Journal on Baltic Security, 2022; 8(2): 41-60

Research Article

Open Access
https://doi.org/10.57767/jobs_2022_0015

Elin Berg and Ulrica Pettersson*

Resilience and Resistance in the Digital Age:

Revisiting the Threshold Effect in Total Defence

Received: 5 July 2022
Accepted: 10 October 2022

Abstract: For several years, the Supreme Commander of the Swedish Armed Forces (SAF), M. Bydén, has acknowledged the significance of digital security threats (Bydén, 2017). Even now, he continues to stress the importance of taking such threats seriously; 'Sweden is attacked everyday by means that harm our society today and in the more long-term. We are not in a military conflict on and about Swedish territory, but we are in a conflict about the values we want to uphold and interests we want to be handled in a democratic way' (Dagens Nyheter, 2022).

Keywords: threshold, digital battlefield, small state, resilience.

Introduction

The use of artificial intelligence (AI), disinformation campaigns in social media, and cyberattacks against critical infrastructure are widely acknowledged as significant contemporary security threats (Weissmann, Nilsson, Palmertz and Thunholm, 2021). For more than a decade, scholars have emphasised the dangers associated with the use of advanced technologies in warfare, such as

* **Corresponding author:** Ulrica Pettersson, ulrica.pettersson@fhs.se. Centre of Special Operations Research - Swedish Defence University
Author: Elin Berg, Department of War Studies and Military History - Swedish Defence University.

the use of semi-autonomous weapons like unmanned aerial vehicles, or more as of late, increasingly sophisticated technologies, i.e., autonomous weapons systems (Završnik, 2016; Johansson, 2018).

Within the multi-domain-battlefield (MDB), traditional land, air, and sea domains extend to encompass space and cyber as well (Wilson, 2018), which make contemporary global conflicts and warfare highly affected by both soft power and technological capabilities (Warren, 2014). Academics, private sector actors, and defence practitioners overwhelmingly agree that social media and everyday digital technologies, meaning any electronic equipment, applications, or platforms that communicate, process, and store data (Hirblinger, 2020), similarly transform the battlefield in such a fashion that either promote or seriously obstruct peace and democracy (Hoskins et al., 2020). Bērziņš (2020) convincingly argued that Russia was moving to conduct primarily sub-threshold warfare, and although the recent war in Ukraine has been conventional to a great extent, the war is indicative of the wide range of capabilities at the disposal of the warring parties, sometimes from stemming from rather unexpected sources.

The previous distinction and dichotomy between *defence* and *offense* increasingly converges in three-dimensional ways, with an expanding grey zone that transforms warfare and broadens the category of actors engaged. As mentioned, this dynamic has been visible in Ukraine, where private actors play important roles in supporting Ukraine's defensive efforts against Russia, e.g., through securing internet access via Starlink (Miller et. al, 2022) or proving that war crimes take place through satellite imagery (Hern, 2022). Digital technologies alter the traditionally embodied nature of warfare, which makes way for non-conventional, algorithmically advanced, and detached ways of harming an opponent (for example Thiele, 2016; Nakasone & Lewis, 2017; Atkinson, 2018). Apart from quotidian technologies that have been harnessed as tools of resistance in war, the same technologies also enable hostile activities that target the population of the adversary. As the online/offline and defence/offense dichotomies blur, so does war and peace, which means that military and civilian actors must navigate challenges that seriously threaten

national security and societal resilience against outside interference in the digital sphere.

Current security debates, particularly in the Baltic Sea region, emphasize the whole-of-society approach to counter new threats, and some governments have (re)introduced total defence models (Fiala and Pettersson, 2020), wherein both military and civilian institutions, as well as individuals, play important parts (Wither, 2020). A related body of research also emphasizes the importance of resistance and resilience in the contemporary security landscape (Maskaliūnaitė, 2021). However, it remains somewhat unclear what are the implications digital technology and a broadened security agenda for military organizations, as well as other governmental agencies or actors that co-constitute total defence. In this article, we elucidate and clarify to how digital security threats influence and problematize traditional understandings of conflict escalation. Sweden will act as the example of the ways in which small states can approach the issue of addressing and countering digital threats. We begin by posing the rhetorical and somewhat provoking question: Is there a point (a digital threshold) where attacks in the digital space are so severe and serious that the attacked state could be considered to be at war despite the fact that no conventional kinetic activities yet have occurred?

