A Taxonomy of Hybrid Threats

The term "hybrid threat" is ubiquitous in current security policy debates, as it encapsulates an elusive range of different types of attack. This analysis argues that constructively engaging with a hybrid threat scenario initially requires a clear understanding of the underlying forms of hybrid warfare.

By Ivo Capaul

The crew of the "Yi Peng 3" is suspected of having damaged two submarine cables in the Baltic Sea at the end of 2024. Deniability is a key feature of hybrid attacks. *Mikkel Berg Pedersen / Reuters*

Western states increasingly face attacks that fall into a gray zone between war and peace. The outbreak of a conventional war on European soil has accentuated this trend. In order to describe this phenomenon, which has played a significant part in destabilizing the security situation in Europe in recent years, the term "hybrid threat" is currently gaining traction. Various cases are cited as evidence that disputes between states are increasingly being played out as hybrid conflicts, such as the instrumentalization of migratory flows by Belarus; the theory – widely circulated on social media by Chinese actors – that the COVID-19 virus originated from a US military research facility; the compromising of the systems of critical infrastructure providers; and the leaking of an intercepted conversation between high-ranking German officials by Russian authorities.

Accordingly, current security debates are shaped by terms such as "age of hybrid warfare" and the "weaponization of everything". Switzerland is not immune to this development either: The term "hybrid threat" has found its way into the federal government's security policy documents in recent years. In particular, one of the four scenarios taken into consideration by the Swiss Armed Forces in its force development is explicitly oriented towards hybrid warfare. Precisely because of the institutionalization of this term, a basic understanding is needed of what "hybrid" means and how this concept can contribute to a better understanding of a threat environment.

This analysis seeks to sharpen the concept of state-driven hybrid threats so that a minimum consensus on the defining elements can be reached based on existing terminology. The fundamental idea behind this taxonomy is that assessing a hybrid threat from the perspective of the target first requires a clear understanding of the forms of hybrid warfare employed by the perpetrator. This policy brief starts by discussing the various definitions and criticisms of the term, before presenting a

© 2024 Center for Security Studies (CSS), ETH Zürich

taxonomy for the categorization of hybrid threats. It also examines an alternative approach to engaging with the issue before finally considering the role of a hybrid threat environment as a starting point in the process of strategy development.

(Too) Wide a Field

Firstly, it should be noted that there is no universally accepted definition of the term "hybrid threat". The regulation *Operative Führung 17* of the Swiss Armed Forces defines the concept of state-driven hybrid warfare as a combination of political, economic, informational, humanitarian, and paramilitary instruments designed to achieve strategic objectives, and which are generally used on an irregular and covert basis. Meanwhile, NATO defines a hybrid threat as "a type of threat that combines conventional, irregular and asymmetric activities in time and space."

For the most part, this matches the EU definition, which describes it as "a mixture of coercive and subversive activity, conventional and unconventional methods (…), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare." The phenomenon is characterized in a similar way in academic circles, for example by Reichborn-Kjennerud and Cullen, who describe hybrid warfare as the synchronization of horizontal escalation (the scaling-up of hostile actions by all military and non-military means of state power) and vertical escalation (intensification, not only of the actions themselves, but also of the coordination of actions across different domains).

As these definitions show, the concept of a hybrid threat is highly abstract. As a result, it has evolved to become an increasingly vague catch-all term used to describe all kinds of variations of non-linear conflict. For example, a public statement by Russian Foreign Minister Sergey Lavrov has been described as a form of hybrid warfare, in the same way as the occupation and subsequent annexation of Crimea by Russian soldiers in unmarked uniforms ("little green men") in 2014. The wide gap between these two examples shows that the concept of a hybrid threat is too broad to clearly distinguish one form of warfare from others.

A further criticism of the term "hybrid warfare" maintains that it does not, in essence, describe a new phenomenon but merely provides a new label for a historically evolved practice. The tendency of states to assert their interests over other states using subversive means and below the threshold of war is arguably as old as the very idea of conflict between states. Indeed, such a notion of warfare is already evident in the writings of Sun Tzu. Still, the current fashionability of the term shows that hybrid warfare concerns a threat scenario with which political and military decision-makers are increasingly grappling, particularly in Western countries.

This growth in interest can be attributed to two key developments. On the one hand, the domains of subversive activity have significantly expanded due to the spread of new technologies such as social media. On the other, subversion clearly becomes an attractive instrument of power that falls below the threshold of war, whenever the potential costs of escalating a conflict are unacceptable to the state in question. This is particularly the case under the conditions of nuclear mutually assured destruction, which is why attacks that would now be described as hybrid were widespread during the Cold War (when they were often referred to as active measures or covert action). In the current age of increasing geopolitical polarization, they can, hence, once again occur more frequently.

> There is no universally accepted definition of the term "hybrid threat".

