14] Using state resources, but portraying it as non-state, in this case, private armies.

[15] The lines between cybercrime and cybersecurity are becoming increasingly blurred and often difficult to distinguish. One geopolitical actor considers a criminal activity (cybercrime) that another may view as a critical security exercise or training.

Hybrid wars are a modern global political trait. They often involve non-state actors such as terrorist groups and are notably linked to Russia's tactics in eastern Ukraine. Additionally, these conflicts represent a form of asymmetric warfare (Herța 2017:135). Kambouris (2024) sees hybrid warfare as an extension of the ages-long approach to both warfare and power grabbing which differ contemporary only as a result of the emerging technologies used by parties involved. Over the years, this technique has been supplemented by new advancements in technology. Conventional weaponry, intelligence information, and espionage techniques have been supplemented over time with biological agents (including the development in nanotechnology resulting in biowarfare and biothreats), surveillance techniques, support of mass migrations, destruction of infrastructure[16], and activity in cyberspace (which could have an impact on both the real and virtual world). A somewhat similar view is offered by Solmaz (2022 cited in Sokoli 2024:3) that hybrid warfare is a complex strategy that merges conventional weapons, irregular tactics, terrorism, and criminal activities within the same conflict zone. It involves the combined use of regular and irregular forces working together towards a unified strategy, employing both military and non-military methods to pose a threat to the enemy. This form of warfare utilises a mix of violent and nonviolent tactics to achieve political objectives, often through non-violent subversive activities. Qureshi (2020) offers a detailed interpretation of hybrid warfare which meant to consist of irregular tactics such as rebellion, insurgency, proxies, and non-state actors; terrorism characterised by unpredictable violence; criminal activities and black market operations, including the smuggling of weapons, drugs, and other illicit items, as well as the involvement of domestic gangs; political strategies such as diplomacy; economic measures such as loans, sanctions, and the sabotage of an economy; informational tactics, including propaganda, misinformation, leaked information, and other information operations; and social strategies involving the domestic population and psychological operations. These actions can be facilitated by official and unofficial lobby groups with a specific agenda, such as think tanks, non-governmental organisations (NGOs), online forum groups, political parties, foundations, and international congresses or conferences. NGOs can act as vehicles of foreign action, leading to internal interference or impediment to internal political processes.

This distinction is that hybrid wars (or warfare) are used outside of nation-states, whereas the social control processes used internally are not so clear or even relevant when

[16] An example of such an important infrastructure that was targeted in the last while are the underwater cables used for the transmission of data and pipes that are utilised for the transportation of valuable resources.

considering the actions of non-state actors. This is due to the problems of establishing exactly the delineation of the interests of specific non-state actors or which arenas are internal or external to them. As a result, they can utilise external social control tools to attain their goals and be in a position to destabilise situations or subdue specific groups of people. Such subdued individuals can be utilised to further destabilise the internal situation.

Various actors (such as armies, states, or non-state actors[17]) can influence the social spheres or infosphere by instilling some of the narratives that support their agendas in various forms or outreach, for example, by using techniques employed by some Internet communities to control information, impact campaigns, influence local or national strategies, create psychological or destabilising operations, initiate covert online activities, generate information warfare (Miller 2019), or employ social engineering techniques (Mitnick 2012). These activities can either be directly executed by the armies or indirectly by so-called “troll farms” (Aro 2020). In 2014, Russia’s military doctrine classified electronic warfare as a type of information warfare. This gives Russia similar benefits to propaganda and cyberattacks, because it is harder to detect and defend against radar and communication jamming than physical attacks. This also makes it challenging to accuse anyone of using electronic warfare in a military court (Aro 2020:83). This is in accordance with what is widely known as the "Gerasimov Doctrine"[18] and what is considered among Russian military strategists as the concept of the New Generation Warfare (Galeotti 2018). It is a conglomerate of ideas and an interpretation of how Valery Gerasimov, a Russian army general, understood modern warfare and the Russian approach to it. This idea relates to the weakening of the enemy by tapping into its problems, creating chaos, and avoiding a head-on confrontation in the first instance by using non-military means. This framework prefers the non-kinetic means of waging war, as when engaging with another country, according to which way of seeing the geopolitics the state is at war with another country.

[17] Like, military and paramilitary groups, criminal networks, and civilian organisations.