Digital Battlefields

Against the backdrop of the coronavirus crisis, online activities and technological developments reached record high levels in 2020 across the globe (Kemp, 2020). Globally, populations connect online more than ever before, and the cyber dimension of the MDB has grown unexpectedly quickly. In the beginning of this new wave of digitalization, international organizations, such as United Nations Institute for Training and Research (UNITAR), warned how violent extremist groups may instrumentalise the issue of COVID-19 in online spaces (2020). Additionally, Hagström and Gustafsson outlined how state actors, through politicians and other representatives,

conduct information warfare through the use of different narratives on the pandemic and the COVID-19 virus as part of greater state competition (2021).

Despite an awareness that security threats and conflict have taken this online turn, investments in traditional military capabilities have grown exponentially. Across the globe, defence budgets have drastically increased in the last couple of years, with financial resources being overwhelmingly allocated to the traditional services (SIPRI, 2020). However, the current security landscape in Europe indicates a necessity to further address the potential harm of digital security threats, as well as the capabilities to detect and counter them.

Political, Social and Economic Disruption through Digital Technology

In this section, we emphasize the ways in which warfare and threats arise where they do not exceed the kinetic threshold of open conflict as outlined in military doctrine. Drawing from the case of Sweden, we will illustrate how digital threats can encompass a wide spectrum of targets to disrupt political, social, and economic interests of an opponent state. In line with kinetic military operations, attacks may be covert or clandestine, and proxies may be used. However, these proxies can be human or not human. For example, an opponent or aggressor could use AI-driven bots or make use of servers in other region as to avoid and deny responsibility.

In the spring of 2022, Swedish authorities had to address claims that its social services were kidnapping Muslim children. The disinformation campaign went viral, causing mistrust among Muslims in and outside of Sweden (Regeringskansliet, 2022). In the online videos that were disseminated through social media, the Swedish Government was accused of being a fascist state where social services place Muslim children in Christian homes with paedophiles and forcing them to drink alcohol. Swedish government officials and social services had to come out in force to deny the allegations (Regeringskansliet, 2022). This case illustrates the danger and subtlety of threats in the digital space, which aim to undermine social cohesion, the legitimacy of governmental agencies, or, as the SAF describes it, 'the glue that holds us [a population] together' (Försvarsmakten, 2021).

When discussing online conflict, one problematic aspect is the increasingly large role of private actors. We previously mentioned the ways in which private companies could support resistance and defensive actions, most recently visible in the context of Ukraine. However, Frances Haugen, a former Facebook employee and whistle-blower, has warned that social media platforms run by Meta, particularly Facebook, have inadequately dealt with online misinformation and disinformation, as well as allowed filter bubbles to proliferate on their platform(s). Haugen argues that Facebook continuously prioritizes profits over people, and she claims that Meta has directly allowed for content that sows ethnic violence in places like Myanmar or Ethiopia (Akinwotu, 2021). These are but two examples wherein actors have used digital technology and social media to fuel grievances between different parties, which may result in persecution of specific groups and even genocide. Other examples include state powers supporting anti-establishment actors in other countries' domestic politics, causing disruption or dissent (Jordan, 2020). An often cited example is the 2016 US presidential elections when bot accounts believed to have ties to Russia spread fake news to defame the Democratic Party presidential candidate Hillary Clinton as well as fostered support for the Republican representative Donald Trump (Bovet and Makse, 2019). Similarly, bot accounts and fake accounts spread misinformation and disinformation about the United Kingdom's 2016 Brexit referendum (Trithara, 2020).

In the summer of 2021 in Sweden, one of the main grocery store chains, COOP, faced a cyber-attack that caused their internal systems to collapse, making it impossible for them to charge customers in over 500 of its stores across the country. This situation came to a climax during ransomware cyberattack, where the main target was the IT firm Kaseya, based in the United States. The hacker group Revil (short for Ransomware Evil), with ties to Russia, is likely responsible for the attack, which affected some 200 organizations and companies that use the company's software (Tidy, 2021). Although this attack only affected COOP by proxy, this temporary but severe

disruption led to enormous amounts of food waste. At first glance, this may appear to be a random event – but from a total defence perspective, the attack posed a considerable threat to Swedish food security and resilience. Once again, such examples highlight the unexpected ways that threats can appear digitally, and the variety of individuals, companies, or institutions that become targets in small states and beyond.

There are also more direct and aggressive forms of tactics, such as cyber espionage and terrorism. Other examples may include swaggering, which entails the demonstration of military power and capability through tactics other than direct kinetic action. This may occur through contentious actions near a country's border or an important military site or the testing of new weapons (Art, 1980). The linkages to digital technologies might seem less evident here; however, one can argue that the use of digital technologies to convey messages during conventional battle or crisis belong to this category as well. All the aforementioned threats and tactics fall under the overarching definition of grey zone conflict, which we define further and expand upon in the following section.

