5

# Conceptualizing and countering hybrid threats and hybrid warfare

## The role of the military in the grey zone

Mikael Weissmann

## Introduction[1]

Challenges related to hybrid threats and hybrid warfare (HT&HW) are today something that is high on the security agenda across the world. The need to manage a range of hybrid measures is widely recognized among experts and practitioners,[2] as well as by key international organizations such as NATO and the European Union (EU).[3] It has become clear that the battlefield of the future exists in the grey zone between war and peace. In this grey zone, you will find non-kinetic effects replacing, or mixed with, kinetic effects. There will be a synergistic assortment of military and non-military activities, ranging from different forms of strategic communication, through active measures as intrusions, special operations, sanctions and subversions, through the use of masked soldiers like to so-called green men in Crimea, cyberattacks, sabotage and terror or proxy warfare, before passing the borderline of war. Thus, today there is a need to be able to develop resilience towards, and capabilities to pursue, effective operations and tactics against HT&HW.

To counter HT&HW, there is a need for a range of actors to work together and use the full range of tools at their disposal. This chapter focuses on one part of the toolbox for countering HT&HW: the military. What role, if any, can and should the military play against hybrid scenarios such as the presence of green men, infrastructure and logistics protection, cyber defence, information and influence operations, or simply in support of civil society?

It is crucial to understand the role of the military in the grey zone. Unless HT&HW can be successfully handled there, the war is likely to have been lost before a conventional war breaks out. Sun Zsu's age-old wisdom that '[t]he greatest victory is that which requires no battle' is as true today as it was 2,000 years ago. This is also a wisdom encapsulated in Russia's style of warfare which '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'.[4]

In other words, when preparing for a conventional high-intensity conflict towards a qualified opponent, you are preparing for a situation that will not happen if your opponent succeeds with its strategy. Thus, it is of paramount importance to analyse and understand what role the military *can* and *should* play in responding to HT&HW today and in the future. The important thing is not if or how the military should contribute, but to allow for making informed decisions and to know what the consequences are with one's choices. Or lack of choices; not choosing is also a choice. It might be that the sole role for the military is to fight during a conventional war – but then this decision should be taken based on well-informed analysis.

The overarching question guiding this chapter is 'Where do the military fit in when countering HT&HW?' More specifically, it is asked, '*What is the role of the military – if any – to counter* HT&HW*?*'. This chapter focus on the role of the military in Western democracies in the Baltic Sea region (Sweden, Finland, Denmark, Estonia, Latvia, Lithuania, Poland and Germany). With its focus on the Baltic Sea region, the chapter will focus on analysing HT&HW relating to Russia. The reason for this limitation is that Russia is identified as the main threat in the threat assessments across the countries in the Baltic Sea region.[5] This is not to say there are no other actors active in the region, but the key actor is nevertheless Russia.

The analysis is conducted using a proposed analytical framework outlining seven dimensions of HT&HW. Using this framework, it will first be analysed *what role the military have today and in the future* across the Baltic Sea region. After that, it will be asked what role the military *should have in the future according to the members of the military themselves.* Here Sweden is used as a case study and structured interviews are conducted with senior officers. The latter dimension is important as it allows to better understand what the profession itself thinks about their role and responsibilities. If able to identify possible discrepancies between the officer's perception and the official strategy, it is possible to enhance ones' ability to operationalize and implement the strategy successfully. One should also note that as a collective, the officer corps can be expected to have shared insight and knowledge on their capabilities, or lack of the same, which if taken into consideration may enhance the ability to defence against HT&HW.

The chapter is structured as follows. First, the two concepts in focus – HT&HW – will be presented and defined. In the following section, the concepts will be operationalized, and an analytical framework of HT&HW that draws together existing Western thinking and the understandings in military and policy frameworks is proposed. Thereafter, the proposed framework is discussed and contrasted with the Russian approach to HT&HW. In section three, the existing official discourse on how the military fit in the context of HT&HW among countries in the Baltic Sea region will be analysed. This is followed, in section four, with a case study analysing what role the members of the military themselves think it should have. The case used is Sweden, and the analysis builds on structured interviews with eighty-two senior officers.

## Conceptualizing hybrid threats and hybrid warfare

As the introduction sets out, HT&HW are problematic concepts and existing scholarship on these phenomena lacks a common definition and the use of terminology remains contested. The term 'hybrid' itself is associated with 'a blend of conventional and non-conventional warfare where a hostile actor is exploiting the blurred area between peace and war'.[6] When moving away from this basic understanding, there is a lack of consensus about the definition as well as of how terms are used. There is also a problem with the tendency to use hybrid threats and/or hybrid warfare as catch-all phrases. To add to the confusion, these two and other terms tend to be used synonymously. Hybrid threat and hybrid warfare are merely two of a variety of terms used to describe a phenomenon, where 'Asymmetrical warfare', 'Sixth Generation Warfare', 'Contactless warfare', 'New warfare', 'Next-generation warfare', 'Ambiguous warfare', 'Asymmetrical warfare', 'Non-linear warfare', 'Full Spectrum Conflict' are a few examples of more or less synonymous terms.[7]

NATO is a case in point. On the page 'NATO's response to hybrid threats' on the NATO website they use hybrid warfare and threats interchangeably.[8] It is said that 'Hybrid methods of warfare, such as propaganda, deception, sabotage and other non-military tactics have long been used to destabilise adversaries' and that 'NATO has a strategy on its role in countering hybrid warfare and stands ready to defend the Alliance and all Allies against any threat, whether conventional or hybrid'.[9] In the same text, NATO talks about hybrid threats as something that 'combine military and non-military as well as covert and overt means, including disinformation, cyberattacks, economic pressure, deployment of irregular armed groups and use of regular forces'.[10] All this is done under the umbrella of hybrid methods, talking about '[h]ybrid methods of warfare', where hybrid methods are 'used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations'.[11] Needless to say, NATO does not offer any conceptual clarity.

One way to conceptualize HT&HW is to understand them as being two sides of the same coin, constituting two viewpoints, or phases, of the same phenomenon. Hybrid warfare concerns active hybrid measures by one actor targeting another actor. In contrast, hybrid threats need not be active measures, but can also be passive – being real or perceived threats for possible future actions against oneself. The difference between real and perceived, as well as the question of whether one is subjected to active and ongoing hybrid measures, does not always have a clear answer. Deception and denial are inherent in hybrid methods, and it is sometimes difficult to know for sure that warfare is ongoing, and in the same way, it is inherently difficult to identify if, and when, a perceived threat of future action becomes a reality. Attempts to deny the presence of masked Russian soldiers in Crimea, and the involvement of different actors in influence operations and cyber operations, exemplify this problem (see also discussion on 'Hybrid Blizzard Model' in Chapter 17). There is also a question of perspective, whether you are the target or perpetrator of hybrid measures; among targets there is a tendency to refer to hybrid threats, even if the hybrid warfare label may also be used after identification of said activity. If you are the source of the threat, you know that it is warfare, which is not threatening to yourself. Regardless, whether a certain measure is labelled a threat or warfare is very much a matter of personal preference – threat or warfare depends on the eye of the beholder.[12]

Despite the existing lack of conceptual clarity and consensus, there is still a need for a conceptual starting point when approaching HT&HW. In this chapter, the starting point consists of two understandings of HT&HW developed by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki and the International Institute for Strategic Studies (IISS). Thy Hybrid CoE characterizes hybrid threat as follows:[13]

1) Coordinated and synchronized action, that deliberately targets democratic states' and institutions' systemic vulnerabilities, through a wide range of means (political, economic, military, civil and information),
2) Activities exploit the thresholds of detection and attribution as well as the border between war and peace, and
3) The aim is to influence different forms of decision making at the local (regional), state, or institutional level to favour and/or gain the agent's strategic goals while undermining and/or hurting the target.

