Nilsson, Niklas, Mikael Weissmann, Björn Palmertz, Per Thunholm, and Henrik Häggström. "Security challenges in the grey zone: Hybrid threats and hybrid warfare." *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm . London: I.B. Tauris, 2021. 1–18. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781788317795.0005>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 10:52 UTC.

Copyright © Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm 2021.
Released under a CC BY-NC-ND licence (<https://creativecommons.org/licenses/by-nc-nd/3.0/>).
You may share this work for non-commercial purposes only, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

Security challenges in the grey zone

Hybrid threats and hybrid warfare¹

Niklas Nilsson, Mikael Weissmann, Björn Palmertz,
Per Thunholm and Henrik Häggström

The greatest victory is that which requires no battle.

– Sun Tzu, The Art of War

The international security environment has in recent years evolved into a volatile and increasingly grey zone of war and peace. Security challenges arising from hybrid threats and hybrid warfare, henceforth HT&HW, are today high on security agendas across the globe. However, despite the attention, and a growing body of studies on specific issues, there is an imminent need for research bringing attention to how these challenges can be addressed in order to develop a comprehensive approach towards identifying, analysing and countering HT&HW. This volume supports the development of such an approach by bringing together practitioners and scholarly perspectives on HT&HW, by covering the threats themselves as well as the tools and means to counter them together with a number of real-world case studies.

Over time the grey zone between peace and war has grown considerably, underscoring the necessity of understanding hybrid warfare and related threats. Russia's actions in Ukraine have manifested this paradigm, being a good example of the problem in thinking about war and peace as binary categories. How does a country or group of countries deal with threats and aggression in this grey area, such as 'little green men' that appear in uniform but without national denomination and refuse to tell where they come from, election-influenced operations or cyberattacks, to mention but a few possible actions.

By uniting the knowledge of both practitioners and scholars, the volume aims to identify the existing tools for countering HT&HW, as well as experiences from a wide set of empirical contexts. Mirroring this, the project is a cross-sector collaboration between the Department of Military Studies and the Center for Asymmetric Threat Studies (CATS) at the Swedish Defence University. The former represents an academic environment where research and teaching are intertwined in a range of subjects

including War Studies, Military Technology and Military History. The latter is a national centre within the Swedish Defence University tasked with developing and disseminating knowledge about asymmetric threats within the context of societal security and resilience.

This volume focuses on the challenge posed by HT&HW to Western democracies, and their ability to address it. Western democracies are not only the type of states most frequently targeted by hybrid measures, but also the most vulnerable. By virtue of being open, pluralistic and liberal societies with freedom of the press and rule of law, Western democracies display both inherent weaknesses that can be targeted and inherent constraints – in particular through the rule of law and basic freedoms – that limit the scope for defensive actions. These vulnerabilities are increasingly recognized by Western governments, which have developed a range of entities to address them, although coordination in many instances remains weak. The later sections outline the growing significance of HT&HW on the security agendas of Western democracies and the challenges they imply, as well as the entities these states have established in response. Although neither list is complete, they provide an overview of the current situation. The final sections provide an outline of the volume's structure and a summary of each chapter.

The rise of HT&HW and the Russia factor

HT&HW are problematic concepts. Contemporary scholarship on these phenomena lacks a common definition and the use of terminology remains contested. In fact, HT&HW are just two of a variety of distinct, but overlapping, concepts employed to describe a similar phenomenon, where 'Asymmetrical Warfare', 'Sixth Generation Warfare', 'Contactless Warfare', 'Grey Wars', 'New warfare', 'Next-generation Warfare', 'Ambiguous Warfare', 'Irregular Warfare', 'Non-linear Warfare', 'Full Spectrum Conflict' and 'Unconventional Warfare' are examples of more or less synonymous terms (see also Chapter 5).²

HT&HW – twenty-first-century style – differ from traditional threats and warfare more in intensity and degree than in kind. The exception is the virtual or digital realm, which empowers new tools and lowers the entry cost of using them. HT&HW denote adversaries or antagonists who aim to achieve outcomes without a war, to disrupt, undermine or damage the target's political system and cohesion through a combination of violence, control, subversion, manipulation and dissemination of (mis)information.³ Hence, they target opposing societies, not combatants.⁴ HT&HW imply the simultaneous presence of a range of possible adversarial means, from threats of war to propaganda and everything in between. They therefore include multiple instruments of power and influence, though with an emphasis on threats, non-military as well as military, operating below the threshold of open war. The identification of HT&HW does not allow for a clear-cut distinction between different forms of actors, be they state or non-state; soldiers or civilians; organized violence, terror, crime or war in a traditional sense. Regardless of the actor from which the threat originates, it has

become customary for such actors to combine and tailor a mix of conventional and irregular means to achieve maximum effect.⁵

The increased attention paid to HT&HW in current Western strategic thinking is thus foremost a reaction to the innovative behaviour of external antagonists. In particular, Russia has emerged as a dark cloud over Europe and the West through its demonstrated ability to engage in 'a style of warfare that combines the political, economic, social and kinetic in a conflict that recognizes no boundaries between civilian and combatant, covert and overt, war and peace [where] achieving victory – however that may be defined – permits and demands whatever means will be successful: the ethics of total war applied even to the smallest skirmish'.⁶

Indeed, Russia's annexation of Crimea and its subsequent aggression in eastern Ukraine prompted a much broader acceptance of HT&HW as a security challenge (see also Chapter 14). The fact that the Ukraine scenario involved not a militia in the Middle East, but a large state bordering NATO, with substantial conventional military resources, spurred a considerable rethinking of Russia as a potential adversary. It also highlighted the need for a comprehensive view of the various methods, conventional and unconventional, lethal and non-lethal, that Russia proved capable of combining and deploying in Ukraine, which are either already being utilized or could potentially be deployed in a conflict with NATO and the West. In this context, to many Western academics and policymakers, the labelling of threats and warfare as hybrid could fruitfully capture the purportedly complex and comprehensive nature of Russia's ability to combine various levers of state power, from the military and economic to the information space.⁷