Defining the Grey Zone

As highlighted above, the contemporary generation of warfare occurs in both traditional and new digital domains, where opportunities arise for actors to take advantage of from a substantial geographical distance (Wirtz, 2017). In contemporary conflict, 'Any space available may be engaged, [which] includes traditional and modern media instruments' (Thiele, 2016). Furthermore, some scholars argue that such technological developments drive conflict and division, since a state border suddenly can be crossed with one computer click (Kaplan, 2017). Online, ordinary citizens become potential targets of unlawful surveillance or persuasion campaigns spurred by AI-driven fake accounts in comment sections. Horn, Spencer, and Kiras argue that state and non-state actors use tactics of sabotage in digital spaces actively to '… achieve national objectives during those murky periods between peace and outright war' (2021). Strategic sabotage in digital battlefields can be both covert and clandestine. General Gerasimov markedly identified new weaknesses in the modern state defence and highlighted that 'the role of non-military means of achieving

political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness' (2014). According to Weissmann et al. (2021), the indistinct state where acts of aggression remain below the threshold for conflict or war but with potential for serious negative impact on national or international security constitutes the grey zone.

In online and offline domains, actions in the grey zone thus share certain characteristics: their hybrid nature, the risks they pose to the military and defence, and their ability to disturb or skew risk analysis (Wirtz, 2017). Grey zone conflict may occur between states or non-state actors that lack direct or acknowledged incompatibilities or history of combat (Jordan, 2021). Disputes may be subject to de-escalation and escalation, just like a in conventional conflict. This dynamic may be harder to ascertain, as patterns of confrontation are non-linear and sporadic, making it difficult to map the context (battlefield) and actors within it. To the contrary, warfare in the grey zone can also backfire and 'weaken the military, political, and economic position of the instigator' (Young, 2015).

Apart from the examples already mentioned, grey zone threats include economic coercion through trade, cyberattacks on critical infrastructure such as energy systems, aggressive intelligence actions, intimidating military deterrence, or political disruption (Young, 2015). Criminal transactions increase with cryptocurrencies, known as digital gold, where the lack of central control or regulation for such currencies, as well as the possibility of doing anonymous payment instalments is useful for states and non-states actors to circumvent embargos or avoid traceability (Wilson and Howcroft, 2022). Grey zone competition is not new, and non-military means such as influencing campaigns, trade wars or disinformation, characterized considerable portions of the Cold War (Hughes, 2020). However, the digital enablers of grey zone competition transform rapidly, and research, as well as practice related to security and defence, struggle to maintain the same pace.

Small states around the Baltic Sea, including but not limited to Sweden, Finland, Estonia, Lithuania, and Latvia, have long recognized the Soviet Union and later Russia, as a highly superior opponent regarding conventional warfare (Fiala and Pettersson, 2020). With this consideration in mind, these smaller states had to identify other means and strategies to defend their sovereignty, which led to the adoption of deterrence- and resilience-focused models (Braw, 2021). Being prepared to pre-empt or resist grey zone threats constitutes important parts of their strategy, culture, and doctrine to this day (Försvarsmakten, 2016). However, as mentioned earlier, those early models need to be updated to deal with contemporary digital threats. Scholars and practitioners alike debate whether the grey zone definition still serves a purpose, both epistemologically and operationally (Mazarr, 2015; Brands, 2016). Other terms like hybrid warfare, competition short of war and competition below armed conflict (Wirtz, 2017) serve as attempts to label this same phenomenon. One side of the debate posits that the grey zone definition no longer is useful, as it often describes anything and nothing, making the term an all-catch phrase (Raine, 2019). However, setting aside '…the question of the term's appropriateness, grey zone literature is assisting our understanding of rivalry waged below the threshold of armed conflict' (Jordan, 2020). In this article, we therefore use the term grey zone, partly because we find that it properly conveys the expanding field that sits in between the war/peace dichotomy, but also because the grey zone has and continues to play an important role in contemporary security debates. However, given this vivid theoretical and doctrinal debate, challenges arise in terms of common language, definitions, and, consequently, interoperability.