While being debated and contested, the Hybrid CoE perspective is arguably a suitable starting point: the Hybrid CoE has been endorsed by both the Council of the European Union and the North Atlantic Council and has a membership that includes the five Western countries in the Baltic Sea region as well as three major external powers (United Kingdom, France and the United States). Their joint framework

> is to serve as a hub of expertise supporting the participating countries' individual and collective efforts to enhance their civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special focus on European security. It is intended that the Centre will offer this collective experience and expertise for the benefit of all participating countries, as well as the EU and NATO. The Centre will follow a comprehensive, multinational, multidisciplinary and academic-based approach.[14]

Thus, Hybrid CoE is the main institution in the Western security architecture tasked to deal with hybrid threats.

For hybrid warfare, this chapter will adopt a definition used by the International Institute for Strategic Studies (IISS), defining hybrid warfare as

> The use of military and non-military tools in an integrated campaign designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilising diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure.[15]

Crucial in this definition is the integrated campaign part, which separates the concept from asymmetric warfare.[16]

A number of central features are shared by the two definitions, which will guide this chapter. Hybrid actions are

1) multidimensional, and
2) coordinated and synchronized,
3) being part of an integrated campaign with a strategic goal,
4) They are also deceptive, and
5) exploit the border between war and peace.

In the current debates, HT&HW tend to be linked to states (or in extension their proxies), which has not always been the case. To view HT&HW as of state-centred warfare is a recent development, the concept having its origin as a way to describe and understand the complexity and efficiency of non-state actors on the battlefield.[17] Here there are 'are similarities between Russian actions in Ukraine and previous examples of non-state hybrid warfare – most notably the in the "blurring" of traditional concepts of warfare, its unfamiliarity, the use of non-military means, and the asymmetric relationship to conventional Western warfighting – have all contributed to labelling these Russian actions as HW'.[18]

## Analytical framework – the seven dimensions of HT&HW

To be able to trace the role of the military in an area where there lacks a consensus on definition and precise terminology, there is a need for an analytical framework. Utilizing in dimensional understanding of HT&HW, the framework is founded in the understandings of HT&HW as manifested in the IISS, the Hybrid CoE, the Multinational Capability Development Campaign (MCDC) framework, the Swedish Strategic Doctrine, the NATO and the EU perspectives.[19] The IISS and Hybrid CoE definitions have been found to be good definitions as outlined earlier. The MCDC Countering Hybrid Warfare project and the Swedish Strategic Doctrine's understanding of strategic tools and means that can affect and threaten Swedish security have been included as they represent two military-focused frameworks of relevance for the Baltic Sea region. The EU view is included as a representation of the lowest common denominator of the members of the EU as a group, and the NATO view represents the same in the case of the Western military collective.

Analysing the six understandings, a total of seven dimensions can be distilled where HT&HW can be located: (1) diplomatic, (2) economic, (3) cyber (technological), (4) information and influence operations, (5) unconventional methods, (6) civil (non-military) and (7) military (see Table 5.1). The dimensions found in the Hybrid CoE and IISS definitions are present in the NATO and EU thinking on HT&HW, as well as in the frameworks of MCDC and the Swedish Strategic Doctrine. The cyber and unconventional methods are not explicitly part of the five instruments of power in the MCDC framework,[20] nor in the Hybrid CoE definition used here, but the two are present in the two organizations understandings and writing on HT&HW. In the case of the Swedish Strategic Doctrine, civilian (non-military) is not its own category of

**Table 5.1** The seven dimensions of hybrid threats and hybrid warfare

| | **Definition** | | **Military frameworks** | | **Policy** | |
|---|---|---|---|---|---|---|
| **Dimension** | IISS | CoE | MCDC | SWE | EU | NATO |
| 1 Diplomatic | Diplomacy | Political | Political | Diplomatic + political | Diplomatic | n/a |
| 2 Economic | Economic | Economic | Economic | Economic | Economic | Economic pressure |
| 3 Cyber (technological) | Cyber | *Is included* | *Is included* | Cyberattacks | Technological | Cyberattacks |
| 4 Information and influence operations | Info | Information | Information | Psychological | Is included, e.g. Disinformation campaigns | Disinformation, propaganda |
| 5 Unconventional methods | Covert and occasionally military operations | *Is included* | *Is included* | Unconventional | Unconventional | Unconventional (deployment of irregular armed groups + covert means) |
| 6 Civil (non-military) | Non-military | Civil | Civil | *Is included* | Non-military | Non-military |
| 7 Military | Military | Military | Military | Military | Military | Military |

Source: Author

strategic tools, but is an integrated part of the total defence idea and also included in the diplomatic, economic, and psychological tools and means.

## The threat – bringing Russia back in

The reason for HT&HW becoming of central importance can be linked to the rise of Russia. As outlined in the introduction, this threat is an actor encapsulated 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.'[21] Russia as the main threat has in recent decades become the dominant understanding among Western states, not least in the Baltic Sea region that is the focus of this study.[22]

The Russian paradigm can be seen manifested in Georgia, Ukraine and Syria, all three being a good example of 'wars' where the division into war and peace as traditionally understood in the West is highly problematic. It is clear that the grey one between peace and war has grown considerably, and so has the need to identify and understand how to handle the full range of hybrid threats that may occur. Such an ability is particularly important in the case of Russia, it being a country where the mindset is to perceive security politics as a zero-sum game where the aim always is to win, with the underlying thinking being founded in a perception of an always ongoing state of war.

So what types of HT&HW are to be expected? As outlined in his excellent review on the evolution of Russian military though, Timothy Thomas did in 2016 observe that hybrid warfare and new-generation warfare (NGW) for many years had been at the centre of attention among US and Russian military analysis.[23] In early 2015 a new term was introduced when General-Lieutenant A. V. Kartapolov introduced what he called 'New-type War' (NTW) as an alternative way to understand the Russian view on contemporary war.[24] In his article in *the Journal of the Academy of Military Science*, Kartapolov discussed the way NATO and the United States conducts war and outlined what would be needed for Russia to confront it.[25] NTW is here best understood as 'describing war's evolving character' while the term New-generation warfare 'may more likely be a reference to a method of war', noting that 'the Russian military views "methods" as composed of weapons and military art'.[26]

As argued by Thomas, 'while the term NTW appears to be the "chosen one" at present (until another concept is offered in the evolution of military thought), the term NGW should not disappear from Western consideration. It should be considered as perhaps the major "weapons" aspect of Russia's "methods" of war.'[27] In this chapter, focus will be on the concept NGW as we are here more interested in methods of war than the larger question of the evolving character of war. More specifically, we will here adopt a schematization of NGW as outlined by Tchekinov and Bogdanov.[28] They divide what they call 'new-generation warfare' into eight phases:

> **First Phase**: non-military asymmetric warfare (encompassing information, moral, psychological, ideological, diplomatic, and economic measures as part of a plan to establish a favorable political, economic, and military setup).

