---

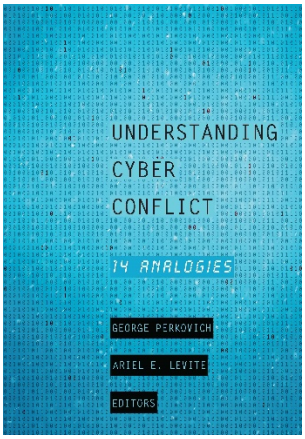
# Intelligence in Cyber—and Cyber in Intelligence

Michael Warner

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



# 1 Intelligence in Cyber— and Cyber in Intelligence

MICHAEL WARNER

Cyber technologies and techniques in some respects originated in the intelligence profession. Examining cyberspace operations in the light of the history and practice of technology helps illuminate both topics.[1] Intelligence activities and cyberspace operations can look quite similar; what we call cyber is intelligence in an important sense. The resemblances between the two fields are not coincidental. Understanding them opens new possibilities for exploring the applicability of intelligence concepts to a growing understanding of cyberspace.

To appreciate the evolutionary connections between these fields, it is necessary to define the multiple functions that intelligence performs. Intelligence guides decisions by providing insight to leaders and commanders, of course, but its definition is broader still. The field has always included espionage and counterespionage, and today it includes technical collection as well. Such clandestine activities are but a short step from covert operations, which fall under the ambit of intelligence organizations in many states. Finally, intelligence, with its partner activities of surveillance and reconnaissance, has become a key component of today's real-time, networked warfare. This chapter explores these functions of intelligence and how cyber capabilities resemble or differ from the capabilities that earlier technologies provided, as well as how cyberspace capabilities and operations pose new policy dilemmas. It does so from a US perspective, but the phenomena and issues discussed here are probably pertinent to other countries too.

## Spy versus Spy

Intelligence has evolved over the last century, giving rise to two overlapping but not congruent definitions of the field. US military doctrine views *intelligence* as information that a commander finds vital in making a decision, plus the sources, methods, and processes used to produce that information. Not all information is intelligence, of course. Only information on the adversary and the conditions under which the commander's force might have to fight is considered *intelligence*.[2] One should note, however, that this concept of intelligence is relatively new. Indeed, it was formally stated in such terms only in the 1920s.[3] Spying,

however, dates to the dawn of history; ancient texts from around the world mention spies and their exploits on behalf of rulers and commanders. The emergence of modern intelligence from classic spy craft resembles a millennia-wide "before" and "after" picture of the subject.

The Chinese sage whom we call Sun Tzu composed one of the earliest reflections on intelligence sometime around 300 BC. His classic *The Art of War* was hardly the first written reflection on this topic, although earlier authors (as far as we know) did not match Sun Tzu's insight and brevity in his thirteenth and final chapter, "On the Use of Spies." He described a lonely and deadly craft that occasionally became very important. A *spy*, in Sun Tzu's telling, might collect secrets, spread disinformation or bad counsel in the enemy's camp, or even assassinate enemy officials. He thus combined a range of activities far broader than merely passing information to his commander. A spy could potentially become a fulcrum of history, providing information or taking direct action to ensure the downfall of a dynasty and a shifting of the mandate of heaven.

Such considerations have relevance today, even for those who no longer see a change in regimes as cosmically important. Spy craft did not evolve much in the two millennia between Sun Tzu's day and the Industrial Revolution, so we can take his ideas as fairly representative of the field up until roughly the age of Napoleon Bonaparte. Indeed, while campaigning, Napoleon ran his spy network from his tent, filing agents' reports in pigeon holes in his camp desk. Even with the spread of intelligence collection by remote and then automated means in the twentieth century, individual spies retained importance for intelligence consumers and systems. Well-placed insiders could and did nullify expensive suites of technical collection assets during the Cold War, and more recently "insider threats" (even if not spies per se) precipitated media leaks that have significantly complicated international relations.

