GLOBSEC
IDEAS SHAPING THE WORLD

THINKING ABOUT HYBRID WAR AND THE 'IMAGINATION RACE'

Mark Galeotti

Summary: Hybrid threats tend to be opportunistic and asymmetric, with antagonists that are quick to capitalise on their successes and learn from their mistakes. Even before considering the institutional and operational responses, countries and alliances need to take a sharp and honest look at their vulnerabilities, as it is far easier to pre-emptively build resilience than to respond in the midst of an attack. In the modern world, after all, non-military threats are every bit as important as military ones, and addressing issues from the adequacy of police and counter-intelligence services to the challenge of corruption will be crucial. Above all, expertise needs to be combined with imagination, because the threat is constantly evolving.

In 2017, Germany's domestic security service (BfV) and its foreign intelligence service (BND) both accused Russia of seeking to interfere in the country's elections.[1] Coming as it did after a series of previous scandals, notably the so-called 'Lisa Case' of 2016 and the sustained hacking of the Bundestag in 2015, this led to a serious backlash, as well as a strengthening of Germany's defences.[2] The evidence of 2021 is that while Moscow has refined its methods and shifted its tactics – instead of seeking to influence the outcomes, it is concentrating on capitalising on the inevitable divisions and rancour election campaigns generate – it is still launching 'active measures,' covert political operations, in pursuit of its wider goal of dividing, distracting and demoralising the West.[3]

This should not surprise us. While it is unlikely that there will be any change in overall strategy so long as the current regime is in power in the Kremlin, there will be constant change in the tactics and instruments deployed.

First and foremost, after all, hybrid war is a struggle of wit, will and imagination. Resisting today's and tomorrow's threats depend not just on resources, planning and societal cohesion – important though all of those undoubtedly are – but also on a clear understanding of the vulnerabilities any antagonists may seek to exploit and what their 'Plan B' and 'Plan C' may be when those particular opportunities are closed to them. Having become used to arms races and space races, we must also accept that we are also engaged in imagination races, too.

To this end, a central theme of GLOBSEC's new initiative, Countering Hybrid Threats: 10 Steps for a Resilient Europe,[4] is the need to combine thought and deed, moving beyond the sometimes-impressive but often-patchy initiatives of the European Union[5] and individual European states. In this, the first of a series of short white papers exploring specific clusters of the ten outline steps, the initial question of how to think about the challenge and build responses out from there will be addressed. There is, after all, a rich debate about how truly new the threat may be and quite what it should be best be called,[6] but either way, it is clear that modern societies are especially susceptible to non-kinetic attacks often well below the threshold of what is generally understood to be war.

KNOW YOUR WEAKNESSES BEFORE YOUR ADVERSARY DOES

Nations need – alone and in partnership[7] – effective agencies to gather intelligence on antagonists' capabilities and intentions. As well as collection, this depends on competent analysis of secret intelligence and open source alike. While some European countries still have substantive analytic capacity, others do not, and this will require

1 'Germany challenges Russia over alleged cyberattacks', Reuters, 4 May 2017, https://www.reuters.com/article/us-germany-security-cyber-russia-idUSKBN1801CA; 'Russia hackers: German spy chief Kahl warns of election disruption,' BBC, 29 November 2016, https://www.bbc.co.uk/news/world-europe-38142968

2 See Constanze Stelzenmüller, 'The impact of Russian interference on Germany's 2017 elections,' Brookings, 28 June 2017, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/

3 'Russia sows distrust on social media ahead of German election', Politico, 3 September 2021, https://www.politico.eu/article/germany-russia-social-media-distrust-election-vladimir-putin/; 'Germany protests to Russia over pre-election cyberattacks,' AP, 6 September 2021, https://apnews.com/article/technology-europe-russia-elections-germany-26ea77a3b96b94d5760aab48c9dfc008

4 'Countering Hybrid Threats: 10 Steps for a Resilient Europe,' GLOBSEC, 16 June 2021, https://www.globsec.org/publications/countering-hybrid-threats-10-steps-for-a-resilient-europe/

5 For a useful and searching overview, see Daniel Fiott and Roderick Parkes, 'Protecting Europe: the EU's response to hybrid threats,' Chaillot Paper 151 (April 2019), https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

6 See, for example, James K. Wither, 'Defining Hybrid Warfare, per Concordiam: Journal of European Security Defense Issues 10:1 (2020), https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf

7 Including through such collaborative structures as the Hybrid Fusion Cell within the EU's Intelligence and Situation Centre (INTCEN).

long-term investment in both specific services and also wider expert communities, as these provide an invaluable adjunct to government analysts and also a corrective to potential groupthink.

