# Metis

# Study

## New hybrid threats

No. 26 | July 2021



Institute for
Strategy & Foresight

# Summary

**In the future, hybrid wars will increasingly come to shape the international security situation. Countries use hybrid threats during peacetime to exploit the vulnerability of complex and highly interconnected societies and to weaken adversaries by creating a permanent state of pseudo-war.**

**Hybrid threats will likely further encroach on more areas of society. Existing security architectures therefore need to become more agile and countries such as Germany need to establish a resilient security culture in order to be able to meet these challenges.**

## Black chameleons

War is a chameleon. Its appearance may change but its very nature – the triad of goal (overthrowing one's adversary), means (use of physical violence), and political purpose (enforcing one's own will) – remains the same. In the Western world in particular, the primary understanding of war as a conventional conflict between countries is an established concept that is quickly proven wrong by even a cursory look at history. Although legally regulated direct warfare conducted by heavy infantry on a designated battlefield was an established concept even in ancient times, Greeks and Romans nevertheless resorted to poisoning wells, burning fields, and using disinformation and deception tactics. Even contemporary concepts such as the "Western way of war" (with its preference for direct, precise warfare and a strong casualty aversion) or "democratic warfighting"(which sees democratic armed forces dominating over autocratic armed forces while complying with rules of warfare) describe only ideal types of war, which in practice are rarely fought without hybrid elements. Armed forces clashing along clearly defined frontlines, sparing the enemy's civilian population, adhering to restrictions on ways and means of using military force – in the colour theory of war, such conventionally fought conflicts are black and thus easy to distinguish from the white of peace. Meanwhile, the grey area is overlooked.

## Most chameleons are grey

From a historical perspective, this ideal, "classical" interpretation of war only applies to a short period of the late modern era and is primarily confined to the geographical space influenced by Europe. The reason why, historically, countries prefer direct warfare is that it leads to a decision based on a relative distribution of power. This understanding of war, however, can be seen as a manifestation of a preference for a state-centric mindset, a focus on strategic priorities (capital city, armed forces, industrial centres), and thus an expression of a decidedly Western perspective. Conventional wars between countries will likely continue to be fought but their frequency and duration have steadily decreased since 1945. The frequency and duration of asymmetric or hybrid wars, on the other hand, have steadily increased. All the signs point towards hybrid wars becoming the increasingly dominant form of warfare. Particular characteristics of such wars include fluctuating conflict intensity, a combination of conventional and asymmetric warfare, and in some instances even the threshold of a state of war (defined in political science as 1000 conflict fatalities per conflict year) never actually being crossed. From the perspective of the "classical" interpretation of warfare mentioned above – as well as from a perspective of international law – these wars linger in the grey area.

"Hybrid warfare" is just the most recent term to become the subject of a decades-long debate aimed at translating shades of grey into clearly defined concepts. The term really began to attract public attention during the Ukraine crisis in 2014. Before that, it had been part of the debate on new wars, low-intensity conflicts [1], fourth-generation warfare [2] and asymmetric conflicts, which began in the mid-1990s. All these definitions of conflict have one thing in common: they are attempts at rationalising and explaining those modern forms of war that veer further and further away from the Western understanding of war as a conventionally fought, state-centred conflict regulated by international law. Empirical research usually focuses on unconventional means of war, guerrilla warfare, insurgency, genocide and terrorism as well as their combination with conventional elements. In most cases, the starting point is quantitative asymmetry, i.e. the inferiority of one conflict party in terms of relative power. It is this asymmetry that forces the inferior side to move beyond direct warfare. Qualitative asymmetry means that inferiority is compensated for with not just conventional means but especially alternative, terrorist, unconventional and criminal approaches. It is at the heart of asymmetric warfare. The goal is to compensate for weakness by highlighting strengths – especially by taking advantage of the enemy's weaknesses.

