The Intelligence Challenges of Hybrid Threats

Focus on Cyber and Virtual Realm

Gregory F. Treverton

CATS
Center for Asymmetric Threat Studies
The Intelligence Challenges of Hybrid Threats
Focus on Cyber and Virtual Realm

CATS
Center for Asymmetric Threat Studies
The Intelligence Challenges of Hybrid Threats

Focus on Cyber and Virtual Realm

Author:
Gregory F. Treverton

CATS
Center for Asymmetric Threat Studies
Preface

What challenges do the realm “Hybrid Threats” pose for the world of intelligence analysis and tradecraft, and how should intelligence agencies adapt? This is the main theme of an extraordinarily timely analysis by Dr Gregory Treverton – former Chairman of the U.S. National Intelligence Council and now Senior Fellow at CATS. No one is better placed than Dr Treverton to contextualize intelligence and its connection to the cyber and influence operation areas. In this study, social media and cyber attacks – often combined with signals and human intelligence – are analyzed in relation to real world events such as the influence operations during the 2016 U.S. elections as well as the Office of Personnel Management hack (2015). We are convinced that this important contribution will be well received by the Intelligence Community and Academia.

Lars Nicander
Director
Center for Asymmetric Threat Studies (CATS)
Contents

Preface 5
Chapter 1: Hybrid Tools and Challenges for Intelligence 9
Chapter 2: Challenges across Intelligence Disciplines 15
Chapter 3: Attributing Cyber Attacks 19
Chapter 4: Attribution and Deterrence 23
Chapter 5: Detecting Social Media-Aided Influence Operations 27
Chapter 6: Taking Advantage of Opportunities 31
Chapter 7: Reshaping Intelligence 35
Chapter 1: Hybrid Tools and Challenges for Intelligence

The intelligence challenge starts with recognizing the range of hybrid threats and what is new about them: the targets are societies, not armies; several tools are used both simultaneously and strategically for maximum effect; and the cyber dimension, along with the social media (SM) and virtual realms offer new, inexpensive avenues of attack.¹ This paper begins there, with the tools, then turns to the challenges of hybrid threats across the elements of intelligence – collection, analysis and relations between intelligence and policy. Then, it turns to the special challenges – but also the special opportunities – of the cyber and virtual realms. The following section focuses on opportunities and picks up the implications for the organizations performing the traditional INTs – HUMINT and SIGINT, especially – and for counterintelligence. It concludes with speculations about how the special challenges of hybrid threats might conduce to a much wider change in the traditional intelligence paradigm.

¹ Andrew Thvedt provided invaluable research assistance in preparing this paper, and I think him.
The Intelligence Challenges of Hybrid Threats: Focus on Cyber and Virtual Realm

Table 1 summarizes the range of hybrid threat instruments:

<table>
<thead>
<tr>
<th>Tools</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propaganda</td>
<td>Enabled and made cheaper by social media, also targeted at home</td>
</tr>
<tr>
<td>Fake news</td>
<td>“Lisa” was portrayed as a Russian-German raped by migrants³</td>
</tr>
<tr>
<td>Strategic leaks</td>
<td>Macron emails leaked 48 hours before the French election</td>
</tr>
<tr>
<td>Funding organizations</td>
<td>China opened Chinese think-tank in Washington</td>
</tr>
<tr>
<td>Political parties</td>
<td>Russia supports sympathetic European parties on right and left</td>
</tr>
<tr>
<td>Organized protest movements</td>
<td>Russian trolls organized both pro- and anti-protests in Houston mosque case</td>
</tr>
<tr>
<td>Cyber tools:</td>
<td>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 knowing it.</td>
</tr>
<tr>
<td>Economic leverage</td>
<td>China sought to punish South Korea for accepting U.S. anti-missile system</td>
</tr>
<tr>
<td>Proxies and acknowledged war</td>
<td>Hardly new, but Russian “little green men” in Ukraine slid into actual combat</td>
</tr>
<tr>
<td>Paramilitary organizations</td>
<td>Russian “Night Wolves” bikers intimidate civilians</td>
</tr>
</tbody>
</table>

What are the special challenges for intelligence? Table 2 lays out the typology of intelligence problems – puzzles, mysteries, and complexities or wicked problems.⁴ Hybrid threats are in the third category. They are wicked less because they involve new actors interacting in ways we haven’t seen, as was the case with terrorists after 9/11. Rather, “by emphasizing elusiveness, ambiguity, operating outside of and below detection thresholds, and by using non-military tools to attack across all of society, hybrid threats represent a new iteration of the complexity found in wicked problems.”⁵

---

² Adapted from Gregory F. Treverton and others, *Addressing Hybrid Threats*, Swedish Defence University Center for Asymmetric Threat Studies, April 2018, available at https://www.fhs.se/download/18.1ee9003b162cad2caa5a384d/1525791813728/Addressing%20Hybrid%20Threats.pdf


⁴ For my discussion of these categories, see Gregory F. Treverton, “Risks and Riddles,” *Smithsonian*, June 2007.