The hybrid terminology thus rapidly gained traction in Western public and political debate, where it has evolved into an all-encompassing view of Russia's international behaviour, permeating the strategic, operational and tactical levels. In the meantime, China has gradually risen as not only an economic but also a military power (see also Chapter 7). The fact that the combined military resources of the West remain vastly superior, certainly to those of Russia and for the time being also to those of China, has encouraged these and other actors to develop and combine other, less resource-consuming means for challenging the global hegemony of the West. Due to the asymmetry in military and economic power, these actors seek ways and means to challenge the West by exploiting the vulnerabilities in existing security institutions as well as Western democracies. Thus, HT&HW have become terms commonly used to describe the strategy of challengers to the global hegemony of the West, aside from Russia also including, for example, China, Iran and North Korea, but also of non-state actors, particularly ISIS and Hezbollah.⁸

Yet, as noted earlier, HT&HW remain contested concepts. Regarding Russia and its actions in Ukraine and Syria, several observers have objected to the portrayal of Russian hybrid warfare as a 'new' approach to war fighting, since the combination of military power with, for example, economic means and propaganda has been part of the toolbox of statecraft since ancient times (see also Chapter 6).⁹ Moreover, the grouping of a variety of non-kinetic means, including economic and informational means, under the heading of hybrid warfare, it is argued, dangerously stretches the concept of 'war'. Yet other critics point out that the concept of hybrid warfare has

become vastly overextended, expanding in scope to cover most of Russian foreign policy, while simultaneously erroneously depicting Russian actions as much more coordinated, strategic and efficient than they actually are.¹⁰ More generally, it has been argued that the extended use of the concept to denote a 'blend' of methods at the strategic, operational and tactical levels, is so vague and all-encompassing that 'hybrid' no longer has analytic utility – rather, current conceptualizations make more sense as a description of contemporary warfare.¹¹

In this light, it should be noted that the view presented by Russian officials, representatives of Russia's armed forces and military theorists, is in large part a mirror image of the understanding in the West. Seminal expressions of the Russian armed forces' understanding of the future of warfare can be found in the speeches of General Valery Gerasimov, Chief of Russia's General Staff, to the Russian Academy of Military Science. Gerasimov has presented a picture of increasingly blurred boundaries between war and peace as well as military and non-military means¹² in which Russia must take measures against the 'hybrid methods' employed by its adversaries.¹³ Indeed, Russian military thinkers and policymakers seemingly believe that warfare is entering a new era where military force becomes increasingly interchangeable with, and perhaps even secondary to, non-kinetic force.¹⁴ However, these and other Russian assessments regarding the future of war draw on observed twenty-first-century Western warfare in Iraq, Afghanistan and Libya, rather than relevant Russian experiences from its own conduct in, for example, Chechnya, Moldova, Ukraine and the south Caucasus.¹⁵

Official Russian assessments of the main threats to the country's national security portray the determination of the United States and its allies to retain their global hegemony at all costs and by all means as the fundamental security challenge that Russia is facing. The description of these means is familiar: the West is assumed to deploy overt and covert military resources, along with economic, diplomatic, informational and cultural means in order to contain Russia.¹⁶ In particular, Russia's official security discourse indicates a concern over vulnerabilities implied by an information sphere and a civil society outside the state's control – not least in its interpretation of the string of 'colour' revolutions in post-communist countries and the Arab spring as covert depositions of legitimate governments by Western intelligence services. In this light, the crackdown on Russia's political opposition and civil society, as well as delimiting public access to channels of information, stem from the perceived threat of Western subversion of Russian society, veiled under the liberal norms of market economic principles, human rights and democratization. Although the validity of these conclusions is arguably questionable, and poorly backed by empirical evidence, the fact remains that hybrid warfare, or *gibridnaya voyna*, is a concept that Russia has imported from the West, which in the Russian context denotes the range of threats that Russia purportedly faces from the West.

Yet while acknowledging the ambiguities and weaknesses of HT&HW, as well as other conceptual labels, we maintain its usefulness in the holistic analysis of how a range of actors, state and non-state strategically combine kinetic and non-kinetic means of power to pursue interests and attain objectives in the contemporary globalized world.¹⁷ Given the inherent understanding that the evolution and attractiveness of the idea of HT&HW is connected with asymmetries in power and resources, the conceptualization

appears particularly useful as a framework for understanding the methods and conduct of challengers to the West on a global or regional scale, particularly Russia, China and Iran. However, this by no means precludes Western democracies from combining various tools of statecraft in a manner that might be characterized as hybrid warfare. Indeed, with all its flaws and ambiguities, the debate on hybrid warfare has served to challenge Western binary thinking on war and peace as well as conventional and unconventional warfare. It has contributed to a more comprehensive understanding of how adversaries may innovatively combine a range of foreign policy tools to target the particular vulnerabilities of Western societies and circumvent their existing defensive structures. And it has underlined the need for holistic analysis to comprehend and act in the contemporary security environment. From an intelligence perspective, it also underscores the need to fuse intelligence from military and civilian agencies, or even between intelligence and non-intelligence agencies.

This volume neither seeks to resolve the ongoing conceptual discussions, nor lets the lack of a consensus definition and the contested terminology distract from the purpose of the book – to enhance our ability to understand, and in the continuation identify, analyse and counter HT&HW. Because of their diffuse nature, the line between a hybrid threat and ongoing warfare is not always evident. Thus, for the purpose of this volume, unless otherwise specified by the chapter author, HT&HW are considered two synonymous labels for the same type of conceptual phenomenon.

The Western response

The meaning of HT&HW is far from new, but the awareness and work to incorporate its implications into the policy, capacity and capacity implementation in Western democracies have gained momentum in recent years. Some pivotal developments include the activities of ISIS between 2013 and 2019 and, as noted earlier, the Russian annexation of Crimea in early 2014. In addition, the Russian combined influence and cyber operations targeting the US election campaign in 2016, and the French election campaign the following year, clearly exposed the need for political and societal awareness, as well as increased coordination and capabilities in Western democracies to address HT&HW targeting the very core values and processes of such states.

