Assessing Hybrid War: Separating Fact from Fiction

Fear of "Hybrid War", a blanket term describing gray zone aggression short of all-out war, remains widespread. Many expect information technology to enable revolutionary gains in this strategic space. Yet, Hybrid War's track record does not support these expectations. Consequently, it is crucial to conduct a more systematic assessment of the different instruments used under this umbrella term.

By Lennart Maschmeyer

For close to a decade, analysts and defense planners have now warned of the looming menace of "Hybrid War". Yet, it remains strikingly unclear which instruments of power politics this involves, and the extent of a threat Hybrid War actually poses. Nonetheless, Western states have expended significant resources to fend off this threat. This year, the EU has announced an entire mission in Moldova tasked with countering "hybrid threats", its first mission of this kind. Hence, it is both urgent and important to assess these threats.

Unfortunately, Hybrid War is notoriously ill-defined. Both policy debates and academia use it mostly as an umbrella term for all kinds of aggression short of all-out warfare. These include, but are not limited to, disinformation, sabotage, subversion, and cyber operations. Russia's takeover and illegal annexation of Crimea in 2014, its support of armed separatists in Ukraine's Donbass region (including through unmarked troops of "little green men"), and a large-scale cyber campaign were perceived to demonstrate the power of these instruments. Academic interest skyrocketed and many scholars have argued that such low-intensity aggression would become the future of warfare. Policymakers picked up these arguments and associated threat perceptions, and have shifted strategy and defense priorities accordingly.

"Hybrid War" as envisioned by the Midjourney AI, October 2023. *Designed by Lennart Maschmeyer and generated using Midjourney*

A Technological Revolution?

Aggression short of war itself is nothing new. States have long employed instruments in the "gray zone" between war and peace. Prevailing conceptions of Hybrid War assume that the use of information technologies makes gray zone aggression more effective. Specifically, there is an expectation that information technologies expand the speed, scale, and intensity of gray zone conflict through cyber and social media influence operations. Cyber operations offer the ability to reach across borders to sabotage infrastructure, cause economic havoc, and disrupt communications at a moment's notice. Meanwhile, social media influence campaigns have the potential to sow panic, create confusion, and sway public opinion to change voting outcomes. Consequently, many expect states

can now achieve outcomes that were not previously possible without going to war.

Reflecting this common threat perception, states have adjusted their defensive strategies and priorities towards countering Hybrid War. NATO has made countering "hybrid threats" a core priority of its strategy in 2015. These threats are understood as a combination of "military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular force". The recent establishment of a European Partnership Mission in Moldova, whose priority is to defend against hybrid threats from Russia, further suggests that policymakers clearly perceive Hybrid War as a significant threat, despite a lack of clear definition. While there are no official figures for budget allocations to this specific threat, given the prioritization of the concept in strategy and official statements, it is reasonable to expect expenditure to be significant. The current debate on adding Hybrid War as a fourth core task to NATOs mission further underlines this point. Even Russia, ostensibly an expert in hybrid warfare, has justified a 70 per cent increase in military spending in 2023 by claiming the need to counter Hybrid War being "unleashed by the West". Meanwhile, China has made influence operations, or cognitive warfare in military terms, a key component of its doctrine in order to make up for its forces' lack of wartime fighting experience.

Prevailing conceptions of Hybrid War assume that the use of information technology makes gray zone aggression more effective.

An Underwhelming Track Record

In contrast to prevailing fears, however, Hybrid War's actual track record is rather modest. The biggest success, by far, is Russia's 2014 takeover of Crimea. However, according to recent research, cyber operations and social media disinformation campaigns played no role in this feat. Rather, this was a traditional subversive operation without any cyber component. It involved subversive proxy actors, primarily fringe religious groups, which handlers from Moscow had groomed over years. Conversely, the Russian cyber campaign against Ukraine that followed in its wake largely fell short of producing measurable strategic gains. Hence, expectations of a technologically enhanced revolution in conflict have not been confirmed.

On the contrary, if Hybrid War allows states to achieve strategic goals that were not previously possible without going to war, then the logical assessment of Russia's "Hybrid War" against Ukraine since 2014 is that it failed since it pursued a full-scale invasion in 2022. One explanation is that Russia failed to achieve its strategic goals, including its primary goal of reversing Ukraine's pro-Western foreign policy. In that case, the core expectation of Hybrid War theorists is proven false by the very conflict that made the concept so popular. Russia went to war precisely because aggression short of full-scale war faltered.

Alternatively, one might argue that Hybrid War alone is incapable of achieving Russia's strategic goals. This would imply that Hybrid War is nothing but "old school" gray zone conflict, making the term irrelevant. Yet, the fear of Hybrid War remains very much alive. Even Russia's initial theory of victory significantly relied on "hybrid" means such as sleeper cells, corrupt local officials, and commando forces, which failed in the face of unexpectedly effective resistance by Ukraine. Importantly, the effectiveness of Ukraine's resistance also defies prevailing fears that hybrid threats erode the cohesion of societies and their capacity to resist aggression over the long term.