Chapter 1: Hybrid Tools and Challenges for Intelligence

Table 2: Puzzles, Mysteries and Complexities or Wicked Problems

<table>
<thead>
<tr>
<th>Type of Issue</th>
<th>Description</th>
<th>Intelligence Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Puzzle</td>
<td>Answer exists but may not be known</td>
<td>The solution</td>
</tr>
<tr>
<td>Mystery</td>
<td>Answer contingent, but key variables, history, analogy</td>
<td>Best forecast, perhaps with scenarios or excursions</td>
</tr>
<tr>
<td>Complexity, aka Wicked Problems</td>
<td>Many actors responding to changing circumstances, no established pattern</td>
<td>“Sensemaking”? Perhaps done orally, with intelligence and policy interacting</td>
</tr>
</tbody>
</table>

The challenges of these wicked problems are fundamental, and they touch on all aspects of the intelligence process. Most fundamental is the challenge to “truth” in the digital age. The great irony of information technology is that all the wonderful applications that were meant to connect people end up by letting them live in their own “echo chambers” where they can see and hear only what they already agree with. The echo chamber effect – or at least the polarization – also holds for material consumed through traditional media, perhaps even more than for social media (SM). Moreover, all the studies suggest that fake news propagates faster on SM than real news. In these circumstances, there can be tolerance for or normalization of “bullshit,” in Harry Frankfurt’s memorable locution. At worst, the trend could lead to a kind of nihilism about ever knowing “the truth.” In any case, the truth seems to be made relative.

The nature of cyber threats and SM spawn a series of related challenges. One is maintaining credibility, both with policy counterparts and with the public. When there is so much information out there, and so many options, how does intelligence lay claim to special credibility, all the more so when leaks are weaponized, like Russia’s release of hacked emails from Hillary Clinton and her campaign manager in the 2016 U.S. elections? To be sure, in that case, the U.S. president himself undermined the credibility of intelligence in the public’s eye by frequently seeming not to accept the firm conclusions of the U.S. Intelligence Community in its January 2017 assessment.

---

9 This and subsequent references to the case of the 2016 U.S. elections and 2017 French elections are from Treverton and others, cited above.
In any case, the cacophony of narratives makes for lots of distractions, one that are pervasive and of high intensity. The usual intelligence challenge of finding the signal amidst noise can become almost overwhelming when adversaries can swarm or swamp with information. The signal becomes hard to find and easy to miss in digital realms. Moreover, people capable of generating signals that intelligence wants to hear may opt out given the noise level – a tendency tempered, however, by the addictive quality of SM.

The same trends blur familiar lines. For instance, only a thin red line remains between rigorous critical thinking and borderline paranoia when trust in all systems is constantly eroded through media like Fox News, Infowars, RT, and Sputnik. So, too, distinguishing what is bluster from real threats is not easy because on the Web everyone exaggerates everything. Online presence is performance. False positives increase.

Anonymity on the Web is a double-edged sword. It is a race between surveillance and technological developments like encryption and the dark web. The famous 1993 New Yorker cartoon below is no longer true for dogs but can still be true for sophisticated cyber hackers. And while trolls and bots in SM can be identified, or at least falsified, that, too, requires some sophistication, and many users will take SM claims at face value, not bothering to dig more deeply.

![Image: "On the Internet, nobody knows you're a dog." Title: Figure 1: “On the Internet, Nobody Knows You’re a Dog”](image_url)

Traditionally, it was information that was weaponized, but now doubt can also be weaponized. Again, take Russia as an example. It is no longer concerned with trying to own the truth. Its aim is eroding trust rather than at pushing a particular set of messages. Language has become “hypernormalized,” in Alexei
Yurchak's phrase describing the end of the Soviet Union. His own language is complicated, but it does evoke elements of current hybrid threats, and perhaps end-states: “during late socialism but before perestroika, the hypernormalized visual representations in authoritative discourse (e.g., political slogans and billboards on the streets, visual propaganda and parades), had been “transparent” and “invisible” to pedestrians. They had not been read solely as constative descriptions and statements but tended to transform into a formulaic landscape that functioned as a set of visual performative acts that enabled reality without describing it in any predictable way.”11

Hybrid threats are advanced and persistent (APTs), which are usually associated with China in the cyber world. Yet in Russian doctrine, operations in the communication space – and, after all, Russia does have “communications management” as a field of study and research – are rarely time limited. Sometimes, with luck, the operations can become self-sustainable; seeds planted in fertile ground may grow without constant care.

Hybrid threats enlarge what might be called the “intervention space,” both physically and virtually. So far, Russia has been by far the largest practitioner of hybrid threats – hence the main intelligence target. However, China has been active too, and there have been hybrid operations in the Middle East and South Asia. The low costs and possibilities of escaping attribution will bring more countries, as well as non-state groups, into play as targets for intelligence and counterintelligence.

And with virtual tools, geography disappears. That was driven home by the 2016 Houston case. In May, a Facebook page called Heart of Texas encouraged its quarter million followers to demonstrate against an urgent cultural menace – a new library opened by a Houston mosque.12 “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.

The final challenge is institutional. Is the challenge for nations to create a new “hybrid intelligence”? Or should the task be thought of as data fusion done better? Cross-cutting enterprise approaches, ones that extend beyond whole of government to whole of society, are attractive in terms of transparency and crowd sourcing, as will be detailed later. But they run counter to powerful cultures of intelligence agencies.


