Journal of Strategic Studies

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fjss20

Strategic studies and cyber warfare

Samuel Zilincik & Isabelle Duyvesteyn

To cite this article: Samuel Zilincik & Isabelle Duyvesteyn (2023): Strategic studies and cyber warfare, Journal of Strategic Studies, DOI: 10.1080/01402390.2023.2174106

To link to this article: https://doi.org/10.1080/01402390.2023.2174106

JOURNAL OF STRATEGIC STUDIES
https://doi.org/10.1080/01402390.2023.2174106

Routledge
Taylor & Francis Group

ARTICLE

Strategic studies and cyber warfare

Samuel Zilincik[a,b] and Isabelle Duyvesteyn[c]

[a]Department of Political Science, Faculty of Social Studies, Masaryk University, Brno, Czechia; [b]Institute of Security and Global Affairs, Faculty of Governance and Global Affairs, Leiden University, The Hague, The Netherlands; [c]Institute of History, Leiden University, The Netherlands

ABSTRACT
This article explores the fashion/popularity of the idea that the exercise of cyber power is a form of warfare. Specifically, the article explains the recent decline of the cyber warfare fashion in academia and discusses its implications for strategic studies. To achieve this, we synthesize observations from previous studies with new quantitative and qualitative data. The article contributes to a growing body of literature by tracing and explaining the history of a particular theme within strategic studies.

KEYWORDS Cyber warfare; cyber war; cyber power; fashion; strategic studies

Introduction

For some three decades, strategic studies communities worldwide have struggled to make sense of cyber power. For this article, we define cyber power as 'the ability to do something strategically useful in' or through 'cyber space'.[1] By cyber space we mean 'a networked system' of 'digital interactions'.[2] The incorporation of cyber power into strategic studies research has progressed significantly, although the distribution of that incorporation has been uneven, both over the course of time and in the depth of scholarly interest. Much of the relevant research on cyber power has only emerged since the late 2000s.[3] Furthermore, the popularity of this research has varied widely among various sub-communities within the field. Some

CONTACT Samuel Zilincik zilinciks@gmail.com Department of Political Science, Faculty of Social Studies, Masaryk University, Jostova 10, Brno, Czechia

[1]The essence of the definition comes from the work of Colin Gray. See Colin Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle: Strategic Studies Institute, 2013), 9; Other scholars have pointed out that cyber power does not cover only what happens in cyber space but also what happens through cyber space. See, for example, Myriam Dunn Cavelty, 'Europe's Cyber-Power', *European Politics and Society* 19/3 (2018), 4.

[2]Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), 3.

[3]This pattern seems to apply across all the relevant journals and also beyond strategic studies scholarship, see Robert Gorwa and Max Smeets, 'Cyber Conflict in Political Science: A Review of Methods and Literature', Working Paper Prepared for the 2019 ISA Annual Convention (Toronto, 2019).

journals have been more welcoming of cyber research than others, depending largely on their intended audience.[4] Nonetheless, incorporating cyber issues into strategic studies scholarship has brought significant changes to the field. For one, a new generation of scholars coming from various backgrounds has built up their careers by exploring the relevance of cyber power to strategic affairs.[5] Furthermore, the field has become divided into 'alarmists', who consider cyber power to be significant to contemporary strategic affairs, and 'skeptics', who expect cyber power to be less potent.[6] New and old research topics have received scholarly attention, and some of these have even become fashionable.[7]

This article explores the fashionableness of the idea that the exercise of cyber power is a form of warfare. More specifically, the article explains the recent decline in the fashion of one manifestation of this idea in the field of strategic studies. The idea originated in the US defence establishment in the 1990s, but it only turned into a 'cyber warfare' fashion in the late 2000s. Strategic studies engaged with the fashion intensely but briefly. This article explains why the field ultimately rejected the fashion and, in the process, shows how even such a brief exposure to a fashion can influence the field in the long term.

We offer a three-fold explanation for the fashion's rejection. First, once the idea turned fashionable under the cyber warfare terminology, its conceptual and social shortcomings became more apparent. Consequently, some strategic studies scholars, but also academics from other fields, were eager to point out these flaws and to reject the terminology. Second, scholars have gradually come up with alternative ways of understanding adversarial digital interactions, ones that do not treat these interactions as a form of warfare. These non-militarized alternatives have allowed scholars to understand digital interactions as a form of 'intelligence contest' or 'cyber conflict'. The cyber warfare terminology then became only one of the several lenses to approach the subject, rendering the former less fashionable. Finally, new militarized concepts have appeared, including hybrid warfare, gray zone warfare and political

[4]For example, journals associated with air forces, such as *Strategic Studies Quarterly*, discuss cyber power more often than the journals associated with naval forces, such as *Naval War College Review*. Similarly, *Survival* publishes more articles on cyber power than *Military Strategy Magazine*.

[5]For example, David Betz, Erik Gartzke, Benjamin Jensen, Lucas Kello, Martin Libicki, David Lonsdale, Jon Lindsay, Ryan Mannes, Thomas Rid, Jacquelyn Schneider, Max Smeets, Danny Steed and many others. Few of these scholars have a formal background in strategic studies. Instead, the majority comes from a wide variety of backgrounds, ranging from political science, international relations, war studies, economics, intelligence studies and computer sciences. Despite this variety in backgrounds, these scholars have significantly enhanced our understanding of how cyber power matters to strategic affairs.

[6]Cameran Ashraf, 'Defining Cyberwar: Towards a Definitional Framework', *Defense & Security Analysis* 37/3 (2021), 279–82.

[7]Gorwa and Smeets, 'Cyber Conflict in Political Science: A Review of Methods and Literature', 8–11. Despite the title, this work also discusses research progress in the mainstream strategic studies scholarship.

warfare. These concepts capture all adversarial exercises of cyber power plus a whole range of other hostile interactions while treating the sum total of these as a form of warfare. Therefore, the need for the cyber warfare terminology declined, and so did the fashion.

The article contributes to a growing body of work that traces the incorporation of cyber power into research on international security and strategic affairs. Some of these works take a broad perspective as they seek to identify the dominant research avenues, methodological issues, and assess how the relevant fields and disciplines have transformed.[8] Other works focus on the history and historiography of narrow topics, such as the issue of cyber deterrence, cyber war or strategic thought related to cyber.[9] Our article contributes mainly to this second, more narrow perspective, though it also discusses more general consequences for the field. The exploration of how and why actors militarize cyber power has become one of the dominant research themes among security studies scholars in recent years.[10] However, the reverse trend, the supposed tendency of people to lose interest in treating cyber power as a form of warfare, has received little scholarly interest.[11] Our article addresses this gap, showing how an exploration of a fashion's decline can constitute a valuable and informative research project.

We present the argument in the following manner. First, the article introduces the idea of treating digital interactions as a form of warfare. Second, it examines how the idea became fashionable and discussed and understood in terms of cyber warfare. Third, it explores the evolution of the cyber warfare fashion in academia, to include showing how the fashion has been in decline for several years now. The penultimate section discusses the reasons for the decline. The concluding section spells out the argument's implications.

[8]Myriam Dunn Cavelty and Andreas Wenger, 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science', *Contemporary Security Policy*, Special Issue: Cyber Security Politics, 40/1 (2020), 5–32; Danny Steed, 'The Strategic Implications of Cyber Warfare', in *Cyber Warfare: A Multidisciplinary Analysis*, James A. Green (ed.), (New York: Routledge, 2015), 73–95; Christopher Whyte and Brian M. Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy* (New York: Routledge, 2019).