During the last few years, the West has been exposed to continuous media reports of specific actions, for example, disinformation or hack and leak operations aiming to change the course of public debate or diminish the credibility of key societal actors. In such an information environment it is easy to get caught in a problem-oriented sense of a continuous barrage of threats and lose sight of the more subtle long-term developments that bolster the capacity to respond and build resilience against them. It is no doubt easier to describe a threat aimed at a specific event or target delineated in time than more subtle shifts in governments or societies. An extensive literature review in 2018 on information influence activities highlights that more is known about the techniques and conduct of these activities than about how to counter them.¹⁸ Let us therefore outline a few examples of capabilities that have recently come into place

and that are relevant in order to understand or diminish the effects of hybrid threats against the West. These include (1) multinational entities and projects, (2) national governmental entities and (3) non-governmental entities.

In 2014 the NATO Wales Summit Final Declaration described 'the specific challenges posed by hybrid warfare threats' and underlined the importance that the alliance develop 'necessary tools and procedures' to enable a response to such threats. They also emphasized that this requires a broad range of efforts related to, but also beyond, traditional military capabilities.¹⁹ The same year saw the initiation of the NATO StratCom Center of Excellence in Riga, Latvia. It is aimed at supporting 'NATO's capability development process, mission effectiveness and interoperability by providing comprehensive and timely expertise in the field of strategic communications'.²⁰ In addition, the NATO Cooperative Cyber Defence Centre of Excellence, established in 2008, has become another important hub for research, training and exercises for the alliance in terms of hybrid threats. One paper illustrating the overlap between hybrid threats from CCD CoE is Brangetto and Venendaal's 'Influence Cyber Operations: The use of cyberattacks in support of Influence Operations', which examines how influencing the behaviour of a target audience becomes the primary effect of a cyber operation.²¹

Illustrating this need for a comprehensive understanding of the threat environment and joint collaboration, the European Center of Excellence for Countering Hybrid Threats was established in Helsinki in early 2017. It aims to constitute an international platform where governments can share best practices, build capability, test new ideas and exercise defence against hybrid threats, as well as facilitating such activities between the EU and NATO.²² To date, Hybrid CoE has twenty-seven member states and a structure focused on three key Communities of Interest: (1) hybrid influencing, including a sub-community on non-state actors, (2) strategy and defence and (3) vulnerabilities and resilience.

The EU Intelligence Analysis Centre (INTCEN) is another key actor capable of intelligence collection and collating such contributions from the EU member states. This results in analyses and assessments in order to provide situational insight to the head of the European External Action Service and the EU leadership.²³ As such, it has an important function in ensuring that a number of overlapping areas, such as those found within the realm of hybrid threats, are understood and tracked.

Also, the European Council decided to create the EEAS East StratCom Task Force during a meeting in early 2015.²⁴ Its task is to develop communication to explain EU policies, as well as support the media environment, in Eastern Partnership Countries. It also analyses and produces reports on disinformation trends and narratives, and actively works to raise awareness of such activities from the Russian state and related actors. This includes maintaining a wide international and member state cooperation to share best practices in strategic communications and enable continued access to objective information.²⁵

Another project worth highlighting is the Multinational Capability Development Campaign Countering hybrid warfare project, a joint effort by the EU and a number of additional contributing nations. It is aimed at informing national and multinational policy, enabling cooperation and offer conceptual guidance related to security and defence.²⁶

A number of governments, especially in the aftermath of the Russian annexation of Crimea, have amplified their focus on HT&HW and initiated capability development to identify, analyse and counter them. Two examples that illustrate approaches related to influence campaigns are Sweden and Australia.

Sweden has a governmental structure built on very independent agencies, where an annual appropriations bill offers a general direction. However, responsibility for detailed planning and implementation resides with the agency responsible for a specific area. In 2016 the Swedish Civil Contingencies Agency (MSB) was officially tasked to develop capabilities to identify and counter information influence activities, and to support other key societal actors in this area of expertise.²⁷ This also coincided with an increased Russian influence focus on Sweden, targeting its host nation agreement with NATO and Sweden's further integration with the alliance as a non-member, as well as sowing doubt about the Swedish political system.²⁸ Since then MSB, in addition to developing their own capacity, has conducted a number of ground-up resilience-building activities. These include visibility via external communication and commentary through various media channels, as well as funding research into state- and non-state-related information influence activities. MSB has also established training and exercise programmes for a large number of public servants, related to election integrity as well as a broader set of influence related challenges. These activities were supported by the 2018 handbook 'Countering information influence activities' developed by Lund University for MSB.²⁹ Other key state actors include the Office for Crisis Management at the Swedish Department of Justice, the Swedish Security Service, the Armed Forces as well as the Swedish Institute and the Swedish National Defence Radio Establishment.³⁰ As of 2018 the Swedish Ministry for Foreign Affairs also has an ambassador assigned the portfolio of hybrid threats.³¹

In Australia on the other hand, the growing challenge of foreign interference, especially from China, has resulted in a number of open discussions and actions by the Australian Government. Starting in 2015, the Australian Security Intelligence Organisation (ASIO) issued warnings to domestic political parties regarding monetary contributions from two Chinese businessmen, deemed an attempt by the Chinese Communist Party to attain leverage in Australian politics.³² Also, since over 1.2 million people of Chinese descent live in Australia and constitute the largest percentage of current migrants, the diaspora is an attractive target for Chinese influence attempts. Compared to Sweden, the Australian response has been a more top-down effort, including legislation and high-level government coordination. For example, Australia decided in 2017 to ban Huawei from participating in its 5G network and introduced the Foreign Influence Transparency Scheme Bill and the Espionage and Foreign Interference Bill the same year.³³ In April 2018, the Australian Government appointed the first National Counter Foreign Interference Coordinator (NCFIC) in the Department of Home Affairs, whose responsibilities include ensuring a whole-of-government effort in this area. This includes drawing on intelligence community capabilities, ensuring the development and implementation of strategy and specific programmes across the government, and interaction to increase the resilience of societal groups or organizations deemed particularly likely targets of foreign interference. In late 2019 it was announced that the NCFIC would acquire funding

to establish a new Counter Foreign Interference Taskforce. In addition, a Foreign Interference Threat Assessment Centre will be established within ASIO.³⁴

