Weissmann, Mikael, Niklas Nilsson, and Björn Palmertz. "Moving out of the blizzard: Towards a comprehensive approach to 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. 263–272. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781788317795.0025>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 15:09 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.

Moving out of the blizzard

Towards a comprehensive approach to hybrid threats and hybrid warfare

Mikael Weissmann, Niklas Nilsson and Björn Palmertz

Water is fluid, soft, and yielding. But water will wear away rock, which is rigid and cannot yield. As a rule, whatever is fluid, soft, and yielding will overcome whatever is rigid and hard. This is another paradox: what is soft is strong.

Lao Tzu

The unifying purpose of this volume has been to address the array of security challenges arising in the contemporary volatile security environment, characterized above all by an increasingly blurred distinction between war and peace. In this inherently complex and increasingly ambiguous environment, the concepts of hybrid threats and hybrid warfare, henceforth HT&HW, are helpful in both structuring an understanding of the nature of the threats we are facing and the strategy and modus of potential adversaries. Thus, the volume has pursued a comprehensive view of the threats as well as the existing tools and means to counter them.

This focus puts the spotlight on the nature of the threats and adversaries and the challenges they pose to Western democracies. However, it fundamentally boils down to the question of the capacity in Western-style democracies and Western security institutions to confront HT&HW, by comprehending the particular vulnerabilities in their societies and addressing them, as well as devising responses to hostile measures by external actors. The particular vulnerabilities and limitations, as well as advantages of Western democracies, call for particular approaches in this environment. Open societies built on the normative foundations of the rule of law, human rights and democracy, necessarily protective of the freedoms of speech, association and the press, need to devise solutions that not only preserve these fundamental freedoms but also draw on their particular strengths. As has been demonstrated in previous chapters, this work is well underway, in the form of numerous entities tasked with analysing and addressing the problem.

Against the backdrop of the existing overload of overlapping concepts coined or reintroduced to capture the nature of the contemporary security environment, and the controversy surrounding their use, the volume has refrained from attempts to invent new labels or engage at length with the conceptual debate. Instead, we have settled for the use of HT&HW as unifying themes for the volume in an attempt to move the discussion away from how phenomena are supposed to be termed to how they can be understood and addressed. As demonstrated by the range of contributions, there is undoubtedly much to be said on this topic. In this light, a particular contribution of the volume is the unified effort of academic scholars and practitioners, from different fields, to provide a common perspective on HT&HW, based on experiences from a wide set of empirical contexts.

For this purpose, the volume was structured into three parts, each providing a distinct perspective on HT&HW. This was intended not only to allow scholars and practitioners, as well as thematically and area-focused authors, equal chance to present their perspectives in their own right. The aim was also to create synergy effects between the different areas of expertise.

The first part gathered perspectives of key Western collective security actors represented by the two international organizations with primary responsibility for upholding the Western security community, NATO and the EU, as well as the single largest and most influential security actor, the United States. With a common point of departure in Russia's 2014 annexation of Crimea, all three actors have faced a necessary reevaluation of their conceptualizations of adversaries, threats and countermeasures. Indeed, the key challenge posed by the events in 2014 was the ambiguity and obscurity of events taking place on the ground, raising serious questions regarding if, when and how to respond to similar attacks against NATO or EU members, below the threshold of actual armed attack. Both NATO and the EU have since devised a series of detection and response mechanisms focused on providing early warning and attribution of aggressive actions, as well as deterrence and retaliation. The reactions can be summarized as a common realization of previously unidentified weaknesses in Western societies and joint efforts to close these gaps.

Given the composite nature of the threats at hand, the responses need to be organized according to the same principles, integrating societal sectors as well as states. Another important takeaway from these chapters is the importance of knowing your adversary. Whereas identifying and attributing threats produces reactive responses, proactively addressing existing vulnerabilities in order to build resilience requires awareness not only of what an adversary does but also why. In this regard, it becomes pertinent to view the world through the adversary's eyes in order to identify strategic objectives and ways to achieve them as well as the adversary's vulnerabilities.

