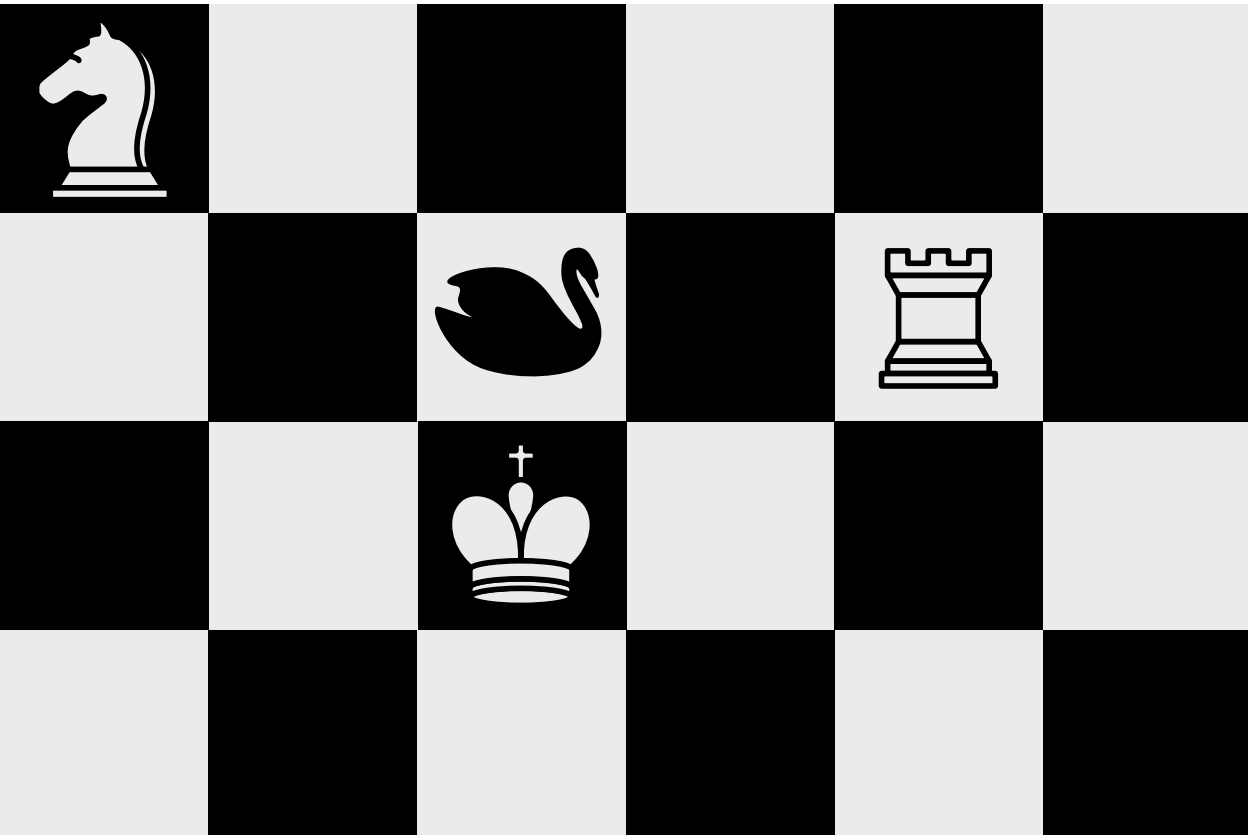
Addressing Hybrid Threats



Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue

Swedish Defence University

CATS
Center for Asymmetric Threat Studies

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Addressing Hybrid Threats

Swedish Defence University
CATS
Center for Asymmetric Threat Studies
Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Addressing Hybrid Threats

Authors:
Gregory F. Treverton
Andrew Thvedt
Alicia R. Chen
Kathy Lee
Madeline McCue

Swedish Defence University
CATS
Center for Asymmetric Threat Studies
Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Title: Addressing Hybrid Threats

Authors: Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue

Printed by: Arkitektkopia AB, Bromma 2018

ISBN 978-91-86137-73-1

For information regarding publications published by the Swedish Defence University, call +46 8 553 42 500, or visit our web site www.fhs.se

Please note that most of the text in this book by US based authors has been written in accordance to American English spelling and grammar rules with exceptions being where organizations use British English and direct quotes are given.

Contents

Preface

Hybrid threats have become the 21st security challenge for Western countries. They reflect significant change in the nature of international security. Change tends to increase feelings of insecurity and, historically, frictions in society, all the more so because hybrid threats are complex and ambiguous. Some people look to the past for answers, while others have forgotten the past. There are those who argue more vigorously for adapting to change, and there are those who try to defend the status quo. In some cases facts turn into views, opinions and perspectives – or worse, vice versa. This means that the picture of the security environment is not simply black or white. It is complex, multi-layered and multi-dimensional. Thus, analysis of what has changed, how it is changed and what does it mean for democratic states is at the core of understanding the nature of the current security environment in Europe.

Six major changes are driving hybrid threats to the fore. The first is the changing nature of world order. The post-Cold War era has come to an end. Relational power – that is the power to change others' beliefs, attitudes, preferences, opinions, expectations, emotions and/ or predispositions to act – is today more important than material power. Relations in international politics are being renegotiated since great and middle powers, in particular, seek to increase their status and extract benefits.

Second, the world sees a new type of network-based action, the dark side of globalization. The internal and external dimensions of security are interconnected more strongly than they have been in recent decades This favors weaker state and non-state actors, for the networks amplify the influencing attempts and give the weaker actors tools of power. The role of the nation-state is called into question, as are alliances with norms and rules that limit responses to asymmetric antagonistic actions.

Third, fast developing technologies, a literal revolution, give rise to new domains like cyber space where national and international rules of the game have yet to be

created. Space is no longer a frontier, but an operating realm, which also presents a challenge to traditional security thinking. In general, new technology provides new tools for influencing.

In particular, the changing domain of information space, and the media landscape, is the fourth major change affecting today's security environment. Digitalization and social media as new opinion builders have changed the speed with which information travels, the way information is produced and the way people are connected across national borders. This change has brought forward the need to understand different political and strategic cultures because information produced in one country can be interpreted in other, very different ways elsewhere. Likewise, the gatekeepers of information are changing. The Internet has become a new battlefield where rules are still being formulated. Fake news, content confusion and opinion-based "facts" agitate the public domain. Trust, one of the fundamental pillars of functioning societies, is eroding.

The fifth change is the changing nature of conflict and war. In today's wars, soldiers should not die and civilian casualties should be avoided. This has led to the debate about the blurred lines between war and peace. This situation presents challenges for traditional military forces as well as for traditional internal law enforcement. It also drive hybrid threats, which seek to stay below open conflict. They are contests between societies, not armies.

Finally, there is generational change. We have left behind the Cold War and even the post-Cold War era. The Cold War had two very distinct features, which underpinned a clear world order: superpower relations – and the ideological struggle between communism and capitalism – dominated, while the fear of nuclear war guided many security policy decisions. During the post-Cold War era, globalization, emphasizing ideas of integration and interdependence, became the fashionable way of describing the world. Today's new generation is a digital generation informed by two contradictory trends – cosmopolitanism and neo-nationalism. Historical memory also changes along with generations, which leaves space for the political manipulation of historical events.

This report, *Addressing Hybrid Threats,* put together by Gregory F. Treverton and his team gives us a rich understanding of what we mean when we talk about hybrid threats – what kind of threats we are facing and what tools are being used against the democratic states. We would like to thank especially Dr. Treverton for agreeing to take on this task and provide his in-depth knowledge and experience, which will be valuable in the future work of the CATS and Hybrid CoE.

Lars Nicander
Director
The Center for Asymmetric Threat Studies

Matti Saarelainen
Director
The European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE

Summary

Russian "little green men" in Ukraine; Russian hacks into the email server of the U.S. Democratic National Committee (DNC); protest and counter-protest over a mosque in Houston, with both sides fake and organized by Russian trolls: these are hybrid threats in the 21st century. Most of them are not strikingly new. The exception is the virtual or digital realm, which empowers new tools and lowers the entry cost of using them – think of web posts by comparison to planting articles in traditional newspapers. The goal of hybrid threats is to achieve outcomes without actual war, and this report focuses on tools short of actual combat. The target is opposing societies, not combatants. Thus, the distinction between combatants and citizens, blurring for decades, breaks down almost entirely. And the tactic is the *simultaneous* employment of the range of possible instruments, from threats of war to propaganda and everything in between.

The focus of attention, and of this report, is Russian hybrid warfare, for good reason: it has been the most active and most brazen. An analysis by the German Marshall Fund's Alliance for Securing Democracy found that the Russian government has used cyberattacks, disinformation, and financial influence campaigns to meddle in the internal affairs of at least 27 European and North American countries since 2004. To be sure, other countries have not been strangers to hybrid threats, and this report will discuss those uses as well.

The range of hybrid tools is wide, as illustrated by this report's two case studies on Ukraine and the operations in the 2016 U.S. elections. Table 1 lays out the range:

Table 1: Range of Hybrid Tools

Tool	Salient Points
Propaganda	Enabled and made cheaper by social media, also targeted at home.
Fake news	"Lisa" was portrayed as a Russian-German raped by migrants.
Strategic leaks	Macron emails leaked 48 hours before the 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: • Espionage • Attack • Manipulation	New tool in arsenal: espionage is old tactic with new, cyber means. Attack has targeted critical infrastructure, notably in Estonia in 2007. Manipulation is next frontier, changing information without the holders know it.
Economic leverage	China sought to punish South Korea for accepting U.S. anti-missile system.
Proxies and unacknowledged war	Hardly new, but "little green men" in Ukraine slid into actual combat.
Paramilitary organizations	Russian "Night Wolves" bikers intimidate civilians.

Both the Ukraine and U.S. elections cases drive home the point that hybrid attackers did not create the vulnerabilities they exploited. Ukraine's political and economic circumstances made it extremely vulnerable to Russian actions, and the deeply polarized American political context of 2016 was an open invitation to Russian meddling. One dimension of vulnerability is proximity and access – plain in the case of Ukraine. A second is societal and political fault-lines: again, this was most obvious in Ukraine, where almost a third of the populations was Russian-speaking. Another fault-line may be generational, with younger people far from memories of the Cold War but very close to social media. So, too, Moscow may have tried to create the warring demonstrations in Houston, but the divide it played on was real.

For Russia, hybrid threatening *is* its strategy. Vladimir Putin has been crystal-clear about his strategic objectives – to dominate Russia's "near abroad" and to see Russia recognized as a major global power. Russia sees the United States and NATO as the leading challenges to its interests and security, especially since 2012, but knows it would lose any major military confrontation. So, too,

it cannot win an economic competition; its Eurasian Economic Union is hardly likely to be a pole of attraction. As a result, Russia seeks to create confusion, chaos and uncertainty among the institutions of its adversaries. It will work to have people, especially inside Russia, look to the West and say "see the West, they are just as corrupt and just inept as you think Russia is. Yet, look at us, we held our ground in Syria, we took back the Crimea our rightful territory, we protect ethnic Russians in Belarus and the Ukraine."

For other nations engaging in hybrid threats, the goals are less clear, and probably more opportunistic. For China, the aims are to distract from, say, its actions in the South China Sea. It has concentrated on cyber tools, pursuing some combination of espionage, signaling capabilities or preparing to add cyber friction in the event of conflict. For instance, Chinese allegedly conducted crippling DDoS attacks against Filipino government networks after the International Court of Justice in The Hague rejected China's historical territorial claims. For other nations, like Saudi Arabia and the emirates feuding in the Gulf, hybrid threats are a relatively low cost, low risk way to signal capabilities or embarrass opponents.

In thinking about the future, the virtual realm has dramatically lowered the cost of propaganda, and cyber operations are also relatively cheap. Those attributes will make the tools all the more attractive to Russia as its economy declines, and they will also tempt other nations. Advancing technology will surely open new opportunities for hybrid threateners. For instance, the planted posts, tweets and bots so far have been almost entirely text. But that will change: technology, especially Artificial Intelligence, is making it easier to fake someone speaking. This will take fake news into the realm of audio and video, which in turn will complicate the task of attributing, and responding to, fake propaganda.

At the upper level of hybrid threats, the future will see, as in Ukraine, new combinations of cyber and kinetic operation. Imagine targeted soldiers receiving a demoralizing message, like those spammed to Ukrainian soldiers. Ten minutes later, the soldiers' compromised phones access recent contacts and send "killed in action" messages to their families. Shortly after, their families keep calling the soldiers, distracting them from duty. Another demoralizing message – "retreat and live" – is followed by the shift from cyber to kinetic action as the compromised phones reveal the soldiers' location' and they are targeted by a massive artillery strike.

In responding, the first imperative is perhaps the Hippocratic oath: do no harm. Open societies are inherently vulnerable, yet it is imperative that they stay open. All of the national good practices in preparing for, and countering, hybrid threats share a number of features:

- They are "whole of government," indeed "whole of society."
- As suggested earlier, vulnerability assessment is the starting point.
- They pay special attention to, especially, the cyber realm. Hybrid threats is a very good one among several reasons to be more serious about cyber defenses

- They are creative in reaching out to the private sector. That is imperative in the cyber realm, where infrastructure assets to be protected are in private hands. But Estonia's Cyber Defence Unit, part of the larger, and volunteer Estonian Defence League is suggestive of the possibilities, as is the help that private sector analysts provided in the U.S. elections case.
- They depend on shared situational awareness. In some countries, that has required changing laws to give intelligence services somewhat more authority to collect information, both inside and outside the country.

The three watchwords in defending against the weaponized information of hybrid threats are awareness, metrics, and responses. The Western nations had been focused on technical threats in cyberspace. As a result, the propaganda dimension of the Russian intervention in the U.S. elections in 2016 came as a surprise, even though it shouldn't have. A group of outside analysts tracking the online dimensions of the jihadists and the Syrian civil war came upon interesting anomalies, as early as 2014, and made the connection to Russia. Now, the Western nations are aware of the threat, as the French elections campaign demonstrated.

Second, it is important to respond quickly to particular information operations, once discovered, both to minimize their impact and to deter other states or groups that might want to emulate the attack. To be sure, chasing every false fact is impossible, but the Macron campaign illustrates the value of countering fake news as fast as possible.

Practitioners and researchers emphasize a number of points in thinking about how to respond:

- *Again, respond with the whole of government – and beyond.* Preparing for hybrid threats cannot be left to the defense ministry alone. For all the limits on what governments can – and should – do, the history of the American radios broadcasting into the Communist countries during the Cold War is worth mining. In retrospect it was more successful than its operators thought at the time.
- *Be skeptical of metrics.* For all the concern, thus far Russia operations in Europe seem to have had most effect on those who were already sympathetic to Moscow.
- *Be careful about targets.* It is worth noting, for instance, that the first target of Russian operations is the Russian people.
- *Play on strength.* Time and again, the same point arises: a great strength of the Western democracies is their free presses. That argues against mimicking adversaries by circulating fake news or undermining the credibility of quality journalism.
- *Recognize the contest is a long one.* The distinction between peace and war is indeed blurred. There are likely to be neither unconditional surrenders nor unqualified victories.

- *Work with target countries.* This might focus on building transparency and fighting corruption, and on internal security reform and defense institution-building. Here, there is considerable post-Cold war experience on which to draw.
- *The Russians are coming.* The U.S. case makes plain that the Russians have both will and capacity to intervene in other nations' elections.
- *Thus, pay close attention to early warning.* The FBI, apparently, warned the DNC in the fall of 2015 of potential hacks into its information systems. It did not, however, make clear that it suspected these were Russian-government sponsored operations. By contrast, and no doubt partly because of the U.S. case, the Macron campaign in France was attentive to hacking and cyber security at least from December 2016, the first round of the election.
- *Tighten links across the public-private divide.* This is a great challenge of the cyber realm in any case. It is easier with regard to elections to the extent that elections plainly are a public good and a government responsibility.
- *Likewise, pay close attention to the infrastructure of elections.* The decentralization of election machinery in the United States was probably an operational advantage (if a forensic liability), for it complicated the attackers' challenge. In any case, the danger of being hacked is increased the more voting is virtual (and the less there are ways to check results after the fact in the way that paper ballots did).
- *In the end, though, the Russians aren't ten feet tall.* For instance, in early 2017 when Russia made allegations of rapes in the Baltic by NATO soldiers, Germans to boot, Lithuania was ready. Its parliament immediately dismissed the story as spurious. And the Macron campaign's "counter-offensive" at least demonstrates that those attacked have options.

Chapter 1: Defining the Issues

- Pro-Kremlin Russian media soon labeled the Russian troops that had moved into Crimea as "little green men," "polite people," or even "polite, armed men," despite wearing unmarked military fatigues and bearing arms.
- As fighting flared in Eastern Ukraine, Ukrainian soldiers were subjected to a barrage of spam messages on social media: "Your battalion commander has retreated. Take care of yourself," or "You will not regain Donbas back. Further bloodshed is pointless," or "Ukrainian soldier, it's better to retreat alive than stay here and die."
- In 2015 and 2016, the U.S. Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC), and the Hillary Clinton campaign were all targeted by Kremlin-sponsored cyber espionage operations, CozyBear and FancyBear, linked to Russian intelligence. The documents and information stolen from these networks were then shared via a persona and website created by the Russian government, Guccifer 2.0 and DCLeaks.com, and later via Wikileaks and mainstream media outlets.
- In May 2016, 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. "Stop Islamization of Texas," it cried. But the 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.

These are hybrid threats, twenty-first century style. Most of them are not strikingly new. With one exception, they differ from previous conflict more in degree than in kind. That exception is the virtual or digital realm, which empowers new tools

and lowers the entry cost of using them – think of web posts by comparison to planting articles in traditional newspapers. Otherwise, what distinguishes this century's hybrid threats is that they have taken to a new point trends that have been visible. The goal is to achieve outcomes without actual war. The target is opposing societies, not combatants. Thus, the distinction between combatants and citizens, blurring for decades, breaks down almost entirely. And the tactic is the *simultaneous* employment of the range of possible instruments, from threats of war to propaganda and everything in between.

In that sense, speaking of hybrid "threats" rather than "warfare" is apt. "Warfare" conjures up armies and bullets. Those surely are at one extreme of hybrid threats in the twenty-first century, but this inquiry is much broader, looking at combinations of kinetic warfare with psychological and cyber operations. By one definition, hybrid threats mean "using multiple instruments of power and influence, with an emphasis on nonmilitary tools, to pursue its national interests outside its borders." [1] The term appeared at least as early as 2005, and was used specifically to describe Hizbollah's strategy in the 2006 war with Israel. Indeed, since there are so many kindred terms for it, and have been through the years, it probably makes sense not to focus on the definition but rather to pay most attention to the specific threats and interconnections involved now – and into the future.[2]

The focus of attention, and of this report, is Russian hybrid warfare, for good reason: it has been the most active and most brazen. An analysis by the German Marshall Fund's Alliance for Securing Democracy found that the Russian government has used cyberattacks, disinformation, and financial influence campaigns to meddle in the internal affairs of at least 27 European and North American countries since 2004.[3] To be sure, other countries have not been strangers to

---

1 Christopher S. Chivvis, "Understanding Russian 'Hybrid Warfare' And What Can Be Done About it," RAND, March 22, 2017, 1, available at https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf. The Center of Excellence definition is: "Hybrid threats can be characterized as coordinated and synchronized action that deliberately targets democratic states' and institutions systemic vulnerabilities, through a wide range of means. Activities exploit the thresholds of detection and attribution as well as the border between war and peace. The aim is to influence different forms of decision making at the local (regional), state, or institutional level to favor and/or gain the agent's strategic goals while undermining and/or hurting the target.

2 See Damien Van Puyvelde, "Hybrid War – Does It Even Exist?" NATO Review, 2015, http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/.

3 As reported in *Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security,* Minority Staff Report Prepared for the Use of the Committee on Foreign Relations, United States Senate, 115 Cong., 2 sess., January 10, 2018, 38, available at https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf. Hereafter cited as "Putin's Asymmetric Assault."

hybrid threats, and this report will discuss those uses as well. As practiced by Russia, hybrid operations illustrate features that are not new with Russia but strikingly present in those operations. They economize on the use of force; Russia "prefers to minimize the actual employment of traditional military force."[4] They are persistent and thus break down the traditional binary delineations between war and peace. They are aimed not at armies but at people, seeking "to influence the population of target countries through information operations, proxy groups, and other influence operations." Russia operations generally seek to capture territory without overt or conventional military force; to create a pretext for overt, conventional military action, and to influence the politics and policies of countries in the West.

Thus, the framework in this inaugural report for thinking about hybrid threats begins with *tools* an adversary might employ, then turns to *vulnerabilities* of the defending state, and to *objectives* the adversary might seek.[5] Other frameworks emphasize the phases of hybrid campaign.[6] Yet since the essence of hybrid warfare is simultaneity, the phases are bound to be opportunistic, depending on how the campaign goes.[7]

To make the discussion concrete, the next two sections provides capsule summaries of two hybrid threats in action – Russian interventions in Crimea and Ukraine beginning in 2013, and in the 2016 U.S. presidential election, with a side-look at similar Russian operations leading up to the 2017 French elections. The report then turns to a careful parsing of the tools, with examples from a number of countries, then does the same for vulnerabilities. Then, it turns to objectives. The section after that looks to the future: where might hybrid threats go, what new tools or techniques might they encompass? It looks at some scenarios. The penultimate section outlines best practices in the responses of many nations, and the concluding section offers recommendations.

---

4 Civvis, 2

5 This is similar to the framework outlined in MCDC Countering Hybrid Warfare Project, *Understanding Hybrid Warfare,* 2017, p. 8, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf. Hereafter cited as "Understanding Hybrid Warfare." Its third leg is linear and non-linear effects of a hybrid warfare attack.

6 See, for instance, the Gerasimov model, in Robert R. Leonhard, Stephen P. Phillips, and the Assessing Revolutionary and Insurgent Strategies (ARIS) Team, *Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014*, United States Army Special Operations Command, June 2015, http://www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf. Hereafter cited as "Little Green Men."

7 In a near-comic irony, the Helsinki COE was itself the target of hybrid threats. See "Hybrid Threats Target Center to Counter Hybrid Threats," available at https://medium.com/dfrlab/hybrid-threats-target-center-to-counter-hybrid-threats-e7d0160d8b3.

Chapter 2: Hybrid Threats in Action: Russia's Interventions in Crimea and Ukraine

At a 2008 NATO meeting in Bucharest, Russian President Vladimir Putin told U.S. President George Bush "You don't understand, George, that Ukraine is not even a state. What is Ukraine? Part of its territories is Eastern Europe, but the greater part is a gift from us."[8] Despite Putin's words, Ukraine has indeed been a state since achieving independence from the U.S.S.R. on December 1, 1991.[9] His comments do, however, reveal the Russian sentiment towards their neighboring country. And following the ousting of pro-Russian Ukrainian President Viktor Yanukovych, Russia annexed the Ukrainian territory of Crimea, on March 18, 2014.[10] In the month leading up to the decision, Russia launched a hybrid campaign which included covert operations, information warfare, and eventually a conventional invasion to take control of the peninsula. Simultaneously, it conducted a campaign in the eastern Ukrainian regions of Donetsk and Luhansk with a mix of political warfare, support of paramilitary groups, and conventional forces. Appendices provide more background on events leading to Yanukovych's dismissal and more detail on Russia's two campaigns – one more traditional in Crimea and the other more hybrid in Eastern Ukraine.

---

8 James Marson, "Putin to the West: Hands off Ukraine," *Time*, May 25, 2009, http://content.time.com/time/world/article/0,8599,1900838,00.html.

9 Ukraine's history under Soviet rule was particularly brutal. Collectivized agriculture created led to the Holodomor, a famine that killed an estimated seven to ten million people.

10 Will Englund, "Kremlin Says Crimea Is Now Officially Part of Russia after Treaty Signing, Putin Speech," *The Washington Post*, March 18, 2014, https://www.washingtonpost.com/world/russias-putin-prepares-to-annex-crimea/2014/03/18/933183b2-654e-45ce-920e-4d18c0ffec73_story.html.