Aside from the efforts of states and governments, a number of non-governmental entities increasingly provide situational awareness and knowledge concerning the techniques and motivations underlying hybrid threats. Bellingcat, an independent international group of researchers, investigators and citizen journalists using open source and social media investigation, has played a public role in a number of cases. For example, in 2018 they revealed the likely involvement of Russian intelligence operatives in the poisoning of Sergei Skripal in Salisbury, UK. They also identified the Russian air defence system responsible for the downing of Malaysian Airlines flight 17 over eastern Ukraine in 2014.³⁵

Another increasingly visible non-governmental resource in recent years has been the Digital Forensic Research Lab at the Atlantic Council. Their aims include identifying, exposing and explaining 'disinformation campaigns, fake news stories, covert military developments, and subversive attempts against democracy'.³⁶ They have covered a number of areas, including far-right messaging on social media platforms, the conflict in Ukraine, disinformation and influence campaigns during elections, and state crackdowns on public protests in, for example, Russia and Iran.³⁷

In sum, the range of entities established in the West to counter HT&HW mirrors a vastly increased awareness of the problem in international, national and domestic settings. Moreover, they also highlight the emergence of numerous cooperative and innovative means for addressing the insecurities implied by HT&HW. Indeed, the multitude of responses are indicative of the increasingly dynamic nature of the present security environment, in which the West is proving capable of not only reacting to the challenges of antagonists, but also of identifying and addressing its own vulnerabilities in this regard as well as devising innovative and creative countermeasures of its own.

Structure of volume

The volume is divided into three parts. Part I presents a practitioner's view on HT&HW, from the perspective of key western actors in this area: NATO, the EU and the United States. Part II focuses on the tools and means employed to conduct and counter HT&HW. It includes chapters taking stock of Russia's military thinking and China's hybrid warfare capabilities, followed by chapters on influence operations and the modern information environment, and multilateral intelligence cooperation. Part II concludes with a chapter on cyberwarfare and the internet. Drawing on the themes identified in Part II, Part III consists of five case studies – the United States, China's political warfare in Taiwan, the Baltics, Ukraine, Iran and Catalonia – demonstrating the employment of these tools and means – how they have been used and countered in practice.

Finally, the conclusion focuses on patterns, practices and implications drawn from the volume. The chapter introduces a dynamic view of HT&HW depicted, presenting what we term 'the Hybridity Blizzard Model'. This model presents a picture of the

dynamics of and between HT&HW and responses and countermeasures. The model not only enables a better understanding of the dynamics themselves, but also of how to identify, analyse and counter HT&HW.

Commencing Part I, Chapter 2, 'NATO and hybrid warfare: Seeking a concept to describe the challenge from Russia', is written by Dr G. Alexander Crowther, Research Professor at Florida International University, former Special Assistant to the Supreme Allied Commander, Europe, and former researcher at the Strategic Studies Institute and the US National Defense University. Dr Crowther argues that NATO faced a resurgent Russia that developed its own concept of Hybrid Operations based on the thoughts of Frank Hoffman, Russia's analysis of perceived aggressive actions by the United States and NATO, and Russia's own past of political warfare. NATO, in turn, reacted by conceptualizing the challenge and a response, then used information (in particular diplomacy) in order to minimize support for Russia and maximize support for NATO, collaborated with Allies and other partners, and used NATO's inherent hard power to deter Russia from escalating to violence. Efforts thus far have been necessary but not sufficient, both Russian hybrid operations and NATO efforts to respond to them will continue for the foreseeable future.

Chapter 3, 'An American view: Hybrid threats and intelligence', is written by Dr Gregory F. Treverton, University of Southern California, and former Chair of the US National Intelligence Council (NIC), and draws on lessons from Dr Treverton's experience in government, most recently as Chair of NIC. The first lesson is the value of reaching out to private sector partners for early warning of hybrid threats. The 2016 Russian interventions in US elections came as a surprise but should not have, for a private group looking at jihadist websites had found anomalies, ones indicating that many of those posing as Free Syria on social media were, in fact, Russians, not Syrians. By the same token, the presence of private companies doing their own attribution of cyberattacks complicates the usual government process of intelligence attributing, then passing the attribution to policy officials for action. Yet in the long run, those companies will be valuable allies if government agencies reach out to them, something that does not come naturally, especially for intelligence agencies.

The second lesson is the importance of seeing the world through Russia's eyes, not to excuse Vladimir Putin but to understand what drives his policy, especially in the 'near abroad'. From Russia's perspective, the United States dismissed Russia after the fall of communism, then encircled it, especially by expanding NATO to Russia's borders. That perspective and the desire to be seen as great is the backdrop for Russia's moves into Ukraine, Syria, Libya, Moldova and elsewhere, and will condition Russian responses to future US and NATO actions in Europe. In responding to Russian initiatives in the grey, or hybrid zone, two tactical lessons stand out: don't demean the West's free press by stooping to Putin's level of disinformation, and don't regard the Russians as ten feet tall.

Chapter 4, 'A perspective on EU hybrid threat early warning efforts', shifts focus to the European Union (EU). Here Dr Patrick Cullen, Senior Research Fellow at the Norwegian Institute of International Affairs (NUPI) and a member of the 'Countering Hybrid Warfare' component of the Multinational Capability Development Campaign (MCDC) presents an academic practitioner's perspective on the development of the EU policy engagement with and response to hybrid threats. Special attention is paid

to the role of the Russian annexation of Crimea in shaping EU perceptions of a new 'hybrid security environment', its decision to work more closely with NATO, and the development of an EU counter-hybrid security threat niche focused on hybrid threats below the threshold of war. Rather than conducting a survey of all EU counter-hybrid threat efforts, this chapter focuses on the development of its hybrid threat early warning and detection mechanism proposed and implemented by its European External Action Service and its Hybrid Fusion Cell.

