Treverton, Gregory F. "An American view: Hybrid threats and intelligence." *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm . London: I.B. Tauris, 2021. 36–45. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781788317795.0008>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 11:22 UTC.

Copyright © Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm 2021.
Released under a CC BY-NC-ND licence (<https://creativecommons.org/licenses/by-nc-nd/3.0/>).
You may share this work for non-commercial purposes only, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

An American view

Hybrid threats and intelligence

Gregory F. Treverton

Introduction

This chapter thus takes a closer look at the means available in the US context for devising a robust response to the challenges posed by hybrid threats and hybrid warfare. The Russian intervention in the 2016 US elections came as a surprise, but it should not have. There was warning but from an unfamiliar quarter. A group of analysts outside the government was tracking the online dimensions of the jihadists and the Syrian civil war when they came upon interesting anomalies, as early as 2014. When experts criticized the Assad regime online, they were immediately attacked by armies of trolls on Facebook and Twitter. Unrolling the network of the trolls revealed they were a new version of ‘honeypots’, presenting themselves as attractive young women eager to discuss issues with Americans, especially those involved in national security. The analysts made the connection to Russia but found it impossible, that early, to get anyone in the American government to pay attention, given the crises competing for both policy and intelligence attention. The government was focused on jihadists, not Russians.¹

I plead innocent: I was then the Chair of the US National Intelligence Council (NIC), and the group looking at jihadists didn’t come to me. Yet, in retrospect, the episode underscored two lessons for me. The first was parochial, but one that struck me over and over again while I was at the NIC. I understood the political imperative of combatting terrorism, but the preoccupation deformed our work: when we looked at Nigeria, there was not much Nigeria there; it was all Boko Haram. And when we looked at Boko Haram, there was not much Boko Haram there either. It was all about identifying and unravelling networks and targeting bad guys. To be sure, we worried about the larger questions: Where does Boko Haram come from, and where is it going? But there was scant opportunity to work on those questions given the press of the tactical.

The second lesson is the first theme of this chapter. Especially in the non-kinetic range of hybrid threats, those of us in governments and intelligence services can find

partners in civil society – but only if insiders reach out in ways that are novel and often uncomfortable. Those analysts outside the government looking at jihadist websites in 2014 didn't need contracts or grants from the government. They just needed to be listened to.

The Russians are hardly the only ones engaged in hybrid threats, but they are for good reasons as the focal point of concern, and are the focus of this chapter. The new elements in hybrid threats – cyber and social media (SM)-aided propaganda – are both relatively cheap, and so will continue to be attractive to Moscow even as they also appeal to other countries and groups on similar grounds.

The second theme of this chapter, drawing especially on my latest time as a practitioner as Chair of the NIC, is that it is all too easy to respond, tit-for-tat, to the latest Russian misbehaviour. That may be the correct policy but needs to be set in the context of a strategic backdrop beyond reflex responses. That is not to excuse Russia under Vladimir Putin but to understand it in the search for better policy, one with less risk of misunderstanding and inadvertent escalation.² This assumption that Russia is now an enemy, whose every action is calculated to confront the United States, now spreads across the political spectrum in the United States. Yet even in the Obama administration, which I last served, there was a kind of visceral hatred for Putin, rooted in the sense that he was a liar who could not be trusted. I occasionally ventured to remind my policy counterparts, ever so gently, that during the Cold War we had also dealt with Soviet liars and cheats but had managed to come to enough agreement to avoid blowing up the planet.

I turn first to the opportunity.

The nature of the threat

Table 3.1 summarizes the range of hybrid threat instruments.

Most of the hybrid toolkit, from money to political parties to proxy combatants ('little green men'), is not new. What is new are cyber tools and SM-aided propaganda, both of which dramatically lower the entry cost: planting an article in a foreign newspaper during the Cold War was hard and expensive; now, trolls can simply post the article, with bots seeking to make it a 'trend', and thus perhaps get picked up by more traditional, quality media.