Protests erupted in the fall of 2013 in Kiev's Independence Square (the Maidan Nezalezhnosti) after President Yanukovych suspended preparations to sign the Association Agreement with the European Union (EU) under its Eastern Partnership program.[11] Yanukovych's decision was a sudden reversal – he had previously indicated a willingness to formalize integration with the EU (likely in response to his rising unpopularity).[12] In Kiev's central square, the pro-Western protests, known as Euromaidan, began without violence and within days 100,000 protesters were on the streets.[13] But amid growing protests and calls for Yanukovych's resignation, the government response and protests turned violent. On February 22, three months after his reversal regarding the Association Agreement, the protesters got their wish as parliament voted to "remove Viktor Yanukovych from the post of president of Ukraine."[14]

Yanukovych's removal was as sudden as his initial change of heart, taking Western and Russian policymakers alike by shock.[15] The results – losing the pro-Russian Yanukovych as a partner in Kiev at the hands of pro-Western protesters – were disastrous for the Kremlin. The reality of this geopolitical defeat was only compounded by Russian suspicions of a U.S. plot to turn Ukraine into a satellite state.[16] Given Ukraine's strategic importance to Russia, both real and perceived, Russian leadership did not wait to reassert the influence over its neighbor that had begun slipping away.

The Kremlin mounted two distinct and simultaneous campaigns in Ukraine. In Crimea, Russia launched an invasion and a propaganda campaign, annexing the territory in March. Pro-Russian demonstrations began the day after Yanukovych's removal and by March 1 the peninsula had been seized, with the Ukrainian government no longer in control of the region.[17] In Eastern Ukraine, Russia

---

11 The Association agreement "was a symbol of hope for those Ukrainians (well represented in the country's central and western regions) who dreamed of integrating with Europe, but not for those (chiefly in the south and east) who favored retaining close ties with Russia." See Rajan Menon, and Eugene Rumer. *Conflict in Ukraine: The Unwinding of the Post-Cold War Order*. MIT Press, 2015.

12 Little Green Men, 28.

13 Jill Langlois, "More Than 100,000 Protests in Ukraine over EU Agreement Delay," *Public Radio International*, November 24, 2013, https://www.pri.org/stories/2013-11-24/more-100000-protest-ukraine-over-eu-agreement-delay.

14 "Ukrainian MPs Vote to Oust President Yanukovych," *BBC News*, February 22, 2014, http://www.bbc.com/news/world-europe-26304842.

15 Menon, *Conflict in Ukraine,* Loc 842.

16 See headlines from RT such as "'CIA fingerprints' all over Kiev massacre – Oliver Stone," https://www.rt.com/news/218899-stone-kiev-massacre-cia/; "Dozens of FBI, CIA agents in Kiev 'assisting Ukrainian security'," https://www.rt.com/news/156692-ukraine-cia-fbi-agents/; and "Moscow: Kiev and western sponsors directly responsible for bloodshed in E. Ukraine," https://www.rt.com/news/156596-moscow-kiev-bloodshed-responsible/.

17 Kathy Lally, William Booth and Will Englund, "Russian forces seize Crimea; Ukraine's interim president decries 'aggression'," *The Washington Post,* March 1, 2014, https://www.washingtonpost.com/world/a-deeply-concerned-obama-warns-russia-against-action-in-crimea/2014/03/01/c56ca34c-a111-11e3-a050-dc3322a94fa7_story.html.

supported a subversive political movement that grew into an armed insurgency. Russian troops were massed on Ukraine's border, weapons and fighters were dispatched in Eastern Ukraine, and self-proclaimed republics were established in Donetsk and Luhansk. When it appeared that Kiev's forces were on the verge of defeating the separatists in the East, Russia intervened with military personnel, weapons, and supplies, pushing the pro-Kiev forces back.[18]

In both Crimea and Eastern Ukraine, Russia adapted to the events as they were unfolding.[19] Though the tools they employed and the objectives they sought in each case were markedly different, both serve as useful cases for understanding Russia's hybrid threats – which culminated in hybrid warfare in Ukraine. Intervention in Crimea was unquestionably a success: Russia was able to secure the surrender all Ukrainian military bases in Crimea in less than a month without firing a shot.

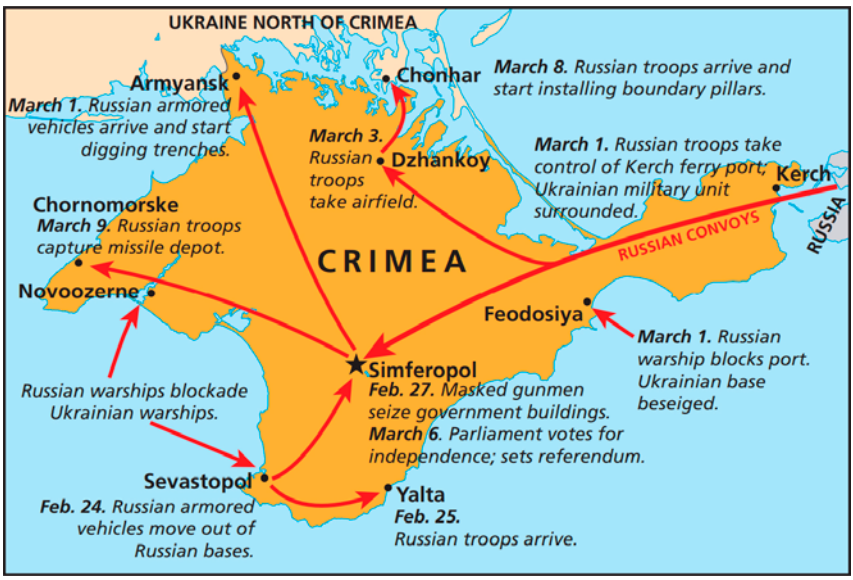


Figure 1: Russian Actions in Crimea.[20]

18 Menon, Conflict in Ukraine, Loc 890.

19 Putin admitted the decision to annex Crimea (and rescue Yanukovych) was made at an all-night meeting on February 22, the same day Yanukovych was removed from office. See "Putin reveals secrets of Russia's Crimea takeover plot," *BBC News*, March 9, 2015, http://www.bbc.com/news/world-europe-31796226. Furthermore, the events that unfolded "suggests that the decision to annex Crimea was not made well in advance. However, operations in Crimea did involve a preplanned covert action, which enabled a conventional invasion." Similarly, "Russia's efforts in Eastern Ukraine proved to be a series of improvisations in response to resistance and friction when the initial political warfare effort foundered." See Michael Kofman and others, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, RAND Corporation, 2017, https://www.rand.org/pubs/research_reports/RR1498.html.

20 Kofman, Lessons from Russia's Operations, Figure 2.1, 7.

2.1 Taking Crimea

On February 22, 2014, battalions of Spetsnaz (elite Russian military intelligence infantry) and Vozdushno-Desantnye Voyska (Airborne Forces or VDV) began mobilization.[21] Two days later, the city council of Sevastopol installed Aleksei Chaliy, a Russian citizen and businessman, as mayor.[22] Naval units arrived in the city square in armed personnel carriers and 200 special forces arrived on February 25 by way of Alligator-class landing ship. These troops were Special Operations Command [KSO], a small unit designed to operate "independently and abroad."[23] In order to mask further movement of troops, Russia launched a snap exercise.[24]

The military exercises on February 26 involved 150,000 troops from the Western and Central Military Districts. An exercise of that size not only flexed Russia's military muscles but also drew attention away from Crimea, where special forces had begun operating and seizing strategic locations. The next day, KSO special forces, VDV, and Spetsnaz, claiming to be a local "self-defense militia," barricaded themselves inside the Crimean Parliament building and raised the Russian flag.[25] While the building was held, the Crimean parliament voted for holding a referendum on Crimea's status on May 25, the same day as Ukraine's presidential elections.

Pro-Kremlin Russian media soon labeled the Russian troops as "little green men," "polite people," or even "polite, armed men," despite wearing unmarked military fatigues and bearing arms.[26] Over the next few days, unmarked special forces expanded their control in Crimea, surrounding Belbek air base, seizing Simferopol airport, and closing Crimean border crossings. Meeting little resistance, they were able to quickly surround and take over strategic facilities.[27] Within a day, three-fifths of Ukrainian Air Defense units in Crimea were in Russian

21 Kofman, Lessons from Russia's Operations, 7.

22 Howard Amos, "Ukraine: Sevastopol installs pro-Russian mayor as separatism fears grow," *The Guardian,* February 25, 2014, https://www.theguardian.com/world/2014/feb/25/ukraine-sevastopol-installs-pro-russian-mayor.

23 Kofman, Lessons from Russia's Operations, 8.

24 Steve Gutterman, "Putin puts troops in western Russia on alert in drill," *Reuters*, February 26, 2014, http://www.reuters.com/article/us-ukraine-crisis-russia-military-idUSBREA1P0RW20140226.

25 Harriet Salem, Shaun Walker, and Luke Harding, "Conflict fears rise after pro-Russian gunmen seize Crimean parliament," *The Guardian*, February 28, 2014, https://www.theguardian.com/world/2014/feb/24/ukraine-crimea-russia-secession.

26 Vitaly Shevchenko, "'Little green men' or 'Russian invaders'?" *BBC News*, March 11, 2014 http://www.bbc.com/news/world-europe-2653215.

27 *Ibid*.

hands.[28] The same day, on March 1, Putin requested parliamentary approval to use troops in Ukraine to protect the Black Sea Fleet and ethnic Russians who faced "real threats to [their] life and health."[29]

On March 1, Sergei Aksenov, Crimea's new premier, "decided to speed up the holding of the referendum on the status of the Autonomous Republic of Crimea," from May 25 to March 30.[30] With a Russian naval blockade further bottling up Ukraine, Denis Berezovsky, the recently appointed commander of the Ukrainian navy, appeared on television to announce his defection.[31] On March 6, a Russian Ochakov Kara-class cruiser blocked the exit to the Black Sea.[32] That same day, parliament again moved up the date of the referendum. This time it was set to be held on March 16, 2014.[33] Over the next week, Russian forces continued to seize Ukrainian military bases in Crimea without much resistance, taking the Ukrainian naval air base at Novofedorovka. The 12th Motor Rifle Brigade entered Crimea from the east.[34]

At this stage, Russian troops began psychological pressure alongside an information operation to prompt defections of Ukrainian troops and officers. Russian troops reached agreements with Ukrainian soldiers trapped inside bases on the Crimean peninsula to continue the sieges without escalating violence.[35] Russian forces sealed off Crimea; physically with troops at northern crossing points and by cutting landline communication, jamming signals, and cutting off electricity to some bases. Russian forces continued to solidify their hold on Crimea until Ukrainian forces were evacuated. With effective control over the peninsula, all that remained was the referendum scheduled for March 16.

---

28 Roger McDermott, *Brother Disunited: Russia's Use of Military Power in Ukraine,* U.S. Army Foreign Military Studies Office, 2015, 11, available at https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/197162. Hereafter cited as Brothers United.

29 "Putin: Russian citizens, troops threatened in Ukraine, need armed forces' protection," *RT*, March 1, 2014, https://www.rt.com/news/russia-troops-ukraine-possible-359/.

30 Sergei L. Loiko, "New Crimea leaders move up referendum date," *Los Angeles Times*, March 1, 2014, http://articles.latimes.com/2014/mar/01/world/la-fg-wn-crimea-referendum-date-20140301.

31 Shaun Walker, "Ukraine navy officers reject plea to defect to Russian-backed Crimea," *The Guardian*, March 3, https://www.theguardian.com/world/2014/mar/03/ukraine-navy-officers-defect-russian-crimea-berezovsky. The day after Berezovsky's defection, he met with their new commander in chief, Serhiy Haiduk, and officers in their Sevastopol headquarters. Urging further defections, the former commander in chief parroted the Russian message "The seizure of power in Kiev was orchestrated from abroad." An officer reportedly responded, "In what way exactly did foreign powers intervene in Kiev, compared to the way they are intervening now in Crimea?"

32 McDermott, Brothers Disunited, 12.

33 Carol Morello and Anthony Faiola, "Crimea sets referendum on joining Russia," *The Washington Post*, March 6, 2014, https://www.washingtonpost.com/world/crimea-sets-referendum-on-joining-russia/2014/03/06/d06d8a46-a520-11e3-a5fa-55f0c77bf39c_story.html.

34 McDermott, Brothers Disunited, 12.

35 Kofman, Lessons from Russia's Operations, 9.

Voters overwhelmingly voted to join Russia. According to Crimean election officials, 83.1 percent of eligible voters participated, with 96.77 percent voting in favor of joining Russia.[36] Only 2.51 percent voted against. The results were highly disputed, and many American and European officials criticized the referendum as illegitimate.[37] The Kremlin recognized Crimea as a sovereign state, after the parliament requested Russia "admit the Republic of Crimea as a new subject with the status of a republic."[38] On March 21, 2014 Crimea was formally annexed by the Russian Federation.[39]

The Crimea operation was more a conventional military take-over than a hybrid operation; surely the Russians do not think of it as the latter. However, while Russian troops were conducting operations in Crimea, the Kremlin was also pursuing an information campaign targeted at the Russian public and Crimean residents. During the seizure of Crimea, the information campaign had three objectives.[40] First was to discredit the new government in Ukraine, which was often referred to as a "fascist junta." Given that the regime in Kiev was almost immediately labeled as fascist by pro-Russian demonstrators in Crimea, Russia was likely organizing, or even leading, the protests and their messages.[41] Russia also sought to highlight the danger faced by ethnic Russians in Ukraine. Finally, the Kremlin emphasized the broad support for Crimea's return to Russia. With tight control over the domestic media, the Kremlin was able to effectively determine Russian opinion regarding the events in Crimea. In 2013, RIA Novosti and Voice of Russia, two state owned media agencies, had been replaced by *Russia Today*, further tightening the government's propaganda machine.[42]

Following Yanukovych's removal, Russia increased its messaging that the change of regime in Kiev was illegitimate and that ethnic Russians were in danger. In Eastern Ukraine and Crimea, most people watched Russian television as their main source of news, preferring it to Russian-language alternatives in Ukraine. Moreover, on March 9, Russian troops turned off Russian-language programming, leaving Russian channels as the only options.

---

36 Carol Morello, Will Englund, Griff Witte, "Crimea's parliament votes to join Russia," *The Washington Post*, March 17, 2014, https://www.washingtonpost.com/world/crimeas-parliament-votes-to-join-russia/2014/03/17/5c3b96ca-adba-11e3-9627-c65021d6d572_story.html.

37 John Bellinger III and Jonathan Masters, "Why the Crimean Referendum is Illegitimate," *Council on Foreign Relations*, March 16, 2014, https://www.cfr.org/interview/why-crimean-referendum-illegitimate.

38 Aleksandar Vasovic and Adrian Croft, "U.S., E.U. set sanctions as Putin recognizes Crimea 'sovereignty'," *Reuters*, March 16, 2014, https://www.reuters.com/article/us-ukraine-crisis/u-s-eu-set-sanctions-as-putin-recognizes-crimea-sovereignty-idUSBREA1Q1E820140317.

39 "Ukraine: Putin signs Crimea annexation," *BBC News*, March 21, 2014, http://www.bbc.com/news/world-europe-26686949.

40 Kofman, Lessons from Russia's Operations, 13.

41 Little Green Men, 55.

42 Stephen Ennis, "Putin's RIA Novosti Revamp Prompts Propaganda Fears," *BBC Monitoring*, December 9, 2013.

Russia took advantage of a grassroots movement running in opposition to Euromaidan, aptly named *Stop Maidan*.[43] *Stop Maidan's* rallying cry was centered around pro-Russian statements such as ""Crimea for stability," "no to extremism," and "no to foreign interference!"[44] The movement used thousands of billboards and visible ads to amplify its message, which largely aligned with Russia's information campaign. Though the *Stop Maidan* protesters denied any ties to Moscow, varying degrees of connection have been alleged.[45]

Internationally, Russia sought to raise doubts regarding the actual events in Crimea and reinforce its narrative. During a March 4 press conference, Putin stated: "Regarding the deployment of troops, the use of armed forces. So far, there is no need for it, but the possibility remains. I would like to say here that the military exercises we recently held had nothing to do with the events in Ukraine. This was pre-planned, but we did not disclose these plans, naturally, because this was a snap inspection of the forces' combat readiness. We planned this a long time ago."[46] When asked if he considered the "possibility of [Crimea] joining Russia," he answered "No, we do not. Generally, I believe that only residents of a given country who have the freedom of will and are in complete safety can and should determine their future." These false statements – Russia had troops operating in Crimea as early as February 22, 2014 – were part of a broad campaign of public deniability.

The information campaign was deployed *simultaneously and synchronized* with the military campaign. By publicly denying any involvement and deploying troops with unmarked fatigues, Russia maintained at least shred of plausible denial, though those paying close attention understood Russia's role. In general, Russia's information warfare "aims at affecting the consciousness of the masses, both at home and abroad, and conditioning them for the civilizational struggle between Russia's Eurasian culture and the West."[47] Russia's messaging surrounding their annexation of Crimea reflected this goal.

---

43 Kofman, Lessons from Russia's Operations, 15.

44 Tom Balforth, "Scenes from Simferopol: The City the World Is Watching," *The Atlantic,* March 6, 2014, https://www.theatlantic.com/international/archive/2014/03/scenes-from-simferopol-the-city-the-world-is-watching/284286/.

45 Robert Coalson, "Pro-Russian Separatism Rises in Crimea as Ukraine's Crisis Unfolds," *Radio Free Europe Radio Liberty*, February 18, 2014, https://www.rferl.org/a/ukraine-crimea-rising-separatism/25268303.html. Other anti-Maidan protesters have reportedly been paid or forced to participate. See: Allison Quinn, "Why Moscow's anti-Maidan protesters are putting on an elaborate pretence," *The Guardian,* February 26, 2015, https://www.theguardian.com/world/2015/feb/26/russia-anti-maidan-protest-moscow.

46 President of the Russian Federation, Vladimir Putin, "Vladimir Putin answered journalists' questions on the situation in Ukraine," March 04, 2014, http://en.kremlin.ru/events/president/news/20366.

47 Little Green Men, 15.

Finally, Russia used non-military and paramilitary elements to confuse the battlespace. Russian special forces were critical, but other elements were also deployed to give the impression of local support. Russian intelligence organized self-defense units comprised of local militia, Cossacks, and former special police. Russian troops also began to wear police uniforms to disguise themselves as part of the local security forces. Volunteers included army veterans, boxers, and members of the biker gang "Night Wolves."

It is also worth noting features that made Ukraine particularly vulnerable in Crimea. In particular, the Russian Black Sea Fleet created a base from which Russia was able to launch operations in Crimea and reinforce its position. Russia masked activity under the guise of troop "reinforcement," which contributed to plausible denial.[48] A history of Russian troops based on the peninsula also contributed to their acceptance by the local population. Indeed, Russia was allowed up to 25,000 troops under the basing agreements for the Black Sea Fleet. This history provided a legitimate excuse for snap exercises along the border, which provided cover for Russian troop movements.

Militarily, Ukraine was in no position to respond. Its military personnel in Crimea numbered between 18,800 and 22,000, predominantly naval personnel with some air defense and Interior Ministry members.[49] Moreover, given the Cold War legacy of confronting NATO, its military bases are positioned on the western side of the country, away from Crimea and Russia. This made it difficult for Ukraine to mount an effective counterattack. Furthermore, prior to the conflict Ukraine's forces were in "terrible condition" even had they been in a better position to respond.[50]

The large number of ethnic Russians and Russian-speaking Crimeans contributed to Russia's success. The Ukrainian government also made missteps that deepened this vulnerability – for instance, down-grading the official status of the Russian language.[51] On the ground, the decision alienated ethnic Russians living in Crimea, which constitute the majority of the peninsula's population.[52] In the information space, Russian officials presented the decision as a "violation of ethnic minority rights," and RT amplified this message.[53]

---

48 McDermott, Brothers Disunited, 11.

49 "Ukraine troops leave Crimea by busload; defense minister resigns after Russia seizes peninsula," *CBS News*, March 25, 2014, https://www.cbsnews.com/news/ukraine-troops-leave-crimea-by-busload-defense-minister-resigns-after-russia-seizes-peninsula/.

50 McDermott, Brothers Disunited, 7.

51 "Ukraine: Speaker Oleksandr Turchynov named interim president," *BBC News*, February 23, 2014, http://www.bbc.com/news/world-europe-26312008.

52 "Ukraine's sharp divisions," *BBC News,* April 23, 2014, http://www.bbc.com/news/world-europe-26387353.

53 "Cancelled language law in Ukraine sparks concern among Russian and EU diplomats," *RT*, February 27, 2014, https://www.rt.com/news/minority-language-law-ukraine-035/.

Finally, the political crisis in Kiev had widespread impacts upon the country but perhaps none more acute than reducing the government's ability to assess and respond to events in Crimea. Russia capitalized on the period in which the Ukrainian government was in transition. The administration following Yanukovych's removal was new and experienced, and was slow to respond to the events in Crimea as they were unfolding. Given the speed with which Russia was able to take control over the peninsula, a quick and decisive response from the government in Kiev would have been critical to mounting any significant resistance.

2.2 Hybrid Warfare in Eastern Ukraine

Yanukovych's removal also touched off Russian operations in Eastern Ukraine, but a notably different series of events unfolded there than in Crimea. Russian troops were quickly sent to the Crimean peninsula, but in Eastern Ukraine, Moscow initially encouraged an anti-government movement. It launched a political warfare campaign rather than sending special forces as a precursor to a conventional invasion. The objective was to destabilize southeastern Ukraine in order to increase control over the region, and if possible, convince the local authorities to accept a federal scheme. The Kremlin used a diverse network of political operatives, businessmen, criminal elements, and powerful oligarchs to oppose Ukraine's new government. The Ukrainian government inadvertently escalated the conflict by arresting the protest leaders and sparking a separatist insurgency. The escalation continued as the protest movement turned to irregular warfare and Russia began conventional reinforcements with its own troops in support of the separatists.

The decision of the Ukrainian parliament on February 23, 2014 to change the official status of the Russian language was acutely felt in eastern Ukraine, where a majority of citizens spoke Russian. Combined with Russia's annexation of Crimea, the situation in eastern Ukraine became combustible. Previously marginalized political organizations on both the right and left mobilized, calling themselves "people's mayors" and "people's governors."[54] Protests broke out in eastern Ukraine in response to the success of the Maidan movement in Kiev and uncertainty surrounding Ukraine's political future. While Russian intelligence probably played a role in inciting and organizing the protests, "public agitation and outcry appeared genuine and not disconnected from the country's political divisions."[55] Still, Russia was also accused of paying Russians to protest and sending protesters by "busloads."[56]

---

54 *Ibid.*

55 *Ibid.*

56 Andrew Roth, "From Russia, 'Tourists' Stir the Protests," *The New York Times,* March 3, 2014, https://www.nytimes.com/2014/03/04/world/europe/russias-hand-can-be-seen-in-the-protests.html.

An early surge of protests began in March. The pro-Russian demonstrators were largely unarmed and began with the seizures of government buildings. Pro-Russian protesters seized the regional government headquarter buildings in Kharkiv and Donetsk from pro-Maidan occupiers March 1[57] and in Luhansk on March 9.[58] In Luhansk the protesters raised the Russian flag and demanded a referendum regarding annexation by Russia. Demands across eastern Ukraine were similar – holding referendum on federal structure, recognizing Russian as an official state language, and creating a Customs Union with Russia.

There is, however, evidence that elements of the early protests were choreographed. In Kharkiv, for example, demonstrations would appear to make a brief effort to break police lines and seize the government building before marching to the Russian Consulate to ask for intervention. The sight would generate intense television footage that Putin might use to support a claim that Ukrainians sought and needed military support, the same argument used to explain the military intervention in Crimea. Both sides showed on-camera resolve, but even as they clashed they would knowingly flash moments of politeness, mutual respect and restraint – as if many of them were a common people caught in their divided rulers' fight. One pro-European observer, Anya Denisenko, would later reduce the events to their essence: "This is," she said, "'information war.'"[59] Other protests "served as grist for Russian state television networks, which hailed the footage of the Russian flag being raised across Ukraine as evidence of a rejection of the new government in Kiev by ethnic Russians."[60] Elsewhere, police forces allowed protesters to hold government buildings for a short period of time.[61]

The leaders of the protest movements seemingly appeared out of nowhere and disappeared just as fast, often arrested by Ukraine. While the arrests removed leaders of the protests, the moves backfired against Kiev. Self-proclaimed governors and mayors without experience were replaced by those who had more experience, ties to Russian security services, military backgrounds, and business interests with Russia.[62] The new leadership was more capable and willing to take direct action

57 Isabel Gorst, "In northeast Ukraine, pro-Maidan occupiers are routed by counter demonstrators," *The Washington Post,* March 1, 2014, https://www.washingtonpost.com/world/europe/in-northeast-ukraine-pro-maidan-occupiers-are-routed-by-counter-demonstrators/2014/03/01/6fb057e0-a162-11e3-9ba6-800d1192d08b_story.html?utm_term=.809b70b02cfa.