[9]Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy* 33/1 (2012), 148–70; Myriam Dunn Cavelty, 'Cyberwar', in *The Ashgate Companion to Modern Warfare*, ed. George Kassimeris and John Buckley (Farnham: Ashgate Publishing Limited, 2010), 123–45; James A. Green and Richard Stiennon, (eds.), 'A Short History of Cyber Warfare', in *Cyber Warfare: A Multidisciplinary Analysis* (New York: Routledge, 2015), 7–32; Elinor C. Sloan, *Modern Military Strategy: An Introduction* (New York: Routledge, 2012), 85–97.

[10]Cavelty and Wenger, 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science', 21–22.

[11]For a rare exception, see Sergei Boeke and Dennis Broeders, 'The Demilitarisation of Cyber Conflict', *Survival* 60/6 (2018), 73–90. However, these authors explore how those responsible for the employment cyber power demilitarize some of its aspects. In contrast, our work focuses primarily on the evolution of (de)militarization in academic discourse.

The idea

The idea of understanding adversarial digital interactions as a form of warfare dates back to at least the early 1990s. The idea emerged in the US military's attempt to make sense of the increased importance of information technologies to contemporary warfare.[12] The idea´s initial foundations were provided by the broader information warfare conceptualization, popular in the US after the First Gulf War.[13] This earlier concept of information warfare was vague as it covered anything from command and control warfare to electronic warfare to psychological operations.[14] However, the US armed services soon began to prioritize the digital aspects of information warfare because of the 'technically-oriented' expertise of those responsible for its implementation.[15] In addition, the armed services began to deliberately elevate the cyber issues associated with 'warfighting support' to the role of 'warfighting' proper to open up new career opportunities for this emerging category of experts.[16] Therefore, the US military was the initial inventor and propagator of the idea.

Other actors also helped to promote the idea. The think tank world's intervention was particularly important. John Arquilla and David Ronfeldt's report for RAND popularized the term 'cyber war' and connected the narrow military focused conception of cyber power with the threat of adversarial cyber-attacks against the broader society.[17] Following this work, and some notable terrorist attacks in the first half of the 1990s, the digital warfare idea was broadened to include attacks against the whole of society, whose increasingly digitalized critical infrastructure was perceived as particularly vulnerable to the exercise of cyber power.[18] The think-tank world also tied this conceptual expansion to the popular debate about 'asymmetric warfare', which concerned the presumed capacity of the US adversaries to by-pass the US armed forces and target the vital organs of the state directly.[19] In addition, media and politicians also militarized the cyber power issue in the early years, though mostly in words rather than in deeds.[20]

[12]Myriam Dunn Cavelty, 'Cyberwar', in *The Research Ashgate Companion to Modern Warfare*, ed. George Kassimeris and John Buckley (Farnham: Ashgate Publishing Limited, 2010), 126–27.
[13]Rebecca Slayton, 'What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018', *Texas National Security Review* 4/1 (2021/2020), 71–72.
[14]Martin Libicki, *What Is Information Warfare?* (Washington: National Defense University, 1995).
[15]Sarah White, 'Subcultural Influence on Military Innovation: The Development of U. S. Military Cyber Doctrine' (Doctoral dissertation, Cambridge, Harvard University, 2019), 377.
[16]Slayton, 'What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018', 63.
[17]John Arquilla and David Ronfeldt, *Cyberwar Is Coming!* (Santa Monica: RAND Corporation, 1992); Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2009), 9.
[18]Ralf Bendrath, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', *Information & Security* 7 (2001), 80–103; Dunn Cavelty, 'Cyberwar', 129.
[19]Ralf Bendrath, Johan Eriksson, and Giampiero Giacomello, 'Cyberterrorism to Cyberwar, Back and Forth: How the United States Securitized Cyberspace', in Johan Eriksson and Giampiero Giacomello (ed.), *International Relations and Security in the Digital Age*, (London: Routledge, 2007), 65.
[20]Bendrath, Eriksson, and Giacomello, 65–67.

Strategic studies scholarship only engaged with the initial idea hesitantly and mostly skeptically.[21] This was probably because most scholars at that time were busy debating the 'New Wars' thesis and the so-called 'Revolution in Military Affairs', neither of which required embracing the idea that digital interactions constitute a form of warfare.[22] Later on, counter- terrorism and counter-insurgency operations became the dominant subjects of strategic studies scholarship, rendering the general issue of cyber power even less salient.[23] Finally, more prosaic reasons, such as the scholars' lack of cyber expertise, may have dissuaded the latter from engaging with the idea more intensely.[24]

The idea gets fashionable

The idea that adversarial digital interactions constitute a form of warfare only became truly fashionable in the late 2000s. A mixture of favorable circumstances contributed to the fashion's emergence. First and foremost, some notable exercises of cyber power took place and drew worldwide attention. These activities included especially the Russian cyber-attacks against Estonia, the Russian use of cyber power alongside conventional military operations in Georgia, and the US-Israeli operation against Iranian nuclear facilities, also known as the Stuxnet attack.[25] These events provided the broader defense community, journalists, and politicians with a great incentive to militarize cyber power not only in words but also in deeds.[26] Notably, the actors dusted off the 'cyber warfare' terminology and employed it to highlight what they perceived to be a salient threat to national security. Additionally, the relevant actors developed institutions, such as the US Cyber Command in 2009, to prevail in what has increasingly been framed and perceived as a cyber war.[27]

This increased attention and institutionalization, in turn, accelerated the US military's embrace of the idea. While the services, especially the US Air Force, continued with the militarization of cyber power throughout the 2000s, the establishment of U.S. Cyber Command offered an impetus for a more concentrated effort. Around this time, the armed forces also fully

[21] Colin Gray, *Modern Strategy* (New York: Oxford University Press, 1999); David Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004); David Betz, 'The More You Know, the Less You Understand: The Problem with Information Warfare', *Journal of Strategic Studies* 29/3 (2006), 505–33.
[22] Christopher Tuck, *Understanding Land Warfare* (London: Routledge, 2014), chapter 9.
[23] Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*, vii – viii.
[24] Gray, 6–7.
[25] Stephen Blank, 'Web War I: Is Europe's First Information War a New Kind of War?', *Comparative Strategy* 27/3 (2008), 227–47; Miroslav Mareš and Veronika Netolická, 'Georgia 2008: Conflict Dynamics in the Cyber Domain', *Strategic Analysis* 44/3 (2020), 224–40; and James P. Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival* 53/1 (2011), 23–40.
[26] Kevin Poulsen. 'Cyberwar' and Estonia's Panic Attack (22 August 2007). Available at: https://www.wired.com/2007/08/cyber-war-and-e/.
[27] Richard A. Clarke, 'War From Cyberspace', *The National Interest* 104 (2009), 31–36.

embraced the linguistic connection of cyber space as a military domain which provided the "foundational metaphor" for subsequent understanding of cyber space as a distinct environment for the conduct of warfare.[28] Additionally, the militarization of cyber space also allowed the military to compete for budget allocations with civilian agencies.[29] Thus, the top-down institutionalization driven by the political elites aligned well with the bottom up effort of the armed services.