> **Second Phase**: special operations to mislead political and military leaders by coordinated measures carried out by diplomatic channels, media, and top government and military agencies by leaking false data, orders, directives, and instructions.
>
> **Third Phase**: intimidation, deceiving, and bribing government and military officers, with the objective of making them abandon their service duties.
>
> **Fourth Phase**: destabilizing propaganda to increase discontent among the population, boosted by the arrival of Russian bands of militants, escalating subversion.
>
> **Fifth Phase**: establishment of no-fly zones over the country to be attacked, imposition of blockades, and extensive use of private military companies in close cooperation with armed opposition units.
>
> **Sixth Phase**: commencement of military action, immediately preceded by large-scale reconnaissance and subversive missions. All types, forms, methods, and forces, including special operations forces, space, radio, radio engineering, electronic, diplomatic, and secret service intelligence, and industrial espionage.
>
> **Seventh Phase**: combination of targeted information operation, electronic warfare operation, aerospace operation, continuous airforce harassment, combined with the use of high precision weapons launched from various platforms (long-range artillery, and weapons based on new physical principles, including microwaves, radiation, non-lethal biological weapons).
>
> **Eighth Phase**: roll over the remaining points of resistance and destroy surviving enemy units by special operations conducted by reconnaissance units to spot which enemy units have survived and transmit their coordinates to the attacker's missile and artillery units; fire barrages to annihilate the defender's resisting army units by effective advanced weapons; airdrop operations to surround points of resistance; and territory mopping-up operations by ground troops. [Bold in original text][29]

As can be seen, Russia strives to utilize the grey zone between peace and war where it is unclear if there has been an attack or not. Furthermore, Russia has also systematically denied acknowledgement when others have tried to pin-point identified attacks to Russia (also see the chapters by Alexander Crowther, Markus Göransson and Niklas Nilsson in this volume.)

The Russian NGW fit well into the here proposed analytical framework, with all seven dimensions included in the eight phases (see Table 5.2). Three patterns stand out. First, while not being explicitly mentioned by name in the schematic presentation, it is clear that the cyber dimension is an integrated tool throughout the eight phases. Rather than being separated into its own phase or as a method, the use of cyber is integrated if to be successful throughout the phases. It important from the first phase of including information, moral, psychological, ideological, diplomatic and economic measures where the cyber dimension will play an important role, to during the commencement of military action and afterwards, with cyber being integrated in today's integrated and networked multidimensional battlefield. Second, the role of information and influence operations is also a crucial aspect in undermining the resilience of its opponent, thereby undermining its society's resilience and the

**Table 5.2** The seven dimensions of hybrid threats and hybrid warfare as used in 'new generation warfare'

| Dimension | Present in New Generation Warfare? | Phase 1 | Phase 2 | Phase 3 | Phase 4 | Phase 5 | Phase 6 | Phase 7 | Phase 8 |
|---|---|---|---|---|---|---|---|---|---|
| 1 Diplomatic | X | X | | | | X | | | |
| 2 Economic | X | X | | X | | X | | | |
| 3 Cyber (technological) | X | X* | X* | X* | X* | X* | X* | X | X* |
| 4 Information and influence operations | X | X | X | X | X | | X | X | |
| 5 Unconventional methods | X | | | X | X | X | X | X | X |
| 6 Civil (non-military) | X | X | X | X | X | | | | |
| 7 Military | X | | | | | X | X | X | X |

*= Is included, though not mentioned explicitly.
Source: Author

countries' ability for national defence. Third, while it sometimes is difficult to draw the exact borders between unconventional-, civil (non-military)-, and military measures, it is clear that all three will be used and hence are to be expected. Here it is important to note that the 'limitation' of Western democracies trying to draw a clear border between war and peace does not encumber Russia; it will simply use the most efficient tool possible to reach its goals without legal constraints.

In conclusion, the seven dimensions do not 'only' fit the Western view of hybrid warfare, but it is also a good fit into the Russian understanding of HT&HW, here represented by Russia's eight-phased 'new generation warfare'.[30] This is of course not surprising, as the Western conceptual understanding has developed in reaction to Russia's perceived behaviour. Or, in the view of the Russians, the other way around.

Sweden can here be used as a good example. The lack of clear threshold is streaming through the Swedish doctrine that is built around the grey-zone idea.[31] Thus, its understanding of reality is very similar to the Russian idea of hybrid warfare. This might not come as a surprise, as what the doctrine does very much is countering a threat from Russia. A reflexive process, the social construction of hybrid warfare and threats, while being very real, are also constructed and continuously reconstructed in the social interaction between actors, here a combination of states, experts, pundit, journalists as well as the public.

## Where does the military fit in?

So then, in which dimensions is there a role to be played by the military? That it plays a role in the 'Military' dimension is obvious; this is the raison d'être of the military. It also goes without saying that the military is to play a critical role in the latter phases of in the schematic model of NGW. In contrast, the military is expected to play no or minimal role in the 'Diplomatic' in the case of Western democracies as those studied here. Also in the case of the 'Economic' dimensions its role is expected to be limited. This said, in the context of cooperation with its civilian counterparts there is always a certain role to be played by the military, especially within a 'Total-' or 'Comprehensive' Defence concept.[32] There may also be a role for the military to counter economic pressure or to ensure the societal and infrastructure needs of the economic sphere. One example here could be to safeguard critical infrastructure and energy security.[33] Here 72 per cent of the interviewed Swedish officers thought that the military should play at least a limited role against economic and psychological attacks on critical infrastructure.[34]

As has been outlined earlier, the cyber dimension plays a central role in current discussions on hybrid threats and hybrid warfare. For example, the EU has increased its cooperation on cyber defence to strengthen its capability. The initial EU cyber defence policy framework was adopted in 2014, and in November 2018 the European Council emphasized the need to build strong cybersecurity, referring to in particular the need to be able to respond to and deter cyberattacks.[35] Cyber also plays an important part in the work of NATO. Here the creation of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn is a good illustration of the importance given to the cyber dimension.[36]

Emphasis on cyber can also be found among the countries in the Baltic Sea region, where cyber defence has become a task where the ministry of defence and the military play an increasingly important role. For example, in the case of Lithuania, its Ministry of National Defence is since 2015 responsible for shaping and implementing the national cybersecurity policy and a National Cyber Security Centre has been established with the task to handle the cybersecurity of state institutions and critical information infrastructure.[37] In Scandinavia, cyber defence is an important and integrated part of the work of the Swedish military,[38] and in Denmark the inter-party defence agreement for the 2018–23 period outlines cybersecurity as one of the particular focus when strengthening the military ability to contribute to national security.[39] There has also been a trend towards developing cyber commands and cyber units. For example, in Poland cyber units 'will be responsible for ensuring cyber security on a continuous basis by coordinating and supervising activities in the cyberspace' and the Polish Armed Forces is to be 'prepared to operate in the dynamic information environment, both proactively and by reacting to hostile actions'.[40] Estonia has developed a Cyber Command, and Latvia has a Cyber Defence Unit linked to its National Guards.[41]