58 Steven Erlanger and Ellen Barry, "Clashes in Ukraine as Rallies Take a Turn," *The New York Times,* March 9, 2014

59 C.J. Chivers and Andrew Roth, "In Eastern Ukraine, the Curtain Goes Up, and the Clash Begins," *New York Times,* March 17, 2014, https://www.nytimes.com/2014/03/18/world/europe/eastern-ukraine.html.

60 Roth, From Russia, 'Tourists' Stir the Protests.

61 Kofman, Lessons from Russia's Operations, 36.

62 *Ibid,* 38.

and command a paramilitary force. In Donetsk, for instance, Pavel Gubarev was replaced as people's governor by Aleksandr Boroday, a Russian citizen.

Protesters in the Donetsk and Luhansk oblasts had engaged in violence following Yanukovych's removal, but Crimea's annexation sparked new demonstrations in April.[63] Separatists sought to bribe and intimidate political officials to adopt their pro-Russian standpoint or leave their positions. Over the next week in mid-April, the government in Kiev launched a counter attack with Ukrainian forces in response to the separatists' gains, but the Ukrainian army was ineffective. Not only did Ukraine's forces lack numbers, but soldiers also reportedly refused to fire on their fellow Ukrainians.[64] Some even switched sides. At this point, Ukrainian soldiers began to defect or simply give up without a fight. The ones that did choose to fight were unable to defeat the rebels.

The Ukrainian military was also a target of bribes, intimidation, and local pressure. Troops were stopped at checkpoints by mobs of locals, taking over their vehicles and forcing them to surrender their weapons. The Ukrainian government continued to launch more attacks in Mariupol and northeast of Donetsk, finding only limited success. They also made attempts to blockade and isolate the separatists, but with Russian support the rebels continued to find victories.

Separatists and pro-Ukrainian forces continued to clash in late April and May. On May 11, the People's Republics of Donetsk and Luhansk held "self-rule" referendums to create two new, quasi-independent entities. The results allegedly showed popular support for self-rule, with 89 percent voter support in Donetsk and 96 percent in Luhansk.[65] On May 22, rebels in Donetsk and Luhansk declared the establishment of New Russia, with Russian Orthodoxy as the state religion and nationalization of private industries.[66] Ukraine's presidential election was held on May 25 and Petro Poroshenko defeated the former prime minister, Yulia Tymoshenko.[67] The next day, the first battle for Donetsk airport began.

---

63 *Ibid, 31.*

64 *Ibid.*

65 Shaun Walker, Oksana Grytsenko, and Howard Amos, "Ukraine: pro-Russia separatists set for victory in eastern region referendum,' *The Guardian,* May 12, 2014, https://www.theguardian.com/world/2014/may/11/eastern-ukraine-referendum-donetsk-luhansk. The referendums had numerous problems, "There were no international observers, no up-to-date electoral lists, and the ballot papers were photocopies. With heavily armed men keeping watch, ambiguous wording on the ballot slip and a bungled Ukrainian attempt to stop voting in one town that ended with one dead, it was clear that this was no ordinary referendum." The results were not recognized by Ukraine and the West.

66 Little Green Men, 32.

67 Shaun Walker and Alex Luhn, "Petro Poroshenko wins Ukraine presidency, according to exit polls." *The Guardian,* May 25, 2014, https://www.theguardian.com/world/2014/may/25/petro-poroshenko-ukraine-president-wins-election.

The battle was a turning point in the conflict. Over two days, Ukrainian forces fought separatist militants, who suffered heavy losses. Pro-Russian rebels said that more than fifty of their soldiers were killed.[68] The Ukrainian army was able to push the separatists out Donetsk's international terminal with air strikes and a paratrooper assault. The battle was also the first of the conflict involving a "large group of volunteers from Russia who arrived to reinforce the separatists."[69] Ramzan Kadyrov, Chechnya's president, allegedly ordered the fighters from the "dikaya diviziya," or "savage division" to Ukraine.[70] The first battle for Donetsk airport was also a turning point in that more Russian soldiers directly supported the separatists.

Russia continued to vertically escalate the conflict. From June to August, the Kremlin supplied the separatists with mechanized equipment, armor, advanced munitions, and medium air defenses.[71] The strong air defense was effective; Ukraine's air force suffered so many losses it was incapable of contributing in the conflict by mid-August. Ukraine's forces were, however, still able to make gains against the separatists. On July 5, the government recaptured several towns held by separatists, including Slovyansk.[72] As the fighting continued, the pro-Russian militants were pushed back into their strongholds of Donetsk and Luhansk after sustaining heavy losses. On July 17, Russian-backed militia fired a surface-to-air missile at Malaysian Airlines Flight 17, killing 283 passengers and 15 crew members, drawing increased global attention to the conflict.[73] By early August,

---

68 Sabina Zawadzki and Gabriela Baczynska, "Fighting rages in eastern Ukraine city, dozens dead," *Reuters,* May 27, 2014, https://uk.reuters.com/article/uk-ukraine-crisis-fighting/fighting-rages-in-eastern-ukraine-city-dozens-dead-idUKKBN0E70N820140527.

69 Kofman, Lessons from Russia's Operations, 43.

70 Courtney Weaver, "Chechens join pro-Russians in battle for east Ukraine," *Financial Times,* May 27, 2014, https://www.ft.com/content/dcf5e16e-e5bc-11e3-aeef-00144feabdc0. A Russian foreign ministry official denied the men were there on official orders. "If they are Chechens, they are citizens of the Russian Federation. We can't control where our citizens go… But I can assure you that we have not sent our forces there." Kadyrov also denied any connection to the fighters. Andrew Roth and Sabrina Tavernise, "Russians Revealed Among Ukraine Fighters," *The New York Times,* May 27, 2014, https://www.nytimes.com/2014/05/28/world/europe/ukraine.html.

71 Kofman, Lessons from Russia's Operations, 44.

72 David M. Herszenhorn, "Pro-Russian Fighters Routed from Stronghold, Ukraine says," *The New York Times,* July 5, 2014, https://www.nytimes.com/2014/07/06/world/europe/ukraine-and-rebels-clash-in-slovyansk.html. Capturing Slovyansk, a long held rebel stronghold, was seen as a significant victory at the time. President Petro Poroshenko gave a statement declaring, "The state flag of Ukraine is proudly waving over the city, which militants thought was their impregnable fortress… "It's not a complete victory and it's not a time for fireworks, but clearing Slovyansk of extremely well-armed bandits has a very symbolic meaning. This is a turning point in fighting militants for the territorial integrity of Ukraine."

73 Catherine E. Shoichet and Ashley Fantz, "U.S. official: Missile shot down Malaysia Airlines plane," *CNN,* July 18, 2014, http://www.cnn.com/2014/07/17/world/europe/ukraine-malaysia-airlines-crash/index.html.

the government had recaptured about 75 percent of territory previously held by the separatists.[74]

At this point, the rebels' outlook was dire. Ukrainian forces had retaken much of separatist territory and were close to regaining border control and encircling them entirely.[75] The republics of Donetsk and Luhansk were in danger of being split, as Ukrainian soldiers drove a wedge between them. Russia's strategy was failing, forcing Moscow to up the ante by launching a conventional invasion in August of 2014. Between August 14 and 24, armored personnel carriers and other Russian military vehicles entered Ukraine. Russia continued to deny any involvement, despite at least 1000 Russian soldiers supporting separatists at the time.[76] Other figures place the number of Russian troops moved into Ukraine at the time at 4,000.[77] Russia continued to deny involvement, but finally admitted to the presence of military personnel after Ukrainian troops captured ten Russian paratroopers.[78] The Kremlin claimed they crossed the border accidentally. By the end of August, the separatists had regained pressure on the Luhansk and Donetsk airports, and threatened Mariupol again.[79]

On September 5, in Minsk, Belarus, negotiators arranged a ceasefire between Ukrainian and separatist forces, referred to as Minsk I.[80] After the ceasefire was signed, Russia intensified its train-and-equip program to improve the separatist forces and mold them into a more conventional force.[81] Though some skirmishing continued, full-scale fighting was on hold. Then, on January 13, 2015, Russia launched another offensive. An artillery strike killed 11 people and the rate of shelling doubled in a period of 24 hours.[82] Two days later, Russian-backed separatists seized Donetsk airport.[83] On February 12, the parties agreed upon

---

74 Little Green Men, 33.

75 Kofman, Lessons from Russia's Operations, 44.

76 Little Green Men, 61.

77 Kofman, Lessons from Russia's Operations, 44.

78 Karoun Demirjian and Annie Gowen, "Ukraine detains Russian paratroopers; U.S. ambassador warns of 'counteroffensive'," *The Washington Post*, August 27, 2014, https://www.washingtonpost.com/world/putin-will-meet-with-ukrainian-counterpart-in-high-stakes-summit-amid-tense-situation/2014/08/26/875db403-5b7b-4d89-8443-5aee1bde6345_story.html?utm_term=.b88ad6d45a6b.

79 Little Green Men, 61.

80 Neil MacFarquhar, "Ukraine Deal Imposes Truce Putin Devised," *The New York Times,* September 5, 2014, https://www.nytimes.com/2014/09/06/world/europe/ukraine-cease-fire.html.

81 Kofman, Lessons from Russia's Operations, 44.

82 Nick Schetko, Ian Talley, and Laurence Norman, "Artillery Strike Kills 11 People in Ukraine," *The Wall Street Journal,* January 13, 2015, https://www.wsj.com/articles/artillery-strike-kills-ten-people-in-ukraine-1421168397.

83 "Russia-backed separatists seized Donetsk airport in Ukraine," *The Guardian,* January 15, 2015, https://www.theguardian.com/world/2015/jan/15/russian-backed-separatists-seize-donetsk-airport-ukraine.

a second ceasefire – Minsk II – that would begin on February 15.[84] The deal was favorable to the separatists and Russia, providing for constitutional reform in Ukraine to decentralize rebel regions and lift restrictions on rebel areas. The issue of Debaltseve, a government-held town surrounded by rebels with ongoing fighting, was left unresolved. On February 18, 2015, Ukrainian soldiers were forced to retreat from the town under enemy fire.[85]

By July 2015, Ukraine began to implement its obligations under Minsk II. The separatists continued to be armed, trained, and equipped by Russia and supported by their troops. Fighting remained cyclical. In the fall of 2015, fighting was largely quiet but picked up in intensity during the winter and spring of 2016. Minsk II marked somewhat of a victory for Russia – if the agreement were implemented fully, Donetsk and Luhansk would be Ukrainian territory but give the Kremlin a "strategic hook."[86]

Now, four years after the crisis began, the situation is largely the same. The conflict grinds on, with low intensity but deadly nonetheless. The violence has killed about 10,000 – with 3,000 civilian deaths – and more than 1.7 million people have been displaced.[87] Fighting continues between forces led by the Ukrainian government and the Russian-backed separatists along an ad hoc border stretching around Luhansk and Donetsk.[88] Given the current state of the conflict, "Russian leaders are likely to consider… Eastern Ukraine to be a strategic success but an unsuccessful operation."[89] Though Russia's operations in eastern Ukraine led to mixed results, Russia succeeded in preventing Ukraine from a complete reorientation westward.

The Ukraine intervention displayed the range of tools as Moscow's disposal – from information and cyber war, though the use of proxies, to direct use of their own forces. Proxies were a prominent feature as Russia supported an array of groups with pro-Russian agendas. In the early phases of the conflict, it sought to foment the rebels and assisted with "volunteer" recruitment in support of the separatists. [90] Russia relied on a range of actors with existing networks to influence

---

84 "Ukraine crisis: Leaders agree peace roadmap," *BBC News,* February 12, 2015, http://www.bbc.com/news/world-europe-31435812.

85 Andrew E. Kramer and David M. Herszenhorn, "Ukrainian Soldiers' Retreat from Eastern Town Raises Doubt for Truce," *The New York Times,* February 18, 2015, https://www.nytimes.com/2015/02/19/world/europe/ukraine-conflict-debaltseve.html?_r=0.

86 Kofman, Lessons from Russia's Operations, 45.

87 Julian Coman, "On the frontline of Europe's forgotten war in Ukraine," *The Guardian*, November 12, 2017, https://www.theguardian.com/world/2017/nov/12/ukraine-on-the-front-line-of-europes-forgotten-war.

88 Adrian Bonenberger, "The War No One Notices in Ukraine," *The New York Times,* June 20, 2017, https://www.nytimes.com/2017/06/20/opinion/ukraine-russia.html.

89 Kofman, Lessons from Russia's Operations, xi.

90 McDermott, Brothers Disunited, 24.

Ukraine. Separatist soldiers were drawn from Russia and other post-Soviet states, tied together by nationalism. The Kremlin also employed a variety of paramilitaries. Organizations such as former members of the Chechen "Vostok Battalion," the Russian Orthodox Army[91], the Night Wolves,[92] Cossack paramilitaries,[93] and Chetnik Guards operated in Ukraine and Crimea.[94] The Wolves' Head Battalion, a Cossack paramilitary that fought in Georgia in 2008, operated in Ukraine in lieu of Russian troops.[95]

Russia's information campaign was aimed both at the West and Ukraine, tuning the messaging for the intended audience. The Kremlin accused the West of meddling in Ukrainian and Russian affairs, while claiming Russia as a defender of democracy in Ukraine. It also claimed to act according to the people's wishes. Beyond justifying it involvement in eastern Ukraine, Russia threatened military action while insisting it wanted peace. It also denied Russian involvement in Ukraine while constantly reminding listeners about its military and even nuclear superiority as warnings.[96] Domestic messaging focused on NATO's threat and the West's plotting. Russia questioned the legitimacy of the government in Kiev, labeling it "fascist" and "Nazi."

In Ukraine and Russia, the concept of Novorossiya became a key aspect of the information campaign. Novorossiya, meaning "New Russia," was chanted by pro-Russian protesters and even mentioned by Putin.[97] The term appealed to

---

91 The Russian Orthodox Army, approximately four thousand strong, began operations in the Donetsk region after the removal of Yanukovych. As their name indicates, the group believes in the Russian Orthodox Church and resents the West's encroachment.

92 The Night Wolves are a Russian motorcycle club founded in 1989 that has approximately five thousand members, many of whom are ex-military. The nationalist group has close ties to the Kremlin, receiving both financial and public support. Putin's has even appeared at their rallies riding a Harley Davidson.

93 Cossack forces are legally sanctioned to "defend Russian borders, guard national forests, organize youth military training, fight terrorism, and protect local government facilities." The group operated in both Crimea and eastern Ukraine.

94 Little Green Men, 44.

95 *Ibid*, 59.

96 Little Green Men, 48.

97 Adam Taylor, "'Novorossiya,' the latest historical concept to worry about in Ukraine," *The Washington Post,* April 18, 2014, https://www.washingtonpost.com/news/worldviews/wp/2014/04/18/understanding-novorossiya-the-latest-historical-concept-to-get-worried-about-in-ukraine/?utm_term=.465ded1052b6. Putin stated "I would like to remind you that what was called Novorossiya back in the tsarist days – Kharkov, Lugansk, Donetsk, Kherson, Nikolayev and Odessa – were not part of Ukraine back then… the center of that territory was Novorossiysk, so the region is called Novorossiya. Russia lost these territories for various reasons, but the people remained." His statement was "relatively accurate, historically: Novorossiya was won from the Ottoman Empire in the late 18th century. Its name, which means "New Russia," is a reflection of that. It became a part of the Ukrainian Soviet Socialist Republic in the early years of the Soviet Union, and remained a part of Ukraine after the collapse of communism."

Russian nationalists seeking to return to a golden age of Russian empire. It was also used as a historical justification for the separatists' actions. Novorossiya was used by the Donetsk and Luhansk republics when they created the confederation of Novorossiya and United Armed Forces of Novorossiya in May 2014.[98] This facet of the information campaign ended around the same period, as it lost its usefulness.

Beyond targeted messaging and propaganda, Russia also involved cyber attacks as part of their information campaign. Distributed denial of service (DDoS) attacks targeted the pro-Maidan movement and Ukrainian government. The country was subjected to at least five cyber espionage attacks between 2013 and 2017.[99] Attacks also targeted Ukraine's election system, delaying the results in October of 2014.[100]

New media facilitated familiar tactics, and Russia was able to leverage social media effectively during the conflict. Pro-Maidan pages on the two largest social-media platforms in Ukraine, VKontakte and Odnoklassniki, were blocked, as they were hosted on Russian servers.[101] The two services were also useful in recruiting for the separatist cause. The messages played to a Ukrainian vulnerability, for Ukraine's security forces' lack of capability was amplified by a lack of will to fight. Many Ukrainian army commanders also spoke Russian, were hesitant to fight against other Russian speakers and did not want to order troop movements into civilian areas.[102]

Defections were common. Russia's tactic of bribing and intimidating soldiers was designed to coerce them into defections. Ukrainian soldiers were subjected to a barrage of spam messages: "Your battalion commander has retreated. Take care of yourself," or "You will not regain Donbas back. Further bloodshed is pointless," or "Ukrainian soldier, it's better to retreat alive than stay here and die."[103] The tactic was effective; members of Ukraine's 25th paratrooper division from Dnipropetrovsk gave up their vehicles to the pro-Russian separatists.[104]

---

98 Kofman, Lessons from Russia's Operations, 52.

99 Major Vasyl Tytarenko, Deputy Chief of the Cyber Security Division, Cyber Defense Center of Armed Forces of Ukraine, "Recent Cyber Events: Lessons Learned," presentation, n.d.

100 Kofman, Lessons from Russia's Operations, 50.

101 *Ibid,* 51.

102 Kofman, Lessons from Russia's Operations, 41.

103 Tytarenko, cited above.

104 Thomas Grove and Gabriela Baczynska, "Pro-Russians take control of Ukrainian troop carriers," April 17, 2014, https://www.reuters.com/article/us-ukraine-crisis-slaviansk-apcs/pro-russians-take-control-of-ukrainian-troop-carriers-idUSBREA3F0K420140416. One soldier said, "All the soldiers and the officers are here. We are all boys who won't shoot our own people," said the soldier, whose uniform did not have any identifying markings on it. They haven't fed us for three days on our base. They're feeding us here. Who do you think we are going to fight for?"

Ukrainian soldiers were not well equipped, paid, or fed, and were asked to fight against their "own people."

Russia's military actions were tied closely to the impact of their information campaign: "The use of conventional invasion can be viewed from two perspectives. On the one hand it represents the failure of Russian information warfare in eastern Ukraine, because it implies Putin's desperation in recouping the failures of his agents there. On the other hand, it represents the logical, culminating sequel in the Russian information campaign, which in part is designed to set the conditions for invasion if necessary."[105]

Finally, throughout the intervention, Russia put political and economic pressure on Ukraine. Russia's political campaign began before military operations. On December 17, 2013, Putin offered Yanukovych (still the Ukrainian president at the time) a lifeline amid instability, taking advantage of Ukraine's financial vulnerabilities. The lifeline took the form of a $15 billion bailout and significant discounts on natural gas imports.[106] Not only was the agreement an attempt to draw Ukraine back into Russia's orbit, it fed into the Kremlin's information operations by suggesting that closer ties to Russia would result in economic prosperity, while, in contrast, closer ties with the EU would compel Ukraine to address debt issues with austerity programs unattractive to Ukrainians.[107]

105 Little Green Men, 33.

106 Darya Korsunskaya and Timothy Heritage, "Russian bailout wins Ukraine economic respite but deepens political rift," *Reuters*, December 17, 2013, https://www.reuters.com/article/us-ukraine/russian-bailout-wins-ukraine-economic-respite-but-deepens-political-rift-idUSBRE9BF11U20131217.

107 Little Green Men, 53.

Chapter 3: Hybrid Threats in Action: Russia's Intervention in the 2016 U.S. Elections

During the 2016 U.S. presidential election, Russia sought to undermine the public's faith in the U.S. democratic process and to damage Secretary Clinton's candidacy and potential presidency. The hybrid influence campaign was threefold, featuring leaks of information Russia had stolen through cyber espionage, overt Russian propaganda, and hacks into election infrastructure, all of which were distinct but done simultaneously and complementarily. Although not the first example of such attempts and surely not the last, Russia's intervention into the 2016 U.S. Presidential election is a stark instance of an influence campaign aimed at undermining the Western liberal democratic order. Russia has long used a blend of covert and overt tactics to advance its goals, but the scope and directness of its actions towards the United States in 2016 was unprecedented. Starting at least as early as the summer of 2015, Russia launched three distinct but simultaneous campaigns in the United States. The first two of these amounted to *weaponizing* information. The hackers and bots involved in the operations also enjoyed the full support of the Russian government, contrary to Putin's insistence on the opposite.[108]

108 Russian President Vladimir Putin said during a press conference on June 1, 2017 that independent Russian hackers may have launched cyber attacks on foreign nations, but that the Russian state was uninvolved and that the hackers acted on their own patriotism. See Andrew Higgins, "Maybe Private Russian Hackers Meddled in Election, Putin Says," *New York Times*, June 1, 2017, https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html?mcubz=3.

A partially declassified U.S. Intelligence Community Assessment (ICA) in early 2017 concluded that, in addition to its longstanding desire of undermining the U.S.-led order, the Kremlin launched an influence campaign with three specific goals: "to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency."[109] The Kremlin also displayed a clear preference towards candidate Trump and so helped to increase his election chances.[110] The ICA also noted that President Putin's dislike for Secretary Clinton was likely to have stemmed from his holding her responsible for the mass protests against him in 2011 and 2012.[111]

The cyber operations conducted against targets associated with the U.S. election consisted of two distinct but related parts – hacks and leaks. In 2015 and 2016, the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC), and the Hillary Clinton campaign were all targeted by Kremlin-sponsored cyber espionage operations. The two hacker groups involved, CozyBear and FancyBear, have conducted similar operations in Europe and North America and employed the same modus operandi (MO) they have previously used against other foreign agencies and states.[112] The documents and information stolen from these networks were then shared via a persona and website created by the Russian government, Guccifer 2.0 and DCLeaks.com, and later via Wikileaks and mainstream media outlets.

Russian intelligence gained access to the DNC network from June 2015 until at least June 2016. CozyBear and FancyBear, the two hacker groups that conducted these operations, are both tied to the Russian government but to intelligence agencies that are at least competitors – the FSB or SVR (the federal security service, successor to the KGB's foreign operations directorate), and

109 U.S. Intelligence Community Assessment (ICA), an unclassified version of which was made public in January 2017, available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

110 U.S. Intelligence Community Assessment (ICA), an unclassified version of which was made public in January 2017, available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

111 *Ibid.*

112 CozyBear was responsible for the 2015 hacks into the U.S. White House, State Department, and Join Chiefs of Staff networks. It has also targeted organizations in Western Europe, Central and East Asia, and Central and South America. FancyBear on the other hand is known to target military- and defense-related units in America, Europe and Asia. FancyBear was also the group behind the German Bundestag and France's TV5 Monde hacks in 2015. See Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *Crowdstrike,* June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

the GRU (main intelligence directorate, military intelligence), respectively.[113] When FancyBear gained access to the DNC network in 2016, it stole the DNC's opposition files on Candidate Trump, which ultimately – but not soon enough – prompted the DNC to hire cyber security firm Crowdstrike to investigate the breach. Crowdstrike was then able to identify both CozyBear and FancyBear in the DNC network and both were subsequently ejected.