Today, the term "hybrid war" is mostly used when asymmetric warfare is employed away from the centre of conflict or the front. One such example is the phones of family members of deployed military personnel being tapped to collect information that might be used to achieve an advantage in combat. Every conceivable method, means and resource is exploited, no matter how strange they may seem on the surface. We speak of hybrid threats when such hybrid approaches take effect beyond clear lines of conflict or are used outside of a conventional state of war. Such threats cause a permanent and latent state of conflict below the threshold of war. Hybrid actors aim to continuously weaken their adversaries in order to compensate for their own inferiority and to better position themselves in the event of a potential conventional war. To this end, social cohesion, essential public goods, infrastructure and services, economic order and public opinion become the target of subversion and disruption in an effort to undermine the adversary. The civilian population of an adversary therefore becomes the primary strategic focus. In this way, hybrid threats generate countless shades of grey in the chameleon that is war, making it almost impossible to analytically define and ascertain a true state of war. The country that is targeted this way is weakened by the permanent state of pseudo-war and forced to turn its focus inward because it is paralysed politically, economically and socially, which allows the aggressor – confident of victory – to either escalate to conventional war or to pursue other global exploits unhindered.

## New shades of grey from the trendsetters Russia and China

We mainly associate hybrid threats with the activities of the Russian Federation and China, since these countries are very active in this area and can in some respects be considered trendsetters. Both countries have considerable military capabilities at their disposal but, in conventional terms, are still inferior to the US-led West. In the case of Russia, relative economic weakness is another factor. To compensate for these deficits and to protect their own ability to act, Russia in particular has expanded asymmetric warfare to include the hybrid component. The Ukraine conflict most notably illustrates the repertoire of common hybrid approaches. This repertoire includes electoral interference in Western countries, efforts to weaken Ukraine's economy, the systematic spread of fake news and propaganda, and cyber activities and espionage against state establishments in Western countries. This wide spectrum of hybrid threats from Moscow supported the conventional warfare of Russian troops in Eastern Ukraine, who deliberately operated without insignias. Although the hybrid war came to an end as the conflict subsided in intensity, the hybrid threats remain and continue to affect Europe, the US and Ukraine today.

Figure 1 illustrates the broad spectrum of hybrid approaches. It ranges from hybrid threats aimed at demoralising and destabilising social cohesion and political stability during peacetime to indirect hostilities using economic sanctions and cyber attacks.

Attacks on private actors – carried out in order to disrupt critical infrastructures, to conduct economic espionage, to cause economic damage or to influence public opinion, for example – continue to be documented and blamed on Chinese or Russian groups. More subversive measures are also common, such as the use of social media influencers and leaks. Supported by state-financed media establishments, such measures help establish parallel realities, counternarratives and "alternative truths".

Many hybrid threats also feature the problem of attribution: the initiators and perpetrators cannot be

1 "New wars" or low-intensity conflicts are conflicts between state and non-state actors which are characterised by struggles for identity rather than ideology, by non-state financing and struggles for political rather than physical control of territory and people.

2 While the first three generations (formation warfare, firepower and mobile warfare) were aimed at physically destroying an adversary's armed forces, fourth-generation warfare is aimed at overcoming the psychological ability of an adversary to conduct warfare by using public pressure to force the hands of political decision-makers.