Chapter 2: Challenges across Intelligence Disciplines

The challenge of hybrid threats comes as the same time as intelligence services are adjusting to a digital world.\textsuperscript{13} That entails coping with packet switched networks, and it requires better access to the huge amounts of data out there, including bulk access. It means doing so in the context of near-constant interference from hacking and computer network attack (CNE), so securing systems from attack is critical. All that data requires enormous storage; because data not relevant today may be tomorrow, intelligence has to create virtual “time machines.” Then, dealing with that data requires both advanced search algorithms, and deep training on the web and its business model, especially in order to do data mining of bulk personal data. Intelligence services are having to adapt to new threats and new methods at the same time.

The main challenge for collection is sheer volume in a world awash with information. It is detecting signals from the pervasive noise when adversaries can swarm and swamp, when fake news propagates faster that “real” news and when bluster makes it hard to distinguish what is a real threat since everything is exaggerated online. Many of the networks are disembodied, with individuals only connected online – limited traffic, with no real world group, lone wolves that have brief encounters but do not make a pack.

A digital underground is emerging, and the more fake news and noise there are in open channels, the more outliers and quality sources will look for spaces to hide – and not just from hacking communities. Fragmentation will increase. In closed societies, where expectation of total digital surveillance is a reasonable

expectation, the instinct might be to go offline completely. In any case, sheer magnitude will drive intelligence into artificial intelligence (AI) both to curate information and then to make sense of it.

Working with partners is very necessary, and both new partners and forms of partnership abound – a critical point for opportunities. Yet official collaboration is increasingly burdened by fears of leaks and the misuse of shared intelligence. Needless to say, revelations in 2015 that the United States had listened in on German Chancellor Angela Merkel’s cell phone cast a pall on sharing between the two countries; so did German intelligence’s relationship with German parliamentary committees, which sometimes leaked classified information that had been shared by Washington. In any case, relationships can rely less and less on the Cold War legacy. The new partnerships necessarily will take intelligence services outside their comfort zones, and underestimating the value of what counterparts, including new ones, provide will be even more counterproductive than in previous periods.

Ideology is still a tool for adversaries, and in that respect the message of the March 2018 nerve agent attack on a former Russian intelligence officer in Salisbury, England, presumably by Russian intelligence, is chilling: even Cold War norms are off, and the West’s somewhat sketchy record of protecting sources doesn’t help. Still, here as in other aspects of responding to hybrid threats, the last thing the Western countries want to do is emulate Putin’s Russia. Rather, it is imperative to stick to values, retain some humility and cast a wider net. Brutality instantly takes away all the remnants of the moral high ground, or if it is conceded that the business is a brutal one, then the question for potential sources becomes “who is scarier?” which is likely to be a self-defeating approach.

For propaganda, placing material in newspapers in the past was harder, but targeting was easier – newspapers had known circulation numbers, known leanings, and known audiences. Cost and ease of publishing are much lower now, but the predictability of audience is less and the task of estimating results harder. Targeting is more complex and fragmented. Message control is more tenuous than in previous periods. In particular, and uncomfortably, intelligence has to know what it wants from SM, even if that answer evolves, recognizing, too, that some of the answers will begin at home – what, for instance, is the effect of Trump’s tweets on other countries?

For analysis, too, the main challenge will be coping with all that information (and misinformation) out there. As figure 2 suggests, a fake news ecosystem surrounds mainstream media, and the objective of hybrid threats, like Russian propaganda in the 2016 U.S. and French elections, is to get that fake news to “trend” and thus be taken seriously by mainstream media. Yet the structure of most intelligence agencies is still mostly a Cold War legacy, based on the over-arching presumption that information is scarce, and the agencies find it hard to deal with ubiquitous data. Thus, the first challenge for analysis is automating analysis of social media/online content, which will require advanced Artificial Intelligence
(AI) to deal with fake videos, sarcasm, irony, snark, memes, gifs, emoticons, stickers, and the like. To be sure, there will also be a need for more and better trained humans, to make sure that analysts remain at the center of the process.

At the same time, too much focus on SM can lead to what might be called “social media mania,” leading to superficial analysis and planning. Noticing second and third-order effects is critical, and, as always with intelligence, low likelihood should not mean less attention if the stakes are high enough. Coping with volatility is a challenge, especially on SM; an item may be viral today but gone tomorrow. Because adversaries are opportunistic, systematically studying their TTPs (tactics, techniques and procedures) is all the more important, granting that whatever picture emerges should not be considered stable or complete. Finally, it will be important to do strategic analysis amid opportunistic behavior – fundamentals may change more slowly than it appears from all the chaos on the web.

The challenges for dealing with policymakers begin with understanding that they often are not well versed in hybrid threats – witness the U.S. Congress meeting with Mark Zuckerberg in the spring of 2018, when lawmakers looked somewhat silly in their ignorance of SM tools. Policymakers are subject to more pressures and distractions; this is the “attention economy,” the competition for the eyeballs of recipients. It, too, is not new but is new in scale.
It is important also to recognize that hybrid threats do also weaponize doubt, because of their very ambiguity and difficulty of attributing. Analysts also have to deal with the thin red line between rigorous critical thinking and borderline paranoia when trust is constantly eroded by outlets dealing in propaganda or sensation, not news. Moreover, policymakers, like the rest of us, will be drawn toward “sexy” social media and trending narratives, while underinvesting resources and attention in deeper trends. And, as always, politicization, leaks, and spinning intelligence findings by policymakers are threats to the enterprise as a whole and an opening for manipulation by adversaries. The inherent ambiguity, along with the cacophony of messages, may make spinning more likely in the hybrid realm.