As the cyber warfare fashion spread across the society, it also attracted more attention from academics. Besides genuine scholarly interest in the subject, at least two other factors contributed to the academics' engagement with, and sometimes embrace of, the fashion. One was the fact that many scholars now understood both the technicalities of digital interactions and their strategic implications. Subsequently, this new generation of scholars was well-equipped to evaluate the utility of cyber power. Another factor concerned funding. Governments in some Western states were now increasingly willing to support cyber security research through generous grants.[30] This was an incentive for security and strategic studies scholarship to engage with the study of cyber power, and with the cyber warfare fashion, in more depth.

The fashion and the academia

The academic engagement with the fashion has followed a pattern already documented in previous studies. For example, Daniel Hughes and Andrew Colarik have amassed quantitative data to assess the frequency of how the terms 'cyber war' and 'cyber warfare' have been used in academic discourse between 1993 and 2016.[31] These authors follow the established trend of dating the emergence of the cyber warfare terminology to the work of John Arquilla and David Ronfeldt.[32] Yet, as the authors point out, the cyber warfare terminology only became fashionable in academia around the late 2000s. Interestingly, Hughes and Colarik point out that the terminology of cyber war and cyber warfare has been on the decline since around 2014. These findings are in accord with a more recent analysis by Robert Gorwa and Max Smeets, who found a scarcity of cyber warfare articles between the years 1990 and 2010, the greatest number of articles between 2010–2015, and

[28] Jordan Branch, 'What's in a Name? Metaphors and Cybersecurity', *International Organization* 75/1 (2021), 50.
[29] Branch, 50; Jon R. Lindsay, 'Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem', *Intelligence and National Security* 36/2 (2021), 260–78.
[30] See, for example: https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security.
[31] Hughes and Colarik, 'The Hierarchy of Cyber War Definitions', 19.
[32] Although Arquilla and Ronfeldt's initial work was think-tank based, the authors also published in *Comparative Strategy*. It is perhaps for this reason that Hughes and Colarik treat the work as a piece of scholarship. See John Arquilla and David Ronfeldt, 'Cyberwar Is Coming!', *Comparative Strategy* 12/2 (1993), 141–65.

a decline in the number of relevant articles from 2016 onward.[33] Hence Gorwa and Smeets also agree that the first half of the previous decade was 'the golden age of "cyberwar" scholarship' and 'the term appears to have fallen out of favour since 2016'.[34] These studies show a pattern of prolonged stagnation, a sudden rise in popularity, and recent decline.

Our own search for quantitative indications, based on academic output and summarized in Table 1, mostly supports these observations.[35] In accordance with previous studies, we have found the same pattern concerning the terms 'cyber warfare' and 'cyber war'. However, we have also found that other terms associated with the fashion, such as 'cyber domain' and 'cyber deterrence', have risen rather than declined in popularity. These findings imply that even though the cyber warfare fashion declined, it has influenced the relevant fields in the long term. Our search results are summarized in the table below.

Qualitative data align with this pattern. No relevant work employing the cyber warfare terminology within the context of strategic studies emerged before the late 2000s. In contrast, the first half of 2010s saw a rise in influential multi-disciplinary works that partly or fully embraced the fashionable terminology.[36] While strategic studies scholarship never fully embraced the fashion, it engaged with the latter vigorously, as evidenced, for example, by the hugely popular work of Thomas Rid but also the 2013 *Journal of Strategic Studies* roundtable dedicated to the subject of cyber warfare.[37] Similar debates occurred in *Strategic Studies*

Table 1. Cyber warfare fashionability in the relevant literature.

Search terms				
Years	"Cyber warfare"	"Cyber war"	"Cyber domain"	"Cyber Deterrence"
1993 – 2009	4	4	0	1
2010 – 2015	43	29	13	3
2016 – 2021	32	16	31	20

[33] Robert Gorwa and Max Smeets, 'Cyber Conflict in Political Science: A Review of Methods and Literature', Working Paper (as per footnote n. 7), 9. The authors did not focus on strategic studies per se but on political science papers in general. They also did not focus on the topic of cyber warfare exclusively but on a broad range of topics discussed in political science publications.

[34] Gorwa and Smeets, 10.

[35] To map the developments of the last few years, we have searched the Web of Science database for articles with relevant terminology in their titles or abstracts and we have focused on the works from International Relations and Political Science.

[36] Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol: O'Reilly, 2012); Richard A. Clarke and Robert A. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Toronto: HarperCollins Publishers Ltd, 2010); James A. Green, (ed.), *Cyber Warfare: A Multidisciplinary Analysis* (New York: Routledge, 2015); and Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

[37] Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013). For the roundtable, see: https://www.tandfonline.com/toc/fjss20/36/1.

Quarterly and International Security, from 2011 and 2013, respectively.[38] Besides increased numbers of books and articles, new journals embracing the cyber warfare terminology emerged. For example, *International Journal of Cyber Warfare and Terrorism* was established in 2011 and *Journal of Law & Cyber Warfare* started publishing in 2012.[39]

The field's engagement with the cyber warfare fashion from the late 2000s through early 2010s is also apparent in the diversification of research topics that strategic studies scholarship found worthy of inquiry. The fashion stimulated, and in some cases even galvanized, interest in research questions associated with traditional forms of warfare. For example, as indicated by the quantitative data, scholars started to pay more systematic attention to the feasibility of cyber deterrence.[40] Others examined the relevance of classical strategic thinkers to the exercise of cyber power.[41] Some also evaluated the potential of distinct cyber weapons.[42] At the same time, all these subjects have been intensely debated for years even after the fashion declined.[43] Therefore, the fashion normalized thinking about aspects of cyber power in military terms.

The decline of the cyber warfare fashion in academia is apparent from the arguments made by individual scholars. Some authors now explicitly reject the use of the fashion's terminology to denote issues related to cyber power.[44] While there have always been voices critical of the fashion, they have come to dominate the debates in recent years. Consequently, Robert Chesney and Max Smeets have recently boldly proclaimed that 'cyber war is

[38]For SSQ debates, see https://www.jstor.org/stable/e26270505. For IS debates, see Erik Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security* 38/2 (2013), 41–73; Jon R. Lindsay and Lucas Kello, 'A Cyber Disagreement', *International Security*, Correspondence, 39/2 (2014), 181–92.

[39]https://www.igi-global.com/journal/international-journal-cyber-warfare-terrorism/1167; https://www.jstor.org/journal/jlawcyberwarfare.

[40]Will Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly* 4/3 (2009), 102–35; Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?', *Journal of Strategic Security* 7/1 (2013), 54–67; Joseph S. Nye, *Cyber Power* (Cambridge: Belfer Center, 2010); Eric Sterner, 'Retaliatory Deterrence in Cyberspace', *Strategic Studies Quarterly* 5/1 (2011), 62–80; and Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace'.

[41]Craig B. Greathouse, 'Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?', in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller (Heidelberg: Springer, 2014), 21–40; Jeppe T. Jacobsen, 'The Cyberwar Mirage and the Utility of Cyberattacks in War How to Make Real Use of Clausewitz in the Age of Cyberspace' (Danish Institute for International Studies, 2014); and Martin Libicki, 'Why Cyber War Will Not and Should Not Have Its Grand Strategist', *Strategic Studies Quarterly* 8/1 (2014), 23–39.

[42]Matthew Crosston, 'Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game', *Strategic Studies Quarterly* 6/4 (2012), 100–118; Adam P. Liff, 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies* 35/3 (2012), 401–28; and Dale Peterson, 'Offensive Cyber Weapons: Construction, Development, and Employment', *Journal of Strategic Studies* 36/1 (2013), 120–24.