Information and influence operations are a crucial feature of the Russian way to conduct hybrid warfare. The exact role of the military to counter this form of warfare is not absolutely clear as this is a broad category which ultimately is about the overall resilience of the society as a whole. Thus, the role of respective armed force is often linked to the joint efforts of the military and civilian defence such as Total- or Collective Defence concepts. As a consequence, the division of labour between the military and civilian agencies varies between countries. It can be assumed that as the military is a key actor in cyber defence they also by necessity play an important part in countering information and influence operations as those are mainly taking place in the cyber dimension. For example, according to a Lithuanian White Paper, 'Russia conducts deliberate information campaigns targeting Lithuanian society using a broad array of means: from television to social media' and one way its National Defence System take direct actions is in the form of the Lithuanian Armed Forces Communications Department who 'monitors and analyses the information domain to determine the targets, the scale and means of the information attacks'.[42] It should here also be noted that since 2014 there is a NATO Strategic Communications Centre of Excellence in Latvia where all countries in the Baltic Sea region are members.

In the case of supporting civilian authorities, there is an outspoken role for the military to support, including the national police in response to non-military threats. A number of areas stand out where there is a clearly defined role: terrorism, border control, and at times of national emergencies such as natural disasters and large-scale accidents.[43] In, for example, Denmark it is outlined that the armed forces and 'will establish a permanent helicopter response based in the Copenhagen area at very high readiness in support of the police's counter-terrorist preparedness' and that '[r]esources will be reserved for Defence to generate units on high readiness to assist the police in case of terror attacks etc'.[44] There are also provisions for providing support to ensure law, order and security. In Latvia, the military shall provide support to the state police 'ensuring order and security' ('*sabiedriskās kārtības un drošības nodrošināšanā*') and in the case of Finland to 'work with other authorities to maintain law and order and security, prevent and stop terrorists and to secure society in general' to give but two examples.[45]

Moving on to unconventional methods. Not surprisingly, this is together with the cyber dimension, an area where there is a central role for the military. One typical example is the response to Ukraine in Lithuania, who formed a rapid response force in of roughly 2,500 soldiers in 2014 with the task to 'react to local armed incidents or border violations during peacetime, such as actions of irregular armed groups, illegal border crossing, violation of military transit procedures, etc'.[46] Denmark plans to do something similar, planning to establish a Light infantry battalion with up to about 500 troops (1 HQ Company and three standing companies) that can 'be deployed by air or ship and may be part of collective defence, some international operations or nationally, including in support of the police'.[47]

Special Operations Forces (SOF), themselves skilled in unconventional methods, play an important role in confronting unconventional methods in a hybrid context. For example, the Estonian Special Operations Force (ESTSOF) is seen as an essential component for Estonia's defence having the capability to conduct unconventional warfare and handling tasks such as 'special reconnaissance and surveillance, military support and direct action'.[48] In the hybrid context, it is also important to note that the military and SOFs often have a focus on learned lessons from Russia's previous behaviour. The Lithuanian SOF, drawing on lessons from Ukraine, has given special attention to 'the capabilities of the SOF to operate in hybrid scenarios'.[49]

Another actor to be mentioned in the context of unconventional methods is the military security services. For example, in Sweden, they 'follow-up and counters different types of threat; the most common threats being the work of foreign intelligence services, organised crime, subversion, sabotage and terrorism'.[50] Finally, it should here also be recognized that while already been included as part of the cyber dimension, cyberattacks are also a form of unconventional methods where the military plays a central role in the defence.

## Responding to hybrid threats and hybrid warfare in the mind of the Swedish officer

How does the official discourse presented earlier fit with the actual thinking among the members of the military? To try to answer this question, structured interviews have been conducted with a total of eighty-two Swedish officers ranging from Captain (OF-2) to Colonel (OF-5) level. Of these, fifty-two were current participants in the Higher Joint Command and Staff Programme (part of either the 2018 or 2019 intake).[51] The question asked was 'How large role do you think the military SHOULD HAVE in meeting the following forms of means and instruments that in different ways may threaten and influence Sweden's security?', asking the respondent to choose on a 5-grade scale where 0 = no role, 1 = small role, 3 = certain role, 4 = large role, 5 = very large role. The same interview guide was used in all three rounds of interviews. The interview guide does not ask about the role of the military in the diplomatic sphere as this is clearly not the role of the military in Sweden.

The role of the military in the military dimension correlates with the findings on the Baltic Sea region as a whole; all respondents think there is a central role to be played by the military. A total of 99 per cent of the respondents thought the military should play a large or very large role against 'Military Intrusions', 'Military Intervention', 'Limited Attack', 'Invasion', and 'Attack by long-range weapons' (average of 99 per cent with the range between the types of measures being 97 and 100 per cent), with 84–100 per cent responding that there should be a very large role (avg. 86 per cent) (Figure 5.1).

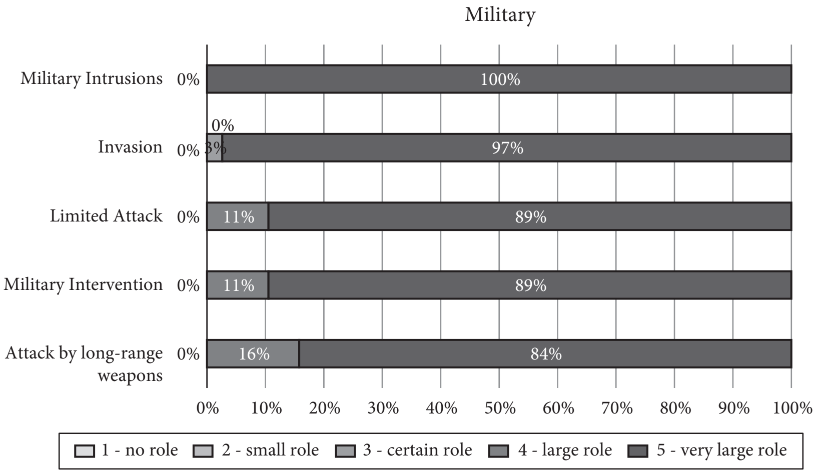

**Figure 5.1** Military dimension.

On the other side of the spectrum, in the economic dimension, only one in five saw a large or very large role for the military in meeting 'Attacks by economic and psychological means against critical infrastructure' (Attack Eco + Psy Crit Infra). While 51 per cent did see a certain role for the military in this area, it is nevertheless clear that this area is not perceived as a core task but rather something that should be handled by civilian institutions. However, the certain role aspect leaves space for the military supporting civilian actors (Figure 5.2).