However, even more important than gathering intelligence on antagonists is doing so on ourselves. Hybrid threats are often – but not always – asymmetric ones from antagonists who have been forced to become 'geopolitical guerrillas' by the strength of a united Europe and the NATO alliance.[8] One of the key virtues of hybrid techniques for such actors – state and non-state alike – is precisely that they are equalisers that permit the weak to attack the strong, often deniably. As such, they tend to be opportunistic, driven by the conjunction of a target of suitable value to the attacker, and a vulnerability of the likely-unaware defender. The murder in Berlin of Georgian Chechen Zelimkhan Khangoshvili in 2019, apparently by a Russian contract killer engaged by the state,[9] had to take place in Germany because that was where the target was, but was facilitated by the Schengen agreement which meant he could fly into France and travel across a national border without checks.[10] Likewise, hostile disinformation and the amplification of divisive political messages is easiest when directed specifically towards communities which already feel alienated and muzzled, from separatists to Eurosceptics.[11]

Hybrid antagonists will generally not waste their time battering themselves against our strengths – they will look for our weaknesses, and therefore it is incumbent on European nations and institutions constantly to explore their own potential gaps and vulnerabilities. This is inevitably an uncomfortable process that demands a degree of honesty and self-critical awareness that is not always habitual, in an age of spin and perception management. To be blunt, many self-assessments confuse activity with impact, chronicling initiatives launched and units established rather than actually presenting hard evidence of progress in practice. The political cost in admitting our failings is often considered before the systemic risk in not being honest about them. This is, however, essential, given that our antagonists will not be so hesitant in looking for ways to expand the threat surface.

This will mean mapping vulnerabilities and comprehensively auditing national processes and structures. Part and parcel of this is to wargame potential hybrid scenarios just as seriously as the military test out warfighting ones. This is not a job for a single agency, nor just the government, as hybrid operations target different sectors of society, whether strategic corruption through business connections or radicalising militant communities. Going beyond such valuable exercises as the European Centre for Excellence for Countering Hybrid Threats (Hybrid CoE) RESILIENT RESPONSE 2020,[12] the threats must be wargamed not just on a whole-of-government but whole-of-society basis, in which everyone from central banks to community organisers can be part of the solution as easily as part of the problem. Nor should this be an ad hoc process: there needs to be a clearly defined agency devoted to hybrid threat assessment and responses, with the expertise to be effective, the authority to be meaningful, and the resources to do the job.

TREAT NON-MILITARY DEFENCE AS BEING AS IMPORTANT AS MILITARY DEFENCE

After all, protecting the integrity of national institutions is every bit as important as defending national borders. Of course, defences against hybrid threats cannot be improved at the expense of conventional security. Europe needs a robust capability to defend itself and its interests, even without the NATO guarantee. Indeed, just as armed forces can also be used as hybrid instruments – aggressive Russian exercises are often more than anything else intended to intimidate and to push alarmed constituencies to lobby for compromise with Moscow out of fear of war[13] – so too a credible national defence helps generate the confidence at home that can help a community resist such pressures.

Nonetheless, this does place a premium on the capacities of European countries police and counter-intelligence agencies, and their ability to support each other both at home and across the Western alliance. If governance and perception are the main battlefields of hybrid war, then domestic security agencies are some of the most crucial defenders, whose capacities must be equal to the challenge. It is easy to criticise the common NATO target that member states ought to spend 2% of their GDP on defence: that it is too little, that it is not the best measures, that it is too easily finessed. Nonetheless, at least it gives a sense of a common baseline, and es-

8 Mark Galeotti, 'Active Measures: Russia's Covert Global Reach', in Graeme Herd (ed), Russia's Global Reach: A Security and Statecraft Assessment (George C Marshall Center, 2021) https://www.marshallcenter.org/de/node/2257#toc-active-measures-as-guerrilla-geopolitics

9 'Death in Berlin: Russian goes on trial for murder of exiled Chechen,' Deutsche Welle, 7 October 2020, https://www.dw.com/en/berlin-russia-murder-chechen-dissident/a-55165044

10 'Suspected Assassin In The Berlin Killing Used Fake Identity Documents', Bellingcat, 30 August 2019, https://www.bellingcat.com/news/uk-and-europe/2019/08/30/suspected-assassin-in-the-berlin-killing-used-fake-identity-documents/

11 Péter Krekó, 'The Drivers of Disinformation in Central and Eastern Europe and their Utilization during the Pandemic,' GLOBSEC Policy Brief (2020), https://www.globsec.org/wp-content/uploads/2020/06/Drivers-of-disinformation-in-Central-and-Eastern-Europe.pdf

12 See RESILIENT RESPONSE 2020 Final Exercise Report (2020) for a comprehensive overview of the exercise, https://www.hybridcoe.fi/wp-content/uploads/2021/03/FER_RERE20_FINAL.pdf

13 Mark Galeotti, 'Heavy Metal Diplomacy: Russia's political use of its military in Europe since 2014,' ECFR Policy Brief, 19 December 2016, https://ecfr.eu/publication/heavy_metal_diplomacy_russias_political_use_of_its_military_in_europe_since/

tablishes the principle that every member is not responsible only for their own security but also for pulling their weight within the organisation as a whole.