[43]Erica D. Borghard and Shawn W. Lonergan, 'Deterrence by Denial in Cyberspace', *Journal of Strategic Studies* Online First (2021), 1–36; Timothy M. Goines, 'Overcoming the Cyber Weapons Paradox', *Strategic Studies Quarterly* 11/4 (2017), 86–111; Samuel Zilincik, Michael Myklin, and Petr Kovanda, 'Cyber Power and Control: A Perspective from Strategic Theory', *Journal of Cyber Policy* 4/2 (2019), 290–301.

[44]Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*.

out', arguing that academia now increasingly eschews the cyber warfare terminology.[45] Similarly, Miriam Dunn Cavelty and Lennart Maschmeyer titled their recent article 'Goodbye Cyberwar' to show the inadequacy of the terminology to capture reality.[46] Thus, in addition to the terminology being less frequent, it also seems to face more active opposition. Therefore, the tone of the academic discourse has become increasingly critical of the cyber warfare terminology in recent years.

In sum, academic and especially strategic studies scholarship only engaged with the cyber warfare fashion for a period of a few years. While some authors embraced the fashion, many never did, and criticism of the fashion has only grown stronger over the years. The data thus suggest that the cyber warfare fashion has been on the decline in strategic studies, while also leaving something behind. How can we explain this decline? The following sections offer a three-fold explanation.

Explaining the fashion's decline

Three factors figure prominently in the explanations for the decline of the cyber warfare fashion in academia: conceptual flaws, alternative non-military perspectives and broader militarized concepts.

Conceptual flaws

The first reason strategic studies scholarship rejected the cyber warfare fashion has been the latter's perceived flaws, especially its incompatibility with the field's conceptual landscape. As mentioned earlier, the basic idea of treating digital interactions as a form of warfare originated outside of strategic studies. It was only when the idea was imported due to the fashionable terminology that its incompatibility with the field's conceptual foundations became apparent. Strategic studies scholars highlighted this incompatibility and noted a number of other perceived flaws.

One common objection has been that the exercise of cyber power does not fulfill the conceptual criteria of war or warfare and thus should not be labeled as such. Most famously, Rid has pointed out that cyber activities do not fulfill the Clausewitzian criteria of lethality, instrumentality, and political purpose, which disqualifies them as acts of war.[47] Along similar lines, Jeppe

[45]Robert Chesney and Max Smeets, 'Introduction: Is Cyber Conflict an Intelligence Contest?', *Texas National Security Review* Special Issue: Cyber Competition (2020), 2.
[46]Lennart Maschmeyer and Myriam Dunn Cavelty, 'Goodbye Cyberwar: Ukraine as Reality Check', *Policy Perspectives* 10/3 (2022), 1–4.
[47]Rid, *Cyber War Will Not Take Place*. However, other scholars have pointed out that this incompatibility may not be insurmountable and can be alleviated by a reconceptualization of other basic building blocks, such as the concept of violence. See, for example, John Stone, 'Cyber War Will Take Place!', *Journal of Strategic Studies* 36/1 (2012), 101–8.

Jacobsen stressed that activities within cyber space are seldom interactive, and thus cannot constitute war in a classical Clausewitzian sense.[48] Since Clausewitz's ideas constitute the conceptual basis of modern strategic studies, strategic studies scholarship is often suspicious of concepts that violate this basis. As Martin Libicki posits, cyber activities constitute warfare only as a metaphor, not a real phenomenon. Metaphors may serve as a discussion starter, but they are not a substitute for a proper analysis because they cannot holistically capture the phenomenon at hand.[49] Hence the critical flaw here is assuming that just because the use of cyber power resembles warfare in some of its aspects, it is appropriate to equate the two. To avoid this conceptual pitfall, some authors purposefully defined or characterized cyber warfare in peculiar ways. For example, Jeffrey Carr defines cyber warfare as 'the art and science of fighting without fighting; of defeating an opponent without spilling their blood'.[50] Similarly, Danny Steed argues that cyber warfare seems most strategically useful in peace, which is a contradiction in terms, because warfare, at least as classically understood, is a war-time activity.[51] These attempts highlight the key conceptual problem instead of solving it.

A different flaw concerns the vagueness of conceptualization. Some authors define cyber warfare so broadly that it encompasses widely diverging phenomena. The resulting concept of cyber warfare then bundles together activities whose only common denominator is that they might occur in or through cyber space. These activities may include anything from simple hacking to physically damaging network systems.[52] This vagueness hinders clear thinking and communication about a phenomenon, and the concept confuses rather than illuminates. The problem with including such a diverse set of activities under the label of warfare becomes apparent once its logical implications are spelled out. As one scholar points out, 'If espionage is an act of war, then America would be at war even with its allies.'[53] This example illustrates how the internal logic of the concept produces absurd observations if its core characteristics are taken seriously, and their implications are examined.

Conversely, other scholars tend to define cyber warfare so narrowly that the concept does not correspond to any existing empirical phenomenon. If cyber warfare is only supposed to refer to some catastrophic attacks against critical infrastructure, then there is no recorded empirical phenomenon that the concept can capture. Most hostile cyber activities occur frequently and have only minor

[48] Jacobsen, 'The Cyberwar Mirage and the Utility of Cyberattacks in War How to Make Real Use of Clausewitz in the Age of Cyberspace'.
[49] Martin Libicki, *Defending Cyberspace and Other Metaphors* (Washington: National Defense University, 1997), 6.
[50] Carr, *Inside Cyber Warfare*, 2.
[51] Steed, 'The Strategic Implications of Cyber Warfare', 86–87.
[52] For a broad overview of the different meanings behind the term cyber war, see Julian Richards, *Cyber-War: The Anatomy of the Global Security Threat* (Basingstoke: Palgrave Macmillan, 2014).
[53] Troy E. Smith, 'Cyber Warfare: A Misrepresentation of the True Cyber Threat', *American Intelligence Journal* 31/1 (2013), 84.

and temporary effects.[54] As Erik Gartzke explains, those who envision catastrophic cyber scenarios tend to argue from capabilities without considering what political objectives such an exercise of cyber power can serve. As he points out 'much that could happen in the world fails to occur, largely because those who can act discern no meaningful benefit from initiating a given act'.[55] Of course, the possibility of some catastrophic act occurring sometime in the future cannot be ruled out. However, the current situation casts doubt on the utility of the idea.

Finally, it has become increasingly apparent that the fashion's conceptual landscape conveys harmful social and political consequences. Besides offering questionable analytical benefits in the short-term, framing exercises of cyber power as a form of warfare is damaging in the long term, at least in Western liberal democracies. As Myriam Dunn Cavelty points out, this kind of militarization makes practitioners see enemies where none may exist. Furthermore, by drawing attention to the military instrument, the cyber warfare fashion motivates neglect of alternative solutions to the problem, such as cooperation with the private sector. The militarization may also mislead the practitioners regarding the extent to which states can control what happens in cyber space.[56] Therefore, the conceptual deficiencies concerning the cyber warfare fashion may negatively impact real-world security politics.

Non-military perspectives on cyber power

The second factor that explains the decline of the cyber warfare fashion is the emergence of multiple non-militarized perspectives on how to understand cyber power. There have always been parallel ways of thinking about cyber power alongside the cyber warfare fashion. As Dunn Cavelty points out, the two common alternative perspectives have included treating cyber power as a technical problem to be resolved by IT experts or as a crime that can be dealt with by police.[57] Yet the militarization of the cyber power discourse temporarily overshadowed these other lenses. It was only after the shortcomings of the cyber warfare fashion became widely apparent that new alternative perspectives gained traction. Below, we review a representative sample of these perspectives. They include seeing the exercise of cyber power as mere cyber conflict or competition, understanding cyber power as one kind of intelligence activity, categorizing various manifestations of cyber power, and viewing cyber power exercises as a state of 'unpeace'. See Table 2 for the rise of these perspectives measured in quantitative data.