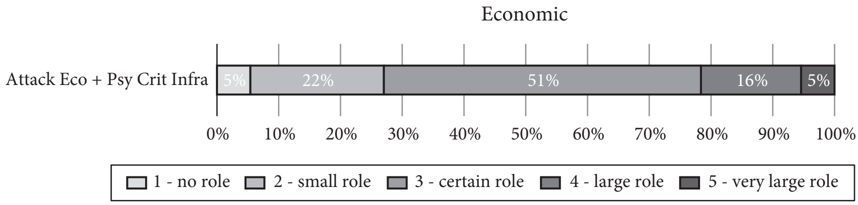

**Figure 5.2** Economic dimension.

Moving on to the cyber and technological dimension. Here the perceived role of the military varies between 'Cyberactivism', 'Cyberattacks' and 'Electronic Warfare'. In the case of cyberactivism, about half the respondents think the military should play a large or very large role, with 42 per cent answering a large role. Only 8 per cent think there is a small or no role to be played. These findings are in line with the focus put on the cyber dimension as outlined earlier, with an increasingly large role being played by different parts of the military. In the case of cyberattacks and electronic warfare, the role of the military is higher. For cyberattacks, as many as 77 per cent of the officers do see the military role as central, with 32 per cent answering a very large role and 42 per cent a large role. For electronic warfare, the importance is even higher with 92 per cent thinking that the role should be central, with 54 per cent answering a very large role and 38 per cent a large role. Considering that two forms of hybrid measures are also a form of unconventional warfare, the large role might not come as a surprise (Figure 5.3).

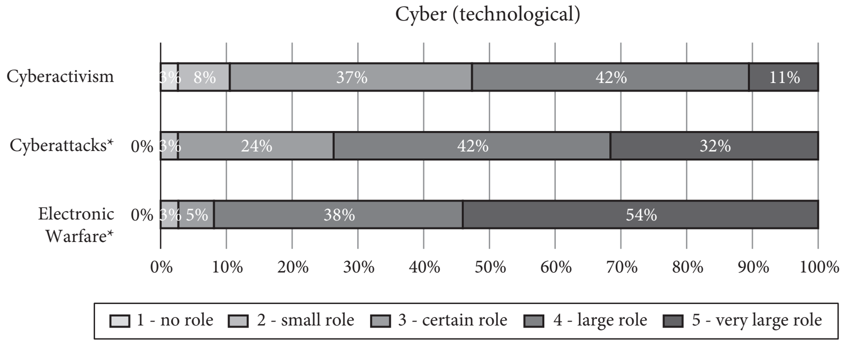

**Figure 5.3** Cyber (technological) dimension.

In contrast, in the area of information and influence operations, the role is seen as more limited. While 58 per cent of the respondents see a certain role for the military in meeting ‘Propaganda’, only 16 per cent saw any larger role to be played. A somewhat larger proportion though there should be a role against ‘Influence operations aimed at political and military decision-makers’ (Influ Ops Pol+Mil), with four in ten thinking that the military should play a large or very large role. In conclusion, as with the case of cyber the more ‘traditional’ or ‘harder’ the threats are, the larger role the officers themselves think that the military should play. Overall, the findings with regard to Swedish officers are in line with the findings on the Baltic Sea region (Figure 5.4).

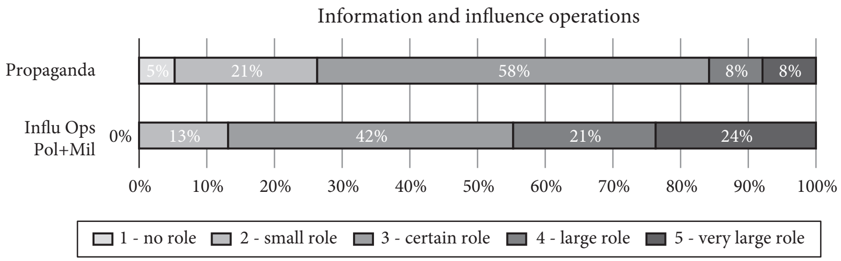

**Figure 5.4** Information and influence operation dimension.

When it comes to ‘non-military asymmetric warfare’ (Non-military Asym Warfare), ‘Subversive activities’ and ‘terror’ no more than 5–11 per cent see a very large role and 25–34 per cent a large role. While the officers clearly see a certain role, in particular in the case of terror, it is not seen as a core task. This is not necessarily something that goes against the outspoken role given to the military, but rather a manifestation of an idea that supporting against non-military activities is something that one should do, as long as focus from the main military tasks is not diverted (Figure 5.5).

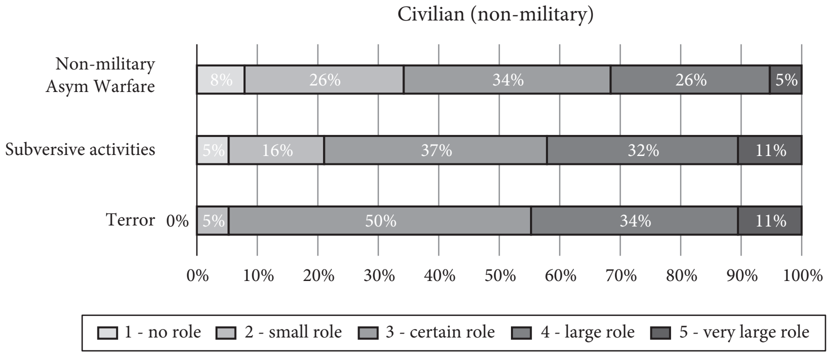

**Figure 5.5** Civilian (non-military) dimension.

In the unconventional methods dimensions, which is a very important area in the context of HT&HW and the grey zone, it is clear in the interviews that there should be a central role for the military. About 90 per cent thought there should be a large role in the case of ‘warfare through proxies’ and cases of ‘masked special forces’, with roughly half of the respondents answering a very large role. A mere 3 per cent thought there should be a small role and none of the respondents thought there should be no role. Also in the case of cyberattacks and electronic warfare discussed earlier, more than half saw a large or very large role for the military (Figure 5.6).

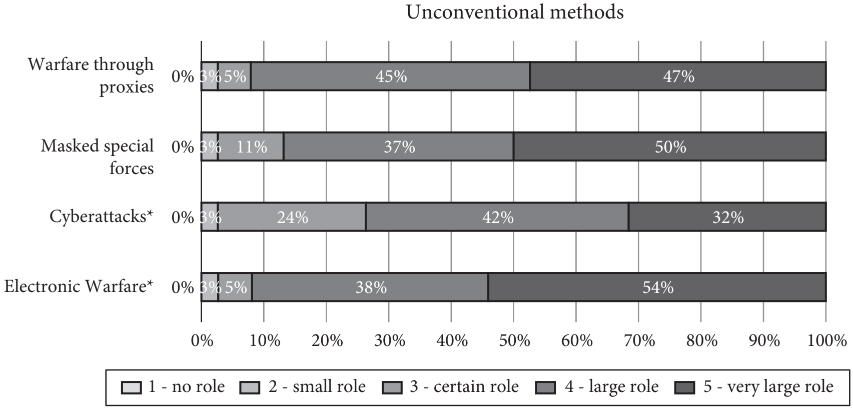

**Figure 5.6** Unconventional methods dimension.

In conclusion, according to at least the Swedish officers themselves, there is a large role to be played by the military in the grey zone to respond to different HT&HW. The importance that should be given to the military varies between dimensions and different measures. There is a tendency to be a correlation between how ‘hard’ the type of threat or warfare is, but at the same time, there is not the understanding that it is only the military dimension that should be the responsibility of the military, nor that it is only in areas of hard security threats that the military should play a role. It can also be concluded that there is also a correlation between what the officers themselves think should be the role of the military and the findings from official documents from countries in the Baltic Sea region. While this might not be surprising, it should not be assumed. It is encouraging to see that the thinking among military officers about where the military fit in when countering HT&HW is corresponding to the official discourse about the same.