Spies have been eclipsed by technical collection, of course, but security and counterintelligence offices continue to focus significant resources on finding (and deterring) enemy agents. Leaders and their advisers intuit the danger that any human penetration poses to technological advantages, military operations, and diplomatic ties. The mere possibility of a spy can disrupt an intelligence bureau or even an alliance; the genuine article can do grave harm and cause effects that reverberate for years. Entire disciplines of the security field (e.g., background checks, compartmentation, and so on) grew up around the imperative to minimize and mitigate the damage that spies could inflict. Counterintelligence, of course, emerged precisely to guard against spies in a more active manner. The most effective counterintelligence operations (like Britain's Double-Cross system in World War II) managed to take control of not only enemy spies but the perceptions of their spymasters as well. They fooled the latter into believing their espionage network was still collecting valuable secrets, which naturally turned out to be misleading "chicken feed."[4]

Cyberspace operations have obvious parallels to traditional human espionage. An *implant*, for example, can sit in a computer for weeks, months, or years, collecting secrets great and small. The finding of such an implant, like catching a

spy, evokes mingled satisfaction and fear. Not finding one, moreover, might not inspire confidence. It could mean there was no intruder to catch. Alternatively, it might mean that one looked in the wrong place.

In strategic terms, catching a spy or finding an implant is not exactly a casus belli, although running a spy (or placing an implant) is obviously a provocation. States have tacitly established protocols for handling espionage flaps. Typically the actual spy stands trial, while his or her foreign case officers are declared personae non gratae and expelled. Foreign intelligence officers (like Russia's Anna Chapman, whom the Federal Bureau of Investigation [FBI] caught in 2010) are jailed in a glare of publicity. Soon, however, when the media's attention has wandered elsewhere, the spies are quietly exchanged for individuals in their homeland's prisons. We have not developed such protocols for handing disconnected computer implants back to their originators, but one suspects that similar understandings around cyber espionage will emerge over time.

How much cyber espionage is there? That depends on how broadly we define *espionage* as the acquisition of data in ways unbeknownst to its "owner." At the risk of stating the obvious, entire sectors of the world economy now rest on the ability of corporations to aggregate and sell information about the online habits of consumers. Few computer users worry about such aggregation. They implicitly permit much (though by no means all) by pressing "Accept" after scrolling through the fine print in lengthy end-user agreements. This chapter must leave such matters to abler minds, though certainly a fair amount of illegal or at least unethical mischief is directed against the software sold to consumers to facilitate the harvesting and sale of their data.[5] Going from such mischief to actively cyber spying on unsuspecting people is a short step. Today anyone with a network connection can be a victim of espionage mounted from nearly anywhere. A cottage industry has grown up around efforts to find and expose such cyber espionage schemes. From the instances uncovered so far, anyone possessing modest resources and sufficient motivation can readily download highly intrusive, capable, stealthy suites of surveillance tools.[6] The publicly available evidence—not to mention the complaints by many governments and the myriad allegations based on leaked documents—should lead any fair-minded observer to conclude that many examples of cyber espionage were perpetrated by state actors.

The counterintelligence parallel with cyberspace operations seems to be developing another analogous aspect as well. The most ruthless counterintelligence services since at least the czars' Okhrana have planted agent provocateurs among groups they deemed to be subversive. Their role was not only to report from within but to incite rash or premature action that would expose and discredit the groups. A whole literary subgenre explored the dramatic possibilities such plots entailed; think of Joseph Conrad's *The Secret Agent* (1907) or G. K. Chesterton's *The Man Who Was Thursday* (1908). Such agents were not just the stuff of fiction—Vladimir Lenin devoted his landmark essay "What Is to Be Done?" (1902) to countering them—and they spread fear and distrust among revolutionaries across Europe before World War I.

