Federal Academy
for Security Policy

Security Policy Working Paper No. 16/2019

"Hybrid Threats": What Can We Learn From Russia?

by Keir Giles

"Hybrid warfare" is not a Russian term. But Russia's use of levers of state power short of open warfare provides a useful case study for clarifying and harmonising Western understanding of "hybrid threats", and considering the best responses to them.

NATO allies have been debating the nature of "hybrid threats" and "hybrid warfare" for over four years, since in 2014-15 the term became suddenly fashionable as Western allies sought a means to describe Russian actions in Crimea and eastern Ukraine. The use of "hybrid" terminology has been criticised on multiple grounds – not least because it is not a helpful framework within which to consider the courses of action open to Russia. Nevertheless the term has permeated through the security debate in Western countries so thoroughly that it probably cannot be uprooted. This in turn gives rise to a further problem, as definition proliferation across countries, and even a failure to agree definitions within individual countries, mean that there is no shared understanding of precisely what is meant by "hybrid".

The complexity of the problem can be illustrated by taking Russia as a case study, and considering the breadth of the range of tools and actors that Russia employs for targeting its adversaries. It is well understood that the "hybrid challenge" from Russia is not a military problem but a whole of government problem. But it is less widely recognised that the challenges are even broader than that, and in fact present a whole of society threat including a range of non-governmental actors. It follows that the responses and countermeasures by Western countries seeking to resist Russia must also be broader than a whole of government effort.

Russia's instruments of "hybrid warfare"

The actors, agencies and organisations available to Russia to carry out hostile actions against its adversaries comprise an impressive array. They include:

- Organised state agencies, including the intelligence services which in Russia, critically, have always had the role of undertaking active interventions against state adversaries, unlike some Western intelligence agencies that concern themselves solely with intelligence collection.
- Military and paramilitary bodies. This includes specific organisations without Western equivalents, such as the National Guard which in addition to its main internal security role has also been observed in combat support functions in Ukraine and Syria, and the Information Operation Troops (*Voyska informatsionnykh operatsiy*, VIO), which are intended not just to carry out cyber and information activities, but also covert or semi-covert physical interventions against communications infrastructure, as was the case in Crimea.

 | ISSN 2366-0805

- Private military companies (PMCs) and proxies, employed as the forward elements of Russia's programme of pushing boundaries of permissible behaviour and carrying out operations that are notionally, even if not plausibly, deniable. These provide an affordable and expendable alternative to Russia's regular military forces, which can be used at lower risk, including risk of the consequences of failure.
- Non-governmental organisations in the commercial sector also cover a broad range, including:
    1. Oligarchs funding and sponsoring political subversion operations and providing a duplicate chain of command;
    2. State-controlled commercial entities, such as the "Night Wolves" (a multinational corporation masquerading as a motorcycle gang);
    3. A variety of organisations promoting rights of "compatriots" and ethnic Russians living abroad;
    4. Other means of exerting economic pressure on adversaries, including regulatory mechanisms, and willing proxies in the target nation;
    5. Cultural coercion such as state-supported doping-programs to enhance Russia's external image.
- The Russian Orthodox Church.
- Organised crime.
- Agents of influence, repeating lines from Moscow and seeking to influence policy in Russia's favour either because they are paid or induced to do so, or out of their own convictions (the "useful idiots").

Backing up all of the above is the threat of use of conventional military force. Whether threatened or actually used, conventional military power provides a backstop for hybrid activities and the context in which they can be employed, and in which Russia seeks greater freedom of action and a permissive environment for it to achieve its geostrategic aims. While "hybrid", "grey zone", and "new generation warfare" have achieved great prominence in Western studies of Russia, they have not replaced Russia's preparation for high end, high intensity conflict. While Russia may seek asymmetric measures to deal with the conventional superiority of the West, and may indeed find that these measures are less expensive, less risky, more deniable and potentially even more effective than open military clashes, this has in no way lessened the urgency perceived in Moscow to prepare for open conflict.