Hybrid threats are 'wicked' problems, less because they involve new actors interacting in ways we haven't seen, as was the case with terrorists after 9/11. Rather, 'by emphasizing elusiveness, ambiguity, operating outside of and below detection thresholds, and by using non-military tools to attack across all of society, hybrid threats represent a new iteration of the complexity found in wicked problems.'³ The instruments are used simultaneously, and their target is opposing societies, not armies.

And with virtual tools, geography disappears. That was driven home by the 2016 Houston case. In May, a Facebook page called Heart of Texas encouraged its quarter million followers to demonstrate against an urgent cultural menace – a new library opened by a Houston mosque.⁴ 'Stop Islamization of Texas', it cried. But the

Table 3.1 Range of hybrid tools

Tools	Examples
Propaganda	Enabled and made cheaper by social media, also targeted at home
Fake news	‘Lisa’ was portrayed as a Russian-German raped by migrants ^a
Strategic leaks	Macron emails leaked forty-eight hours before the French election
Funding organizations	China opened Chinese think-tank in Washington
Political parties	Russia supports sympathetic European parties on right and left
Organized protest movements	Russian trolls organized both pro- and anti-protests in Houston mosque case
Cyber tools:	New tool in arsenal: espionage is old tactic with new, cyber means.
• Espionage	Attack has targeted critical infrastructure, notably in Estonia
• Attack	in 2007. Manipulation is next frontier, changing information
• Manipulation	without the holders knowing it.
Economic leverage	China sought to punish South Korea for accepting US anti-missile system
Proxies and unacknowledged war	Hardly new, but covertly deployed Russian military personnel in Ukraine slid into actual combat
Paramilitary organizations	Russian ‘Night Wolves’ bikers intimidate civilians

^aStefan Meister, ‘The “Lisa Case”: Germany as a Target of Russian Disinformation’, *NATO Review*, 25 July 2016. HYPERLINK ‘<https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html>’ <https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html>.

other side organized as well. A Facebook page linked to the United Muslims of America said that group was planning a counter-protest for the same time and place. In fact, while the United Muslims were a real group, the Facebook page was not its doing. Both the anti- and pro-demonstrations had been organized by Russian trolls.

Crowd sourcing: Changing culture

Opportunities for governments, and for their intelligence services, lie in new media, new networks and new partnerships. However, I know all too well that the culture of intelligence is slow to adapt: when I did a study of the use of SM in intelligence a decade ago, NSA analysts reported getting the question from colleagues, ‘what’s a hashtag?’⁵ Happily, we’ve come a long way since then. The private citizens looking at jihadi websites in 2014 who found evidence of Russian fakery drive home the possibilities of ‘crowd sourcing’ around the world, seeking partners in identifying fake news and planted posts. Alas, this kind of openness and reach to private sector runs very much against the grain of intelligence cultures.

Cyber is another great opportunity. In the short run, private actors upset the traditional paradigm of intelligence and policy: if a hack occurred, intelligence would seek to attribute it to its source, then pass that information in secret for policy to take decisions. Now, private companies are doing attribution too and will go public when it suits them. Yet in the longer run, those companies are a great opportunity for partners, and when they go public it might even ease the ‘sources and methods’ problem for

intelligence because to be credible the companies will have to say something about how they came to their conclusion.

The contours of relations between policy and intelligence were on view in one episode when I was chairing the US NIC. When hacks into the US Office of Personnel Management (OPM) in 2015 resulted in the loss of personal data on more than twenty million Americans, the immediate question was: who did it?⁶ At this point, forensically, the complexity of hybrid threats had been reduced to a puzzle; attribution had an answer. The OPM hack came soon after the SONY hack. In the case of SONY, good work and good luck let US intelligence attribute it to North Korea quickly and with high confidence. Not so in the OPM case. We were pretty sure the hack came from China, but when policy officials pressed for more detail, we were for some time in the position of having to answer, more or less, 'China is a big place'.

