Hybrid War AND HYBRID THREATS

Coping with conventional and unconventional security challenges

By ***Dr. Sven Bernhard Gareis***
German deputy dean at the Marshall Center and professor of international politics at the Westfälische Wilhelms-Universität

It is not a new phenomenon that states at war employ a broad array of instruments besides military forces to achieve their objectives. Deception, propaganda, information campaigns, and irregular or covert operations have always accompanied conventional warfare. These measures aim to demoralize soldiers fighting on the front line and decrease domestic support for the war. They target the human psyche by raising anxieties and fears, seeding doubts, questioning the legitimacy of governments and institutions, and splitting national cohesion along social, cultural, religious or ethnic lines.

In this regard, the hybrid war that the Russian Federation has been waging in Ukraine since 2014, and the threats that it poses to other countries in its nearer or more distant neighborhoods, do not constitute a genuinely new concept of warfare. On the contrary, the doctrine that Russian Chief of General Staff Vladimir Gerasimov presented in 2013, and that has been systematically used in Ukraine since, is based on the assessment that Western countries — first and foremost the United States — have used financial support to opposition parties, deceptive information campaigns and "color revolutions," in conjunction with economic incentives and military posture, to change the security environment in the post-Soviet space to their favor and to Russia's detriment. Based on this perception, Russia is justifiably responding to Western challenges.

Targeted states such as Ukraine — and the West at large — are less surprised by the so-called Gerasimov Doctrine's line of attack than by the degree of precision and determination with which the Russian government under President Vladimir Putin deploys its military and nonmilitary capacities in domains such as cyber, information technology, public opinion, diplomacy and covert military operations. Russia's relative success in Ukraine is largely due to the latter's weak national cohesion, political culture and institutions,

Macedonians protest in front of the EU building in Skopje in May 2017, a few days after violence erupted when angry nationalist protesters stormed parliament. Societal fissures make countries more vulnerable to hybrid tactics. AFP/GETTY IMAGES

and to the West's inability to appropriately respond to Russian aggression.

This helplessness has its reasons: Hybrid measures are purposely applied beneath the threshold of conventional warfare. Unlike soldiers, armored divisions or fighter aircraft crossing borders, it can be difficult to attribute responsibility for cyber attacks or other nonmilitary assaults. There are blurred borders and gray zones: Is Russia supporting separatist movements in eastern Ukraine or has it launched a military aggression against a sovereign country? The European Union, the U.S. and other countries imposed bearable sanctions on Russia, but avoid more energetic action since many Western countries maintain strong economic and political ties with Moscow. It seems as if the West has tacitly accepted that Crimea will not return to Ukraine in the foreseeable future, and eastern Ukraine is still war-torn while the Minsk Agreement has not successfully been implemented.

Among the most effective elements in the hybrid war toolbox are information campaigns that aim to manipulate public opinion, damaging the adversary system's reputation and conveying the aggressor's own narratives.

Against this backdrop, how can states, societies and alliances defend against warfare that does not strive for territorial gains or military dominance, but rather to destabilize, if not destroy, the societal order of a nation or region? The complexity of hybrid warfare requires complex responses and a different set of instruments. However, what is needed first is a thorough analysis of the hybrid threats and a sober assessment of the vulnerabilities within states and societies.

Hybrid warfare and hybrid threats

Since 2014, the terms "hybrid war" and "hybrid threats" have increasingly been used in international security policy discourse. However, with limited exceptions, there is no common definition or concept in political practice or academia that can be used to reliably designate a situation as hybrid war — and therefore no set of political, military or legal measures and procedures that states or organizations can invoke in response to the threat.

Hybrid warfare can be described as a combination of military force — open and covert — and any nonmilitary means that could harm a state, society or international organization such as the EU or NATO. While such means often complement classic military operations in conventional wars, they are essential instruments in hybrid warfare and often outweigh military efforts. According to Gerasimov, the ratio of military to nonmilitary means should be 1 to 4. As elements of an integrated strategy, the means are systematically and flexibly applied where they fit best. In the case of military action, this can be special forces operations by "little green men" without identifying insignia, or covert support of insurgents. Such operations allow the attacker to deny direct involvement and to make the situation as unclear as possible.