The validity of this perspective becomes particularly salient in the second part focused on the tools and means employed to conduct and counter-hybrid warfare. Indeed, the analyses of the approaches of major actors associated with HT&HW in a Western perspective, Russia and China, reveal that the conceptual overstretch accompanying these labels, considered a problem in the Western debate, instead functions as an asset in the strategic thinking of these challengers to the Western security order. In Russia, *gibridnaya voyna*, with its inherent assumption that most of the West's international activity aims to undermine Russia one way or another, functions as a rhetorical

device for identifying domestic or external threats and interpreting these as parts of the West's concerted offensive against Russia. In Chinese writings on the topic, the range of methods associated with HT&HW amount to a comprehensive, cross-domain spectrum denoting perceptions on threat, response and operationalization of hybrid warfare. These increasingly fluctuating borders between the different means associated with HT&HW are apparent in the analyses of information, cyber, intelligence capabilities and the military – indeed, it is questionable to what extent binary divisions into military/non-military or kinetic/non-kinetic means make sense in the current security environment. All the more so since binary thinking regarding the threat risks reproducing itself into the response, thus counteracting the proactive, comprehensive societal approaches deemed necessary to counter HT&HW.

This point is further validated by the contributions in the third section, presenting case studies of the United States, Taiwan, the Baltic States, Ukraine, Iran and Catalonia – demonstrating how the tools and means of HT&HW have been put to use and countered in a diverse set of empirical contexts. The problem of defending against adversaries and hostile actions that – very consciously – operate in the grey zone, below the threshold of actual war, is a recurring theme in these studies. And even if deterrent capabilities in the sense of military force may be very strong, as in the case of the United States, divided responsibilities between civilian agencies and the military, based on perhaps outdated understandings of war and peace, place limitations on the ability to respond. The contrast could not be more apparent when compared to China's policies against Taiwan, which amount to a concerted, sophisticated and strategic combination of means, which nevertheless does not (presently) include the active use of military force.

The point that strategies involving HT&HW are enacted out of a perceived necessity to challenge Western military supremacy by other means is underscored by the example of Iran, which has, due to the perceived existential threat posed by the United States, devised a strategy of guerrilla warfare, in large part performed by proxy forces and in areas outside Iran's territory. In Spain, a concerted Russian information campaign aiming to fuel and broaden national divisions over the Catalanian referendum is a clear example of how actors employing HT&HW seek out and attack vulnerabilities in target countries that are nevertheless pre-existing and do not emerge primarily as an effect of external influence or aggression.

Finally, the case studies also include (at least partially) successful examples of countermeasures against hybrid warfare. In the Baltics, the relatively low level of Russian hybrid activity is attributed partially to the low priority given to the Baltic States in Russian foreign policy, but also to a largely successful deterrence strategy combining military means and broad deterrence by denial below the threshold of an armed attack. Ukraine has, in the midst of an armed but covert attack against the country, proved capable of combining a conventional military response with a sustained informational campaign that has, despite the severe losses incurred, served to expose Russia as the aggressor and consolidated domestic cohesion as well as international support for the country.

The result is a comprehensive view of what may be termed 'hybridity' that, rather than a static picture of actions and responses, provides a cross-sectional and cross-temporal understanding of the interaction between actors, threats, responses and results. Hybridity is a suitable label, having been used in the social sciences 'to

designate processes in which discrete social practices or structures, that existed in separate ways, combine to generate new structures, objects, and practices in which the preceding elements mix'.¹ Modelled below, the Hybridity Blizzard Model provides a picture of how ongoing or potential adversarial hybrid measures and responses to these dynamically impact long-term societal vulnerabilities and resilience.

Towards a model of hybrid threats and hybrid warfare

As has been evident in this book, to fully comprehend and counter hybrid threats and warfare is a complex task, but also a very important one. Further on we will outline a schematic model for how to comprehend HT&HW: 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.

The Hybridity Blizzard Model (simplified version)

The simplified Hybridity Blizzard Model outlines a schematic model of the dynamics of the interrelated relationship between defender and attacker in the short-term as well as long-term perspective, and how the different time and actor dimensions interact (see Figure 17.1). Figure 17.1 depicts these interactive and temporal relationships as

Figure 17.1 Hybridity Blizzard Model, simplified version. Source: Authors.

an ecosystem, which we believe is a good analogy for understanding the dynamics of hybridity, ecosystem being defined as ‘all the living things in an area and the way they affect each other and the environment’.² While admittedly not alive in a traditional sense, ‘living’ is an excellent way to model the intelligent social actors on the battlefield and their use, deception, and denial of using different means and tools in hybrid conflicts. It is also a beneficial way of thinking about the relationship between HT&HW, responses and countermeasures, as well as long-term vulnerabilities and resilience. In short, as an environment where all parts affect each other, all parts are actively affected by intelligent social actors aiming to defeat the opponent.