The episode was a reminder that when an intelligence issue becomes a puzzle, policy officials will want – and expect – certainty that often isn't possible. (Taking off my intelligence hat and putting on a policy one, I admit I didn't mind the difficulty of attribution. Not only was it a useful lesson for policy officers, but since, in my view, the retaliatory options for the United States were unpromising, some delay for thought was welcome.⁷) It was also a reminder that attribution, even when good, is seldom quick. For instance, it took Saudi authorities two weeks to assess the damage from the Shamoon attack in 2012 that erased data on 30,000 of Saudi Aramco's computers.

Working with partners is very necessary, and both new partners and forms of partnership abound – a critical point for opportunities. Yet official collaboration is increasingly burdened by fears of leaks and the misuse of shared intelligence. In any case, relationships can rely less and less on the Cold War legacy. The new partnerships necessarily will take intelligence services outside their comfort zones, and underestimating the value of what counterparts, including new ones, provide will be even more counterproductive than in previous periods.

Traditional intelligence collectors will play their roles in new circumstances, but exactly how remains something of an open question. SIGINT, for instance, now uses SM mostly for targeting traditional collection, especially against terrorists: 'terrorists may have good OPSEC but they also have children, and so when I find an email' HUMINT can be critical but will be pushed into a much broader arena, and find itself collaborating with new partners, including some outside government. HUMINT is probably more critical than ever but little easier. To the extent the targets are foreign, especially Russian intelligence services, they are at least known, and perhaps somewhat 'softer' than Al Qaeda.

Penetrating Russian hacker groups, like the Internet Research Agency, would be valuable in the usual ways, providing indications of Russian targets and methods. One of the great successes of US and fellow intelligence services has been following the 'money trail' of terrorists or drug traffickers. It is a question whether and to what extent virtual currencies, like bitcoin, will make that trail harder to follow as, for instance, hybrid threateners fund parties and propaganda in other countries. So far, the effect seems small, but that may be because the currencies have been used more as investments than as media of exchange.

SM are a great source of intelligence – and warning: as one analyst from the US Defense Intelligence Agency put it to me in identifying Russia soldiers in Ukraine, ‘selfies are our best friend’. As in that case, cell phones may be geolocated, or the location may be inferred from analysis of the selfie – opening an entire new source for GEOINT. So, too, ubiquitous cameras offer GEOINT new opportunities for identifying people and their movements. Taking advantage of them, however, will also require a change in organizational culture: the world is awash in information, yet in my experience, intelligence agencies still tend to give pride of place to their own secret sources and to ask first what they might collect and how, not what is out there already that might help.

Collection will also require new forms of collaboration between HUMINT and SIGINT, one suggested by the increasing practice of human-aided SIGINT. As microwave transmissions gave way to fibre optics in the 1990s, signals no longer could be gobbled up wholesale by satellites. As encryption became unbreakable, the best ways to intercept signals were before they were encrypted, and that meant getting very close to the signaller. These developments drove a closer partnership between clandestine and SIGINT services.

What is still, slightly weirdly, called ‘open source’ is very much a work in progress, especially in the United States. Open source gets treated like another INT when it is in fact, in the words of John Gannon, a former director of intelligence at the CIA, ‘the air we breathe’. In my last incarnation in government, it was tempted to try to play in the ‘big leagues’ by showing its worth on ‘hard’ targets, like proliferation. Those are probably not its comparative advantage, and compounding the mismatch, the US Open Source Enterprise (OSE) has returned to the CIA, rather than the inter-agency auspices of the director of national Intelligence (DNI). It tends to regard SM as just the latest media to exploit, and it goes about validation in a fairly traditional way, looking at location and numbers of retweets, for instance. Ideally, it would become the focal point for matters virtual but unclassified across the entire government, in particular pushing the artificial intelligence (AI) needed to cope with ubiquitous data.

Hybrid threats will reconfigure counterintelligence. After all, preventing foreign powers from hacking into computers or manipulating public opinion would seem the essence of counterintelligence. The awkwardness, though, is that formulation dramatically expands the institutions to be protected to include both infrastructure and virtual providers that are both in the private sector. As vulnerabilities drive adversaries’ targeting, understanding possible target spaces becomes key to channelling resources – online and off. That in turn will require building links inside and outside the government, doing red teaming, and developing fragility indicators and heuristics for potential attack spaces.