[54]Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*.
[55]Erik Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security* 38/2 (2013), 42.
[56]Myriam Dunn Cavelty, 'The Militarisation of Cyberspace: Why Less May Be Better' (Tallinn: NATO CCD COE, 2012), 1–13.
[57]Dunn Cavelty, 3–4.

Table 2. Results of a Web of Science search for non-militarized approaches to cyber power. The search focused on the titles and abstracts of journal articles from International Relations and Political Science categories and excluded the 'cyber warfare' terminology.

Search terms Years	"Cyber conflict" but not "cyber warfare"	"cyber" and "intelligence" but not "cyber warfare"	"Cyber" and "espionage" or "sabotage" or "subversion" but not "cyber warfare"	"cyber" and "unpeace" but not "cyber warfare"
1993–2009	1	2	48	0
2010–2015	10	16	86	0
2016–2021	18	49	185	1

Some authors have suggested that subtle terminological changes may be useful. Accordingly, instead of cyber warfare, they speak about cyber conflict or competition. The proponents of this perspective argue that the term conflict better captures the reality of constant interactions in and through cyber space that may occur both in war and in peace. The conflict terminology also allows for discussing this phenomenon 'without dealing with the value-laden and poorly bounded concept of cyber-warfare, that infers a number of situational political and legal imperatives'.[58] In essence, this approach also seeks to counter what it sees as an unnecessary and even harmful hype about cyber power.[59] This approach also does not confine cyber activities to any one particular institution but allows both civilian and military institutions to exercise cyber power and to deal with its exercise by others.[60] Other authors argue that the terminology of cyber competition is less constraining than cyber warfare because it allows for appreciating the real capacity of cyber power to produce strategically relevant effects. According to this perspective, the use of cyber power may well be an 'alternative to war' rather than its continuation but it can still produce similar strategic effects.[61] The proponents of this perspective thus argue that a simple and a rather subtle change in terminology is enough to fundamentally alter our understanding of how cyber power works in the real world.

Others have made a case that instead of warfare, exercises of cyber power constitute an 'intelligence contest'.[62] Some authors have highlighted the difficulties of establishing a clear conceptual and practical difference between warfare and intelligence in cyber space.[63] For example, Jon Lindsay finds it

[58]David Ormrod and Benjamin Turnbull, 'The Cyber Conceptual Framework for Developing Military Doctrine', *Defence Studies* 16/3 (2016), 281–82.
[59]Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*.
[60]Peter Dombrowski and Chris C. Demchak, 'Cyber War, Cybered Conflict, and the Maritime Domain', *Naval War College Review* 67/2 (2014), 70–96.
[61]Richard J. Harknett and Max Smeets, 'Cyber Campaigns and Strategic Outcomes', *Journal of Strategic Studies* 45/4 (2022), 535.
[62]https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.
[63]Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013), 58.

'surreal' that U.S. Cyber Command essentially conducts traditional intelligence operations such as propaganda and espionage but pretends that these are military activities.[64] Some authors hence suggest that intelligence is a more useful frame to discuss cyber power, because 'most activities in cyberspace have little to do with the use of force'.[65] Indeed, looking at cyber power in this way allows us to see that the purpose of cyber space activities is to manipulate information.[66] Even though some authors argue that digital technology may indeed be revolutionary, assessing it through the prism of intelligence is adequate and evolutionary.[67] While this perspective remains a subject of heated debates, it has unsurprisingly already gained significant traction among intelligence studies scholars.[68]

Another popular perspective advocates for a granular approach of focusing on specific manifestations of cyber power. For example, some authors now unpack cyber power into espionage, sabotage and subversion/destabilization.[69] Other authors point out that what is often termed cyberwar is, in fact, cyber power expressed in the form of 'criminality, activism or vandalism'.[70] Still others have highlighted deception as a prominent manifestation of cyber power.[71] This granular treatment has a clear advantage of being specific and avoiding vagueness. It emphasizes the clarity of thinking above parsimony, making it ideal for academic analysis.

Interestingly, using alternative perspectives to understand cyber power has also roused the alarmist camp. For example, Lucas Kello has suggested that the right perspective to understand the exercise of cyber power is through the prism of 'unpeace'. Kello recognizes the problem of speaking about warfare in peacetime and hence he comes up with this new label. He defines unpeace as 'a new form of mid-spectrum harm and international rivalry that is neither fatal or physically destructive like traditional war, nor desirable or even tolerable like conventional forms of peaceful rivalry'.[72] Whether this idea gets wider traction is yet to be seen. The fact that even

[64]Lindsay, 'Cyber conflict vs. Cyber Command', 261.
[65]Joshua Rovner, 'Cyber War as an Intelligence Contest', *War on the Rocks*, 16 September 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/, paragraph 4.
[66]Ibid, paragraph 11–12.
[67]David Gioe, Michael S. Goodman, and Tim Stevens, 'Intelligence in the Cyber Era: Evolution or Revolution?', *Political Science Quarterly* 135/2 (2020), 191–224.
[68]For one example of such a heated debate, see this roundtable: https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/#intro.
[69]Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard University Press, 2020); Lennart Maschmeyer, 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations', *International Security* 46/2 (2021), 51–90; and Rid, *Cyber War Will Not Take Place*; Smith, 'Cyber Warfare: A Misrepresentation of the True Cyber Threat'.
[70]Julian Richards. *Cyber-War: The Anatomy of the Global Security Threat* (Basingstoke: Palgrave Macmillan, 2014), 73.
[71]Erik Gartzke & Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace, *Security Studies*', 24/2 (2015) 316–348.
[72]Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017), 249.

some alarmists find alternative perspectives on cyber practical, supports the explanation that the emergence of these alternatives contributes to the decline of the cyber warfare fashion.

Broader militarized concepts

The third factor explaining the decline of the cyber warfare fashion has been the popularization of militarized concepts that cover digital interactions plus additional activities. Concepts such as hybrid, gray-zone and political warfare gained traction, inside and outside of academia, around the time the cyber warfare fashion started to decline. See Table 3 for the rise of these perspectives measured in quantitative data. Authors often use these concepts as a substitute for the cyber warfare terminology to capture the idea that hostile digital interactions constitute a form of warfare. Therefore, these concepts, some of which even constitute new fashions, partially devoured the cyber warfare fashion. Hence, while the decline of the cyber fashion is real, it does not imply the rejection of the underlying idea. Instead, the idea keeps surviving under the different labels associated with these new concepts.

The terminology of hybrid warfare rose to prominence after 2014. While initially intended to describe emerging trends on the battlefield, the concept quickly became a catch-all term covering everything from combining different kinds of forces on the battlefield to combining military and non-military instruments of power to the exclusive use of non-military instruments.[73] As previous studies have already shown, hybrid warfare has gradually come to encompass many activities and meanings previously associated with cyber warfare, such as propaganda conducted through digital media.[74] As Chiara

Table 3. Results of a Web of Science search for broader militarized approaches to cyber power. The search focused on the titles and abstracts of journal articles from International Relations and Political Science categories and excluded the 'cyber warfare' terminology.