[18] On a critical comment highlighting how there was a misunderstanding with who invented the doctrine and why it was named that way, Mark Galeotti, who coined the term "Gerasimov doctrine", notes that Russia has no single war doctrine, but rather "a broad political objective — to distract, divide, and demoralize — but otherwise it is largely opportunistic, fragmented, even sometimes contradictory" (Galeotti 2018:n.p.). In addition, to add further to the confusion, a different military general with a similar sounding name was killed during the first two weeks of the Invasion of Ukraine by Russia. This misunderstanding sparked some discussion in the media around the doctrine itself, and some found it very ironic that its ‘inventor’ died at the beginning of the conflict that was meant to be aligned with it.

Financial tactics are vital when in conflict with either conventional or unconventional states. Securing a stable and uninterrupted flow of finances is important. Shadow economies (Herta 2017:136) are partly responsible for the development of new forms of participation in warfare (that finance or profit from the conflict) and prolongation of military conflicts as more resources are drawn from these and utilised for the purpose of war waging. On the other hand, depriving other parties of conflict of funds can also have advantages. Financial warfare includes more sophisticated forms of economic warfare of embargoes, trade sanctions, blockages, and denying access to strategic resources. It includes precise interference with money flow, leading to operations being compromised in part or entirely as a result (Bracken 2007). Some of these financial tactics are upsetting logistic chains (and making some of the economic nodes inaccessible) which are vital because local economies rely on them as a result of globalisation.

Another sign of a potential activity that can be considered a hybrid warfare venture was occurring in November 2024 on the Baltic Sea, where digital infrastructure was targeted. There were media reports that two undersea data cables were cut, which could potentially disrupt communication and interfere with data transmission in the European region. Thus, from a geopolitical point of view, the states that are connected by these cables are potentially earmarked as targets for internal interference. For citizens, there is a possible threat that actions such as where underwater cables are breached might affect their ability to avail access to data (for example, streaming services) or phone services. Even though, at this occasion, there was no major service interruption for citizens, it is likely that the desired effect was achieved, as this act itself attracted a lot of attention. In light of this, the media also recalled another instance that occurred in the Baltic Sea two years earlier. Several months after the full-scale invasion of Ukraine by Russia in September 2022, the Nord Stream gas pipeline was destroyed (Sytas, Erling, and Ahlander 2024). From a geopolitical standpoint, the Baltic Sea, which borders Poland and most of the rivers drain to it, is becoming an arena for increasing the hybrid warfare activities of several international actors.

Entering the domain of critical military studies, with the intensification of the unconventional conflict, both the human domain (which “deals with all human factors such as leadership, organization, motivation” (Krishnan 2015:18)) and “human terrain” (ibid.:18) Poland became the target of a more scrutinised analysis of outside actors (both state and non-state). The importance of Polish territory and Poland as geopolitical players grew since the war broke out in the neighbouring country, Ukraine. Poland became a hub for military

transportation and logistical operations, aiding Ukraine in its efforts to regain its territory and retain its independence. This led to the intensification of all non-conventional interventions taking place in Poland and was orchestrated by outside actors. This is in line with the so-called "new geography of war" (Gregory 2011 cited in Krishnan 2015:22) leading to destabilising states and companies.

Hybrid Warfare and Interference

Russia is known for its interference[19] with the internal matters of other states[20] (Aro 2020; Wylie 2019). There are signs of such direct and indirect interference with internal Polish matters. There are also some examples of recruitment of Europeans, including Polish citizens, who are willing to perform specific tasks (such as setting fires around various European locations to critical infrastructure or buildings of strategic civil and military purposes) which might benefit Russians. This is because European citizens can freely travel across the European Union states without greater limitations and without drawing attention to themselves which could have been the case with people with Russian passports. Belarus, another of Poland's neighbouring countries, is also accused of interfering with internal Polish matters. Apparently, one such example is the so-called "email scandal" [afera mailowa]. It broke out in early June 2021, when news outlets started to share information about the purported correspondence exchanged between senior government officials. The supposed email correspondence was stolen by hackers from the personal email account of one of the most senior governmental representatives who used it for professional reasons[21].

Another sign of hybrid warfare relates to border controls and intensified conflict-oriented approaches around border control mechanisms and potential crimes occurring in regions adjacent to war zones (including human trafficking and refugee exploitation). Owing to the actions of Belarus and Russia, where both states used displaced individuals, the Polish government decided to erect a border wall (which is also the external border of the European Union). This was done to prevent the use of migrants to destabilise the local and national

[19] According to the international law principle of non-interference, sovereign states should not interfere with each other's internal affairs (Naigen 2016).