An open question for counterintelligence is what role there might be for taking the offensive. In principle, the Western countries could seek to sow conspiracy and doubt in Russia’s intelligence cycles. The tactic would draw on their desire to please Putin’s world view. The goal would be to widen the chasms between Russian intelligence services, playing them off of each other and draining their limited resources, much as Russia seeks to exacerbate social divisions in the Western countries. If the offensive required covert insertion of misinformation, though, it would risk descending to Putin’s level, discrediting both facts and media that seek them – thus making truth still more relative.

Duelling narratives

The second lesson I took away from my time in government is that taking Russia's perspective into account, and considering its possible actions as reactions, not as proactively aggressive, can begin to be strategic in the sense of asking 'what if?' and 'what next?' Russian initiatives have included kinetic force, as in the Ukraine, and may do so again, but the main game is a contest of competing narratives. Our narrative is that of the inevitable victory, as Kennan predicted, of democracy over autocracy, capitalism over communism. Needless to say, Putin's view is very different. He described the fall and breakup of the Soviet Union as the 'greatest geopolitical catastrophe' of the last century.⁸ He added, 'Tens of millions of our co-citizens and co-patriots found themselves outside Russian territory . . . The moment we display weakness or spinelessness, our losses will be immeasurably greater.'

From Moscow's perspective, and surely Putin's, in the years after communism's end, the United States and the West dismissed Russia. During the Cold War, we had referred, ruefully, to the Soviet Union as 'Equatorial Guinea with nuclear weapons', but after the Cold War there was some truth to the Russian belief that we treated it that way. The George H. W. Bush administration did a masterful job of handling the Cold War's end, and there was no formal pledge, in the Budapest agreements of 1994 or anywhere else, committing NATO not to expand NATO beyond the unified Germany and or even to Russia's borders. Still, both President Bush and Secretary of State James Baker said things to their counterparties that seemed to imply such commitment.

Surely, NATO expansion during the 1990s is regarded by Russians not just as a 'broken promise' but as an affront to national dignity inflicted on them in a time when Russia was weak, both economically and militarily. The accession of the Baltic States in 2004, which border the Russian Federation, was seen as a threat. The subsequent events in Georgia in 2008 should be viewed in that context. What we regarded as straightforward intervention – but didn't do much about – was for them an attempt to undermine the government of Mikheil Saakashvili, which was very pro-Western and sought to become part of NATO. Russia acted lest another nation on its border defect into the Western alliance.

More generally, after the fall of the Berlin Wall, the Russian people looked to the West for hope and guidance. What they got was a decade of disappointment and economic mismanagement (including by Western advisors). Not just Putin but most Russians felt their dignity as a large country and erstwhile superpower was stripped from them, and that the West, rightly or wrongly, took advantage of them. It was thus understandable that Russians would turn to a strongman nationalist like Putin. His support has dropped in the last years with additional rounds of Russian sanctions and a sagging economy, from 81 per cent in 2018 to under 65 per cent in 2019. Yet his narrative of Russia's again playing a large role on the world stage remains dominant: in 2015, after the annexation of Crimea and the intervention in Ukraine, his approval rating at home reached a stunning 89 per cent.

While the Russians and the Russian leadership are not yearning to go back to creating a Soviet Union, they do care about their position, role and influence in the world and especially in what they call their 'near abroad'. Their influence in the near

abroad not only gives them back a sense of status as a large power but also gives them a buffer against what they view as the expansionist West. From the Russian point of view, much of what we regard as aggressive, Russians see as defensive. The West and the United States are the aggressors and since the fall of the Berlin Wall have been pushing a policy of encirclement vis-à-vis the Russian Federation. Taking this perspective into consideration helps explain how Russia has responded to tension and conflict in the Baltics, the Ukraine and Georgia.