The Threshold Effect from a Small State Perspective

The SAF Strategic Doctrine defines threshold as that which ensures that '…the cost of attack [is] unreasonable for the attacker' (Försvarsmakten, 2016). When analysing Swedish doctrine from 2016 and 2020, the authors note that both documents mention irregular and subversive activities, but it remains unclear how to achieve a non-kinetic threshold and whether this threshold is important. Following such considerations, it is not clear if the threshold effect takes on a different meaning when it comes to digital attacks, or whether the

term is obsolete in these cases. As described in the doctrine, the SAF acts in concert with other agencies and actors in Swedish total defence in ways that deter hostile actions to achieve a threshold effect. In total defence, the military constitutes a threshold against any actor that may attempt to attack or exert pressure on Sweden. Finally, the threshold carries strategic weight through its implied interconnectivity and cooperation with international partners such as the North Atlantic Treaty Organization (NATO) or the European Union (EU) (Försvarsmakten, 2016). Two central government agencies in Swedish total defence that belong to the civilian category are the Swedish Civil Contingencies Agency (SCCA, 2022) and the recently established Psychological Defence Agency (PDA, 2022). However, a search for 'threshold effect' [*tröskeleffekt* in Swedish] on their respective websites resulted in no hits. Although different governmental actors cooperate as part of the wider Swedish security sector, our basic web search implies interoperability issues and a lack of common language between civilian and military actors in total defence. If the concept of the threshold is valid only when it comes to a conventional armed (kinetic) attack, this lack of conceptual stretching could explain why civilian actors do not use the term.

In contemporary warfare, actors harness digital tools where the distinction between peace and war is blurred at best. An aggressor (a state, a non-state actor, or a proxy) can easily conduct severe aggressive activities in the digital space to threaten another state's national security and sovereignty long before a conventional military attack takes place, and the conventional threshold, as currently understood, is exceeded. Digital technologies and digital threats therefore also challenge the military doctrinal understanding of the threshold effect. To return to the issue of a potential digital threshold effect, we reiterate that the SAF doctrine from 2016 and 2020 (Försvarsmakten 2016; 2020) focus solely on the threshold in relation to countering kinetic attacks by potential aggressor(s). The threshold effect as used in the doctrinal context must be adjusted or developed to also include the entirety of today's MBD, which encompasses cyber and space.

Countering Attacks in the Online Grey Zone

The different types of digital grey zone threats outlined in this article '… pose a conundrum for democratic governments trying to ensure that their societies are resilient [… as] the ability of any democratic country to counter hybrid threats, in large part, depends on the willingness of its citizens to support government policies aimed at combating hybrid actors' (Atkinson, 2018). This development remains valid for states of varying sizes and across diverse military capabilities (Thiele, 2016), although we have focused on small states like Sweden for the current study. The use of digital technologies to undermine an adversary and its legitimacy might make a given society less resilient and resistant to potential future military aggression. By dividing and polarising an adversary's population, the resilience and social cohesion may suffer as a result. This can happen as part of preparation for the use of direct force, which was visible in the Russian annexation of Crimea and in its recent military invasion of Ukraine. However, territorial control is no longer always an end state in contemporary conflicts, and we must therefore consider new ways to think about a non-kinetic threshold effect. The new wave of digitalisation triggered partially by COVID-19 highlights the urgency of perspectives that take this changing nature of defence and warfare seriously.

Military actors are aware of the new threats they face in the digital age and that they must understand and assess social media as well as other digital environments. Returning to the case of Sweden since 2020, the SAF collaborates with the Royal Institute of Technology (KTH) in the training of cyber soldiers. Currently, this is Sweden's only centre for cyber soldier conscripts. However, the centre engages in cutting-edge research with the needs of the SAF at its fore as part of a broader effort to prepare and render Sweden's cyber defence and security stronger (Centre for Cyber Defence and Information Security, 2021; Försvarsmakten, n.d.).

Resilience and Resistance to Digital Threats

In this article, we have argued for a need to strengthen interoperability and make sure that actors in total defence share a common vocabulary.

Additionally, we have, through our examples, pointed to the fact that individuals often become targets of campaigns from adversarial states. Given this fact, we will dedicate a part of this paper to address the necessity to link together debates on the threshold effect to concepts of resilience and resistance as well.

Defining resilience is no easy task, as its meaning and application are fluid and context dependent (Vasu, 2016). Both a practical tool and a theoretical concept, it has been used in various social sciences ranging from disaster risk reduction, development studies, and military psychology. In a broad sense, resilience is the capability of a given subject (state, individuals, communities, or environment) to effectively respond to an external shock or threat (Bourbeau, 2013). In military studies, resilience often describes military personnel's mental preparedness for warfare operations or other engagements in contexts shaped by uncertainty, complexity, and physically as well as mentally demanding tasks (Nindl et al., 2018). Here, we would like to acknowledge this vivid and ever-growing research programme, in which scholars and practitioners have examined how to foster digital, cyber, or informational resilience. Some relevant contributions include but are not limited to resilience in relation to online disinformation (Humprecht et al, 2020), information warfare and counter tactics (Clack and Johnson, 2021), and information system resilience (Heeks and Ospina, 2019). Although there are clear connections between these fields and the topic at hand, it lies beyond the scope of the current article to detail how to build and foster digital resilience. However, future scholarship would however do well to link together debates on the grey zone, threshold effect, and resilience.