Moving on to Part II, in Chapter 5, 'Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone', by Dr Mikael Weissmann, Associate Professor, Head of Research at the Land Operations Section and Co-Convener of the Hybrid Warfare Research Group, Swedish Defence University. After an initial conceptual discussion on HT&HW, Weissmann presents an analytical framework operationalizing hybrid threats and warfare. Asking what role the military can and should play in responding to hybrid threats and warfare today and in the future, the framework is then applied on the official discourse in the Baltic and a case study of Sweden analysing what role the members of the military themselves think it should have.

He is arguing that it is crucial to understand the role of the military in the grey zone, as unless hybrid threats- and warfare can be successfully handled there, the war is likely to have been lost before a conventional war breaks out. The chapter concludes that the role of the military needs to be recognized and utilized in the most efficient way possible across the grey zone while at the same time ensuring that democratic principles and the rule of law are upheld. It is encouraging to see that the role of the military in the grey zone is both recognized and in correlation in the official discourse and in the thinking of military officers. This is a good base to build the resilient society and national defence needed to counter hybrid threats and warfare today and tomorrow. This said, there is today a discrepancy between where we are and where we should be.

In Chapter 6, 'Understanding Russian thinking on *gibridnaya voyna*', Dr Markus Göransson, the project leader of the Russia programme at the Swedish Defence University, analyses the concept of *gibridnaya voyna*, which in recent years has gained ground in Russian military scholarship where it is used as shorthand for multidimensional operations conducted by Western states against non-Western adversaries. It is a direct translation of the Western term 'hybrid warfare' yet is used in a somewhat different sense in parts of the Russian scholarship. Employed not only to designate military action at the tactical and operational levels, *gibridnaya voyna* is used also as a catch-all term for Western non-military subversion against Russia. Because of this difference in meaning, previous research has understood *gibridnaya voyna* as being rooted in a peculiarly Russian understanding of war as a sociopolitical phenomenon that may be waged non-kinetically. Dr. Göransson argues that it is mistaken to view the Russian *gibridnaya voyna* discourse as primarily an academic endeavour. It is conceptually and empirically weak and serves mainly a rhetorical function as it allows for the identification of a vast range of perceived threats to Russia. In other words, it provides an analytical framework that securitizes a range of issues as potential dangers to Russia.

In Chapter 7, 'China and its hybrid warfare spectrum' by Dr Lora Saalman, Associate Senior Fellow with Stockholm International Peace Research Institute and Senior Fellow with EastWest Institute, the focus shifts from Russia to China. Dr Saalman argues that there is a tendency in Western analyses on Chinese hybrid warfare to focus on just a few historical texts, including *The Art of War* from the fifth century BCE and *Unrestricted Warfare* from 1999. Yet this narrow emphasis misses the complexity of views on and employment of hybrid warfare in China. A survey of 192 Chinese-language texts reveals that Chinese writings on hybrid warfare are often so inclusive that it can be difficult to decipher what in effect is 'not' part of their strategic thinking on the subject. To provide greater nuance, this chapter explores Chinese analyses along a spectrum, covering unrestricted warfare, information warfare, cyberwarfare, intelligent warfare and kinetic warfare. In doing so, it seeks to provide a more comprehensive baseline for understanding Chinese perceptions on threat, response and operationalization of hybrid warfare.

The actor-focused chapters on Russia and China are followed by three chapters thematically oriented towards specific tools and means. In Chapter 8, 'Influence operations and the modern information environment', Björn Palmertz, Senior Analyst at CATS at the Swedish Defence University, shows that even though the techniques used by state and non-state actors to conduct influence operations are far from new, the modern information environment has resulted in new opportunities as well as vulnerabilities. An increased availability of data on target audiences, easier access to specific target segments, a rapid speed of information dissemination, and ways of staying anonymous or pretending to be someone else are but a few factors that benefit the employment of influence operations, on their own or in unison with other means, such as cyber operations. This chapter discusses how these relate to targeting, and offer examples illustrating a number of influence techniques that have been employed during recent years. These are hacking, leaking and doxing, distributed denial of service attacks, disinformation, social media advertising, organized trolling and amplification by social bots.

Chapter 9, 'Hybrid threats and new challenges for multilateral intelligence cooperation', is written by Henrik Häggström, Senior Analyst, CATS at the Swedish Defence University. Häggström argues that ever since the 9/11 terror attacks, the range of partners in the intelligence world that share information at the international level has grown exponentially. The change has been both quantitative and qualitative and improved multilateral intelligence cooperation. With a view to effectively address hybrid threats and conducting effective hybrid warfare, multilateral organizations such as NATO, the EU and the UN have launched a number of intelligence initiatives in the past years to improve their capacity. These initiatives have involved structural improvements, policy changes, resource allocation and the establishment of new joint hybrid centres. The extent to which the various new intelligence initiatives within the EU, NATO and the UN will actually enhance methods to combat HT&HW is yet to be determined. Lack of trust, cultural differences and the lack of a functioning leadership in NATO, the EU and the UN are among the troubling trends that could hamper future operations.

Chapter 10 on 'Cyberwarfare and the internet: The Implications of a more digitalized world' is written by Anne-Marie Eklund Löwinder, the Chief Information Security

Officer at the Swedish Internet Foundation and one of Sweden's leading IT-security experts and Anna Djup, an analyst with the CATS at the Swedish Defence University. The creation of the internet has allowed the world to become more interconnected. Government, businesses and organizations alike are now dependent on data flows to conduct their everyday business. This connectivity has made information highly valuable and opened up for new attack vectors, generating a market for hacking and data theft. For the open internet to continue to exist as a platform for social and economic growth, users must be able to trust that organizations can protect the systems governing the society and have the capacity to safeguard personal information. The interdependencies created between the internet and critical infrastructure makes it susceptible to cyberwarfare. Cyberattacks are inherently asymmetric in nature as an actor with few means can do a lot of harm to an individual, organization or nation. The combination of poorly designed systems together with new technologies expands the scope and severity of global cyber threats, and how we tackle these threats will have far-reaching consequences for the future of the internet.