[20] For instance, the Russian GRU military intelligence agency is suspected of using non-lethal acoustic weapons against US diplomats, which resulted in the so-called Havana syndrome (AHI) displayed by people attacked by a strong source of sound. In 2021, the Helping American Victims Afflicted by Neurological Attacks (HAVANA) Act was passed by the US Congress as a countermeasure to these actions (Schuster 2024).

[21] Any resemblance to the controversy associated with Hillary Clinton's emails was not an accident. It seems that, in both instances, these leaked emails and the use of personal email accounts for professional use were exploited to influence opinions and undermine government officials.

situation. The wall meant to decrease the use of push-backs by either police, border patrols, or the military, and decrease casualties on both sides[22]. Building walls and using pushbacks acted as consistent deterring strategies. Thus, one side is creating a narrative about a threat to the state's integrity (a form of terrorism) posed by people who cross the borders without the state's control, and the other is claiming that there is an inhuman treatment of people who cross these borders to improve their life circumstances. It is an attempt to reframe the actions of the Polish state as organised state violence. Effectively, the Belarusians are trying to create a narrative of the humanitarian crisis to use defenceless people who are migrating to better lives as a social factor that potentially destabilises the country. This is an attempt to create a narration which might potentially result in mass civil unrest caused by the people crossing the borders, citizens who might oppose the fabricated ineptitude of the state's agents (who were portrayed as those allowing for this situation to happen), or civil rights campaigners who would also be opposing it on the basis of an inhuman treatment of those crossing the borders.

Neither forced migration nor anti-immigration movement occurred in the vacuum. These two need to be considered together to better understand the implications of these processes and the potential rational or motivation behind someone's willingness to make them a social problem that might potentially lead to social unrest. This is because creating social unrest might lead to mass protests or even some form of insurgency against the government at either the local or national level. Intensified border controls on Poland's eastern state borders are a proxy conflict with the Belarusian government. Both parties use migrants to either destabilise the situation in the other country or attain their own goals internally by showing their agency and ability to act according to the state's (or governments') best interest.

At the same time, there are media reports that Belarus is accommodating organised criminal networks responsible for the smuggling of migrants into Europe (while potentially benefiting financially as well from this process) to create a situation which might have a destabilising effect on the public in Poland and Europe. Since 2015, Europe has become a destination for many people who are trying to improve their life situation, escape war conditions, or simply avoid starvation. These people are used instrumentally to create moral panic in the media on the topic of migration. It is very easy to spin most stories about people crossing borders by posing them as a threat to the coherence of society and ways of living.

[22] People on both sides of the border, whether civilians or military personnel, are experiencing significant suffering as a consequence.

Such an approach is an example of the criminalisation of mass mobilisation. Migration is one of these issues at present which is heavily utilised by the far-right in many places in Europe and not only for political gains[23].

Hybrid warfare, as seen its effects in Poland, can be potentially considered through the lens of state crimes. In this case, the state and government agencies of one state try to interfere with the government agencies of another state and influence its citizens. Russia is utilising a range of direct and indirect threats, including nuclear threats, to intimidate Poland and compel its government to discontinue support for Ukraine. In mid-2024, the Russian president called for a change in the Russian nuclear doctrine to threaten the use of nuclear powers in countries which do not have nuclear missiles themselves. This was to empower the ability to intervene and coerce these countries to halt their support for Ukraine.

Global Surveillance and Cyber Warfare

Cyberwar has become an indispensable element of any contemporary armed conflict. It can act as a foreground (similar to hybrid warfare or grey zones) before any physical element of a potential military conflict begins. At present, the divide between civil (internal processes) and military (external interventions) is blurred if not blended completely. At the same time, cyber warfare entered the civil sphere of life and could be as disruptive as physical military conflict itself. In the age of global surveillance of populations by both states and other non-state actors (for example, big technological companies), more activism is entering the public sphere and more people are becoming interested in how data and information about our daily lives are gathered[24]. For example, the Cambridge Analytica scandal illustrates the importance of storing data in a safe way while refraining from sharing it as much as possible. The same scandal sparked new legislative initiatives, but importantly, it became part of the public discourse only a few weeks before the General Data Protection Regulation (GDPR) legislation entered into force in the European Union.