Cyberspace is an ideal realm for hybrid warfare. It transcends classic borders, it interconnects private, public, economic and administrative areas, and it is — despite enormous efforts by powerful states such as the U.S. and China — difficult to control. Cyberspace offers convenient commodities, such as globally interconnected infrastructure, allowing for real-time communication for public, private or individual actors that has boosted international exchange, trade and commerce. At the same time, the far-reaching dependency on these technologies in all areas reveals increasingly existential vulnerabilities. The virtual nature of cyberspace allows all kinds of actors to launch serious attacks that cause considerable damage to individuals, organizations and states and that carry a low risk of being traced. As an instrument of hybrid warfare, cyber attacks can confuse or disrupt communication infrastructure, cause temporary paralysis of public life, and contribute to an overall climate of uncertainty and fear. It can undermine the legitimacy of governments that are unable to protect societies from very real cyber threats. Defending public and economic infrastructure against attacks has become an everyday challenge.

Cyber espionage and cyber crimes pose growing threats to nations, businesses and individuals. The disclosure of hacked information from the electronic communications of prominent politicians can influence elections, as can attacks on electronic voting systems. As revealed by the 2016 U.S. presidential elections, democratic countries must become more attentive to the perils of interference from cyberspace. Revelations, such as those from WikiLeaks, can have negative impacts on national security. Destructive malware such as Stuxnet — allegedly launched by the U.S. to destroy central parts of the Iranian nuclear program — have proven to be a lethal weapon in military arsenals, again without the possibility of clear attribution.

Among the most effective elements in the hybrid war toolbox are information campaigns that aim to manipulate public opinion, damaging the adversary system's reputation and conveying the aggressor's own narratives. In the globalized and digitalized world, such campaigns are not confined to a single target. In Ukraine, Russia countered the 2013-2014 Maidan protests against then-President Victor Yanukovych with a massive campaign that denounced the demonstrators and new leadership (after Yanukovych fled the country) as fascists and sought to compromise their legitimacy and reduce public support in Western countries. Of course, Ukraine is only one theater in the broader Russian hybrid campaign against Western influence in the region. The tactics used there were also meant to weaken Western cohesion in assessments and responses to hybrid threats.

Children study at a school in Marinka, near the front lines of Ukraine's smoldering war in November 2016. Functioning and trustworthy institutions are necessary for a stable society.
AFP/GETTY IMAGES

Information campaigns show manifold faces and use versatile channels. There is blunt propaganda, and there are professionally designed media, such as Russia Today, that present fake news in the guise of serious information. There are troll commentators on online media, reputed experts' comments in popular mass media, and well-funded think tanks and foundations, such as the Dialogue of Civilizations Research Institute in Berlin, that help set agendas for public discussions. An old Cold War-proofed instrument is the creation of message multipliers by financially supporting local movements or parties that are dissatisfied with the political or socio-economic order in their countries.

The primary purpose of information campaigns is to undermine public trust in institutions, structures and procedures in the targeted states and societies, be it by "fake news" or by creating confusion. After the downing of Malaysian Airlines Flight 17 over eastern Ukraine, Moscow attempted to overwhelm the global public's capacity for fact-based assessment and judgment by pushing a plethora of explanations and interpretations — many of them fully or partially contradicting each other. Blurring borders between facts and fiction erodes the basis for serious debate.

How do hybrid threats function?

As already stated, the most important objective of hybrid warfare is to create confusion and destroy trust. Hybrid measures target the foundations of the human psyche: to feel safe and secure is a fundamental desire of every individual. This desire goes far beyond the guarantee of physical survival — human beings have the need to feel respected and to enjoy equality and justice, not only in legal terms, but also with regard to social, economic, cultural, ethnic and religious aspects.

At the national level, these aspects form the foundation of the concept of societal security, which guarantees fair and discrimination-free treatment for all. In their landmark book, *Why Nations Fail: The Origins of Power, Prosperity, and Poverty*, Daron Acemoğlu and James A. Robinson describe those societies as inclusive, in contrast to extractive forms of societal order, which prioritize the well-being of certain social groups (often referred to as elites) at the expense of others.