Attentive watchers of the cyber news will see an echo of these operations. Security services like the FBI seem to be learning how to persuade cyber criminals to switch allegiance while maintaining contact with their online cohorts (on secretly monitored connections, of course). Once the authorities identify the network and record enough evidence against its members to warrant prosecution, the nations involved in the investigation mount simultaneous raids—sometimes across multiple continents—to round up the suspects.[7] Court filings soon expose the mole in the network, of course, but by then the person has been whisked to safety and perhaps even living under a new, state-provided identity.[8] The hacker world today is turning paranoid, worried that many of the anonymous contacts in the dark web have switched sides and started providing evidence. This spreading distrust represents a direct application of counterintelligence tradecraft to cyberspace.[9]

In sum, espionage and counterespionage operations made the jump from the proverbial dark alleys to cyberspace virtually intact. What is new is old. How readily both of these ancient crafts adapted their techniques to the new cyber domain is astonishing. The main difference between their traditional operations and their cyber counterparts is the scale that can be exploited in the latter.

## Common Roots

The history of intelligence provides still another template for understanding cyber operations. Intelligence connected itself to communications technology in the early twentieth century, with profound implications for itself and for diplomacy, security, and privacy. The modern era of communications began with the improvement of the telegraph, allowing quantities of messages and data to be transferred across global distances in near-real time. Wireless telegraphy and then radio broadcasting accelerated this trend, creating mass audiences and markets, as well as new military requirements for not only the equipment to transmit and receive such communications but also the cryptographic support to secure them and the messages they relayed. Intelligence, of course, grew in parallel with what Stephen Biddle terms the "new system" of military operations, in which real-time communications allowed generals to synchronize combined-arms actions involving infantry and artillery, and soon armor, aircraft, and ultimately guided weapons as well.[10] This revolution in military affairs began with the battlefield use of radio in World War I and accelerated across the remainder of the twentieth century. Over the last generation, modern militaries have become dependent on sensors, networks, bandwidth, and surveillance. This dependence is encapsulated in the ubiquity (at least in military affairs) of the term "C4ISR," meaning command, control, communications, computers, intelligence, surveillance, and reconnaissance.

The parallel growth of advanced, technologically enabled intelligence alongside the new system was not coincidental; rather, it was (and is) organic. These two trends share a common root in the widespread impulse across the industrialized powers to gain real-time control of military forces at a distance while

monitoring and frustrating adversaries who seek to control their own assets and forces. This sea change took place quite suddenly and dramatically during World War I, in which vast armies, navies, and soon air forces had to communicate securely in real time or lose to adversaries who did. To cite but two examples, the Russian disaster at Tannenberg in August 1914 showed the occasionally strategic consequences of lapses in communications security, while the Royal Navy's exploitation of German naval systems demonstrated what operational possibilities could be opened by a sustained cryptologic campaign against poor security practices and vulnerable technology.[11] The shift to technical collection and analysis of machine-generated data revolutionized the intelligence business, transforming it seemingly overnight from an ancient craft into an industrial enterprise.

Every Western military sought to learn communications security lessons from World War I. Modern codes and encryption had arisen with the printing press in the Renaissance, but they took off anew with the telegraph revolution in the nineteenth century and especially with the wireless in the twentieth century. The difference between private cryptography and governmental and military systems, of course, was the sensitivity of the information they carried and hence the length of time (in hours, days, months, or decades) that the information's owner would want eavesdroppers to have to devote to decrypting the intercepted messages. Despite the higher stakes for official uses, however, the quality of cryptographic support to both private and government messages for centuries remained roughly equivalent—in other words, not very good. That began to change with governments' quests for reliable enciphering machines for tactical communications, such as the Swiss-made Enigma, which was marketed to commercial firms but was soon adopted and improved by the German military in the late 1920s. These machines had become widespread by World War II, at least among the major combatants in that conflict. In 1939 the use of coded communications had also prompted several states (most notably Britain) to mount concerted efforts to divine the secrets of those enciphering machines and the codes they protected. Enlisting their American allies, soon the British applied a new technology to the problem—the digital computer.

The Anglo-American signals intelligence alliance after World War II hastened the evolution of computers and of America's computer industry in the 1950s. The enduring Anglo-American partnership henceforth kept its team members, particularly the National Security Agency (NSA), up to date with the evolution of computers, their concentration in networks, and the progress of a new field, computer security.

