Dealing With Competitive Opponents in Hybrid Warfare

Ralph D. Thiele

February 2022

Summary

Hybrid warfare has become a threat to our way of life. Western societies need to understanding its implications. NATO, the EU and member nations should develop robust multi-domain instruments for meeting hybrid challenges, while preventing escalation into larger armed conflict. The backbone of resilient infrastructure that can withstand attacks from cyberspace, outer space, and the electromagnetic spectrum has emerged as a key requirement.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, the economy, international relations, and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

The Threat

Hybrid warfare has become a familiar phenomenon. But at a time of climate catastrophes and pandemics, booming technological innovation, geopolitical rivalry and a global reorganization of supply chains, hybrid scenarios below the threshold of war have gained enormous importance. While hybrid threats used to be the weapon of the weak, new technologies and their disruptive potential have made such attacks an effective, hitherto low-risk instrument of power – one that will foreseeably evolve into the gold standard in geopolitical confrontation.

Nobody has described hybrid warfare as aptly as General Valery Gerasimov, the Russian Chief of Defense Staff, who has called it "a clever combination of economic, secret service and many other non-military and military means [that] can transform a flourishing country into a chaotic torso in a short period of time." As we have learned from Russia's recent campaigns on NATO´s Eastern flank**,** hybrid aggressors employ their capabilities in pursuit of hybrid objectives both in and beyond traditional domains (i.e., air, land and sea) and new domains (i.e., space, cyber and the electromagnetic spectrum). The Kremlin aims at people, assets, critical infrastructure and, last but not least, the self-image and cohesion of entire states and societies.

New technologies such as 5G, artificial intelligence (AI), autonomous systems, cyber, quantum and space have had a catalytic effect on hybrid warfare. They improve the starting conditions for hybrid action, expand the arsenal of hybrid actors and thus help to increase the scope of their activities as well as their chances of success. New technologies offer offensive opportunities in particular. At the same time, new technological developments can provide options to better detect, understand, defend against and counter hybrid attacks. Most importantly, new technological trends increasingly make technology itself a "battleground" for hybrid confrontation. Against this backdrop, technology represents an additional domain and an opportunity for hybrid actors to expand the "battlefield" horizontally. The technological domain can even become the centre of gravity of a hybrid confrontation.

Here are a few examples:

Migration

In a malicious hybrid approach, Russia has targeted liberal democratic constitutional states through Belarus via an aggressive, artificially generated migration flow across the Polish and Lithuanian borders. The fierce disputes of the great migration crisis of 2015 are to be reanimated in a targeted manner and the political stability in the European Union is to be shaken. It can be seen how – fuelled by social media – the seeds are growing and the people who pull the cords in this campaign are being forgotten in the public eye. This approach also includes supporting radical political groups and fuelling unrest.

Information and Communication Infrastructure

Hybrid threats fuse industrial age techniques with cyber operations. They use a system of selected visible and clandestine actions, including social engineering, in which the attackers are almost invisible and the target is well-defined. The number and quality of Russian cyber-attacks have grown enormously. One cybersecurity alarm follows the next. The networks and servers of manufacturers, professional and private users, which are particularly endangered by Russian attacks, are only the tip of the iceberg. Spy software in national parliaments

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

and security authorities, in critical infrastructures and weapon systems, give Russia enormous opportunities in economic and political disputes. State, state-sponsored and criminal perpetrators cavort in our networks. They explore, steal, falsify, coerce, and blackmail, as they look for access to research, industrial and state secrets, databases and private accounts.

Social Networks and Media

The use of online services such as social media, messenger services or crypto currencies are an integral part of Russian hybrid campaigns and are also used to finance activists. The focus is on the misuse of Internet platforms for communication purposes, the dissemination of propaganda, recruitment and knowledge transfer. Social networks and media can be manipulated for hybrid purposes – from voting behavior to terrorist mobilization. The instruments Russia uses include state-controlled media at home and abroad. Social media in particular are susceptible to fake news, meant to undermine the trust of Western societies in our own institutions and political elites. Migration and the ongoing COVID-19 pandemic offer ample opportunities for such fake news. Indicators of malign activity can be found across the board, including microtargeting, deep fakes, and technology-sharing between hybrid actors.

Empowered Intelligence Services

In hybrid warfare, intelligence services are in demand like never before. To respond to hybrid threats, we need deep, broad and comprehensive analyses over extended timescales and across actors, regions and issues. **Technologies such as Big Data and AI have large potential to enable a new depth in identifying, tracking and countering hybrid threats. At the same these very technologies enable** new hybrid challenges from technologically advanced opponents.

Multi-domain operations effectively require a feedback loop between political objectives and operations. Intelligence permanently feeds this loop, ensuring decision-makers and operators have the information they need to adjust nimbly. Virtually every form of technical intelligence profits from new technologies, including the emerging fields of cyber and social media intelligence to name a few. Moscow uses its secret services virtually in cyberspace, including through the support of hacker networks, but also increasingly again in real space: political murder has returned as a form of Russian action.

Armed Forces

Armed forces have become another part of the hybrid portfolio. Military strength provides additional opportunities to exploit hybrid methods, even without the active use of force. Moscow´s aggressive, military measures and provocations on land, air, sea, in space and cyberspace have reached alarming proportions, involving military manoeuvres, simulated attacks and large-scale lightning exercises near its neighbours' borders, among other actions. The combination of new technologies and attendent operational concepts have been the key to the successful rise of Russian military capabilities over the past decade.

Multi-domain operations in hybrid campaigns involve outmanoeuvring an opponent, in which the opponent's cohesion is disrupted. This involves skilfully challenging the opponent simultaneously with an unsolvable variety of problems in different domains, thereby overburdening and finally outmanoeuvring him.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Conclusions

At present, Russia is the grand master of hybrid warfare, though China is establishing itself as the coming world champion and there are a number of other rising actors. In order to prevent, defend against and – if necessary – counter and outmanoeuvre hybrid opponents, it is therefore important for political, civilian and military decision-makers, as well as for industry and academia, to develop a common and comprehensive understanding of the implications of new technologies in a hybrid threats/warfare context. NATO, the EU and member nations should develop robust multi-domain instruments for achieving advantage in hybrid campaigns, while preventing escalation into larger armed conflict. Outmanoeuvring opponents requires the backbone of resilient infrastructure that can withstand attacks from cyberspace, outer space, and the electromagnetic spectrum.

***

Remarks: The opinions expressed in this contribution are those of the author.

About the Author of this Issue

Ralph D. Thiele, retired Colonel, is President of EuroDefense (Germany), Chairman of the Berlin-based Political-Military Society, and Managing Director at StratByrd Consulting. In his 40-year military career in the German Armed Forces, he has held key national and international positions. He also offers advice in his honorary and business functions on defence innovation in times of digital transformation. He has most recently published the book “Hybrid Warfare. Future and Technologies.”

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de