The "World Happiness Report 2017" gives empirical evidence to this finding. It highlights the juncture between personal and social happiness and its global ranking shows the close correlation between happiness, and peace and stability. Consensus-oriented Scandinavian nations are the happiest, while war-torn nations in Africa show the lowest degree of happiness. Acknowledging that a correlation does not necessarily indicate a causal relationship between variables, the positive impact of inclusiveness on societal security appears at least to be plausible.

In this respect, the more inclusive and just a society is perceived to be by its members, the more stable it is. And vice versa: deeper social splits and political polarization indicate less trust in institutions, and the more corrupt a system is perceived to be, the more fragile is the society, making it more prone to hybrid intervention from outside.

When social inequality is not accepted as a just outcome of fair competition under equal conditions for all members of a society, feelings of injustice and grievances over discrimination can be easily exploited to widen gaps along social, ethnic or religious lines. As a result, states and societies may disintegrate into antagonistic camps that are no longer able to communicate with each other. The perception of disenfranchisement often makes those groups easy prey for so-called strong leaders with clear-cut and simple "solutions" to increasingly difficult problems. This is compounded by a global trend in the use of media and information: To escape the complexity of problems, more and more people withdraw into filter bubbles that admit only information that reinforces existing preferences, attitudes, opinions or behavior. To avoid cognitive dissonance, contradictory facts or divergent

Latvian soldiers participate in Operation Hazel exercises at the Adazi training field. Military readiness is an important but relatively small facet of resisting hybrid attacks. REUTERS

interpretations are actively excluded from consideration. Consider how an analysis of internet users' search behavior is utilized to create algorithms that propose only goods, services or information that fit existing patterns. With political communication, agitators can reinforce dissatisfaction and foment radicalization in thoughts and action.

Russia capitalized on Ukraine's fragile national identity and seized the opportunity of political transition to carry out a professionally orchestrated hybrid campaign, successfully stirring up resentment within the Russian-speaking populations in Crimea and eastern Ukraine. It is not difficult to predict which leverage points Russia may try to use in other countries outside and within NATO or the EU. In the U.S. and France, Russia pushed "anti-establishment" themes in the respective presidential campaigns of 2016 and 2017. In many European countries, nationalist and xenophobic parties and movements have had considerable success in contesting the benefits of European integration, thus reinforcing the EU's internal crises. Polarization, distrust, anger, and even hatred, weaken states and societies, open avenues for hybrid interference from outside, and thus constitute serious threats to national integrity and stability within individual countries, and to regional and international orders.

Countering hybrid threats

Hybrid measures often overwhelm the defense capacities of a single state and/or challenge groups of states or regions. They require concerted responses both in identifying threats and effectively countering them. Since hybrid threats are primarily of a non-military nature and use versatile guises and channels to make an impact, any alliance or security organization must use analytical capacities to assess whether suspicious incidents are isolated phenomena or are indeed elements of a hybrid strategy. To this end, it is indispensable to further interagency exchange of data, findings and assessments to facilitate analysis of a multitude of distinct events and cases. It is primarily a national task of member states to arrange interagency cooperation among military, police, intelligence services, emergency management authorities and civil administrations. Institutions like the EU Hybrid Fusion Cell, within the EU Intelligence and Situation Centre, or the newly established Finnish Centre of Excellence for Countering Hybrid Threats (supported by several EU and NATO members), are bodies that collect and examine reports and assessments from member states and common agencies that can be used to develop collective countermeasures.

At its Wales (2014) and Warsaw (2016) summits, NATO re-established a focus on collective defense and deterrence. Under the Readiness Action Plan, the Alliance established the Very High Readiness Joint Task Force and deployed

small military contingents to Poland and the Baltic states as an enhanced forward presence, designed to show force to a potential aggressor, as well as to demonstrate the solidarity and determination of its member states. Partner nations such as Ukraine and Georgia receive support in fields such as strategy, doctrine and education, military training assistance, and the (limited) provision of military equipment and nonlethal weapons. Military measures are necessary and crucial to counter the military dimension of hybrid aggression. However, according to Gerasimov's 1 to 4 ratio, the military is only one instrument in the defense toolbox — and most probably not the one of primary importance.