From the beginning, the NSA's expertise in securing digital communications and networks influenced the concepts for and debates over securing computers and the data they stored and shared.[12] Such effects quickly became embroiled in debates over encryption, particularly regarding the extent of the US government's role in fostering high-grade cryptography. For decades the point had been moot, as the best cryptographic solutions were treated as military secrets (which in a sense they were) and their export was banned. With the de facto merging of telecommunications devices and computers by the 1970s, however, a

new dilemma arose—that is, how to secure digital data for governmental agencies, banks, and other institutions that shared sensitive communications and files but did not need export-controlled, military-grade ciphers. The initial answer was the Data Encryption Standard (DES), which the National Bureau of Standards proposed in 1975 after its development by IBM and vetting by the NSA. Various observers soon found weaknesses with the DES algorithm, however. Some alleged that the US government had exploited its role in creating DES to leave "backdoors" in the standard that would allow government officials routine (or at least emergency) access to private data.[13] For their part, the relevant agencies and even a congressional investigation insisted the government had done no such thing.[14] The controversy over DES created a template that has been followed ever since—for instance, in the debates during Bill Clinton's administration about the proposed "Clipper Chip" in the 1990s and the 2015–16 contretemps between Apple, Inc., and the FBI concerning the data residing on a smartphone used by one of the San Bernardino killers.[15] Then as now, various government officials' insistence on some official method of bypassing encryption standards for urgent national security and law enforcement purposes alarmed those who feared that US intelligence had already compromised the standards.[16]

This chapter cannot hope to resolve the policy issues over encryption or allay suspicions about the US government's motives and actions. The author supports strong encryption for everyone and would like all governments to resist the urge to install backdoors in any cryptographic systems. The point of this chapter, however, seeks to add perspective by noting today virtually anyone can routinely use encryption that, historically speaking, is fantastically effective. Nevertheless, governments, hacktivists, and organized criminals have found various ways around that wonderful encryption. Most observers would surely agree that encryption has never been better, yet those observers might nonetheless concede that never have so many users lost exclusive control of so much of their data.[17]

The burgeoning computer security field has an additional connection to intelligence that has been largely overlooked. In certain ways the concepts of computer security grew directly from the painful education in counterintelligence and security practices that US intelligence agencies gained during and after World War II. There was nothing like operating behind the Iron Curtain for making an organization interested in end-to-end security measures. This is precisely why the Central Intelligence Agency (CIA) established a comprehensive "automated data processing" (ADP) security regime that congressional investigators publicly praised forty years ago! Committee staffers surveying federal computer security in 1976 applauded the CIA for its thorough approach, which worked "on the assumption that not only is there potential for compromise in any ADP system[,] it is likely that an attempt will be made to effect that compromise." Though agency officials declined to offer their computer security regime as a template, the committee's study nevertheless suggested "trying to apply certain ADP security techniques which had evolved at CIA to other Federal programs where the issue may not be national security but at stake were

considerations of nearly equal consequence, such as individual privacy data and . . . financial transactions leading to disbursements of large amounts of public funds."[18]

The spread of computers had heralded something novel for both communications and intelligence. Hitherto the devices that secured and transmitted information did not also store it. Computers did, at least as soon as they were given built-in memory. Thus, the level of care taken to transmit messages securely now must extend over the entire life cycle of that data and even to the machines that touch that data. Not only is your current data vulnerable to spies and eavesdroppers, it is now at risk forever in cyberspace. This raised the security bar tremendously for average users as well for governments. Consequently, the NSA since 2009 on its public website has urged "customers" to make prudent preparations now for the day when their encrypted data will be vulnerable to attack by quantum computers.[19] Permanency of data not only has broadened the practice of intelligence (as hinted above) but also has drawn a line of demarcation between some traditional, passive forms of intelligence collection and the new digital methods.

## Everything Goes Digital

The early development of radio suggests yet another aspect to the analogy between intelligence and cyberspace. Certain security and policy issues relating to computers and networks strongly resemble those associated with radio as that earlier medium evolved and spread in the first decades of the twentieth century. Indeed, many of the terms we routinely use to describe the workings of cyberspace—"network," "bandwidth," "wireless," and others—came from radio terminology. As noted, both radio broadcasts and computer data can be intercepted in midstream and analyzed in various ways to deduce information on one's opponents, even if one cannot read the content of the intercepted messages. Both radio and computer communications therefore must be used with care so as not to disclose too much information to opponents.