While quantifying the cost of defences against hybrid threats is next to impossible given the huge disparities in institutional and community resilience, it is not unreasonable for member states of the European Union to address what may be equivalent baseline expectations as to the resources countries ought to spend on, if not policing, at the very least counter-intelligence. Partners, after all, must be able to share classified information and best practice without fearing security weaknesses on their allies' part, just as problems in one country may spread or be intended precisely to have a transnational impact. Likewise, police need to have the training and resources to deal with rioters, protesters and gangster – all of which can be used as shock troops of hybrid warfare – and to do so professionally and proportionately, as often the hope is precisely to create internal unrest and disaffection by forcing a government to over-react.

Effective counter-intelligence also allows for an especially rapid and precise response to hybrid attacks, such as the way the Czech government was able to respond to the revelation that the 2014 Vrbětice explosion was the result of a Russian operation by expelling not just a few Russian intelligence officers but the whole Foreign Intelligence Service (SVR) and military intelligence (GU[14]) stations because BIS, its Security Intelligence Service, had for years been tracking and identifying them.[15]

Above all, this is evident when addressing corruption. Combating this problem is essential for national security and working democracy, because of the very breadth of its corrosive effects, undermining legitimacy and facilitating subversion, and the ways it can be used both as a direct vector for hybrid attacks and a force multiplier for others.[16] It helps organised crime groups survive, for example, and it has been established that they have been used to gather intelligence in the Balkan and Nordic states, at least, and maybe even smuggle operatives across borders.[17] It drains national resources that could otherwise be used to uplift marginalised communities – of the very sort that may as a result be especially vulnerable to disinformation – and generates a perception that the state and the existing social order are hypocritical and unfair. It can also influence policymakers at a national or, especially, local level.

However, this is a struggle which can and must be fought not simply by the institutions of the state, but also civil society, from the media and national NGOs, to local community organisations. Admittedly, whistle-blowers, transparency advocates, opposition parties and investigative journalists can sometimes be manipulated by antagonists involved in hybrid attacks, but far more importantly they are essential to oversight of the state and thus the public trust and systemic legitimacy that is so important in resisting hybrid attacks. They also help monitor and counter malign influence and identify potential weaknesses, whether revealing the inter-connections of financial proxies and front companies, such as with the Panama Papers leak.[18] However inconvenient they may sometimes be to political and economic elites, they need to be protected from harassment and threats, often conducted through the law. There is a balance to be struck – not every journalistic allegation is fair or honest and not every libel action is an unfounded and malicious strategic lawsuit against public participation (known as SLAPP) – but civil society and independent scrutiny must be protected. While the European Parliament's legal affairs, civil liberties and home affairs committees are seeking to develop guidelines for 'anti-SLAPP' legislation, this really needs to be tacked at a national level, too.[19]

BE IMAGINATIVE

Who, after all, thought libel laws could be used by foreign states – or at least their agents and representatives – as a weapon of covert war? When social media first began to become popular, did anyone believe they could be exploited to divide, subvert and misdirect? As universities began to look further afield for grant and endowment funds, should the degree to which countries such as China began to use that as a way of buying influence and silencing critical voices have been predicted?[20]

All this highlights the importance of the 'imagination race,' of the need not simply to identify and respond to today's vulnerabilities, but to try and predict tomorrow's, proactively to address them. After all, every time a weakness is addressed, adversaries will simply look for new ones. For example, having largely been counterpro-

14 Commonly still known by its former acronym, GRU

15 'Na výbuchu ve Vrběticích se podíleli Rusové. Policie hledá muže z kauzy Skripal,' Deník, 18 April 2021, https://www.denik.cz/z_domova/hamacek-babis-vlada-20210417.html

16 Dave Allen, '"A Deadlier Peril": The Role of Corruption in Hybrid Warfare,' MCDC Information Note, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795222/20190318-MCDC_CHW_Info_note_7.pdf

17 Mark Galeotti, 'Crimintern: How the Kremlin uses Russia's criminal networks in Europe,' ECFR Policy Brief, 18 April 2017, https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/

18 ICIJ: The Panama Papers: Exposing the Rogue Offshore Finance Industry, https://www.icij.org/investigations/panama-papers/

19 'EU Parliament to counter lawsuits designed to silence journalists, NGOs,' Euractiv, 11 May 2021, https://www.euractiv.com/section/digital/news/eu-parliament-to-counter-lawsuits-designed-to-silence-journalists-ngos/

20 Salvatore Babones, 'It's Time for Western Universities to Cut Their Ties to China', Foreign Policy, 19 August 2020, https://foreignpolicy.com/2020/08/19/universities-confucius-institutes-china/; Ivana Karásková, 'Countering China's Influence Campaigns at European Universities,' The Diplomat, 22 February 2020, https://thediplomat.com/2020/02/countering-chinas-influence-campaigns-at-european-universities/

ductive in seeking directly to influence European elections in 2017, notably in France[21] and Germany[22], Russian political operations have shifted instead to using social media and other means to amplify the inevitable disruption and division elections generate. This will again require government agencies, bodies not typically known for such traits, to find ways to harness and encourage unconventional thinking and a willingness to try and be as ruthless and flexible as the antagonists.