Part III starts with Chapter 11, 'The US and hybrid challenges: Past, present and future', by Jed Willard, director of the Franklin Delano Roosevelt Center for Global Engagement, Harvard University. Willard argues that the United States has the potential to be a powerful hybrid competitor. Various challenges, however, prevent America from bringing its full range of hybrid capacities to bear. This chapter examines the current American capacity for hybrid warfare. The first section covers strategic, definitional, structural and leadership challenges; exploring, for instance, the competing concept of 'grey zone' conflict and the difficulty of explaining and conducting hybrid competition in a large and complex democracy. The second section looks at the history of American hybrid engagement from the Revolution to the Cold War and then examines present and potential future hybrid challenges for the United States.

Chapter 12, 'China's political warfare in Taiwan', is authored by Dr Gulizar Hacıyakupoglu of the Centre of Excellence for National Security (CENS) and Dr Michael Raska, who is the Coordinator of the Military Transformations Programme, both at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU) in Singapore. This chapter explores the evolving strategic contours of China's political warfare in Taiwan. Certain aspects of China's political warfare are unique to Taiwan, particularly in the historical, cultural and asymmetric-military context. However, the means through which Beijing allegedly injects influence in Taiwan can emerge as the channels for political warfare in other countries if and when a country's legal, political, social and economic framework permits. These channels include (1) diplomatic and (2) legal pressure, (3) economy and (4) manipulation in the information domain. The diplomatic pressure involves the pressuring of companies to review their identifications of Taiwan, convincing Taiwan's diplomatic allies to switch sides and obstructing Taiwan's participation in international organizations. The means of Legal Pressure include capitalization on laws and restriction of access to international organizations that propose international regulations. The economy emerges as a venue for political warfare with the political implications of cross-straits exchanges and the use of monetary pressure or benefits to influence individuals or groups to act in alignment with Beijing's aims and policies. The information manipulation

attempts involve (1) the activities of the agents of influence, information gathering and espionage; (2) spreading influence by way of media; (3) disinformation campaigns and (4) cyberattacks. The chapter concludes with a strategic overview, which situates the question in a global context and suggests that China's political warfare must be viewed in a relative context – through the lens of competitive strategies reflected in the efforts to develop effective countermeasures and responses.

Chapter 13, 'Hybrid warfare in the Baltics' by Dr Dorte Bach Nyemann, Royal Danish Defence College, pieces together three elements relevant to a possible Russian hybrid operation in the Baltic States; the Russian capability to act as a hybrid actor, the Russian opportunities for success if approaching a hybrid warfare strategy and the Russian priorities and aims towards the Baltic States. The case study shows that Russia does have substantial capabilities as a hybrid actor. Hybrid warfare is a low-cost strategy with potentially high gains, however, the activities by Russia appear scattered, not systematically applied and not well coordinated. An institutional framework for conducting hybrid warfare is present in the Baltic States, but an active continuous 'shaping of the battlefield' is at worst low-key and unambitious. The case study explains this by looking closer at Russian opportunities and interests in the Baltic States. It finds that the combination of traditional military deterrence and broad deterrence by denial below the threshold of an armed attack seems to have decreased the Russian appetite for further engagement. Combined with a rather low priority of the Baltic States in Russian foreign policy, this elucidates the lack of hybrid warfare and the low intensity of hybrid threats. However, we must expect Russia to continue to improve and maintain a broad institutional framework for influence in the region.

In Chapter 14, 'De-hybridization and conflict narration: Ukraine's defence against Russian hybrid warfare', Dr Niklas Nilsson, Co-Convener of the Hybrid Warfare Research Group, Swedish Defence University, observes that Russia's aggression against Ukraine has spurred considerable debate on the resilience and defensive capabilities of Western societies in the face of hybrid warfare as a salient feature of the contemporary security environment. However, Ukraine's responses have received much less attention, despite their importance to the dynamics of the fighting per se as well as perceptions of the conflict. Indeed, Ukraine in this regard constitutes an important case of hybrid warfare defence. This chapter examines two key aspects of Ukraine's response to Russian hybrid warfare after the annexation of Crimea. First, Ukraine's focus on conventional military build-up and its ability to counter the Russian-supported separatist forces in Donbas served to de-hybridize military violence in Donbas. Russia had to deploy regular army and artillery units to prevent the Donetsk and Luhansk 'People's Republics' from caving, displaying its considerable political and military engagement in the conflict. Second, Ukraine has sought to take control of the conflict narrative, both by publicizing a considerable amount of evidence of Russia's military involvement and by devising its own information campaign promoting Ukraine's narrative of the conflict. These responses served to deflect Russia's portrayal of the fighting as a civil war, instead demonstrating that Ukraine is defending itself against an external aggressor. In turn, this has been of immense importance to Ukraine's internal cohesion as well as the sustained support offered to the country from its Western partners.

Chapter 15, 'Iran's hybrid warfare capabilities', is written by Dr Rouzbeh Parsi, Head of the Middle East and North Africa Programme, Swedish Institute of International Affairs. This chapter deals with Iran's understanding of hybrid warfare and its own ability in conducting such operations. The Islamic Republic's military capacity has primarily and historically been geared towards defence and guerrilla-style warfare. It sees the United States as its primary enemy and as it cannot defeat the United States or its allies by means of conventional war (lack of resources and technology), it must develop non-conventional means to maintain a credible deterrence. At the same time, Tehran believes itself to be the victim of hybrid warfare by other actors. The war in Syria constitutes a new stage in Iranian military developments as it is now, somewhat gingerly, trying to develop offensive strategies and control territory.