Furthermore, the kinship between intelligence and deception exactly parallels the relationship between radio (and computer) operations and the field of electronic warfare (EW). Radio was weaponized in World War II, and EW has been a standard feature of modern conflict ever since. An opponent's employment of both radio and computer networks can be denied by jamming or flooding of one form or another. And, of course, those who intercept radio transmissions or computer data can be actively deceived by a clever originator. These intelligence dimensions of the new cyber realm (i.e., the principles of attack, defense, and exploitation) are readily apparent; indeed, they guided the US Department of Defense's thinking on information warfare for the first couple decades of this doctrine's existence. EW is thus one of the taproots of cyberspace operations, at least in the United States, as military thinking about command, control, and communications countermeasures in the early 1980s led directly to the earliest policy pronouncements on information warfare in 1992.[20]

Historians should not forget a related point: substantial impetus for the computer industry's maturation derived from the US military's drive to make weapons smarter and to share data to and from the battlefield. This vast field again falls beyond the scope of this exploration of the intelligence analogy, but it is important to note certain additional links between the evolution of computers and the realm of intelligence support to battlefield commanders. Smart weapons emerged in the early 1970s, motivated in part by the Pentagon's desire to increase the precision of bombs in Vietnam (thereby reducing the danger to aircrews and minimizing morally and politically harmful collateral damage to civilians). The weapons were "smart" not only because they could be guided to their targets but also because they depended on intelligence about those targets (e.g., precise locations) and on copious and timely data flows to increase their accuracy and lethality. Such data flows eventually demanded quantum leaps in bandwidth, processing power, and networking architecture. The US military thus helped drive improvements to digital communications to increase their resilience and volume, and in the 1970s it began setting standards for the security of these burgeoning systems and the data they carried. All these developments spurred research in the computer industry and provided growing markets for innovations that initially seemed to lack consumer markets.

Government links with industry had a direct, strategic focus as well. That nexus brought the intelligence and computer sectors together at the dawn of cyberspace. As historian Jonathan Winkler has shown, the US government has jealously guarded a national interest in the progress of international telecommunications, beginning in World War I and continuing unabated to our day.[21] Among many examples, Ronald Reagan's administration in 1984 took note of the de facto blending of the computer and telecommunications fields and found this trend had significant implications for US security. President Reagan accordingly issued a top-secret directive giving the NSA responsibility for setting standards to protect sensitive but unclassified data in all US federal government computers. Though Congress soon overturned Reagan's measure, the mere fact a president had ordered such a step demonstrated the growing overlap between the intelligence and computer security worlds.[22] Washington has quietly secured the strategic high ground in the nation's communications sector, using intelligence both to guard and to exploit that advantage. The importance of that access for the nation's intelligence function needs no reiteration here.

Cyber operations grew out of and still resemble EW, as noted earlier, with one key difference. Traditional EW aimed to guide, target, or protect weapons systems but remained an activity extrinsic to those weapons as such. Cyberspace, in contrast, includes many of those weapons. The "Internet of things" arrived early in modern military arsenals. Their interconnectivity not only makes them smart but also potentially leaves them vulnerable as an adversary could theoretically find ways to make those systems hinder rather than help operations. Here is another way in which cyberspace operations both learn from and affect intelligence activities.

## What Is New in Cyberspace?

So far the parallels described between intelligence activities and cyberspace operations are not merely hypothetical but are already working themselves out in practice around the world. Other parallels can be envisioned as well, at least in listing the possible warning signs that might accompany their emergence over the foreseeable future.

The most obvious and oft-discussed association between intelligence activities and cyberspace operations is the confusion they can cause among those on their receiving end. Human espionage can look quite like subversion or worse as authors such as Sun Tzu and the Indian sage Kautilya noted thousands of years ago. They urged commanders and princes to have their spies assassinate rival chiefs.[23] Active intelligence operations, like cyberspace collection campaigns, are by definition quiet but potentially provocative. They can appear similar to preparations for war, and from time to time they have increased tensions between states. But has anyone gone to war over an intelligence operation that was exposed or blew up in a crisis?