If anything, one could make a strong case that Russia's persistent aggression has enhanced Ukraine's resilience by "training" its defenders in fending off cyber-attacks among other things. Of course, Ukraine has also received significant assistance from its Western partners. Still, while the precise causes of Ukraine's capacity to resist still require more research, there is a striking absence of "smoking gun" evidence proving the success of Hybrid War. This situation is not unique to Ukraine.

In 2007, Russian hacking groups mounted a series of disruptive cyber operations against Estonia in retaliation for the removal of a Soviet statue in an Estonian town. At the time, this was heralded as the advent of cyberwar, illustrating its grave threat to Western societies. Yet, these operations had little measurable impact on Estonia's economy, government, or society and are best classified as temporary nuisances. Instead of eroding Estonia's strength, this aggression galvanized its resilience and directly contributed to the establishment of NATO's Cooperative Cyber Defence Centre of Excellence in its capital Tallinn, which significantly enhanced not only Estonia's but also NATO's cyber capabilities.

Russia's meddling in the 2016 US Presidential Elections offers a plausible case of a successful hybrid warfare operation. Moscow combined the use of cyber operations to hack and leak the Democratic National Convention's emails, as well as the emails of Hillary Clinton's campaign manager John Podesta, social media disinformation to sway voters and exacerbate polarization, and traditional subversion by placing assets in Donald Trump's campaign and subsequent administration. Through these means, Russia may have contributed to the election win of its preferred candidate. A vast amount of alarmist news headlines, followed by dire warning from policymakers and a flurry of academic research mapping purported troll networks on social media suggest this operation was a great success. Yet, despite the intense interest in and research done on this case, there is a striking absence of evidence indicating measurable contributions of these Russian activities toward political outcomes, namely voting outcomes. In fact, a recent study by New York University showed that exposure to Russian influence operations via Twitter did not change attitudes or voting behavior. When assessing Russian hybrid warfare activities over the past decade, there is a striking lack of clear evidence of its effectiveness compared to mounting evidence of its limitations.

A More Systematic Assessment

This situation underlines the urgent need for a more systematic assessment of the strategic role of the diverse gray zone instruments commonly grouped under the concept of Hybrid War. The first crucial step is to identify and distinguish these different instruments. There are multiple relevant types of operations and corresponding effects.

First, influence operations aim to sway public opinion as well as the perception of political leaders. The desired goal is to manipulate political decision-making and outcomes, as well as societal trust and cohesion. Second, sabotage degrades and damages infrastructure and material capabilities. The desired goal is to weaken the adversary and shift the balance of power in one's favor. Third, subversion is a specific

way to achieve some of these goals through the targeted infiltration of adversary societies and institutions. Cyber operations are best conceptualized as new instruments of subversion. Apart from influencing and sabotaging, subversion can fulfill more ambitious goals as well, such as overthrowing a government through an internal coup or by triggering a revolution, either armed or unarmed. This effect is an especially potent instrument of power since it changes the underlying preferences of a state, thus aligning it with one's own interests in a way that goes deeper than coercion through military force. Meanwhile, armed revolution highlights a fourth type of covert operations, namely the clandestine and covert use of force. Clandestine operations refer to hiding the activity itself, such as the stealthy US operation to kill Osama Bin Laden. Covertness in turn refers to hiding the identity of the aggressor, such as through the deployment of unmarked soldiers – the infamous Russian "little green men" in Crimea.

Once the instrument is established, the next steps are determining the larger strategic goals the adversary aims to achieve, and then a careful examination of available evidence on the capacity of the instrument in question to achieve these goals. Finally, based on this evidence, a systematic assessment of the conditions under which these different instruments can succeed helps clarify the extent of the threat.

Lessons from History

For policymakers, the first challenge in countering Hybrid War is to separate fiction from fact. Of course, policymakers must plan for contingencies and consider both past and hypothetical scenarios. However, the best way to realistically project what could happen in the future is to draw inferences from what happened in the past. Accordingly, a useful baseline for addressing future threats is what Hybrid War has actually achieved in practice. Such an assessment, including historical examples namely the use of covert operations during the Cold War, gives reasons for confidence. Fear of influence operations and sabotage is nothing new but was a key theme among Western defense planners and policymakers. Fortunately, these fears were not always justified.

A 1981 report by the US Department of State on Soviet "active measures" provides an instructive example. It argues that the KGB's decades-long expertise in mounting active measures – the contemporary term for hybrid warfare – combined with the openness of Western political and media systems created a ripe environment for Russian influence operations and subversion and drew a pessimistic picture of resulting threats to Western societies. And yet, as we now know, the Soviet Union collapsed soon after. Arguably, the situation is not dissimilar today. Fears among policymakers and defense planners of Soviet influence operations and subversion during the Cold War were mostly based on what could potentially happen, neglecting the significant obstacles involved in producing these desired effects in practice. The same applies to threat perceptions and assessments concerning cyber operations and social media disinformation campaigns. Recent studies found that the vast majority of subversive operations aiming to overthrow regimes failed. Mounting evidence of the shortcomings of cyber operations points in a similar direction. Fortunately, not all that is possible in theory is feasible in practice.