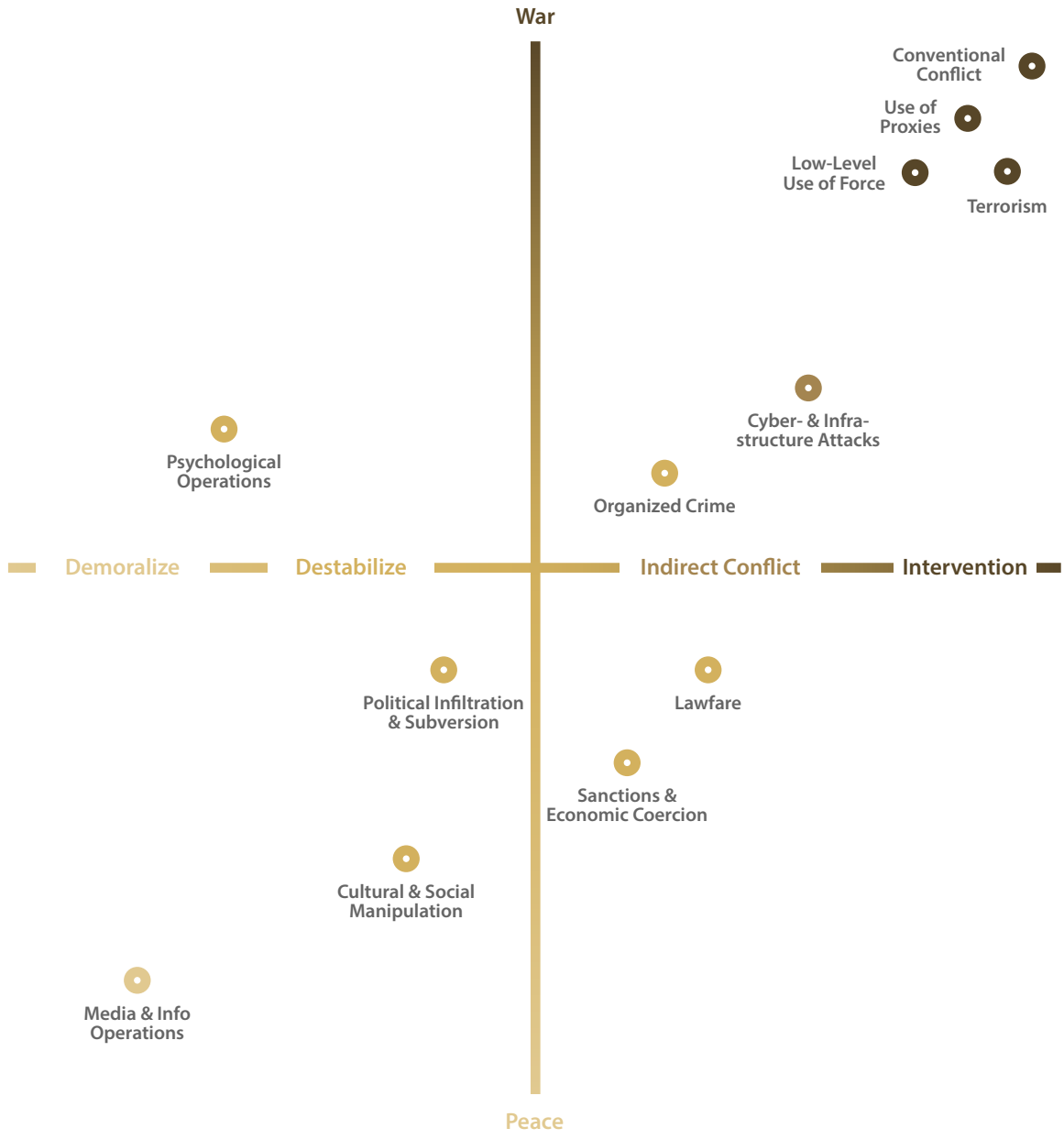



***Fig. 1*** ***Means of hybrid warfare.*** | Source of template: https://cepa.org/lt-gen-ben-hodges-on-the-future-of-hybrid-warfare/

clearly identified, which makes it easier to deny responsibility. Russian propaganda generally has been aimed at the Russian minority in a target country and then develops further from there. This follows the logic of fourth-generation warfare, which sees military measures being targeted not at combatants but at entire societies as well as their decision-makers. By using hybrid measures, Russia thus aims to achieve a strategic effect because it would struggle to win in direct confrontation with NATO and would definitely lose an economic race with the US or the EU. China, on the other hand, uses hybrid measures – especially in the cyber sector – to divert attention away from its own strategic initiatives such as the creation of artificial islands in the South China Sea and the creeping militarisation of economic bases along the Silk Roads.

***Fig. 2*** ***'Lone wolf' hacker as the hybrid threat of the future.*** | Source: https://www.shutterstock.com/g/shock

## Hybrid threats and the grey future

In addition to the forms of hybrid threats we already know, Western countries must prepare for a number of new types of attacks and the exploitation of new weak spots. It will not be enough to simply extrapolate from the experiences and lessons learned in the Ukraine Crisis of 2014. Potential future hybrid threats are especially likely in the legal, financial and communication sectors. Many of them will not be entirely new but will often just be an enhanced version of approaches we already know. What will be new, however, is the quality of these hybrid approaches and their time-sensitive use, which might overwhelm the ability of affected countries to react. The following section looks ahead at possible future areas of hybrid threats, far below the threshold of hybrid wars.