How to define "hybrid" – an inclusive model

If all of these are to be included in the definition of a "hybrid" threat from Russia, it follows that that definition must be simple enough to include all of their possible permutations. Based on the assessment above, we could therefore define "hybrid warfare" as: *"the selection, combination, integration and application of various levers of power to deliver damaging and coercive effect"*.

This definition is short and deliberately leaves a number of factors unspecified:

- It does not specify whether these levers are military, governmental, civil, or state-owned or state backed. They can be either, all, or none.
- It also does not state at what stage of conflict this kind of warfare is waged – whether it is sub-threshold, liminal (also known as threshold–surfing), or all-out war.
- It does not specify the degree of intensity of conflict, which can range from barely detectable to intolerable.

As such, the definition covers both the range of tools that can be employed in hybrid conflict, and the range of circumstances under which it can take place.

How to identify hybrid activities

A definition this broad opens up the question of how a victim would identify that it is being subjected to hybrid warfare. At a low intensity, it might even be difficult for the victim to know that they are under attack. A key task is to determine what combination of unexplained incidents – "things going wrong" – would indicate a coordinated assault. An additional complication is that hybrid threats could develop from the convergence of a number of already existing social, technical or economic problems which is then exploited by an adversary – without it having been necessarily planned, masterminded or coordinated *ab initio*.

Key indicators would probably comprise a mixture of the traditional and the novel. Traditional warning signs would include the arrival in the country, or in a specific region, of meaningful numbers of a specific type of Russian visitor; or civil demonstrations turning into a staged confrontation; or a sudden or escalating pattern of sabotage. New indicators would be connected with Russia's emphasis on the importance of information warfare and conflict, exploiting new technological possibilities to the maximum in pursuing old principles of subversion and information warfare. Russia's information preparation of the battle space will include activities on social media and through more traditional channels of influence, for example in order to establish a *casus belli*; attempted isolation of target audiences, or controlling information flows to them; attacks on or suppression of independent media; and attacks on civilian internet and telecommunications infrastructure, whether through physical intervention, cyber attack, or employment of electronic warfare capabilities.

In all cases, Russia's response to accusations of involvement will be a primary indicator of whether unexplained activity does in fact derive from a hostile campaign by Moscow. Based on patterns of behaviour to date, silence, or a confused and uncoordinated response, could indicate that Russia is not to blame, whereas firm and confident denials of any involvement accompanied by a torrent of obfuscatory disinformation are a reliable sign that action has been ordered at the highest levels in the Kremlin.

How to respond to hybrid attacks

Once a "hybrid attack" has been identified, the obvious next question is how to respond to it. Proposals have been made for developing "counter hybrid toolkits" to assist nations in resisting hybrid interventions. But the contents of these toolkits tend not to be novel, and generally to resemble programs and actions that healthy societies should be undertaking anyway.

These include:

- Ensuring good governance throughout the entire governed territory, and effective law enforcement including law enforcement intelligence and in particular effective control of borders and entry ports.
- Avoiding the vacuums that hybrid actions can exploit – vacuums of knowledge, of attention, of physical presence, and above all of political will.
- Promoting social cohesion, and avoiding the emergence of disaffected and disenfranchised groups and regions; instead, integrating them into society to the maximum respect extent possible so that foreign actors cannot exploit their grievances.

Even the measures that need to be undertaken in response to physical attack resemble methods that should be universal in ensuring national resilience. For example, measures to prevent infiltration and sabotage are largely indistinguishable from counterterrorism programs, and measures to respond to, contain and mitigate the effects of attacks are closely related to humanitarian assistance and disaster relief (HADR) operations.

At the same time the key difference from normal state activity is the need to escalate rapidly in response to hybrid attacks; to respond to them immediately and in such a way as to make the fact of being under attack undeniable. The principle proposed by former Estonian chief of defence Lieutenant General Riho Terras of "shooting the first little green man that appears" has the benefit of immediately lifting the conflict out of the grey zone in the critical early hours of confrontation in order to eliminate confusion, indecision, and excuses for foreign partners to deny that an external attack is taking place.