Reasons for Optimism

Moreover, there are clear signs of unintended "blowback" of influence operations. Subversion, influence and disinformation operations are described by experts like putting a virus in the bloodstream of your enemy. Yet, just like actual viruses, there is a real risk of spread beyond the targeted society. Accordingly, the Mitrokhin archive (a record of KGB operations leaked by the defector Vasili Mitrokhin) documents a growing paranoia among the KGB's leadership over the course of the Cold War about potential traitors in its own ranks, and correspondingly growing efforts and expenditure to hunt down and punish these traitors. These efforts increasingly undermined the KGB's core mission: namely, to weaken the United States. Specifically, there are multiple examples of the KGB leadership, and by extension the Soviet leadership, believing its own propaganda and making policy decisions based on it, with detrimental outcomes. The decision to invade Czechoslovakia in 1968 is one of them. The Soviet leadership expected an impending counterrevolution and overwhelming public support for the Soviet intervention, both of which only existed in Soviet propaganda. Consequently, what was supposed to be a short-term occupation had to be extended for the rest of the Cold War. Russia's invasion of Ukraine, with troops expecting public support for "liberating" the country, suggests a similar situation now. In fact, there is a growing consensus among analysts that Putin, having expelled any non-loyalists from his administration, has been misinformed and prone to believe Russian propaganda. Without access to the Kremlin, this remains hard to prove.

> A more systematic assessment of the strategic role of the diverse gray zone instruments grouped under the concept of Hybrid War is needed.

Perhaps counterintuitively, closed and autocratic systems may be more vulnerable to blowback and dysfunction than open and democratic systems. While the openness of democratic systems facilitates influence operations, the existence of multiple sources of information and competing narratives within the public sphere provides opportunities to challenge and counter disinformation narratives. Of course, this depends on a functioning media ecosystem and becomes increasingly less possible as polarization increases. In closed autocratic systems, however, there are typically far less alternate sources of information and competing narratives. Therefore, autocratic systems are intimately vulnerable to fall prey to their own disinformation and manipula-

Further Reading

Chiara Libisller, **"'Hybrid Warfare" as an Academic Fashion,"** *Journal of Strategic Studies* 46:4 (2023), pp. 1–23.

Rory Cormac / Richard J. Aldrich, **"Grey Is the New Black: Covert Action and Implausible Deniability,"** *International Affairs* 94:3 (2018), pp. 477–94.

Christopher S. Chivvis, **"Hybrid War: Russian Contemporary Political Warfare,"** *Bulletin of the Atomic Scientists* 73:5 (2017) pp. 316–21.

Arsalan Bilal, **"NATO Review – Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote,"** *NATO Review,* 30.11.2021.

Mark Galeotti, **"Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?,"** *Small Wars & Insurgencies* 27:2 (2016) pp. 282–301.

Lennart Maschmeyer, **"The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations,"** *International Security* 46:2 (2021) pp. 51–90.

tion. These structural differences provide strengths and weaknesses, both of which should be considered. Such an assessment suggests a relative advantage for democratic systems that should be a source of confidence in countering disinformation and influence operations.

Closed and autocratic systems may be more vulnerable to blowback and dysfunction than open and democratic systems.

Even if Hybrid War is less effective than is commonly assumed, it still constitutes a potentially significant threat. Hence, the key conclusion is not to dismiss Hybrid War. Rather, effective counterstrategies require a more systematic assessment of the specific instruments involved and how to neutralize them. On the one hand, this means acknowledging the lasting importance of traditional (non-technologically enhanced) influence, sabotage and subversion operations and prioritizing responses accordingly. On the other hand, considering the strategic heritage of the gray zone instruments that Hybrid War comprises is also crucial. Since these instruments are not as new as they may appear, building on counterintelligence strategies and lessons learned from the past can help. In particular, the logic of deception and its value both in offense and defense is important to consider. A significant challenge will be the fact that integrated campaigns, which are comprised of a range of gray zone instruments – both traditional and "cyber" – , will require an integrated response that bridges existing institutional and doctrinal silos.

For more on Military Doctrine and Arms Procurement, see CSS core theme page.

Lennart Maschmeyer is Senior Researcher at the Center for Security Studies (CSS) at ETH Zürich, where he focuses on cyber conflict, power politics, and subversion.

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: Névine Schepers
Language editing: Névine Schepers
Layout and graphics: Miriam Dahinden-Ganzoni

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

Most recent editions:

The Role of Mediation Support Structures No. 331
UN Peacekeeping No. 330
German Military Planning: Aims and Trade-Offs No. 329
Managing Disaster Costs No. 328
Central Asia in an Era of Great-Power Rivalry No. 327
The Promise and Paradox of Science Diplomacy No. 326

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000638728