There all kinds of ways that this can be done, many already in use but needing to be deployed more widely. In military and security contexts, it is quite common to field 'red teams' and 'white hat hackers' to test existing doctrine and tactics, giving them considerable freedom as to how they deliberately seek to beat their own systems. This concept can be expanded – whether to try and anticipate malign propaganda or block new ways of using 'dark money' to buy political influence – to identify potential vulnerabilities before an adversary.

Again, though, this is not simply a matter of an adaptive passive defence, however important that certainly is. Imagination can also be deployed to explore new ways of imposing costs and sanctions on hybrid antagonists. This is an extremely useful way of developing what we could 'hybrid deterrence' on several axes.

Different antagonists have different approaches, but many subcontract their attacks to autonomous agents. In particular, the Kremlin encourages numerous 'entrepreneurs of subversion,' from businesspeople (such as Kontantin Malofeev, who has been accused of stirring up the attempted coup in Montenegro in 2017[23]) to scholars (notably the 'Neo-Eurasianist' Alexander Dugin, who is largely ignored at home, even by the Kremlin, but has a certain following in Europe[24]). These are often 'investing' in attacks, using their own resources to carry them out on their own initiative with the hope or expectation that they will be rewarded for success. They are therefore especially susceptible to what in military terms is called deterrence by denial – they are less likely to invest in an attack if they feel it has a marginal chance of success. Imaginative 'target hardening' against such threats therefore not only minimises their potential effect, it also makes them less likely.

States, though, are the main generators of hybrid attacks directly. Deterrence by denial will generally take second place in this context to deterrence by retaliation. Here, European countries have tended to be relatively predictable in their responses, and instead there is scope for a more imaginative approach to developing a menu of means of punishing an aggressor. In other words, instead of the usual reliance on symmetric means – banning or fining media outlets for an egregious case of disinformation, for example, or expelling intelligence officers under diplomatic cover for an espionage operation – it is worth taking a 'whole of government' approach to retaliation, too. It could be, for example, that the best way of punishing Russia for a cyberattack might be nothing to do with the virtual world, but to provide funds to émigré media outlets challenging the Kremlin's propaganda line at home. While it is important to retain a sense of proportionality – not least to allow scope for escalation – that should not mean overly predictable, let alone inconsequential. The point is to use the same imagination antagonists use to find Western weaknesses likewise to determine the most efficient responses. Deterrence is strongest when adversaries are not only convinced that there will be a cost to any malign actions, but also when they do not know precisely what that may be – so they cannot prepare or make valid cost/benefit analyses – but are certain that they will be meaningful and painful.

Thus, while following White Papers in this series will dig deeper into specific measures to be taken to strengthen resilience, resist hybrid attacks and deter potential aggressors, the first and most basic pre-requisite for what we could call 'hybrid defence'[25] is to be self-critical, honest, thoughtful and imaginative. Without this, no new initiatives, anti-disinformation units, workshops and summits will be enough.

---

21 'Successfully Countering Russian Electoral Interference,' CSIS Briefs, 21 June 2018, https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

22 Stefan Meister, 'What Russia Has Achieved During The German Election,' DGAP, 22 September 2017, https://dgap.org/en/research/publications/what-russia-has-achieved-during-german-election

23 'Putin ally allegedly involved in Montenegro coup plot,' BNE Intellinews, 3 March 2017, https://www.intellinews.com/putin-ally-allegedly-involved-in-montenegro-coup-plot-116855/; Paul Stronski and Annie Himes, 'Russia's Game in the Balkans,' CSIS Paper, 6 February 2019, https://carnegieendowment.org/2019/02/06/russia-s-game-in-balkans-pub-78235

24 George Barros, 'The West Overestimates Aleksandr Dugin's Influence in Russia', Providence, 8 July 2019, https://providencemag.com/2019/07/west-overestimates-aleksandr-dugins-influence-russia/; Anton Shekhovtsov, 'Putin's Brain?', Eurozine, 12 September 2014, https://www.eurozine.com/putins-brain/

25 Mark Galeotti, 'Time to talk about "hybrid defense",' War On The Rocks, 30 July 2015, https://warontherocks.com/2015/07/time-to-think-about-hybrid-defense/