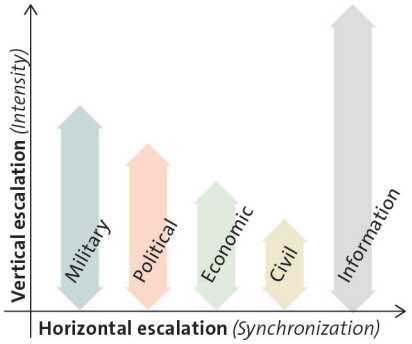
While the concept of a hybrid threat is a relevant category in the current security policy debate – as reflected in its increased institutionalization in the strategy documents of the Swiss DDPS, NATO, and the EU – there is a danger of it becoming an empty phrase devoid of meaning. If all types of conflicts between states that fall short of conventional war can be described as hybrid, then the concept is too all-encompassing and at the same time too vague to meaningfully contribute to the understanding of a threat environment.

Focus on Attack Vectors

One possibility of bringing more clarity to the vague concept of a hybrid threat consists in shifting the perspective away from the threat as perceived from the point of view of the hybrid target and focusing instead on the perpetrator and its attack vectors, which can be placed on the spectrum of hybrid warfare. Hybrid attacks are the only empirically observable elements in the debate surrounding hybrid warfare and can therefore serve as a starting point for an inductive analysis of hybrid threat scenarios. Only by analyzing attacks that have already taken place and that can be classified as hybrid is it possible – in combination with an extrapolation of potential future attacks – to build up a full picture of the hybrid threat situation.

Hybrid Warfare

According to the definition by Reichborn-Kjennerud and Culle



An "attack" is the taking of offensive measures against a specific target. An attack is therefore perpetrated by one actor against another. From this, it follows that a hybrid attack carried out by a state must exhibit three fundamental defining elements: First, a perpetrator, who wants to use the attack to achieve an effect; second, a target (e.g., state institution, civilian population) on which an effect is to be achieved; and third, a hybrid attack vector. This vector constitutes the actual offensive measure and connects the perpetrator and target (see Figure).

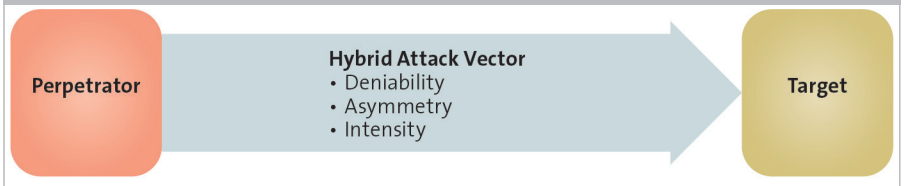
The characteristics of this vector are the elements that make an attack hybrid. To be classified as hybrid, the attack vector must exhibit three properties: First, it must have a degree of *plausible deniability;* second, it must be *asymmetrical;* and third, it must fall in its *intensity* below the threshold of formal warfare. These three criteria, which come from the hybrid threat definitions of the Swiss Armed Forces and the EU require some explanation.

Plausible deniability describes the degree to which the state perpetrating the hybrid

© 2024 Center for Security Studies (CSS), ETH Zürich

attack, or rather its political leaders, can plausibly deny being behind the attack. If there is plausible deniability, this reduces the political cost for the perpetrator, as reprisals by the target (for example in the form of sanctions) will be less likely. For this reason, hybrid attacks are often carried out with the aid of methods typically associated with intelligence services – in other words as operations that are covert (the identity of the perpetrator is hidden) or even clandestine (the attack itself is concealed).

Model to Depict Hybrid Attacks



Source: Own depiction

Asymmetry refers to the domain in which the attack is carried out (social media, economy, civil society etc.). An attack vector becomes asymmetrical if it takes place within domains where the target has insufficient defense mechanisms in place. Essentially, this concept of asymmetry involves a perpetrator utilizing its relative strength to exploit a target's weaknesses. A typical example of a hybrid attack vector is the intentional spreading of disinformation. In open, democratic societies, freedom of expression and freedom of information are held in high regard, which is why government action to tackle disinformation is often very limited.

Finally, the *intensity* of an attack vector addresses a hybrid attack's escalation potential in relation to conventional warfare. In terms of the intensity of its impact on the target, a hybrid attack vector is controlled to such a degree that it remains beneath the threshold of war on the escalation ladder. If a hybrid attack is so intense that the targeted state is forced to launch a conventional armed response, the threshold of war is crossed. An indication that an attack is nearing the threshold of war is when an attack that would otherwise be described as hybrid also has a kinetic dimension. In such cases, a conflict can be described as occupying the gray zone.

One example of a gray zone attack is the way in which the conflict in the Donbas region of Ukraine was conducted by Russia between 2014 and 2022; in other words with the aid of paramilitary units, cyberattacks, and disinformation. In this context it is also worth noting that the intensity of an attack vector behaves inversely to the plausible deniability factor. The higher the intensity of a hybrid attack vector, the lower the plausible deniability tends to be.

If an attack vector exhibits these three characteristics, it can be described as a hybrid attack in line with the above definition. Therefore, a state whose interests are realistically affected by such attack vectors faces a hybrid threat environment.