The concept of resilience is closely intertwined with notions of resistance and the ability and will to withstand or recover from external pressure or malign influence (Stringer and Fiala, 2019). Resilience is a prerequisite for resistance in the event of military aggression or attempts to defame or delegitimise sovereignty by a foreign state or non-state armed group (Fiala and Pettersson, 2020). Resistance, in turn, entails an 'organized, whole-of-society effort,

encompassing the full range of activities from nonviolent to violent, led by a legally established government (potentially exiled/displaced or shadow) to re-establish independence and autonomy within its sovereign territory that has been wholly or partially occupied by a foreign power' (Stringer and Fiala, 2019). A compliant and supportive civilian population undergirds the whole-of-society effort. Consequently, civilians must not only deem intervention and initiatives from the state as legitimate, but they must also be the central actor in resisting any attempt of outside interference or threats (Fiala and Pettersson, 2020).

The Swedish initiative on cyber soldier conscription marks an attempt to broaden the understanding of current conflict environments. To widen their audience and to strengthen the awareness and consequently resilience to digital threats among Swedish citizens, the SAF also released a YouTube documentary series called *When the War Comes*. The episodes cover different security issues that the country faces, with one episode dedicated to hybrid and gray zone threats. The title refers to the *If Crisis or War Comes* pamphlet that all citizens receive by mail as part of Sweden's total defence preparations. The aim is to educate and increase awareness of information operations, thereby increasing popular resilience. One notable difference is the emphasis on when as opposed to if here. This could indicate a shifting, broader view on what constitutes war, and the SAF suggest that battle is not only inevitable but also already ongoing (Försvarsmakten, 2016). Overall, Sweden has taken a few steps towards further developing an overall preparedness towards digital threats. However, as previously highlighted, discussions on interoperability and definitions in this area must continue. It also remains unclear how well civilians are equipped to navigate digital spaces in which malign actors constantly operate and, as such, potentially constitute a civic and *digital* threshold.

In 2016, the United States Special Operations Command Europe (SOCEUR) initiated an effort to design a modernised concept of resilience and resistance. SOCEUR collaborated with the Baltic NATO states of Estonia, Latvia, and Lithuania, as well as with other allies and partners around the Baltic Sea in seminars and workshops. The purpose was to take stock of the lessons learned

from previous stay-behind organizations during WWII (Fiala and Pettersson, 2020). Common efforts between these nations resulted in the articulation of the Resistance Operations Concept (ROC) (Stringer and Fiala, 2019). The ROC (Fiala and Pettersson, 2020) presents a framework to understand how the process of resilience on a national level may increase through the planning, establishment, and development of national resistance capabilities. The concept nicely aligns with debates on total defence and digital technologies, as it emphasises the necessity of converging military power with civilian counterparts to further enable resilience and resistance.

In small states like Sweden, resilience is a prerequisite to withstand external shocks and pressures as well as recover from their effects and resist such influences (Atkinson, 2018). Building resilience can be a powerful remedy against contemporary and complex security threats (Fiala and Pettersson, 2020) that increasingly play out in a digital ecosystem, which civilians inhabit but also hosts militia groups, states, or civil society actors.

The SAF narrates that digital technology and technological developments more broadly are not a panacea of military success but can be tools that contribute to oppression and control by adversaries. However, online spaces and digital technologies can also be potential instruments of fostering a sense of community amongst civilians to strengthen domestic resilience and possibly resistance 'When crisis or war comes'. In turn, resilience needs to be understood as a gradual and continuous process, which occurs spatially both in online and offline. Grey zone threats constantly affect what resilience and defence approaches entail. Therefore, the Armed Forces and their civilian counterparts that together form total defence must conduct ongoing and non-linear analyses to prevent hostile actions from occurring in this grey zone.

Conclusion

Digital battlefields and the tactics used within them have been established and developed with significant speed. Digital threats constitute a natural part of today's warfare and will likely increase in both frequency and intensity in the future. Contemporary technological developments provide a vast palette of tools and opportunities in new hybrid domains. The situation at hand also encompasses new and more diverse actors, which was not imaginable in the era of conventional warfare. Reconnaissance, surveillance, and early warning systems are undergoing rapid transformation and deception and fake news appears to be implemented both clandestine (hidden) and covert (deniable) in digital battlefields.