CozyBear. CozyBear, also known as APT 29, Office Monkeys, CozyCar and CozyDuke, was the first of the two groups to gain access to the DNC network in June 2015. It infiltrated networks through phishing emails, which typically include web links to or attachments of a malicious dropper that installs a malware implant. In the case of the DNC, CozyBear used an implant called SeaDaddy, which is a highly configurable and encrypted exfiltration malware that is almost identical to previous programs linked to the FSB.[114] SeaDaddy allows hackers to exfiltrate data from compromised networks and to monitor the communication channels within them. The implant, configured in .exe format, can run on any Windows computer, and once implanted maintains a backdoor access to allow for task automation and configuration.[115]

FancyBear. FancyBear, also called APT 28 and Sofacy, successfully hacked into the DNC network in April 2016 and was removed soon after it stole opposition files on Candidate Trump. In addition to phishing emails like CozyBear, FancyBear is also known for registering domains that mimic legitimate sites in order to obtain user information as well as to enhance the deceptiveness of its phishing emails. Its primary implant, X-Agent, is a malware that allows for remote commands, file transmissions, and keylogging, a feature that records every keystroke made on a compromised computer which allows for easy access to passwords. X-Agent is also configured to be capable of running on both computer

113 Crowdstrike, the cyber security firm that the DNC hired to investigate its breach, observed CozyBear and FancyBear infiltrating the same networks and stealing similar data. It found that the two groups worked simultaneous likely without knowledge of the other's involvement. See Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. For more information on the adversarial nature of Russia's intelligence services, see Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services,* London: European Council on Foreign Relations (ECFR), 2016, http://www.ecfr.eu/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf.

114 Massimo Calabresi and Pratheek Rebala, "Here's The Evidence Russia Hacked The Democratic National Committee," *Time*, December 13, 2016, http://time.com/4600177/election-hack-russia-hillary-clinton-donald-trump/.

115 For more information on the SeaDaddy implant and its code, see Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *Crowdstrike,* June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

and mobile platforms.[116] In addition to the DNC network itself, FancyBear also targeted a DNC IT contractor called MIS Department. In late March 2016, FancyBear hackers used a misspelled domain, misdepatrment[.]com, to mimic MIS Department. This bogus domain was then linked to an IP address that is known to belong to APT 28.[117]

The hacks into the DCCC were also likely the work of FancyBear. They consisted of the use of a bogus site, ActBlues, which resembles a DCCC donation site called ActBlue, thus consistent with FancyBear's MO. The e-mail used to register for the ActBlues domain, fisterboks@email[.]com, has been used to register sites that have previously been tied to FancyBear. Its registered domains are also tied to the email of the registrant of misdepatrment[.]com, the bogus site used in the DNC hack.[118] The timing of the DCCC hacks also shed light on the Kremlin's involvement: the registration date of the ActBlues domain coincides with the first public report of CozyBear and FancyBear's involvement in the DNC hacks, suggesting that FancyBear's interest in the DCCC likely stemmed from an interest in maintaining access to the Democratic Party's systems.

Hillary Clinton's campaign Chair, John Podesta, was also targeted by Russian hackers in 2016. On March 19, Podesta received an email warning from Google claiming that someone had attempted to sign in to his Gmail account and that he should change his password immediately.[119] One of Podesta's aides unintentionally advanced the Russian operation when he forwarded the email to IT with a typo, writing that the email was "legitimate" rather than "illegitimate." Once the password was changed by clicking the "change password" link, it granted the Russian hackers full access to Podesta's private Gmail account. Podesta's and the Clinton campaign's numerous emails were later published by Wikileaks in early October.

In addition to Russia's cyber capabilities, these three operations also suggest some laxness on the part of U.S. institutions. In September 2015, an FBI official called the DNC to warn that at least one of its computers had been hacked by "the Dukes," or Cozy Bear. Unfortunately, because the FBI agent did not go to the DNC in person, he was only able to reach a part-time tech contractor.

---

116 For more on FancyBear and X-Agent, see Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *Crowdstrike,* June 15, 2016, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

117 For more on the digital fingerprints tying misdepartrment[.]com to FancyBear, see "Rebooting Watergate: Tapping into the Democratic National Committee," *ThreatConnect*, June 17, 2016, https://www.threatconnect.com/blog/tapping-into-democratic-national-committee/.

118 For a full analysis of links between the DCCC hacks and FancyBear, see "FANCY BEAR Has an (IT) Itch that They Can't Scratch," *ThreatConnect*, July 29, 2016, https://www.threatconnect.com/blog/fancy-bear-it-itch-they-cant-scratch/.

119 For a full analysis of links between the DCCC hacks and FancyBear, see "FANCY BEAR Has an (IT) Itch that They Can't Scratch," *ThreatConnect*, July 29, 2016, https://www.threatconnect.com/blog/fancy-bear-it-itch-they-cant-scratch/.

The FBI also never mentioned any suspicion of Russian involvement related to these warnings. While the contractor did conduct a scan of the DNC's computer systems, which revealed no traces of intrusion, he himself admits that he did not look very hard as he had no idea whether the caller had been a real FBI agent or not. More importantly, as a nonprofit group, the DNC lacked the funds for the most advanced cybersecurity tools. When DNC personnel requested more help from the FBI to track down the hacks, the FBI allegedly failed to provide more information. It wasn't until March 2016 when the DNC noticed that certain documents had been extracted from its network that it realized the seriousness of the FBI's warning.[120] The DNC then engaged Crowdstrike.

The timing of the Russian leaks was strikingly strategic. On June 15, 2016, a day after the DNC and Crowdstrike publicly confirmed the Kremlin's hack of the DNC network, an anonymous persona called Guccifer 2.0 emerged online and claimed sole credit for the cyber attack. Guccifer then began to publish some stolen documents, including but not limited to the DNC's opposition research on Trump that had been exfiltrated by FancyBear. On July 22, days before the Democratic National Convention, Wikileaks published about 20,000 DNC emails as part of its "new Hillary Leaks series" which Guccifer claims to have provided.[121] Following these leaks, Wikileaks founder Julian Assange stated during an interview with 'Democracy Now!' that Wikileaks releases are always strategically timed to get a "big political impact."[122] Guccifer 2.0 continued to publish data from the DCCC and from Podesta's private email account in the weeks leading up to the election, both on its own website and via Wikileaks. DCLeaks.com, another outlet linked to Guccifer 2.0 and FancyBear, also released leaked information obtained in Russian operations.[123] Figure 2 outlines the cycle of hacks and leaks.

---

120 Nicole Perlroth, Michael Wines and Matthew Rosenberg, "Little Effort to Investigate in States Targeted by Election Hacking," *New York Times,* September 1, 2017, https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html; Mark Hosenball, John Walcott and Joseph Menn, "The FBI reportedly waited months to tell Democrats that Russians may have played a role in the DNC hack, *Business Insider*, August 3, 2016, http://www.businessinsider.com/fbi-waited-months-to-tell-dnc-of-suspected-russian-role-in-hack-2016-8?r=US&IR=T&IR=T.

121 Guccifer 2.0, Twitter Post, July 22, 2016, 9:44 a.m., https://twitter.com/guccifer_2/status/756530278982684672?lang=en.

122 "EXCLUSIVE: WikiLeaks' Julian Assange on Releasing DNC Emails That Ousted Debbie Wasserman Schultz," *Democracy Now!,* July 25, 2016, https://www.democracynow.org/2016/7/25/exclusive_wikileaks_julian_assange_on_releasing.

123 "Does a BEAR Leak in the Woods?," *ThreatConnect*, August 12, 2016, https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/.

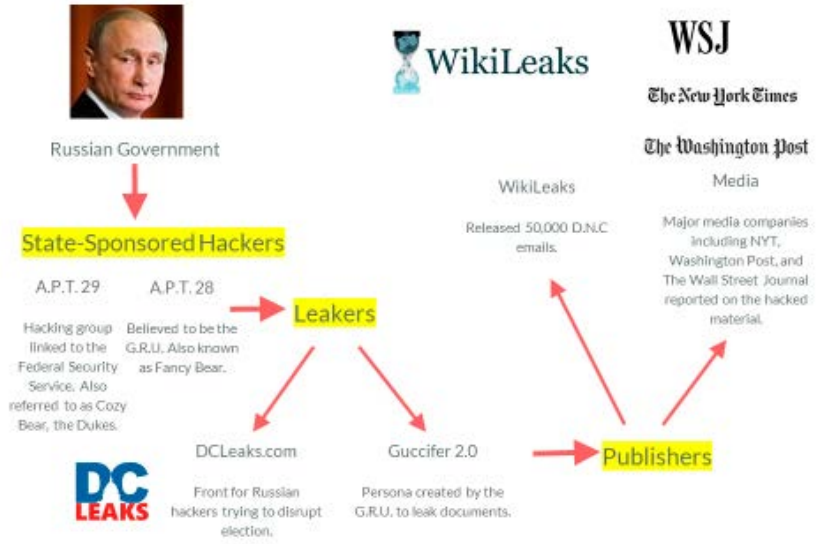


Figure 2: Russian Leaks and Hacks.

As the nature of hybrid threat suggests, and as Assange himself admitted, releases of "secret" documents are not random but are always timed to achieve specific political objectives – in the U.S. case, to influence popular discourse and divert the attention of the media and the public when needed. To underscore this point, notice that the Wikileaks release of stolen DNC emails was three days before the start of the Democratic National Convention. This enabled the emails to dominate mainstream news as the convention took place, with extensive reports of the contents of these emails and with suggestions that more damaging ones were to come. As a result, top DNC officials faced increasing calls to resign, and the contents of the emails – focused mainly on the DNC's apparent favoring of Secretary Clinton over Bernie Sanders – called into question the legitimacy of Secretary Clinton's candidacy. These emails also provided Candidate Trump with ample ammunition to attack both Clinton and the "rigged" U.S. electoral system.

The release of Podesta's private emails was also strategically timed to divert the media's attention from the news of the day. On October 7 at 3:30 p.m., the Obama administration issued a formal statement blaming the Kremlin for interfering in the U.S. election. That afternoon at 4:00 p.m., the Washington Post published the "Access Hollywood" tapes in which Candidate Trump can be heard making lewd statements about women.[124] Half an hour later at 4:30 p.m., Wikileaks began to publish emails stolen from Podesta's email server that tied Clinton to

124 For a transcript of Trump's remarks, taped in 2005, see https://www.nytimes.com/2016/10/08/us/donald-trump-tape-transcript.html.

major banks, an already contentious issue that had been used against Clinton and her campaign throughout the election.[125] While the "Access Hollywood" tapes still dominated the news, Podesta's emails also received abundant reporting. This episode demonstrates the Kremlin's clear preference for candidate Trump and its assistance in helping to increase Trump's electoral chances.

In the second prong of the operation, propaganda, Russian media outlets, not surprisingly, served as outlets for Kremlin messaging. Russia leaders were hardly shy about the emphasis on information operations. During an interview with RT in 2013, Putin stated that he wanted to "break the Anglo-Saxon monopoly on the global information streams."[126] Or his press secretary, Dmitri Peskov, in talking with the *New York Times* cited Kim Kardashian, a popular American celebrity with 55 million Twitter followers, as an example of the reach in mobilizing people. "This will be a signal that will be accepted by millions and millions of people. And she's got no intelligence, no interior ministry, no defense ministry, no K.G.B." "The new reality creates a perfect opportunity for mass disturbances," he said, "or for initiating mass support or mass disapproval."[127]

Botnets, paid human trolls, and Russian news websites such as RT and Sputnik all assisted in propagating the Russian line to English speaking viewers. The Kremlin depended on mainstream media outlets as well as social media to maximize the effect and reach of its operations: many Russian-sourced stories, first reported in RT or Sputnik, were often reiterated and amplified on Twitter or Facebook via botnets and trolls, causing algorithms to trend misleading or false reports that may be picked up by mainstream news coverage. Russian state media often generally covered candidate Trump in a positive light in contrast to Secretary Clinton, who always received negative coverage. In the weeks leading up to election day, there were also increasing reports of potential irregularities or faults with election systems. Additionally, the Kremlin's propaganda campaign also increased the spread of "fake news" that either distorted actual facts or spread misleading stories about Secretary Clinton and the U.S. electoral process. Fake news originating from Russian sources consistently trended on various social media outlets throughout the election cycle.

In early August 2016, for instance, Twitter began to trend news regarding a Turkish protest surrounding the U.S. airbase in Incirlik, Turkey. RT and Sputnik first tweeted reports that thousands of police had gathered at the site. These stories were then promulgated by a group of users who were panicking over the alleged

---

125 Both Sanders and Trump have accused Clinton for cozying up to Wall Street during the election cycle. These emails provided further evidence that Clinton had made paid appearances before big banks. The leaks of Podesta's emails also took place days before the second presidential debate, although Candidate Trump only mentioned Clinton's ties to Wall Street once.

126 https://www.rt.com/news/putin-rt-interview-full-577/

127 https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html?referer=https://t.co/wPy2vnUuw1?amp=1

nuclear weapons stored at the base and questioning why mainstream media did not cover the story. It turned out, however, that these Russian botnets and trolls were prompting a storm of panic over a story that was factually untrue. While a peaceful protest did take place in Turkey, the protest was substantially smaller in scale compared to the reports of RT, Sputnik, and Twitter, and the Incirlik base was not surrounded, contrary to these same accounts.[128]

Reports denigrating Secretary Clinton's health also spread in a similar fashion. While rumors surrounding this issue had circulated regularly throughout the election cycle, in late August Wikileaks tweeted "Clinton looked at drug after suffering from 'decision fatigue'" accompanied by a screenshot of an already released Hillary Clinton email.[129] This was then cited by pro-Russia outlet ThePoliticalInsider.com as evidence for its unsubstantiated claim that Clinton had Parkinson's Disease.[130] The story, which was then reiterated by other fake news outlets and their social media channels, ended up gathering 90,000 Facebook engagements and over 8 million views.[131] Mainstream media sources also picked up on the story, including Fox News.[132] When *The Daily Beast* countered the story the following day, its article received significantly less attention, with only 1,700 Facebook engagements and 30,000 views. The Kremlin's ability to disseminate factually false news and garner significant engagement over legitimate sources is evidence of the Kremlin's robust propaganda network.

An investigation by the *New York Times* and cybersecurity firm FireEye revealed that the Kremlin's Twitter operations rely on an automated Twitter army, or bots, that publishes identical messages simultaneously or just seconds apart.[133] Another

---

128 For more on the specifics of how the Incirlik story spread, see Clint Watts and Andrew Weisburd, "How Russia Dominates Your Twitter Feed to Promote Lies (And, Trump, Too)," *The Daily Beast,* August 6, 2016, http://www.thedailybeast.com/how-russia-dominates-your-twitter-feed-to-promote-lies-and-trump-too.

129 Wikileaks, Twitter Post, August 23, 2016, 5:04 a.m., https://twitter.com/wikileaks/status/768056314761191424.

130 Thomas, "WikiLeaks Just Dropped Bombshell about Hillary's Health… The Truth, REVEALED!," *The Political Insider,* August 23, 2016, http://thepoliticalinsider.com/wikileaks-just-dropped-bombshell-hillarys-health-truth-revealed/.

131 Anonymous research group PropOrNot, which targets pro-Russian propaganda news sources, issued a report analyzing Russia's propaganda campaign against the U.S. during the 2016 election. For more on the Parkinson's case as well as similar others, see PropOrNot, *Black Friday Report: On Russian Propaganda Network Mapping*, 2016, https://drive.google.com/file/d/0Byj_1ybuSGp_NmYtRF95VTJTeUk/view.

132 "Julian Assange Discusses Hillary Health Rumors from Latest Email Release," *Fox News,* August 26, 2016, http://insider.foxnews.com/2016/08/26/julian-assange-discusses-hillary-clinton-health-rumors-latest-email-release.

133 Scott Shane, "The Fake Americans Russia Created to Influence the Election," New York Times, September 7, 2017, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html?mcubz=3.

interesting characteristic is that these tweets are posted in alphabetical order of the usernames of these fake accounts. On Election Day for example, FireEye identified more than 1,700 tweets with the hashtag #WarAgainstDemocrats in various fashions.

Facebook also hosted various Russian-sponsored fake accounts that spread anti-Clinton propaganda and promoted leaks. Similar to Twitter bots, Facebook users can be easily identified to be fake. Often, their Facebook posts were not personal but rather consisted only of pro-Russia, anti-Clinton related news or articles. On their profiles, these users often had filled out their "introduction" overview, which gives information regarding where they grew up, where they went to school or what their job is. However, as the *Times* investigation reported, their high schools or colleges would have no record of them ever attending the school. In September 2017, Facebook officials stated that the company had shut down several hundred fake accounts that they linked to a Kremlin company. This same company also bought $100,000 of ad space during and after the election cycle.

Both Twitter and Facebook have strengthened efforts to crack down on the number of fake accounts found on their platforms. Now, Facebook takes down about a million accounts a day. However, most of their efforts are reactive rather than proactive. Given the number of users – 328 million on Twitter users and nearly 2 billion on Facebook – it is difficult to keep track of every account, and so accounts are taken down mostly after the fact. According to statistics later released by the companies, Russian agents disseminated inflammatory posts that reached 126 million Facebook users, published 131,000 messages on Twitter and uploaded over a thousand videos on YouTube.[134] More recently, Twitter reported that it would notify 677,775 people in the United States who followed one of fake Russian accounts or retweeted or liked a Tweet from these accounts during the election period. The company also identified 13,512 additional accounts, for a total of 50,258 automated accounts as Russian-linked and Tweeting election-related content during the election period (for perspective that number was 0.016 percent of the total accounts on Twitter at the time. Twitter now can detect and block approximately 523,000 suspicious logins daily being generated through automation. In December 2017, it identified and challenged more than 6.4 million suspicious accounts globally per week – a 60 percent increase from October 2017.[135]

The Russian bots and trolls on Twitter and similar social media sites that contributed to the Kremlin's propaganda campaign have been found to have operated behind a common strategy. The users target audiences vulnerable to

---

134 As reported by the *New York Times,* based on company reports to Congress. Mike Isaac and Daisuke Wakabayashi, "Broad Reach of Campaign by Russians Is Disclosed," p. B1, October 31, 2017.

135 Twitter, "Update on Twitter's Review of the 2016 U.S. Election," 19 January 2018, available at https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html.

their influence on both the political right and left, including the alt-right as well as the victims or critics of globalization, immigration, terrorism and economic recession. The biographies of these accounts often include words such as "America," "military," or "Christian" and stories they shared were accompanied by hashtags or phrases that would appeal to these audiences. In the Incirlik case, the fake news story was shared with #NATO, #benghazi, and #trumppence16 to attract Trump supporters.[136]

Interestingly, while the propaganda campaign surprised the United States, there was warning from a group of outside analysts. They had been 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 listen, given the crises competing for attention.[137]

The third element of Russia's interference campaign into the 2016 U.S. Presidential election involved the covert cyber hacking of infrastructure directly associated with the election. While the extent and consequences of these hacks are not as significant as the leaked documents and the spread of fake news from the other two operations, their precise effect is not yet clear. However, the cyber hacking of infrastructure associated with the election, such as voting systems and voter databases, provided the Russians with the techniques, materials, and familiarity with the U.S. election system that can be applied to future Russian influence campaigns – in the U.S. and perhaps elsewhere. It remains unclear whether the hacking had any actual effect on the election outcome. The initial judgment by U.S. intelligence was "no," but elections are the responsibility of U.S. states, which jealously guard their prerogatives, so detailed forensic assessments seem not yet to have been done.[138]

The first evidence of these hacks was in May 2016, when Arizona's voter registration system was taken offline for a couple of days following a FBI warning of a cyber threat. Investigations revealed that hackers had tried but failed to

136 Clint Watts and Andrew Weisburd, "How Russia wins an election," *Politico,* December 13, 2016, http://www.politico.eu/article/how-russia-wins-an-election/.

137 See Andrew Weisburd and Clint Watts, "Trolling for Trump: How Russia is Trying to Destroy Our Democracy, November 2016, available at https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

138 Nicole Perlroth, Michael Wines and Matthew Rosenberg, "Little Effort to Investigate in States Targeted by Election Hacking," *New York Times,* September 1, 2017, https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html.

infiltrate the system. A month later, in June 2016, the Illinois Board of Elections was successfully hacked. The hackers gained access to Illinois' voter database and had access to around 90,000 records including the names, date of births, genders, driver's licenses and partial social security numbers of registered voters. Although it was concluded that no data had been manipulated, investigations also revealed that the hackers had tried but failed to alter some information in the database.[139]

A leaked NSA document dated May 5, 2017 revealed that the GRU targeted at least one voting system manufacturer through spear-phishing e-mails.[140] Although the document does not name the company in question, there are mentions of products made by and emails related to VR Systems, a voting services and equipment retailer. This successful intrusion allowed access to the credentials of local electoral officials, which were then used to launch another spear-phishing campaign on these officials. Beyond VR Systems, hackers targeted at least two other similar election services providers.[141] A U.S. Senate intelligence hearing on the matter in June 2017 also revealed that a total of 21 states' election-related systems had been targeted, including Arizona and Illinois.

While a number of systems were successful hacked, there is still no evidence to suggest that election day vote tallying was affected. In January, intelligence officials concluded that the actual vote count was not influenced by Russian hackers and they maintain this conclusion up until now. However, government officials said that this conclusion does not address whether the hacks of election systems could have prevented voters from casting ballots.[142]

3.1 Comparing Interventions: the French 2017 Elections

There is less information available on this case, largely because it was much smaller and briefer, and has not been the subject of a formal French investigation. The main points, however, are clear: the Russians hacked and released nine gigabytes of emails stolen from Macron's campaign less than 48 hours before the run-off election in May 2017. As with the DNC, the timing was strategic, not giving Macron time to respond since French law forbids candidates from

139 Investigators found that the hackers attempted to delete or alter some voter data in the Illinois database. This was the first and only report of such attempts. See Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider than Previously Known," *Bloomberg,* June 13, 2017, https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

140 The leaked NSA document is available at https://assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf.

141 Nicole Perlroth, Michael Wines and Matthew Rosenberg, "Little Effort to Investigate in States Targeted by Election Hacking," *New York Times,* September 1, 2017, https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html.

142 *Ibid.*

speaking publically in the two days before an election. However, at the 11th hour the campaign did issue a statement saying it had been hacked and that many of the documents that were dumped on the American 4Chan site and re-posted by Wikileaks were fakes. Mainstream media in France carried the statement but said little about the leaks.

The hacking was likely the work of FancyBear, who was also behind hacking the DNC, DCCC, and previously TV5 Monde (which is why France took major steps to protect from hacking). Earlier in the year Macron's campaign said it had been targets of hacking attempts but that all of these attempts failed. The campaign, however, did not closely monitor look-alike sites, like misdepatment in the U.S. case. The propaganda campaign was similar to that in the U.S. election; indeed it employed some of the same bot accounts.

The leaks appeared in a collection of links to torrent files that appeared on the anonymous publishing site PasteBin.[143] The leaks were attributed to Fancy Bear and to Russia by several sources.[144] The phishing domain was similar to a cloud storage site that Macron's campaign used. Trend Micro, a Tokyo based cybersecurity firm, did monitor look-alike websites, which is how it found the phishing domain. Still another firm detected four Macron-related fake domains. In the end, the Russians weren't very good at hiding their tracks. By mid-March, Trend Micro was watching the same Russian intelligence unit behind some of the DNC hacks start building the tools to hack Macron's campaign. They set up web domains mimicking those of his *En Marche!* Party, and began dispatching emails with malicious links and fake login pages designed to bait campaign staffers into divulging their usernames and passwords, or to click on a link that would give the Russians a way into the campaign's network.[145]

The Macron statement said: "The files which are circulating were obtained a few weeks ago thanks to the hacking of the professional and personal email accounts of several members of the campaign," but also warned that among the authentic documents in the leak were "numerous false documents intended to sow doubt and disinformation."

Interestingly, and surely partly because of the earlier DNC hacks, the Macron campaign was attentive to possible hacks from December, the first round of the election. Moreover, the campaign responded to phishing attempts with disinformation of its own. As Mounir Mahjoubi, the head of Macron's digital team, explained: "We went on a counteroffensive…We couldn't guarantee 100 percent

143 https://www.wired.com/2017/05/macron-email-hack-french-election/.

144 http://www.telegraph.co.uk/news/2017/05/06/russian-hackers-blame-emmanuel-macrons-leaked-emails-could/, citing Vitali Kremez, director of research with New York-based cyber intelligence firm Flashpoint. See also https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf.