Finally, in Chapter 16, 'Information influencing in the Catalan illegal referendum and beyond', Dr Rubén Arcos of Rey Juan Carlos University explores hostile information influencing and strategic communication activities in the context of the Catalanian illegal referendum of self-determination and the subsequent unilateral declaration of independence. The Catalanian issue exemplifies how existing vulnerabilities in political and social cohesion can be exploited through disinformation activities. It constitutes a divisive internal political issue that, as such, can be utilized by hybrid actors in information influencing campaigns targeting either foreign or domestic audiences for different aims. These kinds of issues might be utilized for legitimizing political decisions and actions in the domestic arena, or for conveying distorted representations of foreign political systems and societies for different reasons, including weakening the internal cohesion of those targeted societies or transnational political networks. Considering that the holding of the referendum of 1 October 2017 was against the rule of law, it seems more appropriate to speak about pro-Kremlin external/foreign political meddling than of foreign electoral interference. At the same time, domestic actors can also engage in influencing activities, in both legitimate and illegitimate ways, through strategic communication campaigns aiming to manage the perceptions of foreign audiences and produce cognitive, affective and behavioural impacts in domestic stakeholders. Some of the domestic pro-independence actors were proactively seeking to influence the attitudes and behaviours of foreign governments and institutions through strategic communication activities and actions.

The concluding chapter (Chapter 17), *Moving out of the blizzard: Towards a comprehensive approach to hybrid threats and hybrid warfare*, focuses on patterns, practices and implications drawn from the volume. The chapter introduces the 'Hybridity Blizzard Model'. The model comes in three versions, of which the first presents a simplified picture of the dynamics of and between HT&HW, as well as responses and countermeasures. The second version adds a temporal dimension to this relationship, demonstrating how short-term actions and responses relate to long-term vulnerabilities and resilience. The third version, in contrast, aims to provide a more accurate picture of the complex real-world situation. The aim of the model is to enable not only a better understanding of the dynamics themselves but also how to identify, comprehend and act against HT&HW.

Finally, we conclude that a comprehensive, all-inclusive approach is needed to address HT&HW. There is no one threat, no single solution to countering and responding to HT&HW, nor how to build resilience. Nor is there one actor or structure that can succeed both today and tomorrow. As outlined in the proposed model, there is a blizzard out there that needs to be handled. We have to take it for what it is, and adapt and re-adapt when the opponent and the threat constantly changes. The chapter outlines policy advice on how to manage these challenges. The key is to develop a detection system that is simultaneously aware of false-positives and false-negatives. There is also an essential need for pragmatism, flexibility and inclusiveness of actors, sectors and levels – within and between countries. It is crucial that key international organizations work together with different states both within and outside international organizations, as well as ensuring collaboration across sectors and levels and to avoid allowing traditional borders to hinder collaboration. The latter is never as important as when countering HT&HW, as vulnerabilities tend to exist precisely in the border areas between sectors and levels, and this is what the opponent will target. This requires collaboration between the military, political, economic, civilian and informational spheres, which needs to evolve across the public and private sectors, as well as from the local and regional levels, through the national to the international level.

Notes

- 1 We would like to acknowledge support received from Riksbankens Jubileumsfond (RJ) (Grant No. F16-1240:1).
- 2 For a comprehensive discussion on hybrid warfare and its origins, see Ofer Friedman, *Russian 'Hybrid Warfare': Resurgence and Politicisation* (London: Hurst & Company, 2018). Other recommended readings are for example Sean Monaghan, 'Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces', *Multinational Capability Development Campaign (MCDC)*, Information note, March 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840513/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf; Mikael Weissmann, 'Hybrid Warfare and Hybrid Threats Today and Tomorrow: Towards an Analytical Framework', *Journal on Baltic Security* 5, no. 1 (2019): 17–26; Rod Thornton, *Asymmetric Warfare: Threat and Response in the Twenty-First Century* (Cambridge: Polity, 2007); Peter R. Mansoor, 'Introduction: Hybrid Warfare in History', in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, eds Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012); Frank G. Hoffman, 'Hybrid Warfare and Challenges', *JFQ* 52 (1 quarter 2009): 34–9; Frank G. Hoffman, 'Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict', *Strategic Forum*, no. 240 (Washington, DC: Institute for National Strategic Studies, National Defense University, April 2009). <https://www.comw.org/qdr/fulltext/0904hoffman.pdf>.
- 3 Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee and Madeline McCue, *Addressing Hybrid Threats* (Stockholm: Swedish Defence University, 2018), 10 ff.