### Bots with artificial intelligence (AI)

Future technical possibilities open up new scopes of action in the field of AI.[3] This means that the abilities of bots to influence public opinion will increase drastically. AI bots pretending to be human will become more authentic and almost impossible to distinguish from real people encountered on the web. AI bot personas will compile automatically generated articles on political, social or economic topics. Coupled with seemingly authentic deepfake video and audio content, they will get involved in and influence online discourse in their millions. Public opinion in pluralistic democracies can thus be more easily manipulated and shaped from the outside than ever before. Today, computer-generated content, be it text, commentary, images or videos, can still fairly easily be identified as fake. The increased quantity and quality of these fakes will soon require dedicated forensic methods, however.

### Flash attacks in the financial sector

Hybrid threats in the financial sector already exist in the form of hostile company take-overs, strategic patent acquisitions, economic espionage, cyber attacks on stock exchanges and targeted market manipulation. In most cases, the aim is to generate a financial emergency or political pressure in order to restrict the target's capacity to act and to prompt governments to take certain courses of action such as concessions, subsidies, assistance loans or declaration of regulatory latitude. Secret services poaching key personnel also has the potential to cause economic damage. Decentralised finance is expected to create new vulnerabilities in the financial sector. Coupled with state efforts to establish digital – though centralised – blockchain offshoots of the euro, dollar or yuan, vulnerabilities to attack will increase. A current example is arbitrage trading, i.e. taking advantage of differences in exchange rates, interest rates and prices of shares and currencies between different stock exchanges. While conventional market manipulation is characterised by coordinated action of several market players or insider trading, the digital sector now has to deal with flash-loan attacks: anonymous traders borrow millions or billions of dollars for a few seconds, buy securities on the stock exchange and flood another stock exchange until exchange rates fall through the floor. Such flash-loan transactions only take a few seconds and can cause billions in damage, sweep individual companies (e.g. ones dealing in military key technologies) off the market, paralyse national economies, and destabilise currencies. While it used to take years to achieve such effects with traditional means of exerting economic force (e.g. sanctions), it will soon take only a few short destructive blows.

### Triggering environmental disasters

The effects of climate change are creating new ecological vulnerabilities that may become targets for hybrid threats. Multiple targeted instances of arson committed simultaneously in dozens of forest areas could be a way of overwhelming and destabilising national security and crisis management agencies. Cyber attacks against critical infrastructure could also result in environmental disasters. While a state and its society are focused on tackling natural disasters, the state is usually working at capacity or even paralysed. Developments beyond its borders are suddenly much less important, at least in the eyes of the public, and decision-making processes are stalled by more urgent national crises.

### Lawfare

The exploitation of real, alleged or even staged breaches of international law of war – already used as an unconventional method of confronting a superior military power – can mobilise global public opinion. Using law as a weapon thus aims at manipulating international law discourse, at alternative interpretations, or at using one-sided national legislation to support one's own interpretation of international norms and rules. In future, hybrid actors will also use legal proceedings and exploit legal recourse in national courts for their own purposes. One goal of conducting lawfare against national legal systems is to overwhelm. By pursuing so many court cases all the way to the final court of appeal that the caseload becomes unmanageable, the targeted institutions are inundated to the point of paralysis and proceedings are dragged out for years. Another goal is to seek out competing legal interpretations in different countries in an attempt to achieve mutual delegitimisation.

3 See "Quantum technology: Implications for security and defence", Metis Study No. 25 (May 2021)

## Recommendations for action

Due to their social openness, their high level of technological interconnectedness and their focus on the private sector, Western democracies are very vulnerable to current and future hybrid threats. Freedom of press and opinion makes it possible to spread disinformation; the degree of social connectivity increases the risk of chain reactions; the private sector is preparing for potential hybrid risks with an uncoordinated patchwork of measures.