Here the parallel with intelligence can be informative. People have gone to war having bad intelligence that was either misconceived or spoofed by the adversary (see the Iraq War in 2003). Wars have started over assassinations, to be sure, but an *assassination* is by definition a successful operation designed to provoke hostilities and is not the inadvertent cause of them. Outside of these unrepresentative examples, the list gets thin. As noted previously, states by and large do not fight over blown technical collection activities. History yields many such examples of states catching spies or finding wiretaps, telephone bugs, and so on, without those states declaring war in response. The net result of blown intelligence activities is typically the loss (or turning) of the source, sometimes with a well-publicized protest, an expulsion of diplomats, or an execution or two. Even military reconnaissance is not usually dangerously provocative, as a single aircraft or patrol boat can hardly be mistaken for an invasion force. Overflights of the Soviet Union in the 1950s did not provoke a strategic military response by Moscow (apart from the Soviets' downing reconnaissance aircraft such as Francis Gary Powers's U2 in 1960). Similarly, aggressive US overflights of Cuba in the Missile Crisis (1962) agitated local air defense and concentrated minds in Moscow and Havana, but they did not prompt Soviet strikes on the United States.

Cyberspace operations gone awry, like intelligence revelations, so far have not provoked wars. The net effect in cyberspace is typically the quiet purging of an implant, the updating of an operating system, or the closing of a port, combined with perhaps a diplomatic complaint, possibly via the press. The reason for this lack of panic and escalation might have been explained (in another context) by the Atlantic Council's Jason Healey. As he notes, cyberspace operations rarely if ever proceed in isolation. That two states are at odds over some issue certainly assists in the attribution of contemporaneous cyber attacks to one or both of them.[24] Although Healey does not explicitly flip this coin, his argument also hints that policymakers virtually always know some context behind the

events that places noncrisis cyber developments in perspective, usually by showing that the state allegedly perpetrating the cyber transgression is not currently deploying for war.

Can cyber operations cause instability and even escalate a crisis? Of course, they might, if perhaps only because no one can definitively prove that they will not. What we can say is that no cyberspace operation to date has made a crisis spiral into war. Indeed, the United States has experienced more than its share of cyber penetrations and cyber attacks, yet it has never come close to initiating hostilities over a cyber incident. As far as we know, no one else has either. Some observers might cite Solar Sunrise, the Department of Defense's name for a 1998 cyber intrusion that originally looked as if Iraq had penetrated US military networks (and which turned out to be an Israeli hacker working with two American teenagers). Solar Sunrise did indeed unfold amid a diplomatic crisis with Iraq, leading American observers to suspect Iraqi complicity, yet it also happened at a time when Defense Department defenses and cyber decision-making were still nascent. The diplomatic net result of Solar Sunrise was nothing. Calmer heads prevailed, and the United States did not strike Iraq over the misattributed intrusion. What Solar Sunrise proves about crisis instability and escalation is anyone's guess. Nevertheless, every year since 1998, cyber attacks have been misattributed, but so far such mistakes have not caused any wars. One wonders how many years it takes to notice a pattern here.

One note of caution while listing the parallels between intelligence activities and cyberspace operations is that the intelligence-cyber analogy helps to illuminate cyberspace operations but not cyberspace as a war-fighting domain. The analogy also seems stretched when one ranks the relative scales of intelligence activities and cyberspace operations; the former tend to be minute, and the latter look comparatively vast. Other analogies in this volume can help explain such aspects of cyberspace and the events that happen there. Let us then close with the observation that the hitherto tight parallelism between intelligence activities and cyberspace operations could well witness a divergence of potentially strategic consequence. One sees such signs in the lingering reputational damage to the United States and American firms caused by the media's revelations over the last few years. It is difficult to measure the effects, which are primarily commercial and consist of missed opportunities as much as actual expenses. Much anecdotal evidence points to forfeited sales for American products, and Washington has certainly (for the time being) lost control over the global narrative regarding Internet security and privacy. This development adds a new element rarely if ever seen in traditional espionage cases, and we would be wise to remain sensitive to how it unfolds.