In this article, we have outlined some of the challenges that have arisen from these developments from the perspective of a small state. As the Swedish total defence model gradually gets more traction, the Armed Forces increasingly have to rely on their civilian counterparts in deterring aggression to protect Swedish sovereignty. However, it is still somewhat unclear what implications digital technology and a broadened security agenda entail for military organizations and other actors involved in total defence. We have stressed a need for a common vocabulary between these actors to increase interoperability. The ROC argues that nations need to plan for resistance and resilience in peacetime, the grey zone, in war, and under occupation. Military doctrine needs to diverge from the linearity of a traditional conflict scale. At the same time, it is central to realize that technology is not a silver bullet, though online spaces and digital tools can constitute potential vehicles to foster community amongst civilians and as such strengthen resilience.

We have discussed what threats and attacks in the digital space may entail. We asked the rhetorical and somewhat provoking question: Is there a digital threshold where attacks in the digital space are so severe and serious that the attacked state could be considered to be at war although no conventional kinetic activities yet have occurred? We do not claim that there is a clear answer, however, by posing the question, we managed to highlight how the digital battlefield comes with many layers of complexity that compels nations to reconsider whether terms used for kinetic warfare are fit for the purpose of

addressing digital threats. Our aim is that this article opens a debate on the concept of the threshold effect in military doctrine and among total defence actors. The current war in Ukraine has again reminded us that kinetic and non-kinetic tactics meld together in twenty-first century warfare and war in line with the Gerassimov doctrine. Following this development, one must carefully consider the ways in which whole-of-society and total defence models are currently implemented and adjust them according to current trends. Finally, one cannot underestimate the importance of discussions on future defence. The purpose of this article is not to raise advanced empty criticisms but rather to raise salient questions and encourage future research and discussion focusing on digital resilience in order to reach new conclusions for the total defence strategies of the future.

Bibliography

Akinwotu, Emmanuel. (2021) 'Facebook's role in Myanmar and Ethiopia under new scrutiny', *The Guardia*n. 7 October. Available at: https://www.theguardian.com/technology/2021/oct/07/facebooks-role-in-myanmar-and-ethiopia-under-new-scrutiny, (Accessed: 1 July 2022).

Art, Robert J. (1980) 'To What Ends Military Power?' *International Security*. 4 (4), pp. 3–35.

Atkinson, Carol. (2018) 'Hybrid Warfare and Societal Resilience: Implications for Democratic Governance', *Information & Security: An International Journal*, 39 (1), pp. 63-76.

Bērziņš, Jānis. (2014) 'Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy', National Defence Academy of Latvia, *Center for Security and Strategic Research*, *Policy Paper, no. 2*.

Bourbeau, Philippe. (2013) Resiliencism: Premises and promises in securitization research. Resilience: International Policies, Discourses and Practices. Available at: https://www.academia.edu/4434934/Bourbeau_Philippe_Resiliencism_Premises_and_promises_in_securitization_research_Resilience_International_Policies_Discourses_and_Practices_2013_1_1_4_17_Lead_Article, (Accessed: 1 July 2022)

Bovet, Alexandre, and Makse, Hernán A. (2019) 'Influence of fake news in Twitter during the 2016 US presidential election', *Nature communications*. 10 (1), pp. 7–14.

Braw, Elisabeth. (2021) *Producing Fear in the Enemy's Mind: How to Adapt Cold War Deterrence for Gray-Zone Aggression*. Research report, The American Enterprise Institute, JSTOR, Available at: https://www.jstor.org/stable/resrep30207?seq=1, (Accessed: 12 June 2022)

Bydén, Micael. (2017) *Förmågor idag och imorgon* - Rikskonferensen. Available at: https://www.forsvarsmakten.se/sv/aktuellt/2017/01/ob-holl-anforande-pa-folk-forsvars-rikskonferens (Accessed: 12 May 2022)

Clack, Timothy, and Johnson, Robert. (Eds.) (2021) *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*. Abindon, Oxon and New York, NY: Routledge.

Dagens Nyheter. (2022) ÖB: Sverige angrips varje dag. 11 January. Available at: https://www.dn.se/sverige/ob-sverige-angrips-varje-dag/ (Accessed: 30 June 2022)

Fiala, Otto, and Pettersson, Ulrica. (2020) 'ROC(K) Solid Preparedness: Resistance Operations Concept in the Shadow of Russia', *Prism*. 8 (4), pp. 17–28.