## Conclusion

The question asked in this chapter was ‘*What is the role of the military – if any – to counter hybrid threats and -warfare*?’ It can be concluded that there, without a doubt, there is a role to be played by the military. How large of a role varies between the different dimensions of HT&HW, the overall picture showed that the military have a crucial role to play in countering HT&HW and building a resilient society.

In the ‘military’ dimension, the role is obvious; defence against military threats is the core task of the military. In the case of the ‘economic’ dimension, the analysis shows that there is a certain role for the military though it is limited and can be expected to be played out mainly in the context of collaboration with, and support to, civilian institutions. In the case of the 'civil (non-military)' dimension, there is a shared understanding that the military should support against non-military hybrid measures as well as supporting its civilian counterparts when needed, at least as long as focus from the main military tasks is not jettisoned. In fact, official documents show an increasingly outspoken role for the military in supporting civilian authorities. This trend is also logical considering that HT&HW work across conflict dimensions and sectors targeting the weak points.

In the case of the 'cyber (technological)' and the 'unconventional methods' dimensions, it is found that the military does, and should, play a central role. In the case of cyber, it is clear from the official discourse as well as in the interviews that the military does and should continue to have a central role. Cyber is also an area where much work has been done and is done to facilitate the role of the military in relation to cyber defence and cybersecurity. The role of the military should also be understood in relation to cyberattacks and electronic warfare is a form of unconventional methods. For 'unconventional methods' the picture is similar. This is an area where there is a central role for the military according to official discourse as well as the interviews. This includes the security services which play a central role in the work against HT&HW. Their exact role varies between countries, as different countries both organize their military differently and have differences in how they divide responsibilities between military and civilian institutions.

In the 'information and influence operations' dimension, the role is more unclear, both in regard to what it is and what it should be. This is a broad category, and it is an area that is ultimately about the overall resilience of the society as a whole. Consequently, the role of the military is here embedded in joint efforts of military and civilian actors. Nevertheless, as this dimension is deeply integrated with the cyber dimension, there will, for sure, be a role to be played, if not directly, indirectly.

## The way forward

There is evidently a need for a new way of thinking to be able to handle the battlefield of the future that does not recognize either a state peace or of war. This need is particularly true among Western democracies who are embedded in a traditional understanding of international law; in the hybrid era, international law no longer fits with the reality on the ground. Such a need is of course also what is to be expected. The whole idea behind using hybrid methods is to find and exploit your opponent's weaknesses, and the border between peace and war and the limitations and constraints of international law is arguably the Western democracies biggest 'weakness' (and strength?). It is clear from the analysis that there has been, and continues to be, a transformation in the way of thinking surrounding the role of the military. That the mindset is shifting is supported both in the analysis of the official discourse and of the thinking of the officers themselves. There is, of course, a variation between different countries both in regard to how much the thinking has changed, and exactly how it has changed, but the trend is clear.

When deciding on what the role of the military should be, there is a need to strike a balance. If there is too much of pragmatic adaptation to the existing situation, there is at the same time a risk of undermining the democratic principles on which Western democracy is built. Such a path also risks undermining the whole idea of a separation between peace and war, the principles of international law, and in continuation the liberal world order itself. Furthermore, while arguably not something to seek in the first place, neither would such a path necessarily be a recipe for success: the enemy will change and adapt to the new situation, exploiting new weaknesses that over time emerges. In short, warfare is a two-player game with an intelligent opponent. It is essential that the Western countries are flexible, but at the same time, there is a need to ensure to keep to democratic principles and the protection of the existing democratic system. This is the system the military set to defend and if there is no longer a system to defend the question is whether it could be labelled a victory success even if one wins the war. The aim must be to protect our system, not to undermine or destroy the system and become another actor with disregard for democratic principles, international law and the international system as a whole.

In conclusion, 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 HT&HW today and tomorrow. This said, there is today a discrepancy between where we are and where we should be. It should also be recognized that there is no set target for where to go, as the target is continuously changing as the use of, and protection against, HT&HW are a two-sided game. The target will change, and it will not change the way we would like. There will be a continuous process of adaptation and change, with all sides trying to out-think and out-smart each other. There is no end-state, only ongoing interactive process of adaptation and change, with multiple actors. There is also the dimension of trying to beat the other's cycle of identifying weaknesses, decisions and actions against them, an area where, unfortunately, the democratic system is inherently slow. To be successful, there is a need to include actors in all sectors in the best way possible, including the military. It is here crucial to learn from each other, across borders and sectors, both inside and outside the Baltic Sea region.

## Notes

[1] The author wants to acknowledge support from the S. Rajaratnam School of International Studies (RSIS) of Nanyang Technological University where the author was a visiting fellow in the autumn of 2020 hosted by Li Mingjiang. Support has also been received from Riksbankens Jubileumsfond (RJ) (Grant No. F16-1240:1).

[2] For example, James J. Wirtz, 'Life in the "Gray Zone": Observations for Contemporary Strategists', *Defense & Security Analysis* 33, no. 2 (2017): 106–14; John Chambers, 'Countering Gray-Zone Hybrid Threats: An Analysis of Russia's "New Generation

Warfare" and Implications for the US Army' (Modern War Institute at West Point, 2016). https://apps.dtic.mil/dtic/tr/fulltext/u2/1020295.pdf; Martin Zapfe, '"Hybrid" Threats and NATO's Forward Presence', *Policy Perspectives* 4, no. 7 (2016). https://doi.org/10.3929/ethz-a-010717736; Nicholas Barber, 'A Warning from the Crimea: Hybrid Warfare and the Challenge for the ADF', *Australian Defence Force Journal*, no. 198 (2015): 11–22; Fredrik Löjdquist, 'An Ambassador for Countering Hybrid Threats', RUSI. https://www.rusi.org/commentary/ambassador-countering-hybrid-threats; Lyle Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (RAND Corporation, 2019). https://doi.org/10.7249/RR2942; David Carment and Dani Belo, *War's Future: The Risks and Rewards of GreyZone Conflict and Hybrid Warfare,* Policy Paper (Ottawa: Canadian Global Affairs Institute, 2018). https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4059/attachments/original/1539971167/Wars_Future_The_Risks_and_Rewards_of_Grey-Zone_Conflict_and_Hybrid_Warfare.pdf?1539971167; Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict,* SSI monograph (Carlisle Barracks: Strategic Studies Institute and U.S. Army War College Press, 2015).

[3] NATO, 'NATO's Response to Hybrid Threats', 8 August 2019. https://www.nato.int/cps/en/natohq/topics_156338.htm; European External Action Service, 'A Europe That Protects: Countering Hybrid Threats', 13 June 2018. https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en.