In addition to the EU Joint Framework on Countering Hybrid Threats, the EU's decisive strength lies in the social and economic foundations for societal security that it offers to member states. The relatively high degree of freedom, economic opportunity, welfare, functioning institutions, rule of law and nondiscrimination make EU member states with large ethnic minorities less prone to hybrid exploitation of societal splits and cleavages. There is not much an aggressor can offer to outweigh the tangible advantages of considerable welfare, a stable currency or an EU passport with the freedom of movement it guarantees.

As the successes of nationalistic movements in many countries illustrate, EU membership does not provide immunity against external actors stirring up and exploiting dissatisfaction. The likelihood of grievances escalating to unrest or even revolution, however, is very limited. To the contrary, the EU provides a political and legal framework that helps tame political actors and mitigate problematic developments in countries such as Hungary or Poland, where democratic achievements are currently at stake, and bring them back to common standards of democracy, societal security and stability.

Building resilience

As in the case of hybrid warfare, there is no clear definition of resilience. In general terms, resilience describes the ability of a system or an organism to maintain its basic, vital functions, even after having suffered severe damage. In terms of national security, resilience means a country can absorb a military strike, a terrorist act, a cyber attack or a series of lower-scale actions across the spectrum of hybrid warfare and continue, as much as possible, to function normally.

In democratic states, this requires maintaining the balance between necessary security measures and individual freedoms and civic rights, while not transforming into a surveillance state. In this regard, the public's trust in good governance and stable institutions is extremely important. To this end, states must create capable security agencies that can identify and tackle threats and mitigate the consequences of hybrid attacks. To be credible, these institutions need to be strong in analysis and assessment, effective in taking countermeasures, and interconnected with national and international partners.

Effective security agencies are indispensable to defend against hybrid threats. It is, however, equally important to any national security strategy to start with the insight that hybrid actions capitalize and reinforce dissatisfaction, grievances and complaints within states and societies, but they do not produce or import them. Hence, building resilience begins with a relentless analysis of a state's own weaknesses and vulnerabilities. Government, elites, political parties and social groups must find sober answers to the questions inherent in guaranteeing societal security.

The most important indicator of inclusivity is the degree of trustworthiness that political and societal institutions and structures enjoy among the citizenry. This depends on democratic legitimacy and on procedures that are based on the rule of law and that guarantee integrity and transparency. This includes effective efforts to detect and fight corruption, nepotism and any other arbitrary access to resources of power and wealth.

In this context, governments and civil society must provide equal opportunities for all citizens to participate in public, social and cultural life. Are there complaints of discrimination and how seriously are they taken? If there are cleavages and disruptions, what can be done to effectively enhance societal integration? Building societal resilience depends on how serious and trustworthy a government's integration efforts are perceived by the individuals and groups concerned. The most important characteristic that distinguishes a mature and successful democracy from a potentially unstable political system is how the majority treats minorities and how the powerful treat the weak.

How a society deals with the challenges of disinformation, fake news and propaganda can be considered a valid litmus test of its resilience. Responses to information campaigns cannot be confined to counterpropaganda or "strategic communication." As an essential element of hybrid warfare, false information is particularly successful if political communications and public opinion are segregated into partisan camps that live in their own filter bubbles. It takes effort and time to bring people together to discuss solutions to common problems. The fundamental prerequisite is, again, trust and credibility. The less inclusive a society is the more susceptible it is to manipulation of dissatisfied individuals and groups. If state institutions and civil society live up to the values of free and inclusive societies — based on integrity, transparency, rule of law, trustworthy institutions and free media — they can blunt hybrid warfare's sharpest sword.

Conclusion

Hybrid threats are not a new phenomenon, but in this globalized world, with its breathtaking development of ever faster communications, its impacts become massive and dangerous. They pose new challenges for national security policies and agencies — but at the same time, adequate defensive measures open immense opportunities for societies. True resilience requires a certain degree of satisfaction and happiness among all citizens. Responsible governments and civil society actors must take into account the close nexus of societal and national security and strive to make their citizens happier and their nations stronger. □