It might be a truism that, in times when a global surveillance architecture is unfolding, citizens' privacy is at risk. For the purpose of this discussion, let us incorporate both the actions of the states and other entities as part of the global surveillance architecture. This also includes big technological companies which often obtain people's data with permission while installing

[23] Obviously, the subject of the wall at the US-Mexican border was also an important issue during the 2016 elections in the USA, and to a degree was revisited during the elections in 2024.
[24] For example, data can be gathered from the state's own databases or open sources (including social media).

their software, such as mobile apps. In specific circumstances, or as a result of specific equipment, nearly everything and everybody can be continuously identified, tracked, and located. The Cambridge Analytica scandal showed that people's data were being used to sway opinions and, even more so, to stimulate strong emotional reactions that can prompt impulsive actions, which individuals may later regret once their emotions subside. Within the context of new digital wars, we need to look at the mechanisms that interfere with narratives present in public spheres. It was an example of how digital spaces are being used to influence and help sway opinions in real life with tangible real-world consequences.

Along the lines of growing public interest in surveillance and social control, Polish citizens also became much more active in terms of how they volunteered their free time after 1989. Several new non-governmental organisations working in the space of human rights have been established or gained prominence. As a result of the news relating to violations of human and citizen rights in Stare Kiejkuty training camp performed by the US military forces using some questionable interrogation techniques, in the last few years, citizens in Poland became much more sensitive to potential harm and injustice. It is harder to sell to Polish people that some of these controversial examination approaches were as a result of the ‘global war on terror’ as this narrative was blemished years ago in the Polish public sphere during the invasion of Iraq and the premises under which it was done at the time.

Propaganda and False Narratives

Propaganda has entered the digital sphere of life and is currently used to influence opinions and dominate narratives. Propaganda, which is part of the “informational warfare” (Herta 2017:140), is responsible for projecting the power of one side and the weakness of the other (Kaucz 2022). It boosts the morale of the army and citizens on the propagating side and undermines that of the opposition. Additionally, it fosters obedience among citizens and promotes disobedience in the enemy’s populace. Propaganda also seeks to identify and exploit vulnerabilities within specific states' operations and societal structures to achieve the goals set by external actors.

Governments can offer false narratives associated with culture, allowing them to act in accordance with their will. In the Polish case, the Law and Justice coalition government tried to persuade the public that the wall which was being built at the Polish-Belarus border is meant to protect from the so-called "illegal immigrants". According to this rationale, migrants cross

the border, flood the streets, and threaten the state's security and personal safety of citizens. At the same time, supposedly, a mechanism was created in the Ministry of Foreign Affairs to offer Schengen visas to nearly 400,000 people (who would be viewed by the same government as culturally foreign) while failing to comply with the visa protocols and arrangements. The only requirement to receive a visa that way was to have payments transferred to and processed by proxy organisations with links to specific individuals in the Ministry of Foreign Affairs. The Polish Prosecutor's Office is still investigating the case at the time of writing this chapter.

In both cases, it is clear that governments can struggle to create specific narratives about culture and the perceived threats that some cultures pose to the state and its citizens. Individuals involved in these two separate situations often share similar cultural backgrounds and come from roughly the same regions. This makes it nearly impossible to uphold the government's narrative that Poland cannot accept people from different origins and cultural backgrounds. This is especially obvious when the state refuses entry to some at its eastern borders on this basis, yet allows others to enter if there is a financial incentive offered to certain officials.

Conclusions

Criminologists, scholars, and anyone interested in the intersections of war, society, and criminal justice should consider the indirect effects of war on neighbouring countries such as Poland. Consequently, this chapter explores the complex interplay between war, criminology, and societal impacts in the context of countries on the fringes of conflict zones with a particular focus on Poland's experiences. This underscores the need for criminology to expand its scope to encompass the broader societal impacts of war, even in regions not directly engaged in conflict. As the nature of warfare evolves, so too must our understanding of its criminological implications. This calls for an interdisciplinary approach to the societal impact of the fringe effects of war that combines insights from criminology, sociology, critical military studies, international relations, cybersecurity, and human rights.