A related requirement is transparency and international coordination, of the kind recently shown by the Netherlands, Denmark, United States and United Kingdom in responding to Russian cyber attacks and other hostile operations. The key benefit of this transparency and coordination is to remove doubt, provide the basis for international solidarity, and ensure that Russia is aware that it cannot pick off individual countries one by one without their allies supporting them. But a key element in ensuring transparency is greater openness by Western governments with their populations about the degree of hostile action undertaken by Russia on a day-to-day basis. The experience of the front-line states demonstrates that admitting and vowing the condition of almost open hostilities with Russia is a key enabler for society to protect itself through developing an appropriate level of threat perception.

Finally, as the adversary seeks to exploit the target's inability to observe actions and effects, the role and importance of accurate and profound intelligence capabilities is crucial. The nature of hybrid threats, seldom tied to one clearly identifiable entity, actor, or sometimes even state, dictates a requirement for targeted nations to maintain substantial defensive intelligence capabilities as well as joint analysis and multinational fusion facilities. One study[1] identifies two main elements in adequate national-level counter-hybrid intelligence capacity:

- Enhancement of the analysis and collection capabilities of traditional intelligence organisations to detect and respond to non-traditional threat vectors, and
- Creation of big data analysis units capable of detecting potential threats from societal level trends by advanced statistical means.

Managing a whole-of-society approach to hybrid threats

Even a whole of government response to external threats requires complex coordination between government agencies, and a whole of society response is in turn greatly more complex. Many of the actions and initiatives required will be outside the purview of government, precisely because the intended target is society, not just its administration. The critical infrastructure that needs to be protected is in private hands. The centre of gravity for information warfare is public opinion, held by private citizens.

Accordingly there is no template answer for a structure or organisation that is suitable for a western liberal democracy to undertake this kind of coordination, planning and implementation of responses to hybrid threats. Smaller and more agile nations can seek to emulate the total defence concepts of for example Sweden or Finland, but their constitutions and political systems will dictate the art of the possible. In any case, the Russian solution, where the National Defence Direction Centre addresses this problem by bringing together a huge array of military and civilian agencies under the command of the General Staff, is not a usable model for democratic powers.

States should no longer presume that distance lends comfort, and that countries further away from Russia are less at risk of hybrid interventions then the traditional frontline states. According to Russian Chief of General Staff Valeriy Gerasimov, a key feature of information warfare is that there are no rear areas, because information effects can reach "to the entire depth of enemy territory"; and the same is true of Russia's new generation warfare concept as a whole. Deployments in support of NATO's enhanced forward presence (eFP) in Po-

[1] Monaghan (ed.) et al. (2019): *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare* [online], p. 25-34.

land and the Baltic states or activating and moving the Very High Readiness Joint Task Force (VJTF) across Europe, for example, mean that not just the deployed units, but also their families and communities back home are both targets and attack vectors. Countries that provide logistics support and staging for reinforcements to the frontline states lay themselves open to Russia's anti-access and area denial capabilities. This may not necessarily be in kinetic terms, in the form of missile strikes on ports for example, but through all the other means at Russia's disposal to impede or prevent reception and staging of reinforcements and supplies, including political, social, information, economic and cyber interventions. Above all, any NATO ally is by default a target for political warfare intended to undermine its will to meet its treaty obligations.

A critically important element in bolstering national and societal resilience to hybrid threats is raising the awareness of the civilian population, and ensuring an appropriate level of consciousness among the general public as to the real threats faced. As in so many other instances, this is a more straightforward task in the frontline states, where little effort is needed to explain the threat from Russia – particularly among those populations that have suffered mass deportation and murder within living memory. Elsewhere, key leader engagement is essential, admitting and avowing problems, and thereby empowering society, government, and media to take steps to defend themselves.

Leadership education is another important contributor to preparedness. The Finnish model of national defence courses for not only government officials, but also business leaders, custodians of national infrastructure, and key media decision-makers may be difficult or impossible for some other nations to replicate; but engagement must be sought where it can. The key message, for leadership figures and ordinary citizens alike, is that in the new environment of whole of society threats, nobody is too unimportant to be a target; and that consequently, nobody is too unimportant to be involved in defence.

Keir Giles is a Senior Consulting Fellow with Chatham House in London.