145 https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html?mcubz=3&_r=1.

protection" from the attacks, "so we asked: what can we do?" The campaign opted for a classic "cyber-blurring" strategy, well known to banks and corporations, creating false email accounts and filling them with phony documents the way a bank teller keeps fake bills in the cash drawer in case of a robbery.[146] "You can flood these [phishing] addresses with multiple passwords and log-ins, true ones, false ones, so the people behind them use up a lot of time trying to figure them out," Mahjoubi said.[147]

The propaganda campaign was very similar to that mounted against the U.S. election.[148] The goal was to spread fake news and rumors, such as that U.S. agents were meddling in France's finances, that Macron was gay, or that his campaign was funded by Saudi Arabia. The same botnets that had been active for Trump turned, after the U.S. election, to Europe – to the Netherlands, Germany, and, especially France. On Twitter, five percent of users accounted for a full 40 percent of the tweets related to the French election. One account tweeted a whopping 1,668 times in 24 hours, faster than one per minute. And it was hardly alone. For several of these accounts, the tweets were coming through in bursts too fast for an individual to keep up with them, suggesting automation rather than a highly active human.[149] For its part, Facebook removed over 30,000 fake accounts around the French election.[150]

4chan's online image board, which had also played a role in the U.S. case, was mentioned frequently in Le Pen related tweets as a source of where memes originated. In the U.S. case the memes had been anti-Clinton and pro Trump ones. [151] In France, they propagated a claim that Macron used an offshore bank account in the Cayman Islands to evade French taxes. Following up on this story, there was evidence that Reddit users were purposefully repeating identical phrases about this conspiracy theory in order to "Google bomb" – to feed false, verbatim content into sites Google mines to feed their search engine algorithm, in the hopes that they could influence the phrases that Google uses to autocomplete searches beginning with "Macron." Macron's opponent, Marine Le Pen referenced the claim in the debate, accusing Macron of using a tax haven. As a result during the debate, #Bahamas was a trending hashtag on Twitter.

---

146 See https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html?mcubz=3&_r=1.

147 As quoted in http://www.thedailybeast.com/fighting-back-against-putins-hackers.

148 https://thinkprogress.org/russian-bots-where-are-they-now-e2674c19017b/.

149 http://www.slate.com/blogs/the_slatest/2017/05/06/american_alt_right_and_twitter_bots_are_key_to_spreading_french_election.html

hhttp://www.slate.com/blogs/the_slatest/2017/05/06/american_alt_right_and_twitter_bots_are_key_to_spreading_french_election.html

150 https://www.facebook.com/notes/facebook-security/improvements-in-protecting-the-integrity-of-activity-on-facebook/10154323366590766

151 https://medium.com/data-for-democracy/democracy-hacked-a46c04d9e6d1.

Chapter 4: The Hybrid Threat Toolkit

Many of the tools available for hybrid conflict – for example, propaganda, or political and economic levers – are hardly new. The main exception to this is related to the cyber realm, which has both empowered new tools as well as created new opportunities for maximizing the effect of otherwise traditional instruments of influence. However, what defines twenty-first century hybrid threats is the simultaneous and complementary use of many of these instruments to achieve a common objective. As the MCDC report defined, "hybrid warfare is asymmetric and uses multiple instruments of power along a horizontal and vertical axis."[152] A hybrid warfare actor may increase the potency of an operation by intensifying one or more tools (vertical escalation) or by synchronizing multiple tools (horizontal escalation) in order to achieve a greater combined effect.[153] Combined, hybrid warfare seeks to overlay the means and employ them as complements in order to maximize their impact.

Apart from complementarity, the other defining feature of hybrid warfare is the *strategic* use of these instruments of power both vertically and horizontally. This means that they target and exploit *vulnerabilities* of another state, and are employed to achieve specific *objectives*, which may or may not change as the campaign proceeds. These two issues are elaborated in the two chapters following this one.

This section proceeds first by parsing the various tools or instruments of power that an adversary might employ in a hybrid warfare campaign. Then, it turns to a discussion of how these tools may be synchronized in practice, as well as spelling out the advantages and non-linear effects of employing multiple instruments at once.

---

152 Understanding Hybrid Warfare, 8.
153 *Ibid.*

4.1 Propaganda: Old Aims, New Means

Both diplomacy and war have always sought to influence, in the final analysis, the brains of leaders and their people. Everything else has been a means to that end. Information operations – that is, the *weaponizing* of information for strategic objectives – serve as important tools due to their utility in trying to shape the political discourse and popular narrative in many countries. It seems a still-open question how the new media, often mislabeled "social," will affect the battle for those two inches of gray matter in the heads of leaders and their people, but those new social media surely have provided a new avenue for states and groups to exploit to maximize the reach of an information campaign. These new media have driven down the entry cost of information operations: think of the contrast with the Cold War when seeking to plant a story in another country's newspaper was both hard and expensive. Information operations consists of both the channel by which the information is spread as well as the nature of the information itself. The first consists of domestic media outlets targeted towards foreign audiences, state-sponsored think tanks and organizations, and social media platforms. The latter can include views that are advantageous to the hybrid threatener state, leaks of information stolen either via cyber or traditional espionage, and fake news.

4.2 Domestic Media Outlets

This tool is familiar. The Russia propaganda campaigns always have been directed as much inside the country as outside, and while the recent ones were successful, they were for the most part good old-fashioned stuff – buying or suborning traditional media outlets. State-sponsored news outlets, such as Russia's RT and Sputnik, publish both world and domestic news from the perspective of their state sponsor and serve as a platform for the state's ideas and preferences. For example, Sputnik has aided the Kremlin in arguing in favor of Russian involvement in Syria while criticizing the U.S.'s actions in the country. It repeatedly casts Russia's involvement in a positive light, claiming that the Kremlin's help had "prevented Syria from disintegrating and saved the Middle East from chaos."[154] Meanwhile, it also criticized the U.S. for its own Syrian policies. In an October 2017 article, Sputnik reported that "the US insistence on scapegoating the Assad government for all uses of chemical attacks despite serious evidence suggesting otherwise had strongly conditioned the US public to approve continued military action against the Damascus government."[155]

---

154 "US Admitting Syrian Militants Use Chemical Weapons 'Welcome' Overdue Corrective," *Sputnik,* October 21, 2017, https://sputniknews.com/analysis/201710211058422305-usa-terrorists-use-chemicals-syria/.

155 *Ibid.*

These state-sponsored media outlets aim to criticize adversaries' policies while praising their states' own initiatives. The stories published on these sites are aimed at the general public with the hope that many will read these distorted accounts of news and approach these issues with a non-Western outlook. These sites can either be published in English for the purpose of reaching English-speaking viewers, or in Russian for citizens at home or the ethnic Russian population in neighboring countries such as Latvia and Estonia.

This tool, however, despite being well known, is most influential when its stories are shared by popular, local media outlets. In Italy for example, due to a close relationship between Moscow and the most popular party in Italy, M5S, many RT or Sputnik articles are repeatedly spread via M5S' vast network of websites and social media accounts. This serves not only to advance Russia's strategic narratives, but is also a way for Russia to paint geopolitical perceptions of Russia in favorite light among policy-makers and the Italian public. In Italy, Putin has become a symbol of "sovereigntism," with an emphasis in its role as a leader who has fought against globalization and external forces seeking to violate Russia's sovereignty.[156]

4.3 Social Media

The advent of social media has indeed provided a new avenue for adversary states to exploit to reach mainstream media and the general public. Social media can be used to reiterate news from a state's domestic media outlets or to publish new information via state-sponsored accounts, bots, or advertisements. This was a prominent feature of Russia's hybrid warfare campaign in the 2016 U.S. Presidential election. Many Russian-sourced stories that first were reported in RT or Sputnik were then reiterated and amplified on Twitter or Facebook via botnets and trolls, causing algorithms to trend misleading or false reports that the could be picked up by mainstream news coverage. Russian state media generally covered Candidate Trump in a positive light in contrast to Secretary Clinton, who always received negative coverage. These efforts were extremely effective in spreading Russian propaganda as well as false news favorable to Russian interests.

These operations through social media can be especially effective given that many people's main access to news is through social media. In the U.S., a 2016 Pew Research Center report found that 67 percent of adults receive news via sites like Twitter and Facebook, up from 62 percent the year before. For Americans

156 Alina Polyakova, and others, *The Kremlin's Trojan Horses 2.0: Russian Influence in Greece, Italy, and Spain,* Atlantic Council, November 2017, 11, 16, 17, available at http://www.atlanticcouncil.org/images/The_Kremlins_Trojan_Horses_2_web_1121.pdf. Hereafter cited as Kremlin's Trojan Horses.

under 50, the percentage was 78.[157] Indeed, the reach of social media is impressive compared to traditional sources of journalism and communication. Social media allows hybrid threateners like the Kremlin to build a robust propaganda network that can be used to cast doubt on objective truths or domestic policies. It is especially problematic due to its incredible reach and its ability to garner significant engagements online. For instance, as noted earlier, in the 2016 U.S. election campaign, Russian agents disseminated inflammatory posts that reached 126 million Facebook users.

Interestingly, Russia troll networks are much more organized than common visions of trolls operation in isolation. According to a *New York Times* investigation, in 2015 hundreds of young Russians were employed at a "troll farm" in St. Petersburg known as the Internet Research Agency (IRA), where many worked 12-hour shifts in departments focused on different social media platforms.[158] The organization was organized in a kind of vertically-integrated supply chain for internet news. An NBC interview of a former worker at the IRA, Vitaly Bespalov, revealed that workers were highly compartmentalized and used to amplify each other's work.

Meanwhile, the marketing team worked to package all of the misinformation into viral-ready social media formats. At the beginning of each shift, workers were reportedly given a list of opinions to promulgate and themes to address, all related to current events. Over a two-shift period, a worker would be expected to publish 5 political posts, 10 nonpolitical posts (to establish credibility), and 150 to 200 comments on other workers' posts. The professional trolls were also provided "politology" classes that taught them the Russian position on the latest news. Russian media outlets have reported that the IRA was bankrolled by a close Putin associate, Evgeny Prigozhin, a wealthy restaurateur known as the "Kremlin's Chef," whose network of companies have received a number of lucrative government contracts, and who was sanctioned by the Obama Administration in December 2016 for contributing to the conflict in Ukraine. According to one former employee, IRA staff on the "foreign desk" were responsible for meddling in other countries' elections. In the run up to the 2016 U.S. presidential election, for example, foreign desk staff were reportedly trained on "the nuances of American social polemics on tax issues, LGBT rights, the gun debate, and more . . . their job was to incite [Americans] further and try to 'rock the boat.'"

157 Elisa Shearer and Jeffrey Gottfried, "News Use across Social Media Platforms 2017," Pew Research Center, September 17, 2017, available at http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

158 This and the follow paragraph are drawn from Putin's Asymmetric Assault, 44–5.

4.4 Fake News

Fake news, a concept that was propagated during the 2016 U.S. election, includes both distortions of objective truths as well as misleading stories. In the line variously attributed to Thomas Jefferson, Mark Twain and Winston Churchill: "A lie is half-way round the world before truth has its boots on." As indicated by the U.S. case, fake Russian-sourced stories, such as concerns regarding Secretary Clinton's health and the Incirlik incident, received a significant number of views online, which meant that they had reached a large segment of the U.S. population. The spam messages from Russians to Ukrainians, telling them the cause was lost and their commanders had abandoned them, were in the same category. Distorted facts have been at the center of Russian news outlets which do not share the approach to factual evidence and truths that Western journalism would dictate.

The "Lisa" case in Germany was remarkably similar to the Russian operations in the United States.[159] The case dominated German headlines for two weeks in January 2016. A 13 year old Russian-German girl was missing for thirty hours, and was reported by First Russian TV to have been raped by migrants. In the end, German police established that the story was fake – she had been with a friend that night – but not before there was considerable attention to the story. Once the case was on First Russian TV, it was picked up by Russian foreign media like RT, Sputnik and RT Deutsch; the social media and rightwing groups distributed the information on the internet; that led to demonstrations, organized via Facebook, involving the German-Russian minority and neo-Nazi groups; when Russian foreign media in Germany reported from these demonstrations that brought the story to German mainstream media. Finally, Russian Foreign Minister Sergei Lavrov twice commented publicly that the German police and legal system failed to take such cases seriously because of political correctness.

Furthermore, spreading fake news is enabled by social media, which in general does not require verification of published posts and also provides a handy platform to reach audiences. It is especially problematic if fake news are able to "trend" on social media or be picked up and reported by mainstream media. The responsibility of social media, like Facebook and Twitter, to police their content will be continue to be debated. As of now, they recognize they are no longer mere platforms, with no responsibility for content, but they are not yet publishers either, in the sense of taking responsibility for the veracity of what they convey.

159 See Stefan Meister, "The 'Lisa case': Germany as a Target of Russian Disinformation," *NATO Review,* available at https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.

4.5 Strategic Leaks

Information and documents obtained via cyber or traditional espionage can be leaked to influence public opinion, perception, and discourse. The consequences of these leaks range from damaging operational (intelligence-gathering) security to undermining trust in a nation's political system and its leadership. In the U.S. case, the Russians conducted cyber espionage operations on major political organizations and persons, and used strategically-timed leaks to influence the popular discourse and to attack the U.S. democratic process. The Russians used Wikileaks as well as their own sponsored sites, Guccifer 2.0 and DCLeaks.com, to publish stolen materials from the DNC, DCCC and the Clinton campaign. Similarly, in the Russians' French election intervention, the Kremlin leaked stolen files from Macron's campaign 48 hours before the election. Leaks of information can be used to achieve specific political objectives and have been a defining feature of Russian hybrid threat campaigns against the political processes of foreign nations.

4.6 Funding of Organizations

Many countries seek to fund organizations or think-tanks that promote views friendly to their interests. Indeed, promoting ideas that further a country's interest is one of the oldest tools of political and social influence. Russia and China have been active in using this method to increase access to information of their perspectives in Europe and the Western hemisphere. In 2015, Beijing sponsored the opening of a Chinese think-tank called the Institute for China-American Studies (ICAS) – the first of its kind based in Washington. Analysts state that its goal is to spread China's views or policies among U.S. policymakers and to improve the perceptions of China in the West.[160]

Similarly, the Kremlin sponsors a number of organizations across the EU. Some receive funds from the Kremlin (although with opaque funding structures to avoid detection of Kremlin involvement) and many are also chaired by top Russian political figures or Kremlin-linked oligarchs. In 2006, Moscow created the World Coordination Council of Russian Compatriots to coordinate communication between Russian organizations in foreign countries with the Russian government.[161] For example, Russian businessmen with ties to Putin have financed the new Dialogue of Civilizations Research Institute (DOC) in Berlin, which opened in 2016. While DOC denies direct connections to the Kremlin, it has advocated for pro-Russia policies and defended Russian laws and methods. The German newspaper *Frankfurter Allgemeine Zeitung* (FAZ) has described it as an

160 Isaac Stone Fish, "Beijing Establishes a D.C. Think Tank, and No One Notices," *Foreign Policy,* July 7, 2016, http://foreignpolicy.com/2016/07/07/beijing-establishes-washington-dc-think-tank-south-china-sea/.

161 Putin's Asymmetric Assault, 47

"instrument of Moscow's hybrid warfare."[162] Institutions like these, which are funded by adversary states, provide resources and methods for these states to spread their ideas and viewpoints, injecting them into the conversation among policy and think-tank circles in foreign countries.

Kremlin-funded think tanks are primarily focused on legitimizing the Kremlin by painting a more favorable view of its narrative and by defending its policies. However, a number of them have also been alleged to be involved in influence operations abroad. For example, the Russian Institute for Strategic Research (RISS), a Kremlin think tank with offices across the Baltic states, has been suspected of seeking to prevent Montenegro's integration into NATO, influencing Bulgaria's national elections, and thwarting Swedish efforts to strengthen its ties with NATO countries.[163]

Some organizations are also funded by local political parties that are pro-Russia. These are often the result of a desire for closer relations with Russia. In Italy, the far-right Northern League (or LN) has set up the Lombardy-Russia Cultural Association (ACRL) to support political connections with Russia, promote Russian narratives in Italy, and facilitate business relations between LN and Russian entities. Influence LN and ACRL officials also have direct close relations with a number of Russian oligarchs in the business, media, and policy circles.[164]

4.7 Political Parties

The Kremlin also seeks to exert influence via political parties in foreign nations that have close ties with or are funded by Moscow. Latvia's Harmony Centre and Estonia's Centre Party are both suspected of being heavily funded and influenced by the Russians.[165] Similarly, Marine Le Pen's far-right National Front in France has been reported to receive loans from Russian banks, including in support of Le Pen's presidential candidacy in the 2017 French elections.[166] The potential influence of these parties is limited by their inabilities to gain seats in the government. In Latvia and Estonia for example, civilian fears of these Russian-dominated parties gaining political power complicate their efforts.[167]

---

162 Ben Knight, "Putin associate opens Russia-friendly think tank in Berlin," *Deutsche Welle,* July 1, 2016, http://www.dw.com/en/putin-associate-opens-russia-friendly-think-tank-in-berlin/a-19372110.

163 Putin's Asymmetric Assault, 48

164 The Kremlin's Trojan Horses, 14

165 Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses*. Santa Monica, CA: RAND Corporation, 2017, available at https://www.rand.org/pubs/research_reports/RR1577.html.

166 https://www.politico.eu/article/le-pen-russia-crimea-putin-money-bank-national-front-seeks-russian-cash-for-election-fight/

167 Radin, 20.

It is also important to note that pro-Russian political parties can be found on both the left and right of the political spectrum. Nor do they necessarily need to have formal agreements with Moscow. For Russia, the ideological stances of political allies are less relevant than their ability to help Russia in its fight against the West.[168] Rather, these parties – and their policy platforms – are distinguished by their spread of Russian narratives, support for the Kremlin's foreign policies, and proposals for action that contribute to Russia's geopolitical interests. For the most part, these actions are generally anti-American and anti-Western.[169]

At the core of any form of political influence is also the direct diplomatic relationship that leaders from two countries have with one another. Putin, for his part, acutely recognizes this. In Greece for example, he has made it a personal mission to maintain a close relationship with the leadership of Greece's ruling Syriza party. Putin has kept in close communications with Prime Minister Alexis Tsipras, speaking by phone, holding summits, and meeting at the sidelines of multilateral settings such as the Belt and Road Forum held in Beijing in May 2017. Their close relationship is also often captured by media reports and conveys the image of a highly important and symbolic historical relationship between two Orthodox nations.[170]

4.8 Organized Protest Movements

The Kremlin also seeks to exploit protest or separationist movements in Europe. In 2016, Moscow backed anti-European Union groups in a Dutch referendum on trade with Ukraine.[171] Russia also likely supported protest movements, including funding an anti-shale gas media campaign, in Bulgaria, one that sought to combat policies that would reduce Bulgarian dependence on Russian energy sources, which serves as one of the Kremlin's strongest economic source of leverage.[172] These protests resulted in Bulgarian prime minister, Boyko Borisov, cancelling a license for Chevron to explore for shale gas in the country.[173]

4.9 Oligarchs

Moscow maintains a set of connections in foreign countries via Russian oligarchs with ties in politics, business, media, and commerce. These people serve as Kremlin proxies by maintaining close ties with local entities and, if necessary, acting as a

168 Kremlin's Trojan Horses, 2–3
169 *Ibid*, 12
170 *Ibid*, 7
171 Christopher S. Chivvis, "Understanding Russian "Hybrid Warfare": And What Can Be Done About It."
172 https://www.ft.com/content/e011d3f6-6507-11e4-ab2d-00144feabdc0
173 *Ibid*.

force of influence in their respective industries and, ultimately, in the political process. In Greece, for example, a Russian-Greek businessman who is member of the Russian parliament and of Putins' United Russia party, Ivan Savvidis, has significant investments in the Greek economy. Additionally, Savvidis has bought large stakes popular Greek television networks and newspapers. He has worked in Greece in advocating against the pro-Western democratic opposition party.[174]

In Spain, while Moscow may not have an extensive web of official diplomatic or economic influence, the Kremlin benefits from a number of individuals or entities with different positions of influence across Spanish society and politics who sympathizes with Russia's worldview and narrative. They actively promote Russia's worldview, emphasizing the need to understand it, while simultaneously justifying its actions in Syria, Ukraine, or elsewhere. While these individuals may not directly be Russian-placed, they nonetheless help make the country susceptible to potential Russian influence, especially if its civil society is already developing a tolerance for Moscow's worldview and policy choices.[175]

4.10 The Orthodox Church

With strengthened relations with the Russian Orthodox Church, the Kremlin has sought to use the Church as a proxy in European countries that serve to legitimize the Kremlin's narratives, interests, and worldviews. This is facilitated by the fact that the Kremlin and the Russian Orthodox Church have a number of overlapping foreign policy objectives. The Orthodox Church has played a large role in bridging connections between the Greek and Russian leadership and communities. The far-right, pro-Russian political party in Greece, Golden Dawn, has repeatedly made reference to the religious bonds between the Greeks and Russians that make the two countries natural and historical allies.[176] In 2003, a formal working group between the Russian Orthodox Church and the Kremlin was established to facilitate the cooperation between the two countries on a number of foreign policy initiatives.[177]

4.11 Cyber Tools

This is the newest form of threat, and the one still hardest to conceptualize, after twenty years of seeing it in action. At one end, virtually any future kinetic war will be accompanied by cyber attacks on surveillance and command and control. Near that end, cyberwar can be a substitute for kinetic strikes – witness

174 Kremlin's Trojan Horses, 7–8
175 *Ibid*, 21
176 *Ibid,* 8–9
177 Putin's Asymmetric Assault, 53–54

Stutznet. Next on that continuum is attacks aimed specifically at society – at finance, water, power or other infrastructure. So far, those have been relatively few. The celebrated major attacks on the United States – Sony, Office of Personnel Management (OPM), Democratic National Committee (DNC) – have been cyberespionage, using cyber means to extract private, if not secret, information. The first and last were turned into propaganda by the attackers, North Korea and Russia, while the second, by China, created a long-term and uncertain risk. The nuclear analogy for cyber is misleading, in particular because attribution was relatively straightforward for it, not for cyber. The biological analogy seems more helpful: cyber "Armageddon" is unlikely in the extreme because every attack reveals to the victim where it is vulnerable. Thus, the premium is on remediation and prevention.

While the essence of espionage – that is, the covert gathering of information for a purpose – is not new, the existence of the cyber dimension also empowers new tools and lowers the entry cost of using them. Indeed, cyber operations are low risk and low cost, but can yield great results. This makes cyber tools attractive to poorer countries – or to ones whose economic trajectory is downward, like Russia. Indeed one the of the worrisome side effects of the Snowden revelations about NSA and the Vault 7 disclosures of CIA tools have been to drive home to other countries how far behind they are in cyber tools, especially offensive ones, and thus served as an incentive to develop – or buy – better. Ultimately, the cyber realm can be exploited in three ways – espionage, attack, and data manipulation.[178]

Cyber espionage. This is similar to traditional espionage operations, aiming to gather information for the sponsored state. The stolen information collected during such operations can either be relayed via sites like WikiLeaks to influence public discourse and opinion – thereby becoming an essential part of information warfare – or kept covert by the hybrid threatener for its own benefits. APT 28 and APT 29 are two well-known hacker groups with ties to Russian intelligence services, and are known to have conducted a number of espionage operations against foreign nations. In 2015, APT 29 hacked into the U.S. White House, State Department, and Join Chiefs of Staff networks, as well as organizations in Western Europe, Central and East Asia, and Central and South America. APT 28 was also found to have hacked into military- and defense-related units in America, Europe and Asia. It was also behind the German Bundestag and France's TV5 Monde hacks in 2015. Both groups also played a significant role in

178 The Snowden leaks of NSA tools has been well reported. In March 2017, Wikileaks released a set of CIA tools, dubbed "Vault 7" for hacking into cellphones, telephones and other digital devices. See Scott Shane and others, "WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents," *New York Times,* March 7, 2017, available at https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html?_r=0

Russia's influence campaign during the 2016 US Presidential election by hacking into major US political organizations. In additional to hacks and leaks, Russia also conducted covert cyber hacks of infrastructure directly associated with the election such as voter registration systems, voting equipment retailers, and state electoral boards. While the effect of these hacks are not yet clear – although it has been concluded by U.S. intelligence that actual vote count was not influenced by these hacks – it is likely that Russia aimed to gain materials and knowledge of the electoral system which can be applied to render the U.S. more vulnerable to future influence campaigns.