Försvarsmakten [Swedish Armed Forces] (n.d.) Cyberförsvar. Available at: https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/cyberforsvar (Accessed: 1 July 2022)

Försvarsmakten [Swedish Armed Forces]. (2016) Militärstrategisk doktrin [Stratigic Doctrine] MSD 16, Swedish Armed Forces, Stockholm.

Försvarsmakten [Swedish Armed Forces]. (2020) Militärstrategisk doktrin [Stratigic Doctrine] MSD 20. Swedish Armed Forces, Stockholm.

Försvarsmakten [Swedish Armed Forces]. (2021) When the war comes, episode 2, 'The grey area'. Available at: https://www.youtube.com/watch?v=1985OMqm1pE, (Accessed 1 July 2022)

Gerasimov, Valeri. (2015) Chief of the General Staff of the Russian Federation, 'Moscow's Shadows. Analysis and Assessment of Russian Crime and Security', Available at: https://inmoscowshadows.wordprss.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (Accessed: 6 of Feb 2015)

Hagström, Linus, and Gustafsson, Karl. (2021) 'The limitations of strategic narratives: The Sino-American struggle over the meaning of COVID-19, *Contemporary Security Policy*. 42 (4), pp. 415–449.

Heeks, Richard, and Ospina, Angelica V. (2019) 'Conceptualising the link between information systems and resilience: A developing country field study', *Information Systems Journal* 29 (1), pp. 70–96.

Hern, Alex. (2022) Satellite images of corpses in Bucha contradict Russian claims. *The Guardian*. 5 April, Available at: https://www.theguardian.com/world/2022/apr/05/satellite-images-of-corpses-in-bucha-prove-russian-claims-wrong (Accessed: 1 July 2022)

Hirblinger, Andreas T. (2020) *Digital Inclusion in Peacemaking: A Strategic Perspective*. Geneva, Switzerland: Graduate Institute of International and Development Studies, Center on Conflict and Development and Peacebuilding.

Horn, Bernd, Kiras, D. James, and Spencer, Emily. (2021) *The (in)visible hand: Strategic Sabotage*. Ottowa: CANSOF, Wing Winnipeg Publishing Office.

Hoskins, Andrew. et al. (2020) *Digital war*. Cham, Switzerland: Springer Nature Switzerland AG.

Hughes, Geraint. (2020) 'War in the Grey Zone: Historical Reflections and Contemporary Implications', *Survival (London)*. 62 (3), pp. 131–158.

Humprecht, Edda, Esser, Frank, and Van Aelst, Peter. (2020) 'Resilience to online disinformation: A framework for cross-national comparative research', *The International Journal of Press/Politics* 25 (3), pp. 493-516.

Johansson, Linda. (2018) 'Ethical Aspects of Military Maritime and Aerial Autonomous Systems', *Journal of Military Ethics*. 17 (2–3), pp. 140–155.

Jordan, Javier. (2020) 'International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict', *Journal of Strategic Security*. 14 (1), pp. 1–24.

Kaplan, Robert D. (2019) 'A New Cold War Has Begun', *Foreign Policy*. Available at: https://foreignpolicy.com/2019/01/07/a-new-cold-war-has-begun/, (Accessed: 1 July 2022)

Kemp, Simon. (2020) *Digital 2020: Global Digital Overview*. Available at: https://datareportal.com/reports/digital-2020-global-digital-overview, (Accessed: 1 July 2022)

KTH Royal Institute of Technology (2022) *Centre for Cyber Defence and Information Security*. Available at: https://www.kth.se/cdis/centre-for-cyber-defence-and-information-security-1.946971 (Accessed: 1 July 2022)

Maskaliūnaitė, Asta. (2021) 'Exploring Resistance Operating Concept. Promises and pitfalls of (violent) underground resistance', *Journal on Baltic Security*. Vol 7 (1), pp. 27–38.

Mazarr, Michael J. (2015) *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. U.S. Army War College Carlisle. Available at: https://apps.dtic.mil/sti/citations/AD1000186 (Accessed: 1 July 2022)

Mckew, Molly K. (2017) 'The Gerasimov Doctrine', *Politico*. Available at: https://politi.co/2KZQlKd (Accessed 1 July 2022)

Miller, Christopher, Scott, Mark, and Bender, Bryan. (2022) 'UkraineX: How Elon Musk's space satellites changed the war on the ground', *Politico*. Available at: https://www.politico.eu/article/elon-musk-ukraine-starlink (Accessed: 1 July 2022)

Nakasone, Paul M. & Lewis, Charlie. (2017) 'Cyberspace in Multi-Domain Battle', *The Cyber Defense Review*. 2 (1), pp. 15–26.