The simplified Hybridity Blizzard Model includes the time and actor dimension. Both of these are important, as HT&HW is neither a one-off event, nor possible to temporally separate from its context. In this model, we include two actors, the defender and the attacker, along with two temporal dimensions, ‘short-term’ and ‘long-term’. In the short-term perspective, the battle consists of an ongoing reciprocal process between HT&HW conducted by the attacker, and the defender’s different responses and countermeasures in the duel. This is a continuous and ongoing process with no predetermined beginning or end.

In the long-term perspective, the competition is between the defender’s vulnerabilities and the resilience built to ameliorate them. The attacker is expected to identify vulnerabilities in order to exploit them. Vulnerabilities identified by the defender – ‘identification of own vulnerabilities’ – helps to build the defender’s resilience. Efforts to build resilience will logically imply a change in vulnerabilities. Hopefully, the vulnerabilities will decrease, however, change on the defender’s side may theoretically open up new vulnerabilities to be identified and exploited by the attacker – ‘increase or decrease vulnerabilities’ in Figure 17.1. There is also a relationship between the short-term and long-term perspectives (see Figure 17.2). When the

Figure 17.2 Hybridity Blizzard Model, simplified version, temporal dimension. Source: Authors.

attacker considers how to deploy hybrid warfare against the defender, the identified vulnerabilities are key in the ‘target selection’. Also, by targeting weaknesses, *ceteris paribus*, the existing vulnerabilities will be reinforced (and then probably targeted again, and so on and so forth).

There is also a relationship on the defender’s side between short-term responses and countermeasures on the one hand, and the building of long-term resilience on the other hand (see Figure 17.3). Existing resilience affects the defender’s ability to respond and execute countermeasures towards attacks and threats (‘increase or decrease ability to respond’). In turn, responses and countermeasures will increase or decrease the defender’s resilience. In short, there is a back and forth process between the long term and short term on both sides.

Figure 17.3 Hybridity Blizzard Model. Source: Authors.

The Hybridity Blizzard Model

One problem with the simplified model is that while it provides a schematic picture of hybrid conflicts, it fails to account for the chaos, deception and denial aspects of real-world HT&HW. While the simplified model is analytically sound, it simply does not fully account for the mess out there. In order to provide a complementary and more accurate view of the complex security environment, we propose a more complex version of the ‘Hybridity Blizzard Model’. The imagery of a blizzard is useful to depict a situation where the target of HT&HW will be blindly attacked from all possible angles all the time by innumerable small attacks, which cannot be separated from one another or localized, rendering the defender unable to respond and act.

In principle, we could probably add several arrows in Figure 17.3 between all parts. However, this would be of little use to enhance our understanding. Instead, we have focused on the short-term side, outlining the crucial components that best link hybrid conflicts with a blizzard. What makes the situation so messy is the fact that the threats and warfare targeting the defender is not always 'identified', but 'ambiguous', often 'unattributed' and sometimes even 'undetermined or unknown'. As outlined in Figure 17.3, HT&HW are frequently ambiguous and undetected. Adding to the complexity is the risk of false-positives, which not only pose a problem in their own right (crying wolf); they may also in themselves be part of a larger hybrid strategy.

Moreover, HT&HW may be unattributed – inherent in the deception and denial of hybridity – where the origins are either anonymous or covered through the use of proxies.

As if not enough, observed actions or events can be undetermined or unknown, where you do not know if you are observing a hybrid measure or something else. For example, are you observing someone's proxy, or is the 'proxy' in fact the origin and not part of someone's larger strategy/plan? Are the problems with the electricity grid or the glitch in your banking system a manifestation of hybrid warfare, or simply a 'glitch'. Is the threat you perceive against medical or food supply chains a hybrid threat, or is it simply a 'threat' but with no actor origin?

In short, hybridity is depicted not as two schematic arrows back and forth, but as the base of a blizzard of events and actions where the 'normal situation you were supposed to be a part of is now so totally screwed up as to turn the entire scenario into a farce'. And this farce is the reality we live in and have to learn to manage. Sometimes a tale is told of the man who was lost somewhere in Scotland, who asked a farmer if he could tell him the way to Edinburgh. 'Oh sir', the farmer replied, 'if I were you, I shouldn't start from here!' It is not the best joke, but nevertheless a reasonable metaphor for the situation of Western democracies today.³ We may not be where we want to be, but it is where we are. If we are to be successful in countering HT&HW while at the same time upholding our values and norms, there is no other option than to accept the place we are at.