- 4 Patryk Pawlak, 'Cyber Security Woes: WannaCry?' (European Union Institute for Security Studies (EUISS), 2017), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_13_Cyber.pdf; Försvarsberedningen, 'Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025', Ds 2017:66 (Försvarsdepartementet, 2017).
- 5 See e.g. Keir Giles, 'Missiles Are Not the Only Threat', in *Beyond Bursting Bubbles: Understanding the Full Spectrum of the Russian A2/AD Threat and Strategies for Counteracting It*, eds Michael Jonsson and Robert Dalsjö (Stockholm: FOI, 2020).
- 6 Mark Galeotti, 'Hybrid, Ambiguous, and Non-Linear? How New Is Russia's "New Way of War"?', *Small Wars & Insurgencies* 27, no. 2 (2016): 7.
- 7 Michael Kofman and Matthew Rojansky, 'A Closer Look at Russia's "Hybrid War"', Kennan Cable 7 (Wilson Center: Kennan Institute, 2015). <https://www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf>; Peter Pomerantsev, 'How Putin Is Reinventing Warfare', *Foreign Policy*, 5 May 2014. <https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/>; Jānis Bērziņš, *Russian 'New Generation Warfare': More Democracy Is the Solution* (Washington: Center for European Policy Analysis, 2014); Heinrich Brauss, Kalev Stoicescu and Tony Lawrence, *Capability and Resolve: Deterrence, Security and Stability in the Baltic Region* (Tallinn: International Centre for Defence and Security, 2020).
- 8 Hall Gardner, *Hybrid Warfare: Iranian and Russian Versions of 'Little Green Men' and Contemporary Conflict* (Rome: NATO Defence College, Research Division, December 2015); Frans-Paul van der Putten, Minke Meijnders, Sico van der Meer and Tony van der Togt, eds *Hybrid Conflict: The Roles of Russia, North Korea and China* (The Hague: Clingendael Institute, 2018); Andrea Beccaro, 'Modern Irregular Warfare: The ISIS Case Study', *Small Wars & Insurgencies* 29 no. 2 (2018): 207–28.
- 9 Nicu Popescu, 'Hybrid Tactics: Neither New nor only Russian' (European Union Institute of Security Studies, January 2015). https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf; Keir Giles, 'Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power', Chatham House, 21 March 2016. <https://www.chathamhouse.org/publication/russias-new-tools-confronting-west>.
- 10 Bettina Renz, 'Russia and "Hybrid Warfare"', *Contemporary Politics* 22, no. 3 (2016): 283–300. See also Samuel Charap, 'The Ghost of Hybrid War', *Survival* 57, no. 6 (2015): 51–8.
- 11 Robert Johnson, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies* 29, no. 1 (2018): 143.
- 12 Valery Gerasimov, 'The Value of Science in Prediction', *Military-Industrial Kurier*, 27 February 2013.
- 13 Valery Gerasimov, 'Hybrid Warfare Requires High-Tech Weapons and a Scientific Basis', *Military-Industrial Courier*, 9 March 2016.
- 14 Galeotti, 'Hybrid, Ambiguous, and Non-Linear?', 287, 291.
- 15 Timothy Thomas, 'The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation and New-Type Thinking', *The Journal of Slavic Military Studies* 29, no. 4 (2016): 557–9.
- 16 2014 Military Strategy, 2015 National Security Strategy, 2016 Foreign Policy Concept; Valery Gerasimov, 'Russian General Staff Chief Valery Gerasimov's 2018 Presentation to the General Staff Academy: Thoughts on Future Military Conflict-March 2018'. Translated by Dr Harold Orenstein. Army University Press, Military Review, January–

- February 2019. <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Jan-Feb-2019/Gerasimov-Future/>; Sergey Glazyev, advisor to Russian president on issues of economic integration, quoted in RIA Novosti, 8 April 2015.
- 17 Alexander Lanoszka, 'Russian Hybrid Warfare and Extended Deterrence in Eastern Europe', *International Affairs* 92, no. 1 (2016): 178.
 - 18 James Pamment, Howard Nothhaft, Henrik Agardh-Twetman and Alicia Fjällhed, *Countering Information Influence Activities: The State of the Art*, version 1.4 (Lund University, 1 July 2018). <https://www.msb.se/RibData/Filer/pdf/28697.pdf>, 115.
 - 19 NATO, *Wales Summit Declaration*, 2018. https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
 - 20 NATO StratCom CoE, Annual Report, 2017. <https://www.stratcomcoe.org/audited-annual-report-2017>.
 - 21 Pascal Brangetto and Matthijs A. Veenendaal, 'Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations', *8th International Conference on Cyber Conflict (CyCon)*, 31 May–3 June 2016, Tallinn, Estonia. <https://ieeexplore.ieee.org/abstract/document/7529430>.
 - 22 Hybrid CoE, 'What Is Hybrid CoE?'. www.hybridcoe.fi/what-is-hybridcoe/.
 - 23 Rubén Arcos and José-Miguel Palacios, 'EU INTCEN: A Transnational European Culture of Intelligence Analysis?', *Intelligence and National Security* 35, no. 1 (2020): 72–94.
 - 24 European Council (2015-03-20) European Council meeting (19 and 20 March 2015) – Conclusions, Brussels, Paragraph 13.
 - 25 EU EEAS (2018-12-05) Questions and Answers about the East StratCom Task Force. eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.
 - 26 MCDC, Countering Hybrid Warfare Project, summary, <https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare>.
 - 27 Swedish Department of Justice, Appropriation Bill for the Swedish Civil Contingencies Agency, 2016.
 - 28 Martin Kragh and Sebastian Åsberg, 'Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case', *Journal of Strategic Studies* 40, no. 6 (2017): 35.
 - 29 *Countering Information Influence Activities: A Handbook for Communicators* (Karlstad: Swedish Civil Contingencies Agency (MSB), 2019).
 - 30 Edward Deverell, 'Att identifiera och motstå informationspåverkan: En jämförande studie av hur de nordiska länderna organiserar arbetet', *Kungl Krigsvetenskapsakademiens Handlingar och Tidskrift*, no. 1 (2019): 31–54.
 - 31 Fredrik Löjdquist, 'Commentary: An Ambassador for Countering Hybrid Threats', RUSI, 6 September 2019. <https://rusi.org/commentary/ambassador-countering-hybrid-threats>.
 - 32 Nick McKenzie, Chris Uhlmann, Richard Baker and Daniel Flitton, 'ASIO Warns Parties that Taking China Cash could Compromise Australia', *The Sydney Morning Herald*, 6 June 2017. <https://www.smh.com.au/national/asio-warns-parties-that-taking-china-cash-could-compromise-australia-20170602-gwjc8t.html>.
 - 33 Jieh-Yung Lo, 'Chinese Australians Are Not a Fifth Column', *Foreign Policy*, 31 May 2019. <https://foreignpolicy.com/2019/05/31/chinese-australians-are-not-a-fifth-column-china-ccp-australia-morrison-turnbull-espionage-foreign-interference/>.

- 34 Office of the Prime Minister of Australia, 'Stepping up Australia's Response against Foreign Interference', Media Release, 2 December 2019. www.pm.gov.au/media/stepping-australias-response-against-foreign-interference.
- 35 Marc Tracy, 'These Reporters Rely on Public Data, Rather Than Secret Sources', *The New York Times*, 1 December 2019. <https://www.nytimes.com/2019/12/01/business/media/open-source-journalism-bellingcat.html>.
- 36 www.digitalsherlocks.org.
- 37 Digital Forensic Research Lab, medium.com/dfirlab.