The contours of relations between policy and intelligence were displayed in one episode when I was chairing the U.S. National Intelligence Council. When hacks into the U.S. Office of Personnel Management (OPM) in 2015 resulted in the loss of personal data on more than 20 million Americans, the immediate question was: who did it?\footnote{For detail on the hack and how it was discovered, see Brendan I. Koerner, “Inside the Cyberattack That Shocked the US Government,” \textit{Wired}, October 18, 2016, available at https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/} At this point, forensically, the complexity of hybrid threats had been reduced to a puzzle; attribution had an answer. The OPM hack came soon after the SONY hack. In the case of SONY, good work and good luck let U.S. intelligence attribute it to North Korea quickly and with high confidence. Not so in the OPM case. We were pretty sure the hack came from China, but when policy officials pressed for more detail, we were for some time in the position of having to answer, more or less, “China is a big place.”

The episode was a reminder that when an intelligence issue becomes a puzzle, policy officials will want – and expect – certainty that often isn’t possible. (Taking off my intelligence hat and putting on a policy one, I admit I didn’t mind the difficulty of attribution. Not only was it a useful lesson for policy officers, but since, in my view, the retaliatory options for the United States were unpromising, some delay for thought was welcome.\footnote{On the challenge of formulating a response to major attacks, see Tobias Feakin, \textit{Cyber Brief: Developing a Proportionate Response to a Cyber Incident}, Council on Foreign Relations, August 2015.}) It was also a reminder than attribution, even when good, is seldom quick. For instance, it took Saudi authorities two weeks to assess the damage from the Shamoon attack in 2012 that erased data on thirty thousand of Saudi Aramco’s computers.
Chapter 3: Attributing Cyber Attacks

While most elements of hybrid threats are not strikingly new, the digital realm does in fact pose new formidable new challenges. Russia’s interference in the 2016 U.S. election capitalized on the two primary vulnerabilities the digital realm creates – a lowered cost of entry for information operations, and cyber espionage and attack.16 The two elements were employed for synergy. Russia’s messaging during the election was amplified by a coordinated information operation on social media but also relied on more subtle and nefarious attacks in cyberspace. The public nature of social media information operations creates indicators that allow for detection. Most cyber attacks, however, are designed to go undetected, or at the very least, shroud the perpetrator behind layers of obscurity. Effective cyber attribution is thus critical for responding to hybrid threats.

As new vulnerabilities are created in cyberspace, new opportunities for detection and response also present themselves. Detecting malicious cyber activity may indicate the early stages of a hybrid operation. But the situation is similar to identifying influence campaigns – the presence of one hybrid tool does not guarantee the use of other hybrid tools. Malicious actors are also vulnerable

---

16 For the case, see Treverton and others, cited above. See also James Andrew Lewis, “Rethinking Cybersecurity: Strategy, Mass Effect, and States,” Center for Strategic and International Studies, January 2018, available at https://cisis-prod.s3.amazonaws.com/s3fs-public/publication/180108_Lewis_ReconsideringCybersecurity_Web.pdf. “We can begin to approach the problem of cybersecurity by defining attack. While public usage calls every malicious action in cyberspace an attack, it is more accurate to define attacks as those actions using cyber techniques or tools for violence or coercion to achieve political effect. This places espionage and crime in a separate discussion (while noting that some states use crime for political ends and rampant espionage creates a deep sense of concern among states.)”
themselves, as evidenced by Dutch intelligence services compromising the Russian hacking group APT 29 and witnessing their hack of the DNC.17

Despite warnings from the FBI that their computers had been hacked, the Democratic National Committee did not take the threat seriously for seven months, in part because the warnings had been general and did not name Russia as the source. Once they realized the problem existed, they hired CrowdStrike, a private cybersecurity technology company, rather than the FBI, to investigate the problem.18 The CrowdStrike employee assigned to the case examined the DNC servers’ code and quickly identified the string of code that did not belong. He had even seen the exact code before from his earlier work with the military’s Cyber Command and thus knew the culprit – APT 29, a hacker group led by Russian intelligence. In this case, the code was the key that allowed CrowdStrike to attribute the intrusion. In others, it may be source data, tactics, or a combination of factors that allow for successful attribution.

The first step in all cases of cyber attribution is to pull all technical data on the breach or attack, and identify the nature of the attack, what was accessed or disrupted, and the general sophistication of the attack. Then, the following are common criteria for analyzing digital forensic evidence:19

- **Source data.** Metadata, such as “source IP addresses, domain names, domain name registration information, third-party data from sources like Crowdsourse or VirusTotal, email addresses, hashes and hosting platforms can help attribution; however, these data points are easy to spoof.
- **Tools, scripts, and programs.** Other data points such as phishing packages (files and links that purposely send information back to host when activated), the language of the compiler, programming language, compile time, libraries, patterns, and other signifiers can be found in the attacker’s software.
- **Tactics, techniques, and procedures (TTPs).** Perpetrators sometimes have their own “style.” This can range from method of delivery to the way they cover their tracks. Tracking online social media activity in relation to the attack can be useful. So, too, can trying to geotag fake documents or phishing links to isolate real life locations.