The goal should be to avoid misunderstandings and measures that needlessly escalate tension. Think, for instance of reactions to future sanctions, NATO troop build-ups in eastern Europe/Balkans and military exercises or the withdrawal from the INF treaty and the placement of nuclear warheads in Europe. In the case of future sanctions, no matter how much (or little) sanctions have so far hurt Russians, possible additional one, perhaps aimed at excluding Russia from the international banking system, will bite. Those will be viewed much more seriously by the Kremlin and may trigger retaliation in the form of an attack on the US financial system. They also have the unintended side effect of pushing Russia to extract itself from the US-dominated international financial system and transacting in currencies other than dollars – thus insulating itself to some extent from future sanctions. Indeed, Russia has already moved down that road.

On one hand, NATO troop build-ups in Eastern Europe and the Balkans, along with military exercises, demonstrate commitment, and Russia does not see them as an existential threat. On the other hand, they also validate Putin's narrative of NATO militarizing and pushing itself to Russia's borders. The Russians will pocket that validation, and respond by disrupting, pestering, talking of escalation – responses in the grey zone short of conventional conflict.

If the United States' withdrawal from the INF treaty is followed by the placement of nuclear warheads in Europe, that would be seen as an existential threat and would elicit a response by the Russians, which would no doubt start with grey zone measures. And the Balkans remain a key vulnerability in Europe, one over which Russia has tremendous influence. Should events start to suggest that nuclear warheads will be deployed in Europe, Russia could respond by creating havoc starting in the Balkans.

Given that the political stalemate in US politics is likely to continue beyond Trump, this may embolden Russia to make preemptive moves in a number of areas including geopolitical priorities, rhetorical policy and whole of government approach. For instance, given other priorities and disarray, the United States seems to have no time for Libya, and Russia is already stepping into the breach. A stable and Russia-friendly Libya offers huge advantages from an energy security and defence perspective – potential for a naval base in the Mediterranean. Moldova is another country that will be sucked back into the Russian orbit of influence while the United States is distracted and internally focused. Ukraine is tricky, given its upcoming presidential elections. The Russians are already funding various candidates, and in the worst-case scenario, if a pro-Western candidate is elected, they may create enough conflict to maintain the status quo, which is a basket case. The result is a drain on financial resources for the EU and the United States, if also for Russia itself.

Even in rhetoric, the United States has not always been clear that, for instance, interventions in its elections are unacceptable. So, too, its commitment to NATO and article 5 can hardly be restated often enough. And even an organizational change, like creating a Deputy Assistant Secretary of Defense (DASD) for New Generation (grey zone) Warfare, can demonstrate that the Department of Defense is taking these threats seriously, as well as serving as the Defense focal point for a broad approach to hybrid threats.

A ‘whole of government approach’, on which European states are making progress, seems almost an unnatural act for the United States. At least that is my experience. Being more proactive in countering grey zone threats has a military component, to be sure, but it requires all of government to create a coordinated set of tools and weapons to be deployed. Making sure, for instance, that sanctions do not backfire will require the deep involvement of the departments of Treasury, and State as well. So, too, the various private sectors have an important role to play as both eyes and ears for early warning and for speaking with a credibility that governments, as governments, often lack.

Finally, in being more strategic about Russia, there may be value in more dialogue with Russia. Surely, in the wake of Russia’s election meddling, in 2016 and beyond, and the reaction that it stirred in the United States, the dialogue has become very constricted, increasing the risk of misinterpretation and the possibility for escalation. It behooves the United States and its partners to in fact enhance the dialogue on many of the issues and regarding many of these contentious areas so as to reduce the risks of escalation, and perhaps even remove some of the reasons for Russia’s disruptive behaviour.

Lessons for intelligence and policy

Finally, it is worth laying out some of the lessons learned so far. Seven lessons stand out to me.