Cyber attack. The 2010 discovery of Stuxnet in Iran's computer systems led to the realization of a new type of cyber warfare technique. Nicknamed "the world's first digital weapon," Stuxnet was unlike other cyber malware in that it not only stole from compromised networks but also destroyed the physical equipment that the computers controlled.[179] The malware attack included two different versions: the first sought to damage Iran's centrifuges, thereby tampering with the country's enrichment process, and a second version was aimed at manipulating the computer systems of companies that provided industrial control and processing systems for Iran's nuclear program, including the monitoring and control of the speed of centrifuges.[180] In late 2009, over the span of just five months about 1,000 centrifuges were destroyed by the malware.[181] The discovery of *Stuxnet* presents a great dilemma for national security, as it indicates the ability of cyber tools to bring about destruction of equipment in the physical realm. Cyber attacks have targeted critical infrastructure, notably in Estonia in 2007. In response to Estonia's razing of a Soviet monument in the center of Tallinn, attackers targeted virtually all of Estonia's electronic infrastructure – all major commercial banks, telcoms, media outlets, and name servers – the phone books of the Internet.[182]

For China's part, it PLA Unit 61398 – '"Comment Crew" – is the 2nd Bureau of the Chinese People's Liberation Army's General Staff Department's 3rd Department. Its main location is known. The most troubling attack to date by Comment Crew was a successful invasion of the Canadian arm of Telvent. The company designs software that gives oil and gas pipeline companies and power grid operators remote access to valves, switches and security systems. Telvent keeps detailed blueprints on more than half of all the oil and gas pipelines in North and South America, and has access to their systems.

---

179 https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

180 *Ibid.*

181 *Ibid.*

182 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired,* August 21, 2007, available at https://www.wired.com/2007/08/ff-estonia/.

Cyber Manipulation. Hacker groups can also seek to manipulate or change information stored on a computer network once they gain access to a system. In 2015, U.S. National Security Agency (NSA) director Michael Rogers testified that manipulation could pose a serious challenge in the future. "At the moment, most of the [cyber hacks] has been theft," Rogers said, "but what if someone gets in the system and starts manipulating and changing data, to the point where now as an operator, you no longer believe what you're seeing in your system?"[183] Similarly, the Director of National Intelligence (DNI), James Clapper expressed similar concerns, stating: "I believe we'll see more cyber operations that will change or manipulate electronic information to compromise its integrity."[184]

One of the most serious incidents of electronic manipulation was in 2013, when Syrian hackers accessed the Associated Press' Twitter account and tweeted out false reports of a White House explosion that had injured President Obama. This resulted in a 150-point drop in the Dow and "erased $136 billion in equity market value," as reported by Bloomberg.[185] One of the first attempts to manipulate data for political objectives, however, occurred during the 2016 US Presidential election. Russian hackers who gained access to the Illinois voter database attempted but failed to alter registrant information.[186] Data sabotage will only become more frequent in the future and could potentially be more problematic than the other two cyber threats given how hard it is to detect and the potentially devastating effects of even a small alteration.

4.12 Economic Leverage

Economic levers can come in the form of foreign aid assistance, sanctions, and the use of loaned resources as bargaining chips to put pressure on a foreign government. This form of leverage is hardly new by any means, but it remains one of the most important and effective tools to influence decision-making in another country. Economic influence is also not solely limited to trade, but also includes other industries such as energy and tourism.

For its part, the United States long has used economic sanctions against foreign nations, and since the globalization of international finance centers on it, it has become more active and more targeted in its sanctions – for instance, in applying sanctions to particular individuals and not just in terrorist groups

183 http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers-will-change-your-data-not-steal-it

184 *Ibid.*

185 *Ibid*

186 Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider than Previously Known," Bloomberg, June 13, 2017, available at https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

but in Russian and elsewhere. For instance, the recent Joint Comprehensive Plan of Action (JCPOA) with Iran serves as clear evidence of the effectiveness of economic leverage. The sanctions imposed by the United States, the European Union, and the UN all played a role in pressuring Iran's economy. In the end, Iran agreed to nuclear obligations under the JCPOA in exchange for the lifting of sanctions that had been imposed as a result of Iran's nuclear development.

Russia's hybrid warfare campaign against Ukraine also employed a large economic attack package that put pressure on the Ukrainian leadership to deter it from integrating into the EU. The Kremlin used cheap gas and loans to pressure President Yanukovych to abandon the EU-Ukraine Association Agreement negotiations. It also used coercive economic leverage, for example by threatening gas prices increase and cancelling loan programs, to achieve the Kremlin's objectives. It is also important to note that many of these vulnerabilities were created by the Russians, who coerced Yanukovych into signing the original loans deal that was much more favorable to Russian interests than to Ukraine. Russia also recognizes the significance of its energy dominance in the region, as observed by its efforts to invest to build energy infrastructure dependent on Russian resources. For example, Russia's state-owned gas company, Gazprom, has purchased large stakes Greece's energy industry. By providing discounted energy to the country, Russia not only paves the way for future use of its economic leverage, but also thwarts the EU's efforts to neutralize Russia's expansion of its sphere of influence.[187]

China also utilizes its growing economic power as a source of leverage in international affairs. Most recently, it has sought to punish South Korea in order to push back against deployment of the American anti-missile system, THAAD (theater high altitude anti-missile defense). Beijing has scaled back Chinese tourists to the country, banned K-Pop musicians from mainland concerts, censored South Korean television, and businesses have boycotted South Korean brands and goods. While these sanctions have been "unofficial," the latest summit meeting between South Korean president Moon and Chinese President Xi in November 2017 reportedly resulted in Seoul agreeing to military constraints in return for the lifting of these sanctions.[188]

Yet it is worth noting that the effectiveness of economic leverage is dependent on the vulnerabilities of a state's economy to them. North Korea is the classic case: a generation of international sanctions against the North Korean regime has yet to bring Kim Jong-un and his country to serious negotiations. This is partly because China has remained an enormous leak in the sanctions. But North Korea is not as vulnerable to international sanctions because it is barely part of the global economic infrastructure. On the other hand, Iran's economy is more tied

187 Kremlin's Trojan Horses, 6

188 http://www.scmp.com/week-asia/geopolitics/article/2120452/china-wins-its-war-against-south-koreas-us-thaad-missile

to the international economy compared to its North Korean counterpart, which is why sanctions were ultimately effective. Similarly, Ukraine's dependence on Russian gas and its debt to the Kremlin made it incredibly vulnerable to Russian economic instruments of power.

In Russia's case, however, heavy economic investment is a less strategic choice compared to the Chinese. While China benefits from a large economy that allows for it to make large investments in infrastructure or national debt, the Russians have few economic resources available at its disposal. As such, while it seeks to deepen the region's energy dependence on its natural resources, it has not sought to become a major foreign investor in European countries. It is thus also important to recognize that tools such as disinformation, cyber, and political allies are more appealing as a tool of influence. They have a greater potential for destabilizing a foreign country's politics but also come at a much cheaper price compared to economic investment or military actions.[189]

4.13 Proxies

Again, there is little new about proxy or unacknowledged conflict. The United States is hardly a stranger to wars by proxy: in the Revolution, it confronted the Hessians, and was aided by a range of what we'd now call "foreign fighters," drawn by the lure of freedom. During the Cold War, Americans and Russians took pains to assure that their troops never confronted each other directly, and so most conflict between the two was by proxy – in the later Cold War mostly in Africa and Central America. In general, proxy groups are entities that hold views favorable to a foreign state or whose own interests align them with that state. Yet proxies often have interests of their own that diverge from those of their patrons – the classic principal/agent problem.[190] They range from organized states and paramilitary organizations, to political parties, or protest/separationist movements. Proxies can be viewed as a tool to gather intelligence as well as to exert political influence in a foreign country.

4.14 Unacknowledged War

Proxy war slides into this category. Proxies are sometimes not acknowledged, but the secret usually is an open one. So it was with the *contras* in Central America in the 1980s, and the mujahidin fighting Soviet occupation in Afghanistan

189 Kremlin's Trojan Horses, 4

190 For an interesting discussion of these issues in the context of hybrid threats, see Frank J. Cilluffo and Joseph R. Clark, "Thinking About Strategic Hybrid Threats – In Theory and in Practice," PRISM, 4, 1, 49ff. Available at http://cco.ndu.edu/Portals/96/Documents/prism/prism_4-1/prism46-63_cilluffo-clark.pdf.

in the same period. U.S. support to both was an open secret, but the lack of acknowledgement let diplomatic exchanges proceed as though the support wasn't happening; it gave the Soviet Union a fig leaf, especially in Afghanistan. Putin's "little green men" or the so-called "separatists" in eastern Ukraine are in the same category, though Russia has gone to great pains to try to sustain the fiction that they are independent of Moscow.

4.15 Paramilitary Organizations

Russia also funds and equips various paramilitary organizations with pro-Russian or ultranationalist agendas to further its interests on its periphery. One of the Kremlin's most active proxies is the Night Wolves, a biker club and ultranationalist gang that has close ties to President Putin himself.[191] It has been used to intimidate civilians and can be used to operate hybrid activities in a region. During the Crimean crisis, members of the Night Wolves in the region claimed to be there to ensure a free and fair referendum and to assist the local population in fighting against the local fascists.[192] Similarly, a paramilitary group in the Donetsk region in Ukraine called the Russian Orthodox Army has been active in advocating ultranationalist sentiments and expressing outrage towards Western influence in the region. The group is trained to conduct activities such as reconnaissance, defense, and sniping.[193]

While Russia's special forces (SPETSNAZ) are technically part of Russia's military, intelligence and security services, it is also important to emphasize them here. SPETSNAX operate covertly, for example by masking their faces and wearing nondescript attire, thereby providing plausible denial to the Kremlin.[194] These "little green men" played a prominent role in the annexation of Crimea in 2014 as well as in the Georgia crisis in 2008.[195] While this measure of deniability may be superficial, it did weaken the ability of the attacked nation – or NATO – to respond to their involvement without verifiable attribution to Moscow.

4.16 The Synchronization of Tools

These instruments of power and influence, when employed simultaneously to achieve a common political objective, make up hybrid warfare. However, identifying these tools does not permit predictions of what a hybrid warfare campaign will resemble or what kinds of effects it will achieve. The function of each tool

191 Little Green Men, 44.
192 *Ibid.*
193 *Ibid,* 43–44.
194 Little Green Men, 43.
195 *Ibid.*

and the degree to which it is employed are also dependent on the *objectives* of the actor state and the *vulnerabilities* present in the target state, issues that will be taken up in the next two sections. This ambiguity of hybrid warfare is important for a number of reasons:

- First, it makes a hybrid warfare campaign, and the different tools used, not easily detectable. This is especially true in the cyber realm, where verifiable attribution often is difficult, thus complicating the target state in framing a response. Because hybrid warfare also employs instruments across multiple domains, it also allows for a state to stay below both the radar of detection and the threshold for responding under international law. The result slows down even if it does prevent the target state from responding.
- Second, the effects of a hybrid campaign are non-linear, making it unpredictable and thus potentially more devastating than conventional types of warfare. Especially given that certain tools may escape detection, the effects of a campaign may not be observed until they are already in full force. The nature of information campaigns also contributes to this unpredictability, given the role of the virtual domain and social media.
- Third, the ambiguity of hybrid threats facilitates the speed and ease at which a hybrid warfare actor may change targets, objectives, and the tools employed according to how the campaign is progressing. That makes it more difficult for the target to come to a definition of the threat. The various domains involved in hybrid warfare naturally require some form of centralized control, which speeds up decision-making processes of both horizontal and vertical escalation and de-escalation. This thus compounds the ambiguity and unpredictability of hybrid warfare.

The non-linear effects of hybrid warfare were on display in the two episodes showcased in this report. In the Crimea, and especially the Ukraine, case, the multiplicity of instruments allowed Moscow to shift tactics as circumstances changed, while maintaining a least a fig-leaf of plausible deniability. The campaign began with economic pressure on the regime, then turned to political warfare, using a diverse network of political operatives, businessmen, criminal elements, and powerful oligarchs to oppose Ukraine's new government. When pro-Russian protests broke out in March 2013, there is some evidence that Russia choreographed them, paying Russians and sending them into Ukraine. The escalation continued as the protest movement in eastern Ukraine turned to irregular warfare, with Russia primarily in a train-and-equip mode. Throughout, Russia used money, intimidation and propaganda against Ukrainian troops, with some success in creating defections.

By June, Russia had escalated the conflict vertically, by supplying the separatists with better weaponry, especially air defenses. When that proved insufficient, Russia intervened directly in August, sending at least 1000 Russian soldiers (and perhaps as many as 4,000), while all the while denying that it was doing

so. When Ukraine captured ten Russian paratroopers, the Kremlin claimed they had crossed the border accidentally. By September, the combination of shifting Russian tactics had produced enough of a stalemate to lay the basis for the Minsk negotiations – on a basis favorable to the separatists and to Russia.

In the case of the 2016 US Presidential election, Russia's hybrid campaign relied mainly on cyber tools and proxies to support a robust propaganda and disinformation campaign. While much of the commentary on Russia's meddling focused on the leaks that resulted from CozyBear and FancyBear's hacks, it is equally important to notice the timing of the hacks and leaks. CozyBear infiltrated the DNC network in 2015, and stayed quiet for over a year before it was discovered. FancyBear, while it did steal documents from the network, did not leak any data until after allegations of Russian involvement had been publicly reported. This is interesting to note because it suggests that the Kremlin's original objective was mere cyber espionage. Once exposed, however, there were no incentives to stay quiet. A day after these reports were confirmed, the anonymous persona Guccifer 2.0 emerged online and claimed sole credit for the attacks, and the documents were also later relayed via Wikileaks.

Here, the timing of the leaks served two purposes: first, it distracted from the reports regarding CozyBear and FancyBear's ties to Russia; and second, it aimed to shift the blame away from Russia. Similarly, the release of documents stolen from the Clinton campaign were also strategically timed. Podesta's private emails were published on Wikileaks on the same day that the Obama White House formally issued a statement condemning Russia's meddling in the U.S. election, as well as when Trump's "Access Hollywood" tapes were published.

The fact that CozyBear had remained quiet during its cyber espionage operation also shows the Kremlin's dependence on using the cyber realm for intelligence purposes. In this regard, it adopted a "wait-and-see" strategy, acting only when an opportunity presents itself. This is also significant in the context of Russia's hacks into the U.S. election infrastructure. Although these hacks did not serve any direct purpose in the 2016 election, the access gained by the Russians provides opportunities and experiences for the Kremlin to apply to similar campaigns in the future.

Finally, while it is widely recognized that the Russians have indeed meddled in the U.S. election, the use of proxies like Guccifer 2.0 and Wikieaks, and even to a certain extent FancyBear and CozyBear, complicates complete attribution to the Kremlin. To this day, President Putin continues to deny the Russian state's involvement in the election and claims that, even if the hackers were Russian, they conducted these cyberattacks on their own rather than at the Kremlin's directive. This is similar to the "little green men" in Ukraine: despite the evidence that they are Russian forces in mufti, the Kremlin can continue to claim that they are local forces.

Chapter 5: Vulnerabilities

Both the Ukraine and U.S. elections cases drive home the point that hybrid attackers did not create the vulnerabilities they exploited. Ukraine's political and economic circumstances made it extremely vulnerable to Russian actions, and the deeply polarized American political context of 2016 was an open invitation to Russian meddling. That means that the first phase of countering hybrid threats is both imperative and difficult – assessing vulnerabilities at home. Yet democratic governments will find it difficult to admit, let alone assess, that their politics are polarized or that extremist factions are home grown.

But that vulnerability assessment is the first step in preparing to respond to hybrid threats.[196] Not only is that assessment often politically delicate, it is necessarily a whole of government exercise, as will be seen in the discussion of good practices in various countries. The exercise depends on high-quality intelligence, as well as robust counterintelligence, but it needs to identify vital functions of society, and the vulnerabilities within them. One critical dimension is how, and in what ways the country is dependent on digital services, and how vulnerable those ways are to exploitation by a cyber threatener. The assessment probably should include a relevant set of threat scenarios that can be used to support planning for defense.

196 See Aapo Ederberg and Pasi Eronen, "How Can Societies be Defended against Hybrid Threats?" Strategic Security Analysis, Geneva Centre for Security Policy, September 2015, available at http://www.defenddemocracy.org/content/uploads/documents/GCSP_Strategic_Security_Analysis_-_How_can_Societies_be_Defended_against_Hybrid_Threats.pdf.

The dimensions of vulnerability include:

5.1 Proximity and Access[197]

Simple geography makes the Baltic states, as well as Ukraine, vulnerable to Russian hybrid threats. Most obviously, Russia's regional military advantage makes credible the threat of Russian use of force. In the words of one analyst: "A large-scale conventional Russian incursion into the Baltics, legitimized and supported by political subversion, would rapidly overwhelm NATO forces currently postured in the region. If NATO leaders are to have confidence in their ability to deter such an attack, they will likely need to deploy additional forces to the region and to improve certain capabilities within their forces."[198] Russia has relatively easy access to them, all the more so given the presence of Russian speakers. That was obvious in the case of Ukraine. A less noticed case was the abduction of an Estonian national, a member of the Estonian Internal Security Service, on Estonian territory, who was then taken to Russia and tried for espionage – a reminder that vulnerabilities to hybrid threats not limited to national boundaries.[199]

Societal Fault-Lines. Here, the most obvious divide is the presence of considerable numbers of Russian speakers in some of the target countries – over a third of the population in Latvia and almost a third in Estonia and Ukraine, compared to about 8 percent in Lithuania. In all cases, the Russian speakers are concentrated in the capital cities and along the borders with Russia. However, care is called for in reasoning too directly from the presence of Russian speakers to vulnerability to hybrid threats. Still, Russian-speaking population make those countries vulnerable to Russian covert action – for instance, to provoke conflict between Russian speakers and Baltic governments, creating perception that local Russian speakers support Russian military action. And as NATO bolsters its deployments in the Baltic countries, Moscow can play on anti-NATO deployment sentiments among Russian speakers in the region.

---

197 This framework draws on Christopher Chivvis, "Hybrid War: Russian Contemporary Political Warfare," *Bulletin of the Atomic Scientists*, September 1, 2017, available at http://www.tandfonline.com/doi/abs/10.1080/00963402.2017.1362903?journalCode=rbul20&

198 Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses*, RAND Corporation. 2017, available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf.

199 Björn Fägersten, Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence. Center for Transatlantic Relations, available at http://transatlanticrelations.org/wp-content/uploads/2017/02/resilience-forward-book-fagersten-final-version.pdf. Agnia Grigas, "Estonia: Potential Vulnerabilities amid Progress," American Enterprise Institute, December 2017, available at http://www.aei.org/wp-content/uploads/2017/12/Estonia-Potential-Vulnerabilities-amid-Progress.pdf.

Other fault-lines may be generational, with young people for whom the Cold War is distant history less aware of possible threats, perhaps all the more so to the extent that they get most of their "news" from social media. They also may be more inclined to trust the "news" that comes personalized on their phones than are their elders. These issues of fault-lines and social trust are plainly delicate but just as plainly are critical to any vulnerability assessments.

5.2 Political Divisions

Particular events, like the U.S. elections or Britain's Brexit, may sharpen pre-existing divisions, creating opportunities for hybrid threateners to exploit. In May 2016, 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.[200] "Stop Islamization of Texas," it cried. But the 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, but given the political division in the country, the clashing protests could easily have ended in violence.

Political divisions run across countries as well as within them. The need for cohesion in international institutions, like the EU, NATO, and OSCE, provide opportunities for threateners to degrade decision-making by supporting fringe parties, co-opting weak national leaders or dividing countries by modes of negotiation. Indeed, from an attackers perspective, hybrid threats may be attractive because they are ambiguous enough not to fall neatly into NATO processes – neither Article IV's right of members to bring issues of concern, especially about the security of a member, to NATO for consultations, nor the Article V provision than an attack on one is an attack on all.[201] So, too, the Western democracies are dependent on global flows of capital, information and energy. Thus, "growing interdependencies means that resilience is not merely a national affair, and neither is it confined to current interdependencies – others may emerge over time."[202]

---

200 As reported in Farhad Manjoo, "Reality TV, As Produced in U.S. by Russia," *New York Times (international edition),* November 10, 2017, 7.

201 Katie Abbott, "Understanding and Countering Hybrid Warfare: Next Steps for the North Atlantic Treaty Organization," University of Ottawa, March 23 2016, available at https://ruor.uottawa.ca/bitstream/10393/34813/1/ABBOTT%2c%20Kathleen%2020161.pdf.

202 Fägersten, 2.

5.3 Social Media

The role of social media is a theme running throughout this paper. It is indeed the great irony of the Information Technology revolution that all the wonderful apps, like Facebook, intended to connect people instead ended up segmenting them into their own "echo chambers" where they hear only what they already believe. As mentioned earlier, a 2016 survey noted how many Americans turn to social media for their news: 67 percent of adults, up from 62 percent the year before, and for Americans under 50, 78 percent. European seem less prone to turn to social media for news than Americans, but that may just be a time lag. In any event, the echo chambers are tailor-made for hybrid threateners to enflame passions even to the point of violence, as Russians posing as Americans did in the controversy over the Houston mosque.

5.4 Energy Dependence

The states in the Baltic and southeastern Europe remain dependent on Russian energy supplies, especially natural gas. And that constitutes, as the Ukraine case shows, a significant vulnerability. Indeed, the Russian-Ukrainian gas connection has come to crisis in January 2006, January 2009, and June 2014, when Russia terminated supplies, ostensibly over price. In the words of one analyst: "A lack of energy security can expose a country to vulnerabilities because it hinders the country's capacity to provide basic needs to its citizens (such as heat during winter months), as well as fulfill its energy providing requirements to heavy industries and companies – both key components to maintaining efficient and effective domestic sovereignty through the provision of public goods."[203]

Europe's dependence on Russian energy has been an issue in trans-Atlantic relations for forty years, with the current issues surrounding whether to build Nord Stream 2 – pipelines through the Baltic Sea from Russia to Germany.[204] The concern is that the project would further bind Europe to Russian gas and, in the process, reduce transit revenues for bypassed countries, like Ukraine. In a world of increasing energy supply and continued low prices, dependent countries should have the possibility of decreasing their dependence – though it is not as easy as it looks. Most European recipients of Russian gas have contractual obligations into the 2020s. Breaking those, or letting them lapse, in the interest of diversifying supply would entail significant infrastructure costs for LNG terminals or pipelines. And Russian gas will remain competitive in price with alternatives, including American LNG, out to 2030.[205]

---

203 Abbott, 19.

204 See Putin's Asymmetric Assault, 6.

205 See The Oxford Institute for Energy Studies, *Reducing European Dependence on Russian Gas: Distinguishing Natural Gas Security from Geopolitics,* October 2014, available at https://www.oxfordenergy.org/wpcms/wp-content/uploads/2014/10/NG-92.pdf.

Chapter 6: Objectives

For Russia, plainly its strategy for hybrid threats is the same as its general strategy; indeed, hybrid threatening *is* its strategy. Vladimir Putin has been crystal-clear about his strategic objectives – to dominate Russia's "near abroad" and to see Russia recognized as a major global power. Russia sees the United States and NATO as the leading challenges to its interests and security, especially since 2012.[206] Indeed, a 2014 revision to its military doctrine labeled the Alliance as the chief "danger" or "risk" to Russian security.[207]

In particular, integrating former Soviet republics into the European Union and NATO has been a particular hot button, along with the Western countries' efforts to promote democracy and pro-Western values in the region. Putin has referred to the 1990s as a period when the West took advantage of a weakened Russia, and has vowed that now that Russia is strong again, it will not happen again.[208] In this perspective, the "color revolutions" in Eastern Europe are not indigenous movements spearheaded by local activists, but rather regime changes supported and funded by the West. Indeed, one of the drivers of Russia's anti-

---

206 For a thoughtful discussion of the next stage of Russian-American relations, see James N. Miller Jr. and Richard Fontaine, *A New Era in U.S.-Russian Relations: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict,* Belfer Center, Kennedy School of Government and Center for New American Security, September 2017, available at https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-ProjectPathways-Finalb.pdf?mtime=20170918101504.

207 "The Military Doctrine of the Russian Federation," December 25, 2014, available at http://rusemb.org.uk/press/2029.

208 "Transcript: Putin says Russia will protect the rights of Russians abroad," *Washington Post*, March 18, 2014, https://www.washingtonpost.com/world/transcriptputin-says-russia-will-protect-the-rights-of-russiansabroad/2014/03/18/432a1e60-ae99-11e3-a49e-76adc9210f19_story.html.