It is important to emphasise that the discussed matters are not just applicable to a single case of Poland but can offer valuable insights for other regions facing similar situations. One of the ideas behind this chapter was to break away from a focus on war impacts on those directly involved and shift it slightly towards the ripple effects of war. This highlights how even areas not directly involved in conflict can experience significant consequences. The essence of this

chapter was to examine the broader impacts of war-related activities that occur outside the central conflict but are still profoundly influenced by it.

This topic is too broad to be fully captured in only one chapter; however, efforts have been made to encapsulate the importance of examining both the direct and indirect impacts of war on societies, including those not directly involved in the conflict. This was exemplified by Poland's engagement in supporting Ukraine amidst the Russian invasion, which led to a seepage of conflict effects, manifesting through increased militarisation, surveillance, refugee exploitation, and strains on civil rights. Therefore, it was an attempt to shed more light on topics related to the impact of hybrid warfare tactics on societal safety and control, new technologies (particularly artificial intelligence), and how these pose challenges to both perpetrating and combating various forms of warfare and crime. Another important topic related to propaganda, false narratives, and information warfare is the shaping of public perceptions and policy responses.

In addition, this chapter offers a space to discuss the growing military influence in everyday life, increased military expenses, the use of military technology, and the proliferation of military-related information in the public sphere. One of the signs is that the level of social control increases when militarisation intensifies. The growing militarisation of the state and its agencies is very visible in Poland. For example, the debate about the reenactment of mandatory military service re-entered the public sphere after the invasion of Ukraine by Russia. In light of the Russian invasion of Ukraine, the last two Polish governments increased the state's expenditure on military and military technology from the advisory baseline for all NATO countries by 2 percent of gross domestic product (GDP) to 4.7 percent of GDP. A substantial rise in military spending has become highly visible in the public domain. Similarly, narratives are crafted and interpreted to leverage this trend, suggesting benefits, such as boosting the state’s economy or enhancing societal safety.

This picture would not be full without an extensive discussion of the fringes and boundaries of various processes, focusing on how they gradually fade, soften over time, or spread more widely. For example, the blurred lines between internal social control mechanisms and external hybrid warfare tactics highlight the need for a broader criminological perspective. There is also a certain overlap between the way we perceive the elements of social control and hybrid warfare. Often, these two methods are employed using the same tools, with the difference being the source of origin. In most cases, social control is internally oriented, and

hybrid warfare is externally oriented. However, both can be used to gather intelligence, perform reconnaissance, and implement surveillance. In addition, there is a certain overlap between hybrid warfare (cyber warfare) and grey zones (spaces between war and peace) that can be used to carry out conventional and unconventional methods of conflict. and hybrid warfare can be viewed as a form of unconventional, non-kinetic warfare. All of these can lead to massive disruptive effects on societies and states, potentially costing lives and money. Similarly, the actions of state and non-state actors (that finance or profit from conflicts) that might obscure the boundaries between legitimate military actions and criminal activities were analysed. Poland exemplifies how so many of these tactics have entered the public sphere and how some of these might pose threats to people's rights.

Another important matter that was discussed had to do with sources of surveillance and interference in internal matters (domestic versus foreign hindrance). This is a double-edged sword. On the one hand, it is used to protect internal matter and, on the other hand, it can harm the same processes if used incorrectly or abused. Thus, how best to utilise it is an important lesson to be learned from Poland. This is especially obvious when considering these matters in tandem with global surveillance efforts in terms of the importance of safeguarding privacy. This is particularly noticeable when various tools of social control and surveillance are used domestically for ad hoc political purposes. Again, threats may emanate from both domestic and international sources. Domestic threats can arise from state and non-state actors within a nation-state, whereas international threats can originate from foreign states and non-state actors.

In terms of policy recommendations and future research, one of the unanswered questions is how to create and include strategies to mitigate the negative impacts of increased military spending on social services, guidelines for balancing security needs with citizens' rights, and suggestions for international cooperation to address the challenges of hybrid warfare and cyber threats. The immediate response is, for instance, the development of oversight mechanisms to ensure the ethical use of surveillance technologies such as Pegasus software. Further research could potentially shed more light on ethical decision making and legal reforms to protect citizens' rights and ensure accountability for state and non-state actors engaged in hybrid warfare tactics. The case of Poland illustrates the need for criminology to further incorporate analyses of state and non-state actors' roles in hybrid warfare and the criminalisation of migration.