Search terms Years	"Hybrid warfare" but not "cyber warfare"	"Grey zone Warfare" but not "cyber warfare"	"Political warfare" but not "cyber warfare"
1993–2009	0	0	5
2010–2015	5	0	3
2016–2021	75	2	13

[73]Ofer Fridman, *Russian 'Hybrid Warfare': Resurgence and Politicization* (Oxford: Oxford University Press, 2018).

[74]Murat Caliskan and Paul A. Cramers, 'What Do You Mean by "Hybrid Warfare"? A Content Analysis on the Media Coverage of Hybrid Warfare Concept', *Horizon Insights* 4 (2018), 23–35; Silvie Janičatová and Petra Mlejnková, 'The Ambiguity of Hybrid Warfare: A Qualitative Content Analysis of the United Kingdom's Political – Military Discourse on Russia's Hostile Activities', *Contemporary Security Policy* 42/3 (2021), 312–44; and Robert Johnson, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies* 29/1 (2018), 141–63.

Libiseller shows in her article for this special issue, hybrid warfare itself has even become a new fashion, though perhaps it is less popular now than a few years ago.[75]

The concept of gray-zone warfare has also gained prominence in recent years.[76] Its proponents reject the idea that the binary of war and peace covers all possible social interactions. Instead, they argue that many hostile activities today occur between war and peace.[77] Since the advocates of the concept seldom define what they mean by war and peace, or they define the terms rather narrowly, it is easy for them to label any hostile activity as occurring somewhere on a continuum. Indeed, some scholars have already argued that gray zone warfare includes manifestations of cyber power.[78] The gray zone warfare concept currently resembles Kello's cyber power concept of unpeace, constituting a broader umbrella term for all perceived hostile actions short of some mythical 'traditional' war. While possibly not as fashionable as hybrid warfare, gray zone warfare enjoys stable popularity in academia and especially outside, in the think tank world.

Political warfare as a label can be traced back to the late 1940s when George Kennan coined the term.[79] However, the term has only recently started to be applied to the exercises of cyber power. The proponents of the term usually employ it to capture a broad range of politically motivated actions short of war. For example, Mark Galleoti uses the term to describe all aspects of Russian foreign policy, including subversive propaganda efforts conducted through digital means.[80] Similarly, Thomas Paterson and Lauren Hanley also use the term to capture digital subversion.[81] The US Marine Corps *Journal of Advanced Military Studies* Volume 12 Issue 1 is dedicated to political warfare, while several of its articles deal with cyber issues.[82] Even some more skeptical scholars of cyber power have already started to employ political warfare terminology to speak about cyber activities or their consequences. Benjamin Jensen and Ryan Maness, for example, argue that 'cyber operations have become a modern manifestation of

[75]Libiseller, Chiara. '"Hybrid warfare" as an academic fashion', *Journal of Strategic Studies*, in this issue.
[76]Note that some authors do not understand gray zone activities to constitute a form of warfare. See, for example, Michael J. Mazarr, *Mastering The Gray Zone: Understanding a Changing Era of Conflict* (Carlisle: Strategic Studies Institute, 2015). In these cases, the concept of gray zone fits among the alternative perspectives on cyber power discussed in the previous section.
[77]Elizabeth J. Troeder, *A Whole-of-Government Approach to Gray Zone Warfare* (Carlisle: US Army War College Press, 2019).
[78]See, for example, Jahara W. Matisek, 'Shades of Gray Deterrence: Issues of Fighting in the Gray Zone', *Journal of Strategic Security* 10/3 (2017), 1–26; Omer Dostri, 'The Reemergence of Gray-Zone Warfare in Modern Conflict', *Military Review*, 2020, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2020/Dostri-Gray-Zone/.
[79]George Kennan, *Policy Planning Staff Memorandum*, May 1948.
[80]Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (London: Routledge, 2019).
[81]Thomas Paterson and Lauren Hanley, 'Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'deep Fakes', *Australian Journal of International Affairs* 74/4 (2020), 439–54.
[82]Available at: https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-Vol-12-No1/.

political warfare'.[83] Similarly, Christopher Whyte speaks about the 'second-order effects' of cyber power as changing politics, the process he calls 'cyber-enabled political warfare'.[84] The fact that even some of the skeptics find this term useful means that unlike hybrid and gray zone warfare, political warfare has garnered support across the strategic studies community.

To be sure, these concepts suffer from serious conceptual flaws on their own. Hybrid warfare has become such a broad umbrella that it now captures almost any act of hostility across history, rendering the term meaningless.[85] The gray zone warfare literature suffers from poor conceptualization.[86] The absurdity of political warfare as a concept is already apparent from the label itself as all warfare is inherently political. These shortcomings decrease the chances that the concepts would remain popular in academia for prolonged periods of time. Even the once extremely popular hybrid warfare fashion seems to be on decline after the heavy criticism it has suffered. The point is that these new concepts can easily be replaced by yet another fashion, which preserves the idea that adversarial digital interactions constitute warfare but repackages it under different terminology. This, at least, is what the described developments indicate.

Conclusion

At least in the context of strategic studies, the cyber warfare fashion, was indeed 'transitory, vague, and powerful'.[87] Strategic studies scholarship only engaged with the fashion briefly, for a few years. The fashion has been characterized by elusive meaning of its terms, which has ultimately been one of the reasons for its academic downfall. Despite the brief engagement, the cyber warfare fashion changed the field, motivating a re-examination of its foundations, stimulating new research avenues but also challenging the field's conceptual basis and popularizing the idea that has formed the bedrock of subsequent fashions. These consequences warrant more detailed discussion.

First and foremost, it is worth highlighting the fashion's positive impact. The engagement with the cyber warfare fashion provoked genuine debates

[83]Benjamin Jensen and Ryan C. Maness, 'Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist', *Journal of Strategic Studies* 42/2 (2019), 212; Similar argument is also advanced in Brandon Valeriano and Benjamin Jensen, 'Innovation and the Proper Context of Cyber Operations: The Path to Avoid Cyber War', *Marine Corps Gazette* 105/2 (2021), 39–43.

[84]Christopher Whyte, 'Beyond Tit-for-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online', *European Journal of International Security* 5 (2020), 196.

[85]Donald Stoker and Craig Whiteside, 'Blurred Lines: Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking', *Naval War College Review* 73/1 (2020), 1–37.

[86]Adam Elkus, '50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense', *War on the Rocks* (blog), 2015, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/.

[87]Jeffrey Michaels and Chiara Libiseller, 'Introduction', *Journal of Strategic Studies*, in this issue.

about the field's conceptual foundations, which was largely missing before. This exercise was beneficial to the field's further development as it motivated scholars to re-examine their long-held assumptions about what is war, violence, strategy, etc. Furthermore, the fashion also stimulated the development of novel research questions and normalized thinking about cyber power in terms of vocabulary associated with traditional warfare. This effect, in and of itself, was not inherently bad for the field. In fact, even though the fashion has ultimately been rejected, it constituted a stimulus for the field's growth in new directions. This is worth keeping in mind when engaging with other fashions; the mere process of engagement may have some positive consequences.

Second, the fashion's negative impact is hard to overlook. Even though the core fashionable terminology has not caught up, some corners of strategic studies scholarship have been sympathetic to the underlying idea of treating digital interactions as a form of warfare. This at least partly favorable reception made it easier for subsequent fashions to infiltrate the field and wreak further havoc on its conceptual landscape. Hence, some of the current confusion about what constitutes war and peace, or about what the means of strategy are, is a legacy of the idea first imported through the cyber warfare fashion. This is again something to bear in mind in future encounters with any sort of fashion: the field's conceptual landscape suffers when it is challenged to accommodate ideas imported from the outside.