Clinton intervention in the 2016 elections was Putin's belief that she had instigated unrest during Russia's parliamentary elections in 2011.[209]

Thus, from Moscow's perspective, much of what it is doing is defensive, responding to the concern that the United States and its allies are on the offensive, seeking to undermine the political integrity of Russia. In this view, Russia's opponents are using a variety of political and economic tools to penetrate Russian society. In response, Moscow ejected the U.S. Agency for International Development, and closed numbers of non-governmental organizations.[210]

Given its position and perspective, Russia has played a weak hand very well. It knows that, while it has local military superiority on its border, it would lose any major military confrontation. So, too, it cannot win an economic competition; its Eurasian Economic Union is hardly likely to be a pole of attraction. So Russia seeks to change by other means the regional and global national security systems of the Western adversaries. It continues to do this by creating confusion, chaos and uncertainty among the institutions of their adversaries. It will work to have people, especially inside Russia, look to the West and say "see the West, they are just as corrupt and just inept as you think Russia is." Yet, look at us, we held our ground in Syria, we took back the Crimea our rightful territory, we protect ethnic Russians in Belarus and the Ukraine."

Hybrid threats provide new measures of power and influence. While the end of the Cold War seemed to end the risk of immediate military conflict in Europe, Russia has always felt vulnerable on its Western front, and controlling the countries in its periphery has been at the heart of the country's core interests in the 21st century. The NATO alliance, which has slowly spread to Russian borders, is extremely problematic, but the U.S. deterrent makes it difficult for the Kremlin to take any overly active steps. With hybrid warfare, however, the deployment of both conventional and unconventional tactics has allowed the Kremlin to take relatively smaller steps in any individual domain that can nonetheless strengthen its own power vis-à-vis the West's. What makes hybrid warfare attractive is the rising costs of conventional or overt methods of warfare. The anonymity and ambiguity inherent in hybrid threats, along with the potential to yield high rewards, means that hybrid warfare's prominence in foreign affairs will only increase in the future.

---

209 Joby Warrick and Karen DeYoung, "From 'reset' to 'pause': The real story behind Hillary Clinton's feud with Vladimir Putin," Washington Post, November 3, 2016, https://www.washingtonpost.com/world/national-security/fromreset-to-pause-the-real-story-behind-hillary-clintons-feudwith-vladimir-putin/2016/11/03/f575f9fa-a116-11e6-8832-23a007c77bb4_story.html?utm_term=.f23256f5020f.

210 See "Russia expels USAID development agency," BBC, September 19, 2012, http://www.bbc.com/news/world-europe-19644897; and "Russia: Four years of Putin's 'Foreign Agents' law to shackle and silence NGOs" (Amnesty International, November 2016), https://www.amnesty.org/en/latest/news/2016/11/russia-four-years-of-putins-foreignagents-law-to-shackle-and-silence-ngos/.

A thumbnail sketch of recent Russian influence operations in Sweden summarizes both strategy and tactics, along with some shortcomings. It underscores that those operations are relatively cheap, so they are a natural for a state that is, in many respects, a failing one.

- *Expanding in concentric circles.*[211] Surely, Russia is the poster-child for influence operations. It is hardly alone, though, in taking public diplomacy seriously. Since the inception of its English language TV network Russia Today in 2005 (now RT), the Russian government has broadened its operations to include Sputnik news websites in several languages and social media activities. These measures have been complemented with coordinated campaigns, using Western public relations firms, think-tanks and lobbyists to further Russian foreign policy goals. Moscow, however, has also been accused of engaging in covert influence activities – behavior historically referred to as "active measures" in the Soviet KGB lexicon on political warfare. Those have increased since Georgia and Ukraine. They have expanded in concentric circles – first against Russia itself and the domestic population. Indeed, one of the striking issues at meetings the Centre of Excellence has sponsored was whether Russian operations represented a resurgent Russia flexing its muscles or a weak one trying to bolster domestic support with nationalist action. The second circle is the post-Soviet space, the "near abroad," and the third, since 2014, is Europe and beyond.
- *Back to the Cold War.* Public diplomacy, like RT or Sputnik, is important but problematic. Like past Soviet propaganda, Russian public diplomacy today can also be wildly inconsistent. The West is portrayed as weak but at the same time as a near- existential threat to Russia. Europe is described as both xenophobic towards refugees, but foolish for allowing so many of them to seek asylum. Russia's current approach seems "back to the Cold War," with fronts, fake documents, and financing for sympathetic parties – all interconnected as "active measures."
- *Information warfare is part of national security.* Thus it is defensive, not offensive. Russia is under threat. Information campaigns are meant to support Russia's interests, not necessarily Putin – to get sanctions removed or support Russia's annexation of Crimea. This lineage runs far back, to the Protocols of the Elders of Zion in Czarist times before World War I. And Russia efforts can draw plausibility from sources closer to home: for instance, Russia alleges that the CIA killed JFK, but Oliver Stone's movies come close to making the same

211 For more detail, see Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies*, January 2017, DOI: 10.1080/01402390.2016.1273830, available at http://www.tandfonline.com/doi/abs/10.1080/01402390.2016.1273830.

point. Trying to plant stories in legitimate media was not easy. Social media makes it much easier. Still, Russia has planted a number of forged documents, ranging from Sweden appropriating fertile soil from Ukrainian farmers, to Poland lambasting the Swedish government for the country's neutral position during World War II to the civilian nuclear energy company Westinghouse fomenting nuclear accidents in Ukraine with its sub-quality fuel produced in Sweden. So far, though, there is no evidence of that Russia's measures have had an effect on strategic decision-making in Sweden. That is a contrast to other countries, where some parties actively support the Kremlin.

- *Convergence of right and left.* Russia is active with groups on both the right and the left, and the two often work together. For instance, as elsewhere in Europe, RT and Sputnik in Sweden have attracted readers and contributors from the far right, the far left, populists, libertarians, conspiracy theorists, Wikileaks supporters, peace organizations and environmentalists. And the Russians play hardball, seeking to discredit those who uncover Russian influence operations.

For other nations engaging in hybrid threats, the goals are less clear, and probably more opportunistic. For China, the aims are to distract from, say, its actions in the South China Sea. It has concentrated on cyber tools, pursuing some combination of espionage, signaling capabilities or preparing to add cyber friction in the event of conflict. For instance, Chinese patriot hackers/cyber warriors allegedly conducted crippling DDoS attacks against Filipino government networks after the International Court of Justice in The Hague announced that it rejected China's historical territorial claims.[212] China's first cyber campaign against Philippines in connection with the territorial dispute came in April 2012, following a tense standoff between Chinese and Filipino vessels. Vietnam is also a popular target of Chinese cyber units; for instance, in May 2014 following an incident with a Chinese oil rig in Vietnam-claimed waters, Chinese hackers gained access to sensitive information about Vietnam's diplomatic and military strategy. During these territorial disputes, patriotic hackers often engage in attacks almost indistinguishable from organized government cyber units. And the countries attacked – Philippines, Vietnam, Taiwan, Malaysia, Brunei – are very unprepared to counter Chinese cyber units.

Iran typically operates below threshold of conventional warfare, using a blend of military and paramilitary tools, including proxy forces, missiles, cyber tools, maritime forces, and information ops to shape and coerce regional actors to its advantage. It uses small maritime craft to swarm US naval ships in Gulf – designed to aggravate another military without justifying full-scale response.

212 See Anni Piiparinen, "China's Secret Weapon in South China Sea: Cyber Attacks," *The Diplomat*, 22 July 2016, available at https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/

It makes use of proxies, like Hizbollah and Houthis, using them infiltrate and influence state institutions in countries with weak governance, such as Lebanon and Iraq. It has been clever in information ops in maritime space – for example, it widely circulated reports and videos of Iranian forces detaining and embarrassing stranded US sailors, thus promulgating an image of Iranian power, for both domestic and international consumption.[213]

North Korean attacks on banks probably derive from the "Willie Sutton" reason – that is where money is, and the hacks have produced big gains for North Korea. As the hack on SONY demonstrated, its cyber capabilities are improving, and it also makes use of other asymmetric threats, like small subs for espionage and sabotage operations.[214] For other nations, like Saudi Arabia and the emirates feuding in the Gulf, hybrid threats are a relatively low cost, low risk way to signal capabilities or embarrass opponents.

The terrorist groups in the Middle East – ISIL (Daesh), Al Qaeda (AQ), the Taliban – are no strangers to hybrid techniques.[215] The use of propaganda, interpreting genuine facts in ways which support their narrative, conspiracy theories, emotional appeal. They make use of "lawfare," seeking to turn legal systems against their enemies, to delegitimize them. ISIL has the most developed propaganda messaging and most developed use of social media, taking a segmented and targeted approach to specific audiences, just as Western media organizations do. Taliban and AQ make less use of cyber and internet than ISIL, which uses those tools not just for propaganda but also radicalization and recruitment globally. It has also used extreme violence as political messaging, and is good at linking violence/terrorism to its broader propaganda effort.

At higher levels of conflict, Hizbollah was the prototype for asymmetry in its 2006 war with Israel.[216] The 34-day military conflict summer shocked the Israeli public and surprised the international community with the effectiveness of its fight against Israeli Defense Forces. Hizbollah displayed all elements of hybrid warfare, carefully staying beneath the level of full conventional war: "…simultaneous use

---

213 Melissa Dalton, "How Iran's Hybrid-War Tactics Help and Hurt It," *Bulletin of the Atomic Scientists.* 2017, available at http://web.a.ebscohost.com.ezp-prod1.hul.harvard.edu/ehost/detail/detail?vid=0&sid=be69a849-c1c5-4049-8ccd-09468ea3c726%40sessionmgr4008&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=aph&AN=124996706

214 Bradley Martin, "The Regime that Will not Die: The North Korean Hybrid Threat," *International Affairs Review at George Washington University*, 25 March 2013. Available at http://www.iargwu.org/node/476

215 "Global Strategies: Hybrid Warfare in the Middle East," London School of Economics. February 2017. http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-Hybrid-Warfare-in-the-Middle-East.pdf.

216 Andreas Jacobs and Guillaume Lasconjarias, "NATO's Hybrid Flanks: Handling Unconventional Warfare in the South and the East," NATO Defense College Research Division. April 2015, available at https://www.files.ethz.ch/isn/190786/rp_112.pdf.

conventional arsenal, irregular forces and guerrilla tactics, psychological warfare, terrorism, and even criminal activities with support from multi-dimensional organization and capable of integrating very different sub-units, groups or cells into one united, large force." It also challenged Israel with a broad propaganda campaign, with its TV and radio stations depicting Hizbollah and its leader as the new spearhead of resistance against Israel.

Chapter 7: Thinking about the Future of Hybrid Threats

The nature of hybrid threats at present is, not surprisingly, the starting point for thinking about the future. For most threateners, like Russia, the attributes that make hybrid threats attractive now will only become more attractive as its own economic decline continues. The virtual realm has dramatically lowered the cost of propaganda, and cyber operations are also relatively cheap. It also seems likely that another attribute of power Russia has – nuclear weapons – will become more important in future hybrid threatening. Already, nuclear threats, to "escalate to de-escalate," are an implicit element of Russia's hybrid strategy.[217] It is not easy to see exactly how Moscow might play on nuclear threats more heavily in the future but it does seem likely that it will.

In one area, advancing technology will surely open new opportunities for hybrid threateners. So far, the planted posts, tweets and bots have been almost entirely text. But that will change: technology, especially Artificial Intelligence, is making it easier to fake someone speaking. This will take fake news into the realm of audio and video, which in turn will complicate the task of attributing, and responding to, fake propaganda.[218]

---

217 For instance, in 2009, Nikolai Patrushev, Secretary of the Russian National Security Council, indicated that in the proposed new version of the nuclear doctrine, released in February 2010: "We have corrected the conditions for use of nuclear weapons to resist aggression with conventional forces not only in large-scale wars, but also in regional or even a local one." See Mark B. Schneider, "Escalate to De-escalate," U.S. Naval Institute *Proceedings,* 142, 2 (February 2017), available at https://www.usni.org/magazines/proceedings/2017-02/escalate-de-escalate.

218 See James Vincent, "New AI research makes it easier to create fake footage of someone speaking," *The Verge,* July 12, 2017, available at https://www.theverge.com/2017/7/12/15957844/ai-fake-video-audio-speech-obama.

At the upper level of hybrid threats, the future will see, as in Ukraine, new combinations of cyber and kinetic operation. In one sequence, eminently plausible after the Ukraine intervention, targeted soldiers will first receive a demoralizing message, like those spammed to Ukrainian soldiers. Ten minutes later, the soldiers' compromised phone will access recent contacts and send "killed in action" messages to their families. Shortly after, their families will keep calling the soldiers, distracting them from duty. Another demoralizing message is sent – "retreat and live." The cyber operation then shifts to kinetic action as the compromised phones reveal the soldiers' location and they are targeted by a massive artillery strike. Not long after, there is an infantry and tank attack.[219]

As the U.S. Army's latest concept document stresses, foes will make life as difficult as possible for U.S. troops by not declaring themselves to be the enemy, or, by "combining regular and irregular forces with criminal and terrorist enterprises to attack [U.S.] vulnerabilities while avoiding its strength."[220] For instance, at the upper levels of hybrid conflict, one analysis found it conceivable that Iran, which can't attack the United States directly, might seek to do so using proxies – Hizbollah or the Mexican drug cartels – in an effort to remain if not anonymous then at least difficult to clearly identify.[221]

In many respects, China's experience with hybrid threats and warfare goes back to Sun Tzu. Then, imperial Chinese rulers pursued a "four methods approach" in dealing with "barbarian" neighbors. First was to divide them by "using barbarian to fight barbarians," hiring mercenaries and building strategic alliances to ensure division among those neighbors. Today's counterpart might be "diplomatic warfare" – neutralizing adversaries through public diplomacy, support for local insurgencies and pressure in international organizations. For imperial China, the next step was bribes and tribute for foreign leaders in order to dissuade them from attacking China; the current parallels in Chinese trade and aid are straightforward – economic warfare combined with "soft," or perhaps "sharp" power. Next, if need be China would build fortifications in order to deter outside

219 For a collection of articles about cyber threats and responses, from the perspective of the U.S. Department of Defense, see Defense One, *Cyber Warfare,* December 2017, available at http://www.defenseone.com/assets/cyber-warfare-dec/portal/.

220 As quoted in Patrick Tucker, "How the US Army Is Preparing to Fight Hybrid War in 2030," *Defense One,* October 9, 2017, available at http://www.defenseone.com/technology/2017/10/how-us-army-preparing-fight-hybrid-war-2030/141634/.

221 Frank Cilluffo and Joseph Clark, "Thinking about Strategic Hybrid Threats – In Theory and in Practice," Center for Complex Operations, PRISM, 4, 1, available at http://cco.ndu.edu/Portals/96/Documents/prism/prism_4-1/prism46-63_cilluffo-clark.pdf.

attack; the parallel with its current build-up in the South China Sea is striking. Only if all else failed would China resort to direct military action.[222]

In this vein, so far, China's use of hybrid tactics has been more restrained than Russia's. China has not actually used conventional military force.[223] Instead, it has employed paramilitary, coast guard, or militia while keeping regular forces over horizon. It has "salami-sliced" in the South China Seas, enabling it to achieve its political and territorial agenda without triggering a forceful US military response. It has also made very aggressive use of "lawfare" – announcing its Air Defense Identification Zone (ADIZ), rejecting the arbitration award in favor of Philippines – while assertively employing economic tools, for instance again South Korea, while Chinese money finds its way to Australian political parties.

The future is likely to see new forms of hybrid campaigns in new parts of the globe. For instance, Greece, Italy, and Spain bore the brunt of both Europe's economic crisis in 2008 economic crisis and it refugee crisis in 2015.[224] The countries experienced double digit unemployment and income drops, coupled with reductions to social safety nets. EU-imposed austerity measures began to succeed by 2016, but in the short run, they bred resentment among citizens against the EU, mainstream parties, and the Western model of liberal democracy. When the refugees began arriving, that only increased the polarization. The circumstances were tailor-made for Russian overtures while providing an opening for political parties oriented toward the East rather than the West. Moscow provided political and media support to pro-Russian forces, seeking to build on historical, religious, and cultural ties, and using, either directly or through proxies, a chain of pro-Moscow civil society organizations to promote Russia's goal of weakening the EU and NATO.

In another example, one recent study of Russian and Chinese influence in Argentina, Peru, Poland, and Slovakia concluded that those Russian and Chinese initiatives in media, culture, think-tanks and academia reflected neither a "charm offensive" nor the exercise of "soft power." They were hybrid, not quite hard but not soft either.[225] They were "sharp" power, not based on attraction or persuasion, but rather on distraction and manipulation. The goal, as with Russian actions in the U.S. elections, is to discredit democracy and built support for autocracy

---

222 Benjamin David Baker, "Hybrid Warfare with Chinese Characteristics," *The Diplomat,* September 23, 2015, available at https://thediplomat.com/2015/09/hybrid-warfare-with-chinese-characteristics/.

223 *The Evolution of Hybrid Warfare and Key Challenges*, Hearings before the House Armed Services Committee, 115 Cong., 1 sess., 22 March 2017, 10, available at https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg25088/pdf/CHRG-115hhrg25088.pdf.

224 See Kremlins' Trojan Horses.

225 See U.S. National Endowment for Democracy, *Sharp Power: Rising Authoritarian Influence,* December 2017, available at https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.

especially in countries where democratic roots remain shallow. And the methods verged on the electoral campaigns Russia mounted in the United States and France.

At lower levels of hybrid conflict, the future of the hybrid threats will depend on how technologies and norms develop in the virtual world. As suggested earlier, the big social media providers, like Facebook and Twitter, are now poised awkwardly: on one hand, they recognize that they can no long fashion themselves as mere platforms, with no obligations regarding the content they convey, but, on the other, are far from conceiving themselves as publishers responsible for their content. Presumably, the algorithms that make web providers better and better at anticipating what particular consumers will want and where they will be tomorrow will also make them better at separating Russian trolls masquerading as French from real French people. A first step, one already being implemented by several providers, would not change content but rather warn that the people posting may not be who they purport to be. Another possibility, though perhaps one more labor intensive, would be to publish the post with an accompanying "fact check." More generally, there are many good arguments – from bullying to crime and beyond – to make the web less anonymous. It is hard to predict the fate of efforts to make it so, but most of those would make real attribution of web content easier even if it didn't change that content.[226]

In the cyber world, the open question is whether the major powers will develop even crude rules of the road that might bear on the likelihood that cyber threats and methods will be employed in hybrid conflict.[227] The 2015 agreement between the United States and China, one since emulated by other nations in their relations with China, not to conduct cyberespionage for economic purposes is at least a starting point.[228] Certainly, no agreements are likely to be accepted by rogue states like Iran or North Korea, but they are likely to be hybrid threateners with limited, and mostly regional, capacity in any case.

Looking at the Baltics, the worrisome prospect, as suggested earlier, is that the main card Russia has to play is its local military superiority. One analyst imagines hybrid scenarios of nonviolent subversion, covert violent action, and

---

226 For a thoughtful critique of the Facebook and Google business model, and suggestions about what to do about it by an early investor in Facebook, see Roger McNamee, "How to Fix Facebook – Before It Fixes Us," *Washington Monthly,* January/February/March 2018, available at https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/.

227 See David D. Clark and Susan Landau, "Untangling Attribution," National Research Council.2010. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, available at https://www.nap.edu/read/12997/chapter/4.

228 For the agreement and background, see John W. Rollins and other, "U.S.-China Cyber Agreement," Congressional Research Service, October 16, 2015, available at https://fas.org/sgp/crs/row/IN10376.pdf

conventional aggression supported by political subversion.[229] Given the gains in standard of living and increasing integration of many Russian speakers in the Baltics, Russia will likely have difficulty using nonviolent tactics to destabilize these countries. Russian covert violent action is also unlikely to succeed on its own, given preparations by the security forces of Estonia and Latvia to "shoot" Russian "little green men" – that is, Russian forces that are deployed covertly without attribution. The preparedness and competence of Baltic security forces could force Russia to choose between losing the conflict or escalating to conventional war with NATO.

229 Radin, cited above, pp. 13–30.

Chapter 8: Responding to Hybrid Threats

In conceiving of responses, the first imperative is perhaps the Hippocratic oath: do no harm. Open societies are inherently vulnerable, yet it is imperative that they stay open. The relatively wide open worldwide web that offers new possibilities to hybrid threateners is also now essential to open global commerce. So, too, democracies can be slow and cumbersome, but that too is part of the system we value. It is imperative to protect free speech, and to remember that it is not the state we are trying to protect, but rather its citizens. Thus, there are cautions about how far democracies want to go.

Still, it is not as though democratic capacity to wage hybrid warfare is completely empty. The democracies are no strangers to information operation, covert operations and use of proxies. Still they face three challenges in responding to hybrid threats.[230] First, since hybrid threats engage the whole of government – and, indeed, of society beyond – they will find it harder than autocratic opponents to coordinate decision-making across different levels of power, and to do so at speed. As an analyst put it, speaking of the United States: "Success in hybrid wars also requires small unit leaders with decision-making skills and tactical cunning to respond to the unknown – and the equipment sets to react or adapt faster than tomorrow's foe. Organizational learning and adaptation would be at a premium, as would extensive investment in diverse educational experiences. What institutional mechanisms do we need to be more adaptive, and what impediments does our centralized – if not sclerotic – Defense Department generate that must be jettisoned?"[231]

---

230 See Kaan Sahin, "Liberal Democracies and Hybrid War," International Institute for Strategic Studies, December 16, 2016, available at https://www.iiss.org/en/militarybalanceblog/blogsections/2016-629e/december-e473/liberal-democracies-and-hybrid-war-cccb.

231 Frank Hoffman, "Hybrid Warfare and Challenges," National Defense University. Institute for National Strategic Studies, 2009, available at http://www.dtic.mil/docs/citations/ADA516871.

Second, and related, the checks and balances, bureaucracy, and separated institutions that characterize democracies will complicate hybrid warfare operations. Finally, hybrid conflict challenges important ethical principles. In the words of one analyst: "democracies can[not] wage hybrid war in a comprehensive and orchestrated way like their autocratic and non-state counterparts can. If they did, they would compromise the very essence of what they seek to defend."[232]

All of the national good practices in preparing for, and countering, hybrid threats share a number of features:

- They are "whole of government," indeed "whole of society."
- As suggested earlier, vulnerability assessment is the starting point.[233] That is awkward but necessary. It needs to concentrate especially on the cyber realm, against the triple threat in the cyber realm – espionage, attack and manipulated information.
- They pay special attention to, especially, the cyber realm. Since cyber, along with social media, are the main new ingredients in hybrid threats, special attention to both makes sense. There are many good reasons for nations to be more serious about their cyber defenses, and hybrid threats is a very good one.
- They are creative in reaching out to the private sector. That is imperative in the cyber realm, where infrastructure assets to be protected are in private hands. But Estonia's Cyber Defence Unit, part of the larger, and volunteer Estonian Defence League is suggestive of the possibilities, as is the help that private sector analysts provided in the U.S. elections case.
- They depend on shared situational awareness, with access to reliable intelligence and high quality analysis, and also depend on robust counterintelligence efforts. In some countries, that has required changing laws to give intelligence services somewhat more authority to collect information, both inside and outside the country.

8.1 Britain

The British approach is a whole of government one. Its core is COBRA, the cabinet office briefing room A, a crisis center. As an emergency council, Cobra meets to discuss high-priority issues that cross departmental borders within

232 Sahin, cited above.

233 Cederberg, A. and Eronen, P., 2015a. How can societies be defended against hybrid threats? Strategic Security Analysis, 9(1): 1–10. Cederberg, A. and Eronen, P., 2015b. Wake up, West! The era of hybrid warfare is upon us. Geneva Centre for Security Policy, 31 August [online]. Available at: http://www.gcsp.ch/News-Knowledge/ Global-insight/Wake-up-West!-The-Era-of-Hybrid-Warfare-Is-Upon- Us (Accessed 19 January 2017).

government. Who attends depends on the nature of the crisis.[234] The very name COBRA encourages attention, and so whether or not it's up and running, and which officials are attending: these are themselves newsworthy. It starts with the intelligence assessment. The process is trial and error, which it is bound to be for any country. For instance, the COBRA process was tried during the 2008 financial crisis, but didn't really work. The crisis was longer, which put pressure on stretched officialdom, plus it was necessary to engage industry leaders, for whom the setting was uncomfortable – a reminder that arrangements will have to be tailored to fit the challenge at hand.