Nindl, B., Billing, D., Drain, J., Beckner, M., Greeves, J., Groeller, H., Teien, H., Marcora, S., Moffitt, A., Reilly, T., Taylor, N., Young, A. and Friedl, K. (2018) 'Perspectives on resilience for military readiness and preparedness: Report of an international military physiology roundtable', *Journal of Science and Medicine in Sport*. 21 (11), pp. 1116–1124.

PDA - Psychological Defense Agency [Myndigheten för psykologiskt försvar] (2022). Available at: https://www.mpf.se (Accessed: 1 July 2022)

Raine, J. (2019) 'War or peace? Understanding the grey zone', IISS. Available at: https://www.iiss.org/blogs/analysis/2019/04/understanding-the-grey-zone, (Accessed: 1 July 2022)

Regeringskansliet. (2022) Disinformation campaign against Swedish public authorities regarding social services. Available at: https://www.government.se/articles/2022/02/disinformation-campaign-against-swedish-public-authorities-regarding-social-services (Accessed: 1 July 2022)

SCCA - Swedish Civil Contingencies Agency [Myndigheten för samhällsskydd och beredskap] (2022) Available at: https://www.msb.se/sv, (Accessed: 1 July 2022)

Stockholm International Peace Research Institute (2021) 'World military spending rises to almost $2 trillion in 2020', *SIPRI*. Available at: https://www.sipri.org/media/press-release/2021/world-military-spending-rises-almost-2-trillion-2020 (Accessed: 1 July 2022)

Stringer, Kevin D. & Fiala, Otto C. (2019) 'The ROC: The Resistance Operating Concept: Special Operations Command Europe's Collaborative Approach within Unconventional Warfare', *Special Warfare*. 32 (3).

Thiele, Ralph D. (2016) 'Building Resilience Readiness against Hybrid Threats – A Cooperative European Union/NATO Perspective', Available at: https://www.semanticscholar.org/paper/Building-Resilience-Readiness-against-Hybrid-%E2%80%93-A-Thiele/e84ee04e90228cc69a8029e2cc8b2b67cd22bdf5, (Accessed: 1 July 2022)

Tidy, Joe. (2021) 'Swedish Coop supermarkets shut due to US ransomware cyber-attack', *BBC News*. 3 July. Available at: https://www.bbc.com/news/technology-57707530 (Accessed: 1 July 2022)

Trithara, Dakoda. (n.d.) 'Securitizing Disinformation: The Case of Westminster's Digital, Culture, Media and Sport Committee', *Democracy and security*. (ahead-of-print), 1–28.

United Nations Institute for Training and Research (2020) *Impact of COVID-19 on Violent Extremism and Terrorism*. UNITAR. Available at: https://www.unitar.org/learning-solutions/publications/impact-covid-19-violent-extremism-and-terrorism (Accessed: 1 July 2022)

Vasu, Norman. (2016) 'Resilience and National Security*: "Everyone Has a Plan 'Til They Get Punched in the Mouth",* in *State, Society and National Security*. *World Scientific*. pp. 93–102. Available at: https://www.worldscientific.com/doi/abs/10.1142/9789813140127_0007 (Accessed: 1 July 2022)

Warren, T. Camber. (2014) 'Not by the Sword Alone: Soft Power, Mass Media, and the Production of State Sovereignty', *International organization*. 68 (1), pp. 111–141.

Weissmann, Mikael, Nilsson, Niklas, Palmertz, Björn, and Thunholm, Per. (2021) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris. Available at: http://www.bloomsburycollections.com/book/hybrid-warfare-security-and-asymmetric-conflict-in-international-relations (Accessed: 26 August 2021)

Wilson, D. (2018) 'The Anatomy of Two-Level Maintenance in Multi-Domain Battle', *Army Sustainment*. 50 (1), pp. 32-35.

Wilson, Tom, and Howcroft, Elizabeth. (2022) 'Cryptocurrencies in a time of war', *Reuters*. 4 March. Available at: https://www.reuters.com/technology/cryptocurrencies-time-war-2022-03-04 (Accessed: 1 July 2022)

Wirtz, James J. (2017) 'Life in the 'Gray Zone': observations for contemporary strategists', *Defense & Security analysis*. 33 (2), pp. 106–114.

Wither, James Kenneth. (2020) 'Back to the future? Nordic total defence concepts', *Defence Studies*. 20 (1), pp. 61–81.

Young, Elizabeth. (2013) 'Decade of War: Enduring Lessons from a Decade of Operations', *PRISM*. 4 (2), 123.

Završnik, Aleš. (2016) *Drones and unmanned aerial systems: legal and social implications for security and surveillance*. Cham: Springer.