[4] Mark Galeotti, *Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right* (Prague: Mayak Intelligence, 2016), 7.

[5] See e.g. Ministry of National Defence, 'White Paper Lithuanian Defence Policy' (Vilnius, 2017). https://kam.lt/download/59163/wp-2017-en-el.pdf; 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); Republic of Latvia, 'The National Security Concept', 2016. https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf; Ministry of National Defence, 'The Defence Concept of the Republic of Poland', 2017. https://www.gov.pl/attachment/fae62ff2-0471-46e1-95bd-c3c4208234a7, 23–6; Prime Ministers' Office, 'Government's Defence Report', Prime Minister's Office Publications, July 2017. https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf, 8–10; The Danish Government, 'Foreign and Security Policy Strategy: 2019-2020', 2018. https://um.dk/~/media/um/danish-site/documents/udenrigspolitik/aktuelle%20emner/udenrigs%20og%20sikkerhedspolitik/2019-20/foreign%20and%20security%20policy%20strategy%202019-2020.pdf, 11–13.

[6] Nupi, 'Multinational Capability Development Campaign 2015-18 (Countering Hybrid Warfare)', Nupi, accessed 17 March 2020. https://www.nupi.no/en/About-NUPI/Projects-centres-and-programmes/Multinational-Capability-Development-Campaign-2015-18-Countering-Hybrid-Warfare.

[7] For a discussion on terminology, see Chapter 1 in this volume. 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 includes Mikael Weissmann, 'Hybrid Warfare and Hybrid Threats Today and Tomorrow: Towards an Analytical Framework', *Journal on Baltic Security* 5, no. 1 (2019): 17–26; Sean Monaghan, 'Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces', *Multinational*

*Capability Development Campaign (MCDC)*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840513/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf;
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' (National Defense University Washington DC Institute for National Strategic Studies, 2009); Frank G. Hoffman, 'Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict', *Strategic Forum* (Washington, DC: Institute for National Strategic Studies, National Defense University, 2009).

[8] Nato, 'NATO's Response to Hybrid Threats'.

[9] Nato, 'NATO's Response to Hybrid Threats'.

[10] Nato, 'NATO's Response to Hybrid Threats'.

[11] Nato, 'NATO's Response to Hybrid Threats'.

[12] One further differentiation between the labels hybrid threats and hybrid warfare that has emerged in the authors discussion with public officials is legalistically based, arguing that we should talk about hybrid threats as 'warfare' is something that may only take place at times of war.

[13] The European Centre of Excellence for Countering Hybrid Threats, 'Hybrid Threats: Countering Hybrid Threats', *The European Centre of Excellence for Countering Hybrid Threats*, accessed 22 March 2019. https://www.hybridcoe.fi/hybrid-threats/. Their definition is being altered over time. The version used here originates from 22 March 2019. At the time of writing (3 March 2020) the explicit listing of the 'wide range of means' has been deleted and 'the border between war and peace' has been replaces by 'the different interfaces (war-peace, internal-external, local-state, national-international, friend-enemy)'. For details see https://web.archive.org/web/*/https://www.hybridcoe.fi/hybrid-threats/.

[14] The European Centre of Excellence for Countering Hybrid Threats, 'Hybrid CoE - the European Centre of Excellence for Countering Hybrid Threats', accessed 5 March 2020. https://www.hybridcoe.fi/.

[15] International Institute for Strategic Studies, *The Military Balance 2015* (Abingdon: Routledge for the International Institute for Strategic Studies (IISS), 2015), 5. In *The Military Balance* the definition originates in descriptions of Russia's hybrid warfare, but the definition itself has a general bearing and need not be limited to Russia but can be applied on other actors as well.

[16] Hybrid warfare is a concept that is very close to asymmetric warfare. The two may look different, but in reality, they are very similar. Hybrid and asymmetric warfare are both about compensating for one's own military weakness compared to ones' opponent. Simply put, if you have a stronger opponent, you need to find other solutions than conventional warfare. However, often asymmetric warfare is used as a broader concept. This can for example be seen in how NATO and EU talks about hybrid threat/warfare as being 'asymmetrical'. Hybrid warfare is something that is more guided with a clear direction and targeted – as seen in the 'integrated campaign' part in the definition used in this chapter. Thus hybrid warfare is something that can be linked to an actor and its strategic goals, which need not be the case for asymmetric warfare.

Irregular warfare should also be mentioned. It is similar to asymetrical and hybrid warfare, the key difference being that is built on the presence of a non-state actor –

normally in the form of insurgency or terrorist actor with the end goal in obtaining political power to achieve political-, social-, economic and/or religious change (David Jordan et al., *Understanding Modern Warfare* (Cambridge: Cambridge University Press, 2016), ch 13). However, as with the other concepts discussed here irregular warfare is often used as a catch-all phrase referring to a broad range of undefined warfare that is not conventional warfare.

17 Erik Reichborn-Kjennerud and Patrick Cullen, 'What Is Hybrid Warfare?', Norwegian Institute of International Affairs (NUPI), Policy Brief, January 2016. http://hdl.handle.net/11250/2380867, 1–2. Also see Frank G. Hoffman, 'Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges', *PRISM* 7, no. 4 (2018): esp 36–40; Hoffman, 'Hybrid Threats'; David E. Johnson, *Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza* (Santa Monica: RAND, 2010); Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington: Potomac Institute for Policy Studies, 2007) for discussion.

18 Reichborn-Kjennerud and Cullen, 'What Is Hybrid Warfare?', 2.

19 Sean Monaghan, Patrick Cullen and Njord Wegge, *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare* (MCDC, March 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf; Cullen, Patrick; Reichborn-Kjennerud, Erik, 'MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare' (MCDC, January 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf; Swedish Armed Forces, *Militärstrategisk Doktrin [Military Strategic Doctrine]: MSD 16* (Stockholm: Swedish Armed Forces (Försvarsmakten), 2016); High Representative of the Union for European Commission Foreign Affairs and Security Policy, 'Joint Framework on Countering Hybrid Threats: A European Union Response', European Commission, Brussels, 6 April 2016, JOIN(2016) 18 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN; The European Centre of Excellence for Countering Hybrid Threats, 'Hybrid threats: Countering Hybrid Threats' (Also see note 12.); Nato, 'NATO – Official Text: Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 08-Jul.-2016', https://www.nato.int/cps/en/natohq/official_texts_133163.htm; International Institute for Strategic Studies, *The Military Balance 2015*.

20 The MCDC framework separates between 'Instruments of power' which are the dimensions listed here and 'Target vulnerabilities', that is, what the hybrid actions are targeting at, which are political, military, economic, social, infrastructure and information. (Monaghan, Cullen and Wegge, *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare*; Patrick Cullen and Erik Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project* (MCDC, January 2017)). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

21 Galeotti, *Hybrid War or Gibridnaya Voina?*, 7

22 On the view of the countries in the Baltic Sea region, see note 5 above. It should be noted that the Russian perspective and narrative about history and what has happened since the end of the Cold War is different from the Western security narrative.

23 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): 554–75.