Future research directions could involve more empirical studies on the consequences of militarisation in non-war zones. There is also the potential for comparative studies to examine the experiences of other countries bordering conflict zones, in order to distinguish between the universal impacts of war and those that are specific to the local context. This includes discussing how the peripheral impacts of war challenge existing criminological frameworks, and necessitate the integration of war and conflict studies into mainstream criminology. Future research could also focus on developing more robust theoretical frameworks to address these complex issues as well as empirical studies to better understand the long-term societal impacts of living on the fringes of war. Additionally, there is a pressing need to explore the ethical and legal responses to the challenges posed by new forms of warfare and surveillance. There is also space to reflect on the broader societal implications including the impact on populations living in the shadow of conflict, the effect of militarisation and surveillance, and the long-term consequences of a gradual erosion of democratic governance and social cohesion. Therefore, it is crucial to study these fringe effects.

In conclusion, this chapter highlights the critical importance of a nuanced, comprehensive approach for understanding the criminological aspects of modern warfare. It provides an examination of the peripheral effects of war on societies, particularly focusing on Poland's experience of the ongoing conflict in Ukraine. It also emphasises the need for continued vigilance in protecting civil and human rights in an increasingly complex global security landscape. It is also vital to consider the societal impacts of both the immediate and long-term consequences of the fringe effects of war.

References:

Amnesty International. 2022. ‘Poland: Use of Pegasus Spyware to Hack Politicians Highlights Threat to Civil Society’. Retrieved 9 October 2024 (https://www.amnesty.org/en/latest/news/2022/01/poland-use-of-pegasus-spyware-to-hack-politicians-highlights-threat-to-civil-society/).

Aro, Jessikka. 2020. *Trolle Putina*. Wydanie I. Kraków: Wydawnictwo Sine Qua Non.

Azad, Tahir Mahmood, Muhammad Waqas Haider, and Muhammad Sadiq. 2023. ‘UNDERSTANDING GRAY ZONE WARFARE FROM MULTIPLE PERSPECTIVES’. *World Affairs* 186(1):81–104. doi: 10.1177/00438200221141101.

Bauman, Zygmunt. 2001. *Globalization: The Human Consequences*. Repr. New York: Columbia University Press.

Bauman, Zygmunt, and David Lyon. 2013. *Liquid Surveillance: A Conversation*. Cambridge, UK ; Malden, MA: Polity Press.

Bracken, Paul. 2007. 'Financial Warfare'. Retrieved (https://www.fpri.org/article/2007/09/financial-warfare/).

Brown, Michelle. 2017. 'Visual Criminology'. in *Oxford Research Encyclopedia of Criminology and Criminal Justice*. Oxford University Press.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, Colo: Lynne Rienner Pub.

Cohen, Stanley. 2002. *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*. 3rd ed. London; New York: Routledge.

Deleuze, Gilles. 1992. 'Postscript on the Societies of Control'. *The MIT Press* 59(Winter):3–7.

Enloe, Cynthia H. 2004. *The Curious Feminist: Searching for Women in a New Age of Empire*. Berkeley: University of California Press.

Ericson, Richard Victor, and Kevin D. Haggerty, eds. 2019. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Galeotti, Mark. 2018. 'I'm Sorry for Creating the "Gerasimov Doctrine"'. *Foreign Policy*. Retrieved (04/04/2024).

Herța, Laura-Maria. 2017. 'Hybrid Warfare – A Form of Asymmetric Conflict'. *International Conference KNOWLEDGE-BASED ORGANIZATION* 23(1):135–43. doi: 10.1515/kbo-2017-0021.

Horsley, Mark. 2017. 'Forget "Moral Panics"'. *Journal of Theoretical & Philosophical Criminology* 9(2):84–98.

Jamieson, Ruth. 1998. ‘Towards a Criminology of War in Europe’. in *The new European criminology: crime and social order in Europe*, edited by V. Ruggiero, N. South, and I. R. Taylor. London New York: Routledge.

Kambouris, Manousos E. 2024. *Hybrid Warfare 2.2: Where Biothreats Meet Irregular Operations and Cyber Warriors in the 21st Century*. Cham: Springer Nature Switzerland.

Kaucz, Błażej. 2019. ‘Book Review. The Death of the Gods: The New Global Power Grab by Carl Miller’.

Kaucz, Blażej. 2022. *The Militarisation of Behaviours: Social Control and Surveillance in Poland and Ireland*. 1st ed. Cham: Springer International Publishing AG.