Classification of Threats

The fact that the three underlying criteria are not binary variables is central to this taxonomy. They are not either fulfilled or not fulfilled but exist on a spectrum. Assessing the extent to which the criteria are met allows for the classification of three different hybrid threats environments (see Table). The terminology used in this classification is consistent with that of the EU.

Furthermore, this sort of classification is helpful in clarifying the competences of those state actors that are primarily responsible for defending against attacks in the three threat scenarios presented in the table. For example, the identification and interception of *Hybrid Operations* are primarily tasks for the intelligence services, while a state's armed forces only take on a leading role if the threshold of *Hybrid Warfare* is exceeded.

> This analysis proposes the three criteria of deniability, asymmetry and intensity to classify hybrid attacks.

An Alternative Approach

An alternative approach to disentangling the concept of hybrid threats could involve breaking it down into numerous sub-categories. This approach is based on the negation of the term's expressive power. The attacks described here as hybrid would be discussed in the context of the respective domains in which an attack vector is deployed. By following this approach, individual attacks would not be considered as related phenomena and would therefore be analyzed separately.

The advantage of this approach is that it gives rise to clearly definable categories, thus allowing a more detailed analysis of attack vectors within their respective domains. However, there are at least two drawbacks to this approach. First, by their very nature, hybrid attacks affect overlapping domains. For example, an online disinformation campaign takes place in the cyber domain and in the information domain, making the investigation of such an attack within just one domain shortsighted. Second, the concept of hybrid threats explicitly addresses the integrated strategy of a perpetrator spanning multiple domains.

By breaking down the hybrid concept into individual domains, one of the core elements of a hybrid attack – namely, the combination of attack vectors to achieve a specific effect against a target – is lost. Taking such an integrated perspective toward a threat situation is relevant, particularly when countering hybrid attacks, as this is likely to require the coordination of various security policy instruments by a state. Consequently, at the strategic level (on which this analysis is focused), it does not make sense to break down the concept of a hybrid threat into its domains. In this respect, the integrated nature of hybrid threats is paramount. In terms of operational response, on the other hand, a breakdown of threats into different domains can certainly be useful in clarifying which state institution is responsible for implementing countermeasures.

Toward Strategy Development

The term "hybrid threat" is ubiquitous in security policy debates as it encapsulates an elusive range of different types of attack in a single catch-all term. At the same time, this means that its definition is increasingly being expanded, making it more and more vague. This issue could be resolved by defining a hybrid threat environment based on the abstract characteristics of the attack vectors that can be classified as hybrid.

© 2024 Center for Security Studies (CSS), ETH Zürich

Categorization of Hybrid Threats in line with the Definition Criteria of the Hybrid Attack Vector

Term	Deniability	Asymmetry	Intensity	Examples
Hybrid Interference	High: *plausible deniability*	Strongly asymmetrical	Below the threshold of war	Disinformation via social media
Hybrid Operations	Medium: *somewhat plausible deniability*	Asymmetrical	Below the threshold of war	Sabotage of critical infrastructure
Hybrid Warfare	Low: *implausible deniability*	Paramilitary	Conflicts in the "gray zone" (close to the threshold of war)	Little green men, weaponized migration
Conventional Warfare	No deniability	Military (symmetrical warfare)	Threshold of war exceeded	Russia's full invasion of Ukraine since 2022

Source: Author's categorization based on terminology used in Wigell, Mikkola and Juntunen.

To be able to carry out such a classification, this analysis proposes the three criteria of deniability, asymmetry and intensity, based on the terminology of the Swiss Armed Forces, NATO, and the EU. The extent to which these criteria are fulfilled can serve as a frame of reference for creating an overview of the hybrid threat environment. In addition, this approach helps better anchor the assessment of a hybrid threat in empirical reality. To complete an assessment of the threat using this method, it would also be necessary to analyze the specific objectives pursued by the perpetrator in carrying out the hybrid attack. This aspect was not considered in the analysis presented here.

Finally, it is worth emphasizing that the concept of a hybrid threat is a guide that helps to understand and categorize an empirically observed threat environment. What it definitely is not is a strategy in the sense of a conception of how the instruments of state power should be deployed in response to hybrid threats from the target's perspective. This would be a subsequent step, which would presumably require a whole-of-government or whole-of-society approach. In order to draw up such a strategy, it is, however, first necessary to gain a clear understanding of the specific threat environment.

For more on military doctrine and arms procurement, see CSS core theme page.

Ivo Capaul is a Researcher in the team "Defense Policy and Armaments Acquisition" at the Center for Security Studies (CSS) at ETH Zürich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Lucas Renaud
Language editing: Ivo Capaul, Névine Schepers
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: css.info@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

Most recent editions:

Government Trust in Times of Crisis No. 351
The Swiss Neutrality Debate: An Overview No. 350
Georgia at a Crossroads No. 349
The Changing Nature of the EU's and NATO's Partnerships No. 348
Japan's Approach to Peace Promotion No. 347
Mediation as a State Enterprise in Türkiye No. 346

© 2024 Center for Security Studies (CSS), ETH Zürich
ISSN: 2296-0244; DOI: 10.3929/ethz-b-000710887