## Conclusion

We hardly need an analogy to compare cyberspace operations with intelligence activities, as one exaggerates only a little to say they are mostly the same thing. A biologist might likewise say the same about dinosaurs and birds, for the latter

developed from the former with no evolutionary "seam" to distinguish the two types of animals (indeed, they are both members of the *dinosauria* clade). We also know from Sun Tzu that intelligence is concomitant with force; intelligence guides and sharpens force, making it more secret, subtle, and sometimes more effective. Further, force follows people and wealth; thus, wherever they are, aggressors will try to use force to control those people and to take the wealth.

Cyberspace operations can and do work along the same lines, for the same purposes, and for the same leaders. The steadily growing scale of intelligence activities expanded dramatically with the global diffusion of cyberspace, allowing formerly state-monopolized means and capabilities to be used by almost anyone with an Internet connection. That same diffusion of intelligence tools in cyberspace also made virtually everyone a potential collector of intelligence or a potential intelligence target. The lines between spying and attacking have always been blurry in intelligence activities as well as in cyberspace operations. Both are inherently fragile and provocative. While neither is necessarily dangerously destabilizing in international relations, we must learn to perform cyberspace operations as we learned to perform intelligence activities—that is, with professional skill, with strict compliance with the law, and with careful oversight and accountability.

## Notes

Michael Warner serves as the command historian for US Cyber Command. The opinions in this chapter are his own and do not necessarily reflect official positions of the command, the Department of Defense, or any US government entity.

1. The Joint Chiefs of Staff define *cyberspace operations* as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." Joints Chiefs of Staff, Joint Publication 3–12 (R), *Cyberspace Operations* (February 5, 2013), v, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

2. See Joint Chiefs of Staff, Joint Publication JP 1–02, *Department of Defense Dictionary of Military and Associated Terms* (November 8, 2010 [as amended through October 15, 2015], http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf), which defines *intelligence* as "the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations" (and the product of this activity and the organization performing it).

3. Michael Warner, "Intelligence as Risk Shifting," in *Intelligence Theory: Key Questions and Debates*, ed. Peter R. Gill, Stephen Marrin, and Mark Phythian (London: Routledge, 2008), 26–29.

4. J. C. Masterman broke this story in *The Double-Cross System in the War of 1939 to 1945* (New Haven, CT: Yale University Press, 1972).

5. *See* Josh Chin, "Malware Creeps into Apple Apps," *Wall Street Journal*, September 21, 2015.

6. For example, Citizen Lab at the University of Toronto's Munk School of Global Affairs has done yeoman service tracking spies in cyberspace for nearly a decade. See the nonprofit lab's assessment of FinFisher's surveillance software used in more than thirty states: Bill Marczak et al., "Pay No Attention to the Server behind the Proxy: Mapping

FinFisher's Continuing Proliferation" (October 15, 2015), https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/. Several of the larger antivirus and Internet security companies have fielded their own research arms to find and publicize state-based and criminal espionage.

7. A case in point is the FBI's takedown of the hacktivist group Lulz Security, or LulzSec, by turning one of its leaders in 2011. The hacker in question was Hector Xavier Monsegur, called "Sabu" by other members of LulzSec. The bureau had initially arrested Monsegur in 2011 and made mass arrests of LulzSec members on March 6, 2012. See Mark Mazzetti, "F.B.I. Informant Is Tied to Cyberattacks Abroad," *New York Times*, April 24, 2014.

8. See the FBI's unsealed affidavits here: "LulzSec Indictment Documents," *The Guardian*, March 6, 2012, http://www.theguardian.com/technology/interactive/2012/mar/06/lulzsec-indictment-documents-prosecution-complaints.

9. Saul O'Keeffe, "Hacking Underworld Riddled with Secret FBI Informants," ITProPortal, July 24, 2015, http://www.itproportal.com/2015/24/07/hacking-underworld-riddled-secret-FBI-informants/.

10. Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton: Princeton University Press, 2004), 28.