Klein, Josh R. 2016. ‘Cultural Criminology of War’. Pp. 369–87 in *The Palgrave Handbook of Criminology and War*, edited by R. McGarry and S. Walklate. London: Palgrave Macmillan UK.

Kraska, P. B. 2007. ‘Militarization and Policing--Its Relevance to 21st Century Police’. *Policing* 1(4):501–13. doi: 10.1093/police/pam065.

Krishnan, Armin. 2015. ‘Mass Surveillance, Drones, and Unconventional Warfare’.

Lee, Jaemin. 2022. *Artificial Intelligence and International Law*. Singapore: Springer Nature Singapore.

Mathiesen, Thomas. 1997. ‘The Viewer Society: Michel Foucault’s `Panopticon’ Revisited’. *Theoretical Criminology* 1(2):215–34. doi: 10.1177/1362480697001002003.

McGarry, Ross, and Sandra Walklate. 2015. ‘Introduction: Placing War within Criminology’. Pp. 1–18 in *Criminology and War*, edited by S. Walklate and R. McGarry. Routledge.

Miller, Carl. 2019. *The Death of the Gods: The New Global Power Grab*.

Mitnick, Kevin D. 2012. *Duch w sieci: przygody najbardziej poszukiwanego hakera na świecie*. Bielsko-Biała: Wydawnictwo Pascal.

Münkler, Herfried. 2005. *The New Wars*. Cambridge Malden MA: Polity.

Naigen, Zhang. 2016. ‘The Principle of Non-Interference and Its Application in Practices of Contemporary International Law’. *Fudan Journal of the Humanities and Social Sciences* 9(3):449–64. doi: 10.1007/s40647-016-0126-y.

Policja. 2024. ‘Broń - Pozwolenia, Wybrane Statystyki’. Retrieved 22 October 2024 (https://statystyka.policja.pl/st/wybrane-statystyki/bron/186394,Bron-pozwolenia.html).

Polish Press Agency. 2024. ‘Szef MON: Mamy Rekordowy Budżet Na Obronność [Minister of National Defense: We Have a Record Defense Budget]’. Retrieved 29 October 2024 (https://www.pap.pl/aktualnosci/szef-mon-mamy-rekordowy-budzet-na-obronnosc=).

Schuster, Steve. 2024. ‘Newly Filed Report with Federal Court Seeks Havana Syndrome Transparency’. *Wisconsin Law Journal*. Retrieved (https://www.proquest.com/scholarly-journals/newly-filed-report-with-federal-court-seeks/docview/3049976747/se-2?accountid=14504).

Shaw, Martin. 2012. ‘Twenty- First Century Militarism: A Historical- Sociological Framework’. in *Militarism and international relations: political economy, security and theory*, *Cass military studies*, edited by A. Stavrianakis and J. Selby. New York: Routledge.

Sokoli, Ylli. 2024. ‘Serbia’s Hybrid Warfare: Consequences for Neighboring Countries’. *Journal of Contemporary European Studies* 1–16. doi: 10.1080/14782804.2024.2338116.

Sytas, Andrius, Barbara Erling, and Johan Ahlander. 2024. Retrieved 20 October 2024 (https://www.reuters.com/business/media-telecom/lithuania-steps-up-surveillance-sea-following-damage-undersea-cable-2024-11-19/).

Szakolczai, Árpád. 2000. *Reflexive Historical Sociology*. London; New York: Routledge.

Szakolczai, Árpád. 2017. *Permanent Liminality and Modernity: Analysing the Sacrificial Carnival through Novels*. London; New York: Routledge, Taylor & Francis Group.

Turner, Victor W. 1995. *The Ritual Process: Structure and Anti-Structure*. New York: Aldine de Gruyter.

United Nations. 1994. *Memorandum on Security Assurances in Connection with Ukraine's Accession to the Treaty on the Non-Proliferation of Nuclear Weapons*. Vol. 3007.

Uyangoda, Jayadeva. 2005. 'Introduction'. *Asia Exchange* 21(1):1–14.

Wylie, Christopher. 2019. *Mindf*ck: Cambridge Analytica and the Plot to Break America*. First edition. New York: Random House.

Yeomans, Henry. 2019. 'Historical Context and the Criminological Imagination: Towards a Three-Dimensional Criminology'. *Criminology & Criminal Justice* 19(4):456–74. doi: 10.1177/1748895818812995.