---

Chapter 3: Attributing Cyber Attacks

- **Trying to get into the attacker’s head.** Understanding their goals can provide critical insight. Here, the connection to HUMINT is plain.

- **Understanding business drivers.** Knowing what is going on within companies can help predict problems. For example, if a company is preparing to release innovative products, they become a more attractive target. This underscores that, like terrorism, cyber operations cannot easily be divided between “home” and “abroad.” Better understanding of vulnerabilities at home is key to anticipating threats from “abroad.”

- **Geopolitics.** This analysis attempts to determine an actor’s identity by placing the actions under the lens of current events, tying a variety of assumptions over stakeholder motivations to the technical forensics of a cyberattack. This also begins to move from forensics toward a more strategic understanding of the threat.

As the attribution case becomes more complex, and the attack more sophisticated, additional measures can be taken to determine identity of the attackers. One report cited more than a dozen additional techniques, some of them technical: store logs and trace back queries; exploit/force attacker self-identification (e.g., beacons, web bugs, cookies, watermarking); perform input debugging; observe honeypots/honeynets; modify transmitted messages; employ forward-deployed Intrusion Detection Systems (IDSs); transmit separate messages (e.g., iTrace); perform filtering (e.g., Network Ingress Filtering); reconfigure and observe network; implement spoof prevention; query hosts; secure host/routers; insert host monitor functions (e.g., “Hack Back”); surveil attacker; match streams (via headers, content, and/or timing); employ reverse flow; combine sets of techniques.20

While there are many tools for attributing and responding to threats in cyberspace, an experienced actor can make the challenge more difficult. Some approaches to avoiding attribution include:21

- **Spoofing source information,** or forging the sender’s identity.
- **Using a “reflector host,** who replies to a forged sender and thus really replies to the actual victim, hiding the attacker’s location.”
- Employing other subtle protocol exploits.
- **Employing a “laundering” host** to transform the data and obscure the source.
- **Altering the time period of attack** can make it difficult to effectively attribute. An attack can be carried out very quickly or over a period of months.

---


21 Ibid, 82.
Given the challenges of detecting and responding to threats in the cyber realm, effectively countering hybrid threats requires a whole of society response. CrowdStrike’s involvement in responding to the Russian cyber threat is hardly unique. Private companies can and should play an important role in responding to hybrid threats. The U.S. Department of Defense cyber strategy of 2015 notes the private sector’s “significant role in dissuading cyber actors from conducting attacks.” Indeed, the private sector has frequently been involved in attribution.

Examples include “FireEye’s report, “APT28: A Window Into Russia’s Cyber Espionage Operations,” indicating Russian involvement in a variety of espionage activities against private sector and government actors”; Novetta’s report, “Operation SNM: Axiom Threat Actor Group Report,” indicating Chinese government involvement in cyber espionage against a variety of private companies, governments, journalists, and pro-democracy groups”; and “CrowdStrike’s report, “CrowdStrike Intelligence Report: Putter Panda 64,” identifying Unit 61486 in the Chinese PLA as being responsible for the cyber-enabled theft of corporate trade secrets primarily relating to the satellite, aerospace, and communication industries.”

In the short run, the attribution activities of private firms upset the usual interaction between intelligence and policy, and thus run counter to the culture of intelligence. Traditionally, when a cyber attack occurred, intelligence would do attribution in secret, then pass the results to policymakers for decision about what to do next. Now, though, private actors doing their own attribution will make the results public when it suits them. That upsets the tidy government process, but it has long-run advantages. Not only are those private companies potential collaborators for intelligence, including with no formal agreements at all, but the fact of their attributions, along with what they reveal about how they know, may diminish the “sources and methods” issues for intelligence services.

Beyond cyber technology companies assisting with attribution and cyber forensics, all companies need to more effectively secure their own and their customers’ data. Since hybrid techniques blur the lines between combatants and citizens, individuals should also take steps to secure their own accounts, just as they should be wary of manipulated information on social media. The DNC’s failure to take cyber security seriously enough in 2015–16 was critical to Russia’s successful attack.

---


23 Ibid, 27.
Chapter 4: Attribution and Deterrence

An intriguing side-question, one that runs from intelligence into policy, is to what extent attribution can act as a deterrent. Work on cyber crime is suggestive, even though most cyber attacks with criminal intent are neither very significant nor damaging, and generally amount to minor disruptions in services. As in all cases of attribution, the current first step for both governments and the private industry, is to perform “track and trace” and make a record of what was either stolen or disrupted in the attack. When technical data is not enough to trace more advanced groups, investigators will turn to known online communities and social media to conduct surveillance. They will look for “chatter” with regards to the attack in question – specifically, for key elements of the attack event that either were not made public or that can only have been known by the perpetrator. Investigators then try to place an origin of the ‘leaked’ information and if it leads to a username, attempt to identify that person.