11. At Tannenberg an outnumbered German army defeated two Russian armies in detail after overhearing their plans broadcast en clair. The Russians apparently lacked compatible codebooks. The Royal Navy turned the tables on German ships and naval aircraft by geo-locating their transmissions and monitoring their stereotyped messages, which upon analysis revealed patterns that clearly indicated upcoming operations.

12. I treat this in more detail in "Notes on the Evolution of Computer Security Policy in the US Government, 1965–2003," *IEEE Annals of the History of Computing* 37, no. 2 (April–June 2015).

13. Gina Bari Kolata, "Computer Encryption and the National Security Agency Connection," *Science* 197 (July 29, 1977): 438.

14. US Senate, Select Committee on Intelligence, "Involvement of NSA in the Development of the Data Encryption Standard," 95th Cong., 2d sess., April 1978.

15. The San Bernardino, California, attack occurred in December 2015, when two individuals, Syed Rizwan Farook and Tashfeen Malik, killed fourteen civilians and injured twenty-two others in a shooting at the Inland Regional Center. The two assailants were killed in a gunfight with police. After police recovered Farook's cell phone, the FBI asked Apple to unlock the device, as the bureau believed that information related to the attack was on the phone. This request launched a nationwide debate regarding whether Apple should unlock the device. The dispute ended when the FBI purchased a vulnerability to access the device for more than $1 million. For more information, see Adam Nagourney, Ian Lovett, and Richard Pérez-Peña, "San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead," *New York Times*, December 2, 2015, http://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html; and "FBI Paid More than $1M for San Bernardino iPhone 'Hack,'" *CBS News*, April 21, 2016, http://www.cbsnews.com/news/fbi-paid-more-than-1-million-for-san-bernardino-iphone-hack-james-comey/.

16. Witness, for example, recent allegations over dual elliptic curve deterministic random bit generator, or Dual_EC_DRBG encryption, as well as FBI director James Comey's public warnings that his bureau is "going dark" because it cannot unlock the encryption in perpetrators' smartphones. The NSA insists it uses publicly available encryption suites for its own data. "NSA relies on the encryption and standards we advocate for and advocate for the encryption standards that we use," Anne Neuberger, then director of the agency's Commercial Solutions Center, told a radio audience in 2013. "[W]hat we

recommend for inclusion in those cryptographic standards, we use ourselves in protecting classified and unclassified national security systems." See "Threat Information Sharing Builds Better Cyber Standards, Expert Says," Federal News Radio Custom Media, October 3, 2013, 5:05 p.m., http://federalnewsradio.com/technology/2013/10/threat-information-sharing-builds-better-cyber-standards-expert-says/.

17. "Purdue's Gene Spafford was correct, but early, when he likened network security in the absence of host security to hiring an armored car to deliver gold bars from a person living in a cardboard box to someone sleeping on a park bench." See Daniel E. Geer Jr., "Cybersecurity and National Policy," *Harvard National Security Journal* 1 (April 7, 2010).

18. US Senate, Committee on Government Operations, "Staff Study of Computer Security in Federal Programs," 95th Cong., 1st sess., February 1977, 135–37, http://babel.hathitrust.org/cgi/pt?id=mdp.39015077942954;page=root;view=image;size=100;seq=3.

19. The NSA "will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B [encryption algorithms], we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer." See NSA, "Cryptography Today," January 15, 2009, https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm.

20. For more on this, see my recent article, "Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014," *Cyber Defense Review* (Army Cyber Institute), August 27, 2015, http://www.cyberdefensereview.org/2015/08/27/notes-on-military-doctrine-for-cyberspace/.

21. Jonathan Reed Winkler, *Nexus: Strategic Communications and American Security in World War I* (Cambridge, MA: Harvard University Press, 2008).

22. Warner, "Notes on the Evolution," 10–12.

23. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1971 [1963]), ch. 13. See also books 1, 2, and 13 of Kautilya's *The Arthashastra*, trans. L. N. Rangarajan (New Delhi: Penguin Books India, 1992).

24. Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington, DC: Cyber Conflict Studies Association, 2013), 265–72.