24 Thomas, 'The Evolution of Russian Military Thought', 570–3.

25 Thomas, 'The Evolution of Russian Military Thought', 570. In his article he outlined a template for NTW which is included as an appendix in Thomas article (p. 575).

26 Thomas, 'The Evolution of Russian Military Thought', 556.

27 Thomas, 'The Evolution of Russian Military Thought', 556.

28 Tchekinov and Bogdanov cited in Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga: National Defence Academy of Latvia, Center for Security and Strategic Studies, 2014), 6.

29 Bērziņš, *Russia's New Generation Warfare In Ukraine*, 6 citing Tchekinov and Bogdanov. Bold in original.

30 Bērziņš, *Russia's New Generation Warfare In Ukraine*.

31 The doctrine outlines a wide range of different strategic measures and instruments that may threaten and influence Swedish security divided into six dimensions: diplomatic-, economic-, psychological-, political-, unconventional- and military means. Swedish Armed Forces, *Militärstrategisk Doktrin [Military Strategic Doctrine]: MSD 16*, 35.

32 See e.g. Ministry of Defence, 'Comprehensive National Defence in Latvia', accessed 27 February 2020. https://www.mod.gov.lv/sites/mod/files/document/Comprehensive%20National%20Defence%20in%20Latvia.docx; Government of Sweden, 'Sweden's Defence Policy 2016 to 2020', Government Offices of Sweden, 2 June 2015. https://www.government.se/information-material/2015/06/swedens-defence-policy-2016-to-2020/; Viljar Veebel and Illimar Ploom, 'Estonia's Comprehensive Approach to National Defence: Origins and Dilemmas', *Journal on Baltic Security* 4, no. 2 (2018): 10–22.

33 See e.g. Nato, 'BRUSSELS SUMMIT DECLARATION: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 11-12 July 2018', Press Release, 11 July 2018. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf, §78; Jukka Savolainen, *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure: Weapons of Mass Disturbance (WMDi)?*, Working Paper, The European Centre of Excellence for Countering Hybrid Threats, November 2019. https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Working-paper_WMDivers_2019_rgb.pdf.

34 Survey conducted with eighty-two Swedish officers, see section on 'Responding to Hybrid Threats and Warfare in the Mind of the Swedish Officer' for details.

35 Council of the European Union, 'EU Cyber Defence Policy Framework (2018 update)' 14413/18, Brussels, 2018. http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf; Council of the European Union, 'OUTCOME OF THE COUNCIL MEETING: 3652nd Council meeting, Foreign Affairs (including Defence)', Brussels, 19 and 20 November 2018 14399/18 (Brussels, 2018). https://www.consilium.europa.eu/media/37952/st14399-en18.pdf.

36 'NATO Centres of Excellence are nationally or multi-nationally funded institutions accredited by NATO. They train and educate leaders and specialists from NATO member and partner countries, assist in doctrine development, identify lessons learned, improve interoperability and capabilities, and test and validate concepts through experimentation. They offer recognized expertise and experience that is of benefit to the Alliance and support the transformation of NATO, while avoiding the duplication of assets, resources and capabilities already present within the NATO command structure.' ('Centres of Excellence: NATO's ACT', accessed 27 February 2020. https://act.nato.int/centres-of-excellence.)

37 Ministry of National Defence, 'White Paper Lithuanian Defence Policy', 55.

38 Ministry of Defence, 'Defence Agreement 2018–2023', accessed 25 February 2020. https://fmn.dk/temaer/forsvarsforlig/Documents/danish-defence-agreement-2018-2023-pdfa.pdf; Försvarsmakten, 'Cyberförsvar – Försvarsmakten'" accessed 27 February 2020. https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/cyberforsvar/. Also see Government of Sweden, 'Sweden's Defence Policy 2016 to 2020', 5.

39 Ministry of Defence, 'Defence Agreement 2018–2023'.

40 Ministry of National Defence, 'The Defence Concept of the Republic of Poland', 46.

41 Estonian Defence Forces, 'Estonian Defence Forces', Estonian Defence Forces, accessed 24 February 2020. https://mil.ee/en/defence-forces/; Ministry of Defence, 'National Armed Forces Cyber Defence Unit (CDU) Concept', 2013. https://www.zs.mil.lv/sites/zs/files/document/cyberzs_April_2013_EN_final.pdf.

42 Ministry of National Defence, 'White Paper Lithuanian Defence Policy', 54.

43 See e.g Government of Sweden, 'Sweden's Defence Policy 2016 to 2020', 6; Ministry of Defence, 'Defence Agreement 2018–2023'; Estonian Defence Forces, 'Estonian Defence Forces'; National Armed Force, 'Galvenie Uzdevumi [Main Tasks]', accessed 28 February 2020. https://www.mil.lv/index.php/lv/par-mums/par-nbs/galvenie-uzdevumi; 'Finnish Defence Forces as Part of the Society – the Finnish Defence Forces', accessed 26 February 2020. https://puolustusvoimat.fi/en/a-part-of-society; Minister of National Defence of the Republic of Lithuania, 'THE MILITARY STRATEGY OF THE REPUBLIC OF LITHUANIA', 17 March 2016. https://kam.lt/download/51934/lt%20military%20strategy%202016.pdf; Ministry of National Defence, 'White Paper Lithuanian Defence Policy', 47; German Ministry of Defence, 'Defence Policy Guidelines: Safeguarding National Interests – Assuming International Responsibility – Shaping Security Together', German Ministry of Defence, Berlin, 27 May 2011. https://www.bmvg.de/resource/blob/16136/0c1b6d8d0c0e6ba0aed5f0feb0af81d8/g-03-110527-vpr-engl-data.pdf, 10–11.

44 Ministry of Defence, 'Defence Agreement 2018–2023'.

45 National Armed Force, 'Galvenie uzdevumi [Main tasks]'; Finnish Defence Forces, 'About Us', accessed 26 February 2020. https://puolustusvoimat.fi/en/about-us.

46 Ministry of National Defence, 'White Paper Lithuanian Defence Policy', 31.

47 Ministry of Defence, 'Defence Agreement 2018–2023'.

48 Estonian Defence Forces, 'Special Operations', Estonian Defence Forces, accessed 28 February 2020. https://mil.ee/en/landforces/special-operations/.

49 Ministry of National Defence, 'White Paper Lithuanian Defence Policy', 37.

50 Swedish A. Forces, 'The Intelligence and Security Service – Swedish Armed Forces', accessed 27 February 2020. https://www.forsvarsmakten.se/en/about/organisation/the-intelligence-and-security-service/.

51 Three rounds of interviews were conducted, one in October 2019 and two in February 2020. When controlling for variations between the three datasets, only minor variations were identified. What stands out is a somewhat lower score on the role in the case of 'cyberattack' and 'subversive activities' among the two datasets of army officers (Avg. of 3.74 and 2.72 vs 4.03 and 3.26) and a higher score on 'Subversive actions against Sweden in various areas such as electronically, space, land, and / or in the radio spectrum, including the use of special operations' (Avg. 4.85 vs 4.05). Nevertheless, while there is a substantial difference in the latter case there is still an agreement that there are clearly a role for the armed forces.