Cyber criminals might be thought of in three categories. The first set of groups typically are younger, less experienced people who tend to commit crimes at the lower end of the spectrum, with limited damage. They can usually be found rather easily through basic track trace methods. In principle, they can also be deterred by simply threatening to reveal their identity and thus make them vulnerable to basic law enforcement. The second set of groups is comprised of more experienced individuals or small groups. Their attacks generally are more centered on financial crime and service disruption. They typically are active on “hacker forums, and usually require outside investigative measures to apprehend. Deterring them, though, is similar to deterrence for the first set.

24 This typology is adapted from Clement Guitton, “Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence, Journal of Cyber Criminology, 6. 2 (July–December 2013).
By contrast, the third set of groups are extremely well-organized. Their online social presence is either lacking, or untraceable. Their targets are major government services, company services, and their hacks are responsible for serious high profile damages. Their technical and social understanding of the industry allows them to act with near impunity. Moreover, the line between state sponsored and non-state groups is blurred given both the complexity and nature of the attack. The state sponsors are surrounded by a coterie of government-financed “private” security firms, and both governments and sophisticated criminal groups have access to a network of individual freelance hackers.

The only way to apprehend them is to consistently watch for mistakes and patterns, but prevention or deterrence is well near impossible. They know the industry inside and out, and so take advantage of stagnate security. Systems that are constantly changing, with dedicated, round the clock staff to evaluate changing threats, usually do not fall victim even to these sophisticated group. Google, Microsoft, Amazon are examples; in contrast, victims like Equifax, VISA, and Master Card, had stagnate systems and thus were prey for hackers.²⁵

The majority of criminal hacks come from groups in the first two categories, with motives ranging from personal gain, résumé building for careers in cyber security, or “practical jokes.” Generally, if the attack is small scale, limited to light damage, such as thefts of cash or website manipulation, then it is likely one of the first two sets of groups. Companies are less likely willing to report attacks from these groups to police or agencies for fear that negative press will cause them to lose business; they tend to deal with these groups internally for investigative purposes. The only time companies will make this group public is when enough evidence has been gathered to press formal charges in the courts if they choose to go down that avenue.

In contrast, serious cases of corporate theft of IP, massive global service disruption, mass compromising of accounts, and leaked data with significant political and financial ramifications are done by groups in the third category. These groups require all forms of government and private institutions to assist in the investigation, and therefore, in order to manage risk companies usually seek immediate help. Thus, the rub is that while most criminal cases can be deterred through attribution and the accompanying prospect of law enforcement, that “most” is the ones that are limited in scope of attack, disruption, or even theft.

The sophisticated groups, where the majority of major attacks originate, are all-but impossible to deter with current attribution techniques because they have enough experience in both the trade and the industry to transcend law enforcement and private security barriers. Indeed, the nature of the web itself works against

²⁵ It is worth noting, though, that Google Docs was the object of a massive phishing attack in the spring of 2017.
Chapter 4: Attribution and Deterrence

attribution: IP and other addresses are easy to spoof, DNS registrations lack source authentication, and both criminals and state groups have access to proxy servers, encryption, anonymization and the like. Therefore, on the crime front there is currently no effective way to stop major attacks before they are hatched. Probably, for companies and for governments, the best that can be done is to either wait for groups to make a mistake that breaks their cover or consistently develop systems to combat the hybrid threat.

The examples from cyber crime are instructive, though there remains the big strategic question of whether, and when, nation-state cyber attackers might want their actions attributed to them, as a demonstration of what they can do. The Russian attackers in the 2016 elections either were pretty careless in covering their tracks or didn't mind the actions being attributed to them. And the Russian services used many of the same methods in their attacks during the French elections in 2017. Still, attribution is often ambiguous; as one industry leader noted: “… many private firms and security researchers are quick to reach a conclusion on who is behind an attack based on code and infrastructure re-use, as well as the tactics, techniques, and protocols (TTPs) they have previously ascribed to bad actors with cute names. The methods typically would not pass a court of law’s evidentiary standards, but are good enough for Twitter.” Putin’s insistence, despite all the U.S. analysis, that Russia was not behind the 2016 U.S. election hacks suggests a circumstance much like Israeli nuclear weapons: Russia shows what it can do while pretending it isn’t, thus trying to reduce the risk of responses to its actions.

Chapter 5: Detecting Social Media-Aided Influence Operations

Social media is often a critical medium for employing, and thus detecting, influence operations and possible hybrid threats. Russia’s election interference in the United States was successful not only because of hacks and well-timed leaks alone; the campaign also relied on Russian media outlets, paid human trolls, and bots to amplify the message. Of course, the presence of an information campaign does not guarantee the adversary has employed, or will employ, other tools (kinetic, economic, etc.). Though a hybrid threat, by the definition employed here, involves the use of multiple tools synchronously, it does not require social media-driven influence operations to be one of the tools. Yet the report on hybrid threats cited earlier suggests they are often present. Digital tools have lowered the cost of entry of information campaigns, which played an important role in the hybrid operations case studies examined in that report – Russia’s interference in the 2016 U.S. presidential election, intervention in Crimea and Eastern Ukraine, and influence on the 2017 French elections. Troll accounts, botnets, and ongoing digital influence campaigns may be the proverbial canary in the coal mine for hybrid threats. Fortunately, twitter bots, online trolls, and thus influence operations rely on public posting, which has key indicators and makes identifying this aspect of hybrid operations possible.