In December 2017, the British Intelligence and Security Committee published its Annual Report for 2016–2017.[235] The report examines the national security threats facing the country, from Northern Ireland related terrorism to cyber security. While it never explicitly mentions hybrid warfare, unconventional capabilities, asymmetric approaches, or new generation warfare, it addresses specific vulnerabilities and tools relating to the hybrid threat, especially in the cyber realm. The cyber threat is significant and diverse, targeting "all sectors of society… From government networks, to companies, to individuals."[236]

Learning from the cyber operation interfering in the 2016 US presidential election – that "Russia was no longer concerned about its activities remaining covert, and that it was adopting a more brazen approach to its cyber activities" – Britain places a greater importance of securing systems controlling the critical national Infrastructure.[237] This includes securing Britain's political system from cyber-attacks. The objectives of such attacks may be to "undermine the integrity of the UK's political processes," "subverting a specific election…. With a countervailing benefit to the hostile actor's preferred side," "poisoning public discourse," and targeting those who "might be open to subversion or political extremism."[238]

To address these challenges, the National Cyber Security Centre (NCSC) tracks known perpetrators, provides best practices to vulnerable individuals, collaborations to counter disruption and propaganda, and increasing data security. Britain is also invested in offensive cyber capabilities through the National Offensive

234 Joey Gardiner, "What Is COBRA? *The Guardian,* 21 October 2002, available at https://www.theguardian.com/politics/2002/oct/21/Whitehall.uk.

235 "Annual Report 2016–2017," *Intelligence and Security Committee of Parliament,* December 20, 2017, http://mepoforum.sk/wp-content/uploads/2017/12/UK-Intelligence-Security-Committee-2016-2017.pdf

236 *Ibid,* 29.

237 *Ibid,* 32. The report states, "State actors are highly capable of carrying out advanced cyber attacks; however, their use of these methods has historically been restricted by the diplomatic and geopolitical consequences that would follow should the activity be uncovered. Recent Russian cyber activity appears to indicate that this may no longer be the case."

238 *Ibid.*

Cyber Programme (NOCP) to develop "a dedicated ability to counter-attack in cyberspace" and act as a deterrent.[239]

In October 2016, Britain launched The National Cyber Security Centre, uniting previously separate parts of the government that dealt with cyber security.[240] The creation of a central organization to deal with cyber security threats enables the NCSC to achieve its goal of "protect[ing] our critical services from cyber attacks, manag[ing] major incidents, and improv[ing] the underlying security of the UK Internet through technological improvement and advice to citizens and organisations."[241] The NCSC collaborates with individuals, industry, and organizations and shares assessments through the Cyber Security Information Sharing Partnership (CiSP).[242]

In June 2016, the House of Commons Defence Committee published a report focusing on Russia's threat and the implications for security policy. The report focuses on the full range of challenges posed by the Russian military and unconventional capabilities. Britain's MoD addresses the threat posed by disinformation and propaganda with the 77 Brigade. The unit, established in September 2014 and reshaped in July 2015, aims to "challenge the difficulties of modern warfare using non-lethal engagement and legitimate non-military levers as a means to adapt behaviours of the opposing forces and adversaries."[243] Britain also calls for NATO to increase resources and fully develop a strategy to counter Russian propaganda and disinformation effectively.[244]

---

239 *Ibid,* 43.

240 "2017 Annual Review," *National Cyber Security Centre*, October 3, 2017, https://www.ncsc.gov.uk/news/2017-annual-review.

241 "About the NCSC," *National Cyber Security Centre,* June 9, 2017, https://www.ncsc.gov.uk/information/about-ncsc. The NCSC "understands cyber security, and distills the knowledge into practical guidance that we make available to all," "responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK," "uses industry and academic expertise to nurture the UK's cyber security capability," and "reduces risks to the UK by securing public and private sector networks."

242 2017 Annual Review, 7.

243 "Russia: Implications for UK defence and security – First Report of Session 2016–2017," *House of Commons Defence Committee,* June 28, 2016, https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf, 36-37. The 77 Brigade is organized into columns: "No.1 Column – Plans support focusing on the behavioural analysis of actors, audiences and adversaries; No.2 Column – Provides the detailed synchronisation and delivery of effect; No.3 Column – Provides highly deployable specialists to other parts of the Armed Forces and other Government organisations; No.4 Column – Provides professional specialists in Security Capacity-Building in Defence; No.5 Column – Media Operations and Civil Affairs," and the No.7 Column provides Engineer and Logistics Staff.

244 *Ibid,* 37.

8.2 Finland

Finland is another example of a comprehensive security approach in which "society's vital functions are secured through collaboration between authorities, the business community, civil society organisations and individual citizens."[245] This broad approach is necessary for effectively defending against hybrid threats because such attacks do not discriminate between sectors, civilians, government, and military targets. Finland's Ministry of Defence published the Security Strategy for Society as the framework for hybrid defense.[246]

Beyond simply publishing strategic documents, Finland has also taken concrete steps to improve its capabilities. Taking responsibility for the European Centre of Excellence for Countering Hybrid Threats is a clear example. Other efforts include: "the state works to improve the national situational awareness in cyberspace and is an active partner in regional defence initiatives and exercises. The government has also established the National Cyber Security Centre. The computer emergency response team (GOVCERT) and 24/7 functioning of the public sector are being created and improved. Authorities and resources for the police and military, intelligence included, working in the cyber domain are thoroughly looked at. In regard to regional partnerships, Finnish experts have been sent to NATO's Centres of Excellence in Tallinn and Riga and all branches of the Finnish Defence Forces have taken part in the military exercises organised in the greater Baltic Sea region." [247]

At the same time, Finland has framed legislation to give "more expansive powers to conduct intelligence gathering inside and outside Finland's borders" to their military and security agencies. This will broaden the armed forces' authority "to conduct human, signals, information system, and telecommunications intelligence operations." [248]

8.3 Sweden

Russian intervention in the U.S. and French elections was hardly lost on Sweden, which has its own elections on September 9, 2018. Sweden's Prime Minister, Stefan Löfven, said Russia poses the biggest threat, but does not rule out others attempting to sway the results as well. He also added: "We will not hesitate to expose those who try to do something, because we know that operations are

245 Cederberg and Eronen, 9.

246 "Security Strategy for Society," *Ministry of Defence of Finland*, December 16, 2010, https://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf.

247 Cederberg and Eronen, 9.

248 "Finland launches national security initiatives defending against hybrid threats," Defense News, April 28, 2017, https://www.defensenews.com/pentagon/2017/04/28/finland-launches-national-security-initiatives-defending-against-hybrid-threats/.

underway at the moment."[249] Prime Minister Löfven also announced an initiative to create a new body "responsible for bolstering the 'psychological defence' of the Swedish public by "identifying, analysing, and responding" to "external influence" campaigns." This would be a re-creation and a 2.0-version of a previous cold war agency – The Board of Psychological Defence – which was absorbed in 2009 by The Civil Contingencies Agency (MSB), who took over and developed the function for national crisis management situations. MSB today has the government lead in countering hostile influence operations. Other steps include increased funding for Swedish intelligence and cyber-defense services.

8.4 France

In France, Emmanuel Macron proposed legislation to battle fake news and election interference.[250] While this falls short of a comprehensive strategy to counter hybrid threats, it does target Russia's election meddling efforts, which he was a target of during his recent victory over Marine Le Pen. During the campaign Macron accused Russia of employing a "hybrid strategy combining military intimidation and an information war." The proposed legislation includes requiring websites to disclose who is financing them and a cap on sponsored content spending. The law goes even further to counter what Macron dubs "propaganda articulated by thousands of social media accounts" during election seasons by allowing authorities to remove the content or block the website. The CSA, the country's media watchdog, would be given more powers to "fight any destabilization attempt by television channels controlled or influenced by foreign states."[251]

8.5 Estonia

As mentioned earlier, in 2007 Estonia was hit by a three-week Russian cyber attack in response to the relocation of a Soviet WWII memorial.[252] The wave of DDoS attacks disabled websites by overwhelming the servers hosting the sites with artificial traffic. The attack targeted the websites of the Estonian president, parliament, government ministries, political parties, three of the six major news organizations, two large banks, and communications firms. A year later, Estonia

249 Andrew Rettman and Lisbeth Kirk "Sweden Raises Alarm on Election Meddling," *EU Observer,* 15 January 2018, available at https://euobserver.com/foreign/140542.

250 Angelique Chrisafis, "Emmanuel Macron promises ban on fake news during elections," *The Guardian*, January 3, 2018 https://www.theguardian.com/world/2018/jan/03/emmanuel-macron-ban-fake-news-french-president.

251 Yasmeen Serhan, "Macron's War on 'Fake News'," *The Atlantic,* January 6, 2018, https://www.theatlantic.com/international/archive/2018/01/macrons-war-on-fake-news/549788/.

252 Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian,* May 16, 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

opened the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, the capital city.[253] It supports "capability, cooperation, and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation."[254]

In 2011, Estonia formed the Cyber Defence Unit of the Defence League, which had been planned since the 2007 cyber attacks.[255] The Cyber Defence Unit is part of the larger Estonian Defence League, a volunteer organization linked to the Estonia's armed forces (Estonian Defence Forces).[256] The volunteer based cyber united "is made up of average citizens outside of government who are specialists in key cyber-security positions, patriotic individuals with information technology skills, and experts in other fields (e.g., lawyers and economists) who wish to volunteer outside of their daily jobs to protect Estonian cyberspace."[257] The Cyber Defence Unit promotes public-private sector cooperation, strengthens awareness, and prevention of cyber security threats in Estonia.[258] Its goal is to "enhance the preparedness of the population to defend the independence of Estonia and its constitutional order by relying on free will and self-initiative."[259] Given that hybrid threats target all aspects of society, a comprehensive approach to security that involves all actors is critical. The Cyber Defence Unit addresses a key aspect of the hybrid threat – building Estonian resilience, enhancing ability to respond to a potential cyber-attack, and turning a vulnerability into a strength.[260]

---

253 "NATO opens new centre of excellence on cyber defence," *NATO,* May 14, 2008, https://www.nato.int/docu/update/2008/05-may/e0514a.html.

254 "NATO Cooperative Cyber Defence Centre of Excellence – About Us," *NATO,* https://ccdcoe.org/about-us.html.

255 "Government formed Cyber Defence Unit of the Defence League," *Republic of Estonia Ministry of Defence,* January 20, 2011, http://www.kaitseministeerium.ee/en/news/government-formed-cyber-defence-unit-defence-league.

256 Kadri Kaska and others, "The Cyber Defence Unit of the Estonian Defence League – Legal, Policy and Organisational Analysis," *NATO Cooperative Cyber Defence Centre of Excellence,* 2013, https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf.

257 Monica M. Ruiz, "Is Estonia's Approach to Cyber Defense Feasible in the United States?" *War on the Rocks,* January 9, 2018, https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.

258 Kaska, 5.

259 *Ibid,* 11.

260 The CCDCOE's analysis concludes, "By participating in the various activities foreseen by law – both training and exercises as well as providing assistance to governmental bodies and critical infrastructure providers – the members of Cyber Defence Unit not only refine their knowledge and skills but create the informal communication channels and relationships of trust that are central to effective cooperation in case of a major cyber incident. Thereby, they not only improve the capability and capacity of the Cyber Defence Unit, but indirectly also contribute to stronger cyber resilience and threat response capability for their employers and the wider society." *Ibid,* 27–28.

8.6 European Union

In April 2016, the EU released the Joint Framework on countering hybrid threats – a European Union response.[261] The framework contains 22 actionable proposals to "counter hybrid threats and foster resilience of the EU and Member States, as well as partners."[262] Though improving the resilience of member states is critical as "most national vulnerabilities are country-specific," the EU hopes to effectively respond to common threats targeting cross-border networks on infrastructure. The first action called for Member States to identify key vulnerabilities. Other actions included improving protection and resilience of critical infrastructure, coordination on cyber responses, targeting hybrid threat financing, and increasing coordination with NATO.[263] Indeed, one of the silver linings in the cloud of hybrid threats is much closer collaboration between the EU and NATO. That has been a prominent future of all the Centre's meetings on hybrid threats. The history of cooperation between the two is checkered at best, but hybrid threats plainly engage both, and, so too, the lanes in the road for each are not brightly painted, so real interchange is required. The Joint Framework also called for the creation of an EU Hybrid Fusion Cell to offer a single focus for analyzing hybrid threats.

On July 19, 2017, the European Commission released an update on the steps taken to implement the 2016 Joint Framework on countering hybrid threats.[264] The EU Hybrid Fusion Cell was created to provide all-source analysis on hybrid threats. Cooperation with non-member states also increased, with the launch of a pilot risk survey in Moldova to identify key vulnerabilities and target assistance to those areas. The EU has also adopted an "EU Playbook" for countering hybrid threats.[265] The document details the procedure for an EU response to a hybrid threat (see figure 3 below). The EU Hybrid Fusion Cell is critical in initially identifying a threat before a full crisis emerges.

---

261 "Joint Framework on countering hybrid threats – a European Union response," *European Commission,* April 6, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

262 The Joint Framework defines hybrid threats: "While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes."

263 A full list of all 22 actionable items is available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

264 "Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead," *European Commission,* July 19, 2017, http://europa.eu/rapid/press-release_IP-17-2064_en.htm."

265 "Joint Staff Working Document – EU operational protocol for countering hybrid threats 'EU Playbook'," *Council of the European Union,* July 7, 2016, http://statewatch.org/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf.

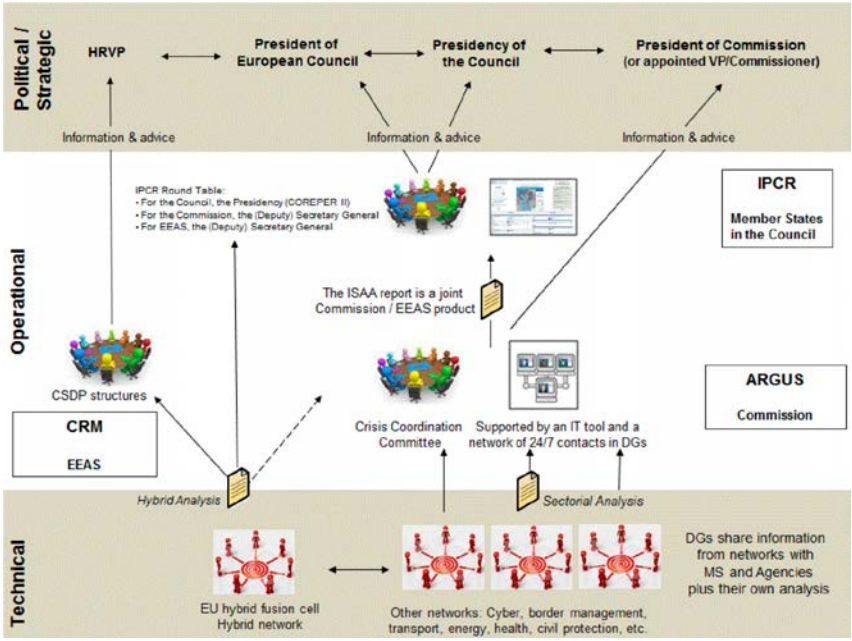


Figure 3: EU Process for Responding to Hybrid Threats.[266]

266 Source: Joint Staff Working Document – EU operational protocol for countering hybrid threats, "EU Playbook."

Chapter 9: Recommendations

The three watchwords in defending against the weaponized information of hybrid threats are awareness, metrics, and responses. [267] The Western nations had been focused on technical threats in cyberspace – crime, espionage and attacks on critical infrastructure. As a result, the propaganda dimension of the Russian intervention in the U.S. elections in 2016 came as a surprise, even though it shouldn't have, as the earlier case discussion makes clear. Recall the group of outside analysts tracking the online dimensions of the jihadists and the Syrian civil war when they came upon interesting anomalies, as early as 2014, and made the connection to Russia.

More recently in Europe, however, increasing awareness of the threat has enabled society, media, and governments to put appropriate defenses in place. In Germany, public awareness and interest in hostile information operations had been aroused by the "Lisa" case, in which Russia attempted to stoke anti-immigrant sentiment. The media blackout in France helped blunt the effect of Russia's interference in the presidential election; but Macron's campaign was also aware of Russia's attempts to influence the outcome and took countermeasures. Leaders in other Western nations should be open and outspoken about the nature of the challenge, as doing so has been shown to be highly effective in raising public awareness and decreasing potential targets' susceptibility to information operations.

The second most important response is responding quickly to particular information operations, once discovered, both to minimize their impact and to deter other states or groups that might want to emulate the attack. To be sure, chasing every false fact is impossible, but the Incirlik incident and the Macron

---

267 This discussion parallels that of Council on Foreign Relations, *Countering Russian Information Operations in the Age of Social Media,* November 21, 2017, available at https://www.cfr.org/report/countering-russian-information-operations-age-social-media

campaign both illustrate the value of countering fake news as fast as possible. It remains unclear why the Russians were so inactive in the German elections in autumn 2017. It may be that they thought events were going in their direction in any case, but one reason may be that they understood that, given awareness, their actions would be uncovered. Attention would be drawn to what they *did,* not the messages they were trying to convey.

Practitioners and researchers emphasize a number of points in thinking about how to respond:

- *Again, respond with the whole of government – and beyond.* Preparing for hybrid threats cannot be left to the defense ministry alone. And it will be necessary to reach out to the various private sectors. Indeed it remains a question how much government can do on its own. Certainly, Western governments will face, for good reasons, limits on what they can do that do not apply to Russia. And almost anything governments say openly will be dismissed by some target audiences. That said, the history of the American radios broadcasting into the Communist countries during the Cold War is worth mining. In retrospect it was more successful than its operators thought at the time.
- *Be skeptical of metrics.* For all the concern, it remains hard to assess how much the Russian operations affected the U.S. election outcome by comparison to mediocre campaigning and FBI director Comey's eleventh hour announcement about Hillary Clinton's emails. And thus far Russia operations in Europe seem to have had most effect on those who were already sympathetic to Moscow.
- *Be careful about targets.* It is worth noting, for instance, that the first target of Russian operations is the Russian people.
- *Play on strength.* Time and again, the same point arises: a great strength of the Western democracies is their free presses. That needs to be recognized and protected as a major asset. That argues against mimicking adversaries by circulating fake news or undermining the credibility of quality journalism.
- *Recognize the contest is a long one.* The distinction between peace and war is indeed blurred. There are likely to be neither unconditional surrenders nor unqualified victories.
- *Working with target countries is essential.* Those might focus on building transparency and fighting corruption, and on internal security reform and defense institution-building. Here, there is considerable post-Cold war experience on which to draw.
- *The Russians are coming.* The U.S. case makes plain that the Russians have both will and capacity to intervene in other nations' elections. That plain lesson is the most important. Since the Cold war, Moscow has attempted to disrupt the democratic process in Western countries. What is different in this case, in addition to the new cyber tools, is the explicit purpose not merely

of disruption and sowing mistrust but also of seeking to tilt the election in favor of a particular candidate.

- *Thus, pay close attention to early warning.* In this case, the FBI, apparently, warned the DNC in the fall of 2015 of potential hacks into its information systems. It did not, however, make clear that it suspected these were Russian-government sponsored operations. Nor did it do so in ensuing months, and the DNC did not become alarmed until March 2016 and did not engage CrowdStrike until May. By contrast, and no doubt partly because of the U.S. case, the Macron campaign in France was attentive to hacking and cyber security at least from December 2016, the first round of the election.
- *Early warning and attribution are tricky but not impossible.* The hacks and leaks in this case were fairly quickly and firmly attributed to Russia's hand, and the FBI already suspected Russia when it reached out to the DNC in the fall of 2015. And the group of outside analysts has suspected the Russian hand as early as 2014. At least countries, like France, Germany and Sweden, with elections in 2017 and 2018 knew or will know where to look and not be distracted. Indeed, one upside of the U.S. attack is that everyone is more careful now and more focused on Russian hackers. There is a lot more information out there.
- *Tighten links across the public-private divide.* This is a great challenge of the cyber realm in any case. It is easier with regard to elections to the extent that elections plainly are a public good and a government responsibility. But, as with Mrs. Clinton's emails and also Mr. Macron's, private citizens and their private correspondence will be targets. On the government's side, the need is to stretch discretion and be as clear about warnings as possible. The FBI needed to tell the DNC in the autumn of 2015 that it suspected the Russians. In the event, the FBI officer, though, was apparently not confident enough in his case (and perhaps his interlocutor) to communicate that suspicion. The Bureau would not have needed to say why it suspected the Russians, though given the activities of private companies, like CrowdStrike, in cyberspace to say why would seem to have posed little risk to "sources and methods."

The role of private companies is a complicating but also promising facet of cyber. The companies do upset the traditional government process: when a hack occurred, intelligence agencies would seek to attribute it, then pass that information in secret to policy agencies, which would decide what to do – name and shame, go after individuals, retaliate and so on. Now, however, private companies will be doing attribution on their own and will reveal their conclusions when they choose. Governments will have less discretion in deciding whether or when to attribute. But the companies will not only be useful partners, their public attributions will also make it easier for governments to protect their own sources and methods.

- *Likewise, pay close attention to the infrastructure of elections.*[268] The decentralization of election machinery in the United States was probably an operational advantage (if a forensic liability), for it complicated the attackers' challenge. To the extent that European election infrastructure is more centralized, it is a more tempting target. That may be offset, however, if the election system doesn't exaggerate, as does the American, the importance of a few critical districts or areas of the country. In any case, the danger of being hacked is increased the more voting is virtual (and the less there are ways to check results after the fact in the way that paper ballots did).
- *In the end, though, the Russians aren't ten feet tall.* The Russian hacking probably wasn't decisive in the U.S. election (by comparison, say, to FBI Director James Comey's eleventh-hour intervention). Russian cyber attacks on France's TV5Monde succeeded in taking it down but raised the question of what was the point. Similarly, Russian efforts to discredit François Hollande probably had less effect than *Paris Match's* reporting. Speed and forthrightness in responding are critical. The Incirlik fake news story faded quickly once news outlets began publishing pictures of the actual protests. Similarly, in early 2017 when Russia tried its allegations of rapes in the Baltic by NATO soldiers, Germans to boot, Lithuania was ready. Its parliament immediately dismissed the story as spurious.[269] And the Macron campaign's "counter-offensive" at least demonstrates that those attacked have options.

268 The Belfer Center for Science and International Affairs, Harvard Kennedy School, *Cybersecurity Campaign Playbook,* November 2017, is a common-sense and useful guide to thinking about cyber defenses in campaigns. See https://www.belfercenter.org/sites/default/files/files/publication/Playbook%201.3.pdf

269 See http://www.dw.com/en/nato-russia-targeted-german-army-with-fake-news-campaign/a-37591978.

Addressing Hybrid Threats

Hybrid threats have become the 21st security challenge for Western countries. They reflect significant change in the nature of international security. Change tends to increase feelings of insecurity and, historically, frictions in society, all the more so because hybrid threats are complex and ambiguous. Some people look to the past for answers, while others have forgotten the past. There are those who argue more vigorously for adapting to change, and there are those who try to defend the status quo. In some cases facts turn into views, opinions and perspectives – or worse, vice versa. This means that the picture of the security environment is not simply black or white. It is complex, multi-layered and multidimensional. Thus, analysis of what has changed, how it is changed and what does it mean for democratic states is at the core of understanding the nature of the current security environment in Europe.

This report gives us a rich understanding of what we mean when we talk about hybrid threats drawing upon two case studies: Russia's interventions in Crimea and Ukraine and in the 2016 U.S. presidential election. It also addresses what kind of threats we are facing and what tools are being used against the democratic states.

Addressing Hybrid Threats was put together by Dr. Gregory F. Treverton and his team for the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in collaboration with the Center of the Asymmetric Threat Studies (CATS) at the Swedish Defence University.

Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue

ISBN: 978-91-86137-73-1

Swedish Defence University
Box 27805
SE-115 93 Stockholm
www.fhs.se

Swedish Defence University
CATS Center for Asymmetric Threat Studies
Hybrid CoE The European Centre of Excellence for Countering Hybrid Threats