- Recognize that hybrid conflict is war by other means. Cyber and virtual conflict are the wars of the future, society against society.
- Intelligence is best done as a ‘whole of society’ enterprise, with lots of, in effect, crowd sourcing in both the cyber and virtual realms. Warfighters plainly have a role to play, especially at the end of the spectrum where hybrid shades into kinetic. But the military shouldn’t be the dominant element.
- Just as hybrid techniques blur the lines between combatants and citizens, they are another reason why companies and citizens should be wary of cyber threats and manipulated information on SM. Like the rest of us, the US Democratic National Committee was, in 2016, more interested in getting its work done than in protecting its networks. Its mistake made it easier for the Russians to hack into the emails of John Podesta, Hillary Clinton’s campaign manager.
- The question of retaliation as an element of deterrence is a complicated one. Surely, there is a growing market of companies offering private companies advice

about how to retaliate, or 'hack back'. And the Macron campaign in France, alert to Russian intervention, mounted a suggestive counterattack, flooding phishing emails with junk to distract the perpetrators.

- For countries, the guidance is probably that of Hippocrates – do no harm. That especially applies especially to the United States, given its dependence on the virtual realm, hence vulnerability. More often than is comfortable, it may have to emulate Lyndon Johnson's line about the mule in the rain, just standing there and taking it. Prevention and defence, then remediation and attribution are critical. Retaliation will most often take the form of naming and shaming, perhaps accompanied by indictments of foreign perpetrators who aren't likely to be extradited.
- In any case, the great strength of the Western democracies is their free media, and so the last thing they should want to do in retaliation is emulate Putin in ways that compromise or discredit those media engaged in telling true news, not fake.
- Finally, while autocracies, like Russia, have advantages in the cyber realm, shamelessness among them, they are hardly ten feet tall. The Russians were sloppy enough in both the American and French elections to raise the question: Did they want us to know what they were doing, perhaps as a demonstration of their capability?

Notes

- 1 See Andrew Weisburd, Clint Watts and J. M. Berger, 'Trolling for Trump: How Russia Is Trying to Destroy Our Democracy', *War on the Rocks*, 6 November 2016. <https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/>.
- 2 This paper draws on work by colleagues – commentary by Ydir Vissers and a paper by David Patterson.
- 3 Patrick Cullen, *Hybrid Threats as a 'Wicked Problem' for Early Warning*, Hybrid COE Strategic Analysis, 4 June 2018. <https://www.hybridcoe.fi/publications/strategic-analysis-may-2018-hybrid-threats-new-wicked-problem-early-warning/>.
- 4 As reported in Manjoo Farhad, 'What Reality TV Teaches Us About Russia's Influence Campaign; State of the Art', *New York Times (international edition)*, 8 November 2017. <https://www.nytimes.com/2017/11/08/technology/russia-election-reality-tv.html>.
- 5 The study was, alas, classified. For an unclassified version of part of it, see Gregory F. Treverton, *New Tools for Collaboration: The Experience of the U.S. Intelligence Community*, Center for Strategic and International Studies, 29 January 2016. <https://www.csis.org/analysis/new-tools-collaboration>.
- 6 For details on the hack and how it was discovered, see Brendan I. Koerner, 'Inside the Cyberattack That Shocked the US Government', *Wired*, 18 October 2016. <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>.
- 7 On the challenge of formulating a response to major attacks, see Tobias Feakin, *Cyber Brief: Developing a Proportionate Response to a Cyber Incident*, Council on Foreign Relations, August 2015. https://www.cfr.org/sites/default/files/pdf/2015/08/Proportionate_Response_CyberBrief.pdf.

- 8 BBC News, 'Putin Deplores Collapse of USSR', *BBC News*, 25 April 2005. <http://news.bbc.co.uk/2/hi/4480745.stm>; and Kattie Sanders, 'Did Vladimir Putin Call the Breakup of the USSR "the greatest geopolitical tragedy of the 20th century?"', *PolitiFact*, 6 March 2014. <https://www.politifact.com/factchecks/2014/mar/06/john-bolton/did-vladimir-putin-call-breakup-ussr-greatest-geop/>. The English version from the Kremlin archives uses the word 'disaster'. The Associated Press translation substituted 'catastrophe'.