The fashion lens usefully highlights the difference between the general idea and its fashionable manifestations. The underlying idea of treating adversarial digital interactions as warfare has been around for decades, but its specific manifestations only became fashionable when the social circumstances became favorable. This observation implies a crucial question that has to be resolved. Rather than focusing on the specific fashion, such as cyber warfare or hybrid warfare, it is crucial to examine the idea that digital interactions constitute warfare. Strategic studies scholarship must resolve the question whether the idea, and its implications, make sense or not. If yes, the field will have to alter its conceptual landscape to accommodate the idea. If not, there are non-militarized alternatives which we can employ to assess the utility of cyber power, although strategic studies, because of its military focus, may not be the best field to utilize these. What certainly does not make sense is postponing the decision. If we do not resolve this question, the production of terminologically fashionable but internally similar concepts will continue and, while bringing some benefits, it will also keep ravaging any meaningful conceptual basis we have developed in the meantime.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Samuel Zilincik is a doctoral student of security and strategic studies at Masaryk and Leiden Universities and a lecturer at the University of Defence in the Czech Republic. His research interests include military strategy in general and its emotional aspects in particular.

Isabelle Duyvesteyn is Professor of International Studies at Leiden University in the Netherlands. She obtained her PhD from the Department of War Studies at King's College in London and has worked on issues related to strategy, contemporary war and peace, as well as rebel governance and legitimacy.

Bibliography

Arquilla, John and David Ronfeldt, *Cyberwar is Coming!* (Santa Monica: RAND Corporation 1992).

Arquilla, John and David Ronfeldt, 'Cyberwar is Coming!' *Comparative Strategy* 12/2 (1993), 141–65. doi:10.1080/01495939308402915.

Ashraf, Cameran, 'Defining Cyberwar: Towards a Definitional Framework' *Defense & Security Analysis* 37/3 (2021), 274–94. doi:10.1080/14751798.2021.1959141.

Bendrath, Ralf, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection' *Information & Security* 7 (2001), 80–103. doi:10.11610/isij.0705.

Bendrath, Ralf, Johan Eriksson, and Giampiero Giacomello, 'Cyberterrorism to Cyberwar, Back and Forth: How the United States Securitized Cyberspace', in Johan Eriksson and Giampiero Giacomello (eds.), *International Relations and Security in the Digital Age* (London: Routledge 2007), 57–82.

Betz, David., 'The More You Know, the Less You Understand: The Problem with Information Warfare' *Journal of Strategic Studies* 29/3 (2006), 505–33. doi:10.1080/01402390600765900.

Blank, Stephen., 'Web War I: Is Europe's First Information War a New Kind of War?' *Comparative Strategy* 27/3 (2008), 227–47. doi:10.1080/01495930802185312.

Boeke, Sergei and Dennis Broeders, 'The Demilitarisation of Cyber Conflict' *Survival* 60/6 (2018), 73–90. doi:10.1080/00396338.2018.1542804.

Borghard, Erica D. and Shawn W. Lonergan, 'Deterrence by Denial in Cyberspace' *Journal of Strategic Studies* (2021), 1–36. doi:10.1080/01402390.2021.1944856.

Branch, Jordan., 'What's in a Name? Metaphors and Cybersecurity' *International Organization* 75/1 (2021), 39–70. doi:10.1017/S002081832000051X.

Buchanan, Ben., *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge: Harvard UP 2020).

Caliskan, Murat and Paul A. Cramers, 'What Do You Mean by "Hybrid Warfare"? A Content Analysis on the Media Coverage of Hybrid Warfare Concept' *Horizon Insights* 4 (2018), 23–35. doi:10.31175/hi.2018.04.02.

Carr, Jeffrey., *Inside Cyber Warfare* (Sebastopol: O'Reilly 2012).

Chesney, Robert and Max Smeets,'Introduction: Is Cyber Conflict an Intelligence Contest?' *Texas National Security Review* (2020), 2–10. Special Issue: Cyber Competition.

Clarke, Richard A., 'War from Cyberspace' *The National Interest* 104 (2009), 31–36.

Clarke, Richard A. and Robert A. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Toronto: HarperCollins Publishers Ltd 2010).

Crosston, Matthew., 'Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game' *Strategic Studies Quarterly* 6/4 (2012), 100–18.

Dombrowski, Peter. and Chris C. Demchak, 'Cyber War, Cybered Conflict, and the Maritime Domain' *Naval War College Review* 67/2 (2014), 70–96.

Dostri, Omer., 'The Reemergence of Gray-Zone Warfare in Modern Conflict' *Military Review* (2020). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2020/Dostri-Gray-Zone/ .

Dunn, Cavelty. and Myriam, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge 2009).

Dunn, Cavelty and Myriam, 'Cyberwar', in George Kassimeris and John Buckley (eds.), *The Research Ashgate Companion to Modern Warfare* (Farnham: Ashgate Publishing Limited 2010), 123–44.

Dunn, Cavelty and Myriam, *The Militarisation of Cyberspace: Why Less May Be Better* (Tallinn: NATO CCD COE 2012), 1–13.

Dunn, Cavelty and Myriam, 'Europe's Cyber-Power' *European Politics and Society* 19/3 (2018), 304–20. doi:10.1080/23745118.2018.1430718.

Dunn, Cavelty, Myriam, and Andreas Wenger, 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science' *Contemporary Security Policy* 40/1 (2020), 5–32. Special Issue: Cyber Security Politics. doi:10.1080/13523260.2019.1678855.

Elkus, Adam., '50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense' *War on the Rocks* (2015). https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/.

Farwell, James P. and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War' *Survival* 53/1 (2011), 23–40. doi:10.1080/00396338.2011.555586.

Fridman, Ofer., *Russian 'Hybrid Warfare': Resurgence and Politicization* (Oxford: Oxford UP 2018).

Galeotti, Mark., *Russian Political War: Moving Beyond the Hybrid* (London: Routledge 2019).

Gartzke, Erik., 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth' *International Security* 38/2 (2013), 41–73. doi:10.1162/ISEC_a_00136.

Gioe, David, Michael S. Goodman, and Tim Stevens, 'Intelligence in the Cyber Era: Evolution or Revolution?' *Political Science Quarterly* 135/2 (2020), 191–224. doi:10.1002/polq.13031.

Goines, Timothy M., 'Overcoming the Cyber Weapons Paradox' *Strategic Studies Quarterly* 11/4 (2017), 86–111.

Gomez, Miguel A. N., 'Arming Cyberspace: The Militarization of a Virtual Domain' *Global Security and Intelligence Studies* 1/2 (2016), 42–65. doi:10.18278/gsis.1.2.4.

Goodman, Will., 'Cyber Deterrence: Tougher in Theory Than in Practice?' *Strategic Studies Quarterly* 4/3 (2009), 102–35.

Gorwa, Robert and Max Smeets. 'Cyber Conflict in Political Science: A Review of Methods and Literature'. Working Paper Prepared for the 2019 ISA Annual Convention. Toronto, 2019.

Gray, Colin., *Modern Strategy* (New York: Oxford UP 1999).

Gray, Colin., *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle: Strategic Studies Institute 2013).

Greathouse, Craig B., 'Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?', in Jan-Frederik Kremer and Benedikt Müller (eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (Heidelberg: Springer 2014), 21–40.