At the same time, democracies are also more adaptive, innovative and resilient than other forms of government. If they shed at least some of their state-centric thinking, they can adapt to new challenges. In order to continue to be able to counter the totality of hybrid actions of Russia and China, the following recommendations for action should be considered so as to increase the ability to absorb and recover [4].

### Investing in resilience mechanisms

- Establish legally binding minimum standards for cyber security and constantly adapt them to technological developments.
- Increase the resistance and responsiveness of state institutions by making sensitive procedures less bureaucratic.
- Establish methods for decoupling critical infrastructures and create redundancies in order to interrupt chain reactions in the event of crisis.

### Establishing early warning

- Create an interagency early warning system to identify organised disinformation.
- Integrate early detection abilities of private actors from the industrial, energy and IT sectors into a national early warning system.
- Establish a supplementary system of information exchange on a national level.

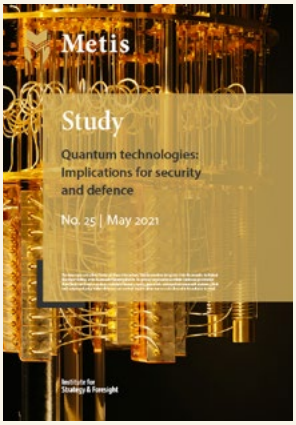
### Increasing resilience

- Establish a national crisis reaction and crisis management system and link it to EU and NATO institutions for multinational coordination.
- Expand civil-military cooperation beyond reactive administrative assistance towards proactive prevention and to include private actors.
- Expedite cooperation between state, public and private actors in particular, and coordinate counter and security measures.
- Establish subsidiary coordination and resilience mechanisms, from the level of administrative district to that of member state and all the way up to the EU and NATO.
- Intensify strategic communication with the public on hybrid threats in order to increase awareness.
- Establish a security culture through awareness-building and information campaigns.
- Ensure that countermeasures follow a networked, national and interagency approach (whole-of-government approach) while national activities, on the other hand, are augmented by including private actors in order to achieve the goal of resilience across society (whole-of-nation approach).
- Intensify cooperation between the government and private sector, which should go beyond symbolic declarations; statutory provisions and incentives need to be created for private companies to allow close cooperation with state institutions without economic disadvantages.

4 See "Resilience", Metis Study No. 21 (November 2020).

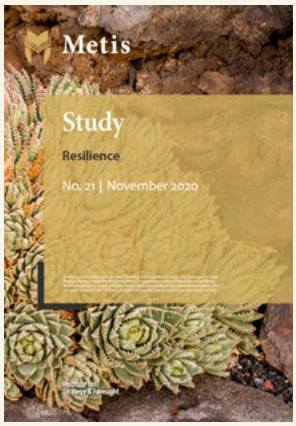
# Metis Publications

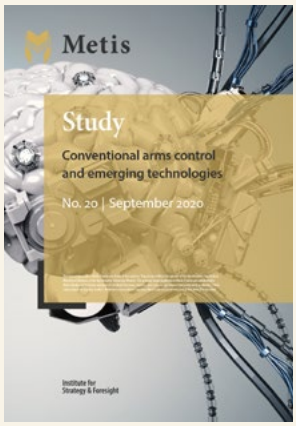
**Published to date and also available on the Metis website at metis.unibw.de**



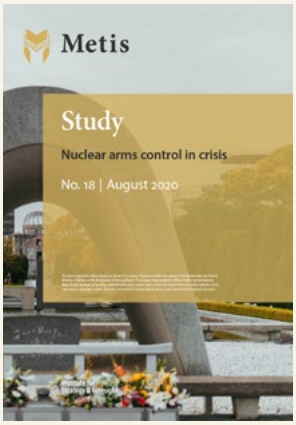











Metis

## IMPRINT


**Publisher**

Metis Institute
for Strategy and Foresight
Bundeswehr University Munich
metis.unibw.de



**Author**

Dr. Konstantinos Tsetsos
metis@unibw.de



**Creative Director**

Christoph Ph. Nick, M.A.
c-studios.net

**Image credits**

Cover photo & p. 6/7: https://www.shutterstock.com/g/shock

**Original title**

*Neue hybride Bedrohungen*

**Translation**

Federal Office of Languages

**ISSN-2627–0609**