Automated accounts differ from a human driven accounts in numerous important ways – the degree to which they appear as a real person, level of automation, activity, and purpose – but many send signals that can reveal their nature. There are three identifiers: “time-oriented information (temporal markers), content-oriented information (semantic markers), and social-oriented

28 Tréverton and others, cited above.
The intelligence challenges of hybrid threats: focus on cyber and virtual realm

Temporal markers are often the simplest way of identifying bots, as the data is the easiest to gather and the indicators are the strongest. An account can be identified as a bot with high degrees of certainty if tweets are sent at a rate unreasonable for human activity or on a specific schedule. Semantic markers require more advanced analysis: can they effectively communicate when messaged at on social media sites and does the content of their posts make consistent sense? Network markers can identify bots if their network connections are primarily with other bots, though this information requires more sophisticated tools to gather.

The Atlantic Council’s Digital Forensic Research Lab (DFRLab) suggests that political bots share three qualities: activity, amplification, and anonymity. It also identifies activity, or temporal markers, as the lead characteristic of political bots. The more bots tweet, the more they push their desired message. The rate of tweeting also matters – 72 tweets per day over a period of months qualifies as suspicious, 144 per day is highly suspicious, and over 240 tweets per day is “hypertweeting.” Political bot accounts typically have high rate of amplification, or retweets, on a certain political message. Anonymity is decided on a simple criterion: is the account’s profile information too impersonal to be credible?

A team at Indiana University created Botometer, formerly BotOrNot, an automated tool to identify social bots. They propose six criteria for identifying bots: network, user, friends, temporal, content, and sentiment. Like other similar tools, entering an account will return a score that analyzes how likely it is that the account is automated. Numerous other online tools allow for simple detection or tracking of bot accounts, though their accuracy is not guaranteed. These websites include https://botcheck.me/, which analyzes Twitter accounts to classify them as “high-confidence bot accounts.” The Hamilton68 Project, part of the Alliance for Securing Democracy at the German Marshall Fund of the United States, tracks Russian propaganda “in near real-time,” examining both trends from official Russian accounts and bot or troll accounts linked to influence operations.

---


Chapter 5: Detecting Social Media-Aided Influence Operations

Though detecting bot accounts and influence campaigns involves uncertainty, these efforts are important for potentially catching early warning signs of hybrid campaigns. In many cases uncovering a bot-assisted social media campaign will not indicate the use of other hybrid tools. But tracking SM influence operations is a useful practice in and of itself. Reaching out to the private sector for bot detection and trend tracking provides many more “eyes” and is critical in developing a whole of society response to hybrid threats.

The possibilities are suggested by the 2016 U.S. elections case. While the propaganda campaign surprised the United States, it should not have, for there was warning but from an unfamiliar quarter. A group of outside analysts 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.\(^\text{33}\) Yet the case drives home the point that governments and their intelligence service can draw on lots of help from citizens who are actively monitoring SM for their own reasons. And governments do not have to do much reaching; simply being open to \textit{listening} may be enough.

Chapter 6: Taking Advantage of Opportunities

Opportunities for intelligence lie in new media, new networks and new partnerships. However, the culture of intelligence is slow to adapt; in one study of social media in intelligence a few years ago, NSA analysts reported getting the question from colleagues: “what’s a hashtag?”34 The private citizens looking at jihadi websites in 2014 who found evidence of Russian fakery drive home the possibilities of “crowd sourcing” around the world, seeking partners in identifying fake news and planted posts. Alas, this kind of openness and reach to private sector runs very much against the grain of intelligence cultures. Cyber is another great opportunity. In the short run, private actors upset the paradigm of Intelligence attributing in secret for policy to take decisions. Now, private companies are doing attribution too and will go public when it suits them. Yet in the longer run, those companies are a great opportunity for partners, and when they go public it might even ease the “sources and methods” problem for intelligence.

Traditional intelligence collectors will play their roles in new circumstances; exactly how remains an open question. SIGINT, for instance, now uses social media mostly for targeting traditional collection, especially against terrorists: “terrorists may have good OPSEC but they also have children, and so when I find an email…” HUMINT can be critical but will be pushed into a much broader arena, and find itself collaborating with new partners, including some outside government. HUMINT is probably more critical than ever but no easier. To the

34 The study was, alas, classified. For an unclassified version of part of it, see Gregory F. Treverton, *New Tools for Collaboration: The Experience of the U.S. Intelligence Community*, Center for Strategic and International Studies, January 2016, available at https://www.csis.org/analysis/new-tools-collaboration,
The extent the targets are foreign, especially Russian intelligence services, they are at least known, and perhaps somewhat “softer” than Al Qaeda. As one former CIA chief of station put it:

“This is an intelligence challenge. We need to collect the intelligence on their plans and intentions. That means penetrating their intelligence services so that we can track what they are doing and then prevent, preempt, and counter their espionage against us. One good example was the 2010 arrest of the SVR ‘illegals.’ As far as our resources, we are tracking a lot of different state and non-state actor threats, such as terrorists, and criminals, the Chinese and a host of others. The question for the intelligence community is whether they have enough resources to track Russian targets.”