Green, James A. (ed.), *Cyber Warfare: A Multidisciplinary Analysis* (New York: Routledge), 2015.
Harknett, Richard J. and Max Smeets, 'Cyber Campaigns and Strategic Outcomes' *Journal of Strategic Studies* 45 (2020), 534–67. Online First. doi:10.1080/01402390.2020.1732354.
Hughes, Daniel and Andrew Colarik, 'The Hierarchy of Cyber War Definitions', in G. A. Wang, Michael Chau, and Hsinchun Chen (eds.), *Intelligence and Security Informatics* PAISI: Pacific-Asia Workshop on Intelligence and Security Informatics (Cham: Springer 2017), 15–33.
Iasiello, Emilio., 'Is Cyber Deterrence an Illusory Course of Action?' *Journal of Strategic Security* 7/1 (2013), 54–67. doi:10.5038/1944-0472.7.1.5.
Jacobsen, Jeppe T., *The Cyberwar Mirage and the Utility of Cyberattacks in War How to Make Real Use of Clausewitz in the Age of Cyberspace* (Copenhagen: Danish Institute for International Studies 2014).
Janičatová, Silvie and Petra Mlejnková, 'The Ambiguity of Hybrid Warfare: A Qualitative Content Analysis of the United Kingdom's Political–Military Discourse on Russia's Hostile Activities' *Contemporary Security Policy* 42/3 (2021), 312–44. doi:10.1080/13523260.2021.1885921.
Jensen, Benjamin and Ryan C. Maness, 'Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist' *Journal of Strategic Studies* 42/2 (2019), 212–34. doi:10.1080/01402390.2018.1559152.
Johnson, Robert., 'Hybrid War and Its Countermeasures: A Critique of the Literature' *Small Wars & Insurgencies* 29/1 (2018), 141–63. doi:10.1080/09592318.2018.1404770.
Kello, Lucas., *The Virtual Weapon and International Order* (New Haven, CT: Yale UP 2017).
Libicki, Martin., *What is Information Warfare?* (Washington: National Defense University 1995).
Libicki, Martin., *Defending Cyberspace and Other Metaphors* (Washington: National Defense University 1997).
Libicki, Martin., 'Why Cyber War Will Not and Should Not Have Its Grand Strategist' *Strategic Studies Quarterly* 8/1 (2014), 23–39.
Libiseller, Chiara., '"Hybrid warfare" as an academic fashion' *Journal of Strategic Studies* in this issue.
Liff, Adam P., 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War' *Journal of Strategic Studies* 35/3 (2012), 401–28. doi:10.1080/01402390.2012.663252.
Lindsay, Jon R., 'Cyber Conflict Vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem' *Intelligence and National Security* 36/2 (2021), 260–78. doi:10.1080/02684527.2020.1840746.
Lonsdale, David., *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass 2004).
Mareš, Miroslav and Veronika Netolická, 'Georgia 2008: Conflict Dynamics in the Cyber Domain' *Strategic Analysis* 44/3 (2020), 224–40. doi:10.1080/09700161.2020.1778278.
Maschmeyer, Lennart., 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations' *International Security* 46/2 (2021), 51–90. doi:10.1162/isec_a_00418.
Maschmeyer, Lennart and Myriam Dunn Cavelty, 'Goodbye Cyberwar: Ukraine as Reality Check' *Policy Perspectives* 10/3 (2022), 1–4.

Matisek, Jahara W., 'Shades of Gray Deterrence: Issues of Fighting in the Gray Zone' *Journal of Strategic Security* 10/3 (2017), 1–26. doi:10.5038/1944-0472.10.3.1589.

Mazarr, Michael J., *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle: Strategic Studies Institute 2015).

Michaels, Jeffrey and Chiara Libiseller,'Introduction' *Journal of Strategic Studies* (forthcoming): in this issue.

Nye, Joseph S., *Cyber Power* (Cambridge: Belfer Center 2010).

Ormrod, David and Benjamin Turnbull, 'The Cyber Conceptual Framework for Developing Military Doctrine' *Defence Studies* 16/3 (2016), 270–98. doi:10.1080/14702436.2016.1187568.

Paterson, Thomas and Lauren Hanley, 'Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes' *Australian Journal of International Affairs* 74/4 (2020), 439–54. doi:10.1080/10357718.2020.1734772.

Peterson, Dale., 'Offensive Cyber Weapons: Construction, Development, and Employment' *Journal of Strategic Studies* 36/1 (2013), 120–24. doi:10.1080/01402390.2012.742014.

Richards, Julian., *Cyber-War: The Anatomy of the Global Security Threat* (Basingstoke: Palgrave Macmillan 2014).

Rid, Thomas., *Cyber War Will Not Take Place* (Oxford: Oxford UP 2013).

Rovner, Joshua. 'Cyber War as an Intelligence Contest'. *War on the Rocks*, 16 September 2019. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

Singer, Peter W. and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford UP 2014).

Slayton, Rebecca., 'What is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018' *Texas National Security Review* 4/1 (2021, 2020), 61–96.

Sloan, Elinor C., *Modern Military Strategy: An Introduction* (New York: Routledge 2012).

Smith, Troy E., 'Cyber Warfare: A Misrepresentation of the True Cyber Threat' *American Intelligence Journal* 31/1 (2013), 82–85.

Steed, Danny., 'The Strategic Implications of Cyber Warfare', in James A. Green (ed.), *Cyber Warfare: A Multidisciplinary Analysis* (New York: Routledge 2015), 73–95.

Sterner, Eric., 'Retaliatory Deterrence in Cyberspace' *Strategic Studies Quarterly* 5/1 (2011), 62–80.

Stevens, Tim., 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace' *Contemporary Security Policy* 33/1 (2012), 148–70. doi:10.1080/13523260.2012.659597.

Stoker, Donald and Craig Whiteside, 'Blurred Lines: Gray-Zone Conflict and Hybrid War—two Failures of American Strategic Thinking' *Naval War College Review* 73/1 (2020), 1–37.

Stone, John., 'Cyber War Will Take Place!' *Journal of Strategic Studies* 36/1 (2012), 101–08. doi:10.1080/01402390.2012.730485.

Troeder, Elizabeth J., *A Whole-Of-Government Approach to Gray Zone Warfare* (Carlisle: US Army War College Press 2019).

Tuck, Christopher., *Understanding Land Warfare* (London: Routledge 2014).

Valeriano, Brandon and Benjamin Jensen, 'Innovation and the Proper Context of Cyber Operations: The Path to Avoid Cyber War' *The Marine Corps Gazette* 105/2 (2021), 39–43.

Valeriano, Brandon and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford UP 2015).

Warren, Jason W., 'On "Social Media Warriors: Leveraging a New Battlespace"' *Parameters* 50/3 (2020), 127–38. doi:10.55540/0031-1723.2680.

White, Sarah. 'Subcultural Influence on Military Innovation: The Development of U. S. Military Cyber Doctrine'. Doctoral dissertation, Harvard University, 2019.

Whyte, Christopher., 'Beyond Tit-For-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online' *European Journal of International Security* 5 (2020), 195–214. doi:10.1017/eis.2020.2.

Whyte, Christopher and Brian M. Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy* (New York: Routledge 2019).

Zilincik, Samuel, Michael Myklin, and Petr Kovanda, 'Cyber Power and Control: A Perspective from Strategic Theory' *Journal of Cyber Policy* 4/2 (2019), 290–301. doi:10.1080/23738871.2019.1635177.