Conclusion

It should by now be without doubt that HT&HW needs to be addressed through a comprehensive, all-inclusive approach. There is no one threat, no correct answer on how to counter and respond to HT&HW, nor how to build resilience. Nor is there one actor or structure that can succeed both today and tomorrow. As outlined earlier, 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.

In the Introduction, we used a quote from Sun Tzi as a way to understand the purpose of hybrid warfare – 'The greatest victory is that which requires no battle.' How then do we avoid losing the war? The best solution is not to seek battle, but to find ways to be the one achieving such a victory. One way to get there is to think about HT&HW in the same way as Lao Tzu thought about water.

Water is fluid, soft, and yielding. But water will wear away rock, which is rigid and cannot yield. As a rule, whatever is fluid, soft, and yielding will overcome whatever is rigid and hard. This is another paradox: what is soft is strong.

The paradox of soft as strong is a good guide when thinking about HT&HW and its responses and countermeasures, as well as about resilience and vulnerabilities. In order to be successful, one cannot focus only on hard defence or hard security issues, nor to seek battle. This would risk resulting in the wearing away as a result of the opponent's hybrid warfare; the hybrid measures are fluid, soft and yielding and will overcome whatever is rigid and hard. The opponent will identify soft targets, work opportunistically to target identified vulnerabilities, seeking ways to avoid or circumvent your detection mechanism, neutralizing your ability to respond and retaliate. This is outlined in Figure 17.3, where the attacker seeks to avoid detection of attacks, using proxies and other means to remain anonymous. Threats may even be undetermined or unknown to you, where you may not know that you are targeted or that there is a threat. This is how rigidity and hardness will be overcome. In a similar way, your defence also needs to be fluid, soft and flexible. That is the only way to achieve victory against an opponent disregarding peace and war, using the full scale of hybrid means.

Applying a cost benefit analysis to the targets of an opponent may not place core government agencies and coordination centres at the top of the list. Indeed the benefit in disrupting them would be great, but as they are most likely also prepared and skilled in averting threats against their area of responsibility a positive outcome becomes uncertain and the risk for rapid exposure great. Instead, this analysis may benefit areas that fall in between the responsibility of agencies, blind spots where threats may be identified slowly and a response take some time to sort out. The local government level may be easier to approach through middlemen or proxies as they are not as used to apply a national security filter to new venture proposals or offers to purchase land or assets. The private sector may be easier to influence since they seldom have access to the same intelligence as core agencies and operate based on business aims that may not take the long-term strategies of a foreign state into account. Any situation where the actor utilizing hybrid means can stay undetected, deflect the perception of what is going on, while continuing to inject uncertainty is potentially beneficial. Even if many efforts fail and each victory is small, the limited cost per operation compared to employment of traditional military means makes it a highly attractive alternative. In addition, it offers a greater degree of deniability, opportunity to evaluate and redirect on short notice, and grow a freedom of action without considerable response from the opponent.

Practical advice

But how do we manage these challenges in practice? The key is to develop a detection system that is simultaneously aware of false-positives and false-negatives. There is a need for pragmatism, flexibility and inclusiveness of actors, sectors and levels – within and

between countries. The hybrid measure will not come where you expect it, at least not all the time. When countermeasures are successful, the opponent will change its pattern of attack. All actors need to be included, and both short- and long-term perspectives need to be attended to. The response cannot be divided; long-term vulnerabilities are the target for hybrid warfare, and resilient societies will enhance the effect of responses and countermeasures. The idea of building a total- or comprehensive defence is, at least in principle, a good model to succeed with this.

More concrete, it is crucial that key international organizations such as NATO and the EU work together with different states both within and outside international organizations. It is also important to include dedicated organizations such as the Hybrid CoE and the different NATO centres of excellence. In addition, though also part of NATO and many of the dedicated centres, the US is a key actor that is of foremost importance to the protection of Western democracies against HT&HW. HT&HW should be countered through the overlap of capabilities and experiences of the collective that, symbolized in the intersection in Figure 17.4.

Figure 17.4 International collaboration. Source: Authors.

It is also essential to collaborate across sectors and levels and to avoid allowing traditional borders to hinder collaboration. This 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 Nestor García-Canclini, 'Hybridity', in *International Encyclopedia of the Social & Behavioral Sciences*, ed. Neil J. e. Smelser and Paul B. e. Baltes (Amsterdam: Elsevier, 2001), 7095.
- 2 Definition from Cambridge Dictionary.
- 3 Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (Basingstoke: Palgrave Macmillan, 2012), 285.