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

SM are a great source of intelligence – and warning: as one analyst from the U.S. Defense Intelligence Agency put it in identifying Russia soldiers in Ukraine, “selfies are our best friend.” As in that case, cell phones may be geolocated, or the location may be inferred from analysis of the selfie – opening an entire new source for GEOINT. So, too, ubiquitous cameras offer GEOINT new opportunities for identifying people and their movements.

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

What is still, slightly weirdly, called “open source” is very much a work in progress, especially in the United States. It is tempted to show its worth on “hard” targets, like proliferation, which probably are not its comparative advantage, and the U.S. Open Source Enterprise (OSE) has returned to the CIA, rather than the inter-agency auspices of the director of national Intelligence (DNI). It tends to regard SM as just the latest media to exploit, and it goes about validation in a

---

fairly traditional way, looking at location and numbers of retweets, for instance. Ideally, it would become the focal-point for matters virtual but unclassified across the entire government, in particular pushing the AI needed to cope with ubiquitous data.

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

On former senior intelligence officer compared the cyber task with the counterintelligence challenges, from a NATO perspective:

“If we are not talking about preparing for a conventional Russian attack, cyber is arguably the most important thing that NATO needs to be focused on. It’s also an area where NATO can pretty easily coordinate with each other and, indeed, I think it’s been doing so in terms of sharing of information on that kind of threat. Counterintelligence is a lot harder because it gets into conducting mole hunts and trying to find out where you are penetrated as an organization – whether it’s NATO, CIA or DIA. That is a much harder and more sensitive thing to do. But the cyber stuff has really got to be out there in front. It is close to being number one in my book.”

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

---

36 Ibid.
Chapter 7: Reshaping Intelligence

In the end, might the challenges of hybrid threats help to break out of what has become a tired and industrial notion of the intelligence cycle – as presented in a very old version in figure 3? To be sure, the cycle never quite represented reality, in the sense that the press of events often required the cycle to be short-circuit-ed. More fundamentally, however, while the cycle may have made some sense as a paradigm during the Cold War, it cannot possibly do so now. Then, there was indeed a certain industrial character to trying, especially, to solve the puzzles about the Soviet Union. Intelligence knew what it was looking for; in the phrase popularized by former U.S. Secretary of Defense Donald Rumsfeld, it was trying to find the “known unknowns – things we knew we didn’t know.”

Now, we are often in the position of not knowing what we don’t know, Rumsfeld’s unknown unknowns. So intelligence cannot start with a requirement, for it doesn’t know what is required. Those outsiders following jihadi websites in 2014 found an answer before they knew the question. In that sense, intelligence needs to become sequence neutral. Now that Information is ubiquitous, intelligence should also be information neutral, only prizing its special sources when they add real value. Now that computers are so powerful and data so abundant, looking for interesting similarities or correlations is the name of the game. And, ultimately, if intelligence were part of a whole of society response to hybrid threats, that would put pressure on it to turn its analytic culture upside

37 For one critique, see Arthur S. Hulnick, “What’s Wrong with the Intelligence Cycle”, Intelligence and national Security, 21, 6 (2006), 959–979.
38 The distinctions were not new with Rumsfeld, but he used them famously in a Pentagon press briefing, December 12, 2002. Known unknowns are what we know we don’t know, and known unknowns are what we don’t know we don’t know.
down: if those products were to be shared with private sector partners in the fight against hybrid threats, including many without security clearances, the products would need to start with open sources, adding bells and whistles from secret sources only if and as necessary.

Figure 3: Canonical Intelligence Cycle.\textsuperscript{39}

\textsuperscript{39} U.S. Army, circa 1948, courtesy of Sir David Omand.
The Intelligence Challenges of Hybrid Threats

What challenges does “Hybrid Threats” pose for the world of intelligence analysis and tradecraft, and how should intelligence agencies adapt? This study is a part of CATS’ project on intelligence connected to Influence Operations, and is sponsored by the Swedish Civil Contingencies Agency (MSB). It addresses the new realm of hybrid threats and challenges, and the roles for the world of intelligence analysis and tradecraft.

In this study, Dr Gregory Treverton – former Chairman of the US National Intelligence Council and now Senior Fellow with CATS – analyzes social media and cyber attacks as well as signals and human intelligence in relation to real world events.

The intelligence challenge starts with recognizing the range of hybrid threats and what is new about them – targets are now societies, not armies; several tools are being used both simultaneously and strategically for maximum effect; and it explores how the cyber dimension, along with the social media (SM) and other virtual arenas offer new, inexpensive avenues of attack. This important analytical contribution begins with the tools, then turns to the challenges of hybrid threats across the elements of intelligence – collection, analysis and relations between intelligence and policy.

Then, it turns to the special challenges for intelligence agencies – but also the special opportunities – that exist across a range of cyber and virtual domains. In particular it focuses on the implications for the intelligence organizations performing the traditional ‘INT’ functions (HUMINT and SIGINT) and for counterintelligence. It concludes with perspectives on how the special challenges of hybrid threats might conduce to a much wider change in the traditional intelligence paradigm.