International Journal of Intelligence and CounterIntelligence, 0: 1–26, 2022

ISSN: 1521-0561 print/0885-0607 online
DOI: 10.1080/08850607.2022.2095544

JOHN A. GENTRY

Cyber Intelligence: Strategic Warning Is Possible

Abstract: Governments and private security firms have studied many intelligence aspects of cyberconflict, but the public literature has not described the existence of a strategic cyber warning function or addressed the question of whether strategic warning of significant cyberattacks is possible. This article argues that it is, but technical characteristics of cyberspace and the rapidly evolving nature of cyber-related conflict make cyber warning more difficult than traditional strategic warning. Addressing these complexities requires specialized teams of experts. In the U.S. case, new warning skills and institutions are needed.

Cyberspace is a complex new domain of communication and economic activity that also is an arena of espionage and many forms of interstate conflict, which has led to growing concerns about cybersecurity and thoughts about ways cyberspace is used for aggressive purposes.[1] The rapid growth of cyberspace and its dynamic evolution make understanding its current state, let alone its potential, challenging. By many accounts, companies and Western governments, including the U.S. government, have had difficulty adapting to the changing cyberthreat environment even when they

Dr. John A. Gentry is an Adjunct Professor with the Edmund A. Walsh School of Foreign Service, Georgetown University. He formerly was an Intelligence Analyst at the Central Intelligence Agency, where he was for two years Senior Analyst on the staff of the National Intelligence Officer for Warning. He is co-author of Strategic Warning Intelligence: History, Challenges, and Prospects. *The author can be contacted at jag411@georgetown.edu.*

understand aspects of it, indicating that intelligence is not serving policymakers well.[2] This generalization holds despite periodic public hints that the U.S. Intelligence Community (IC) provides some tactical warning intelligence[3] and the U.S. National Intelligence Strategy notes the importance of tracking and countering cyberthreat actors.[4] The IC was slow to appreciate politically oriented Russian information operations in the United States in 2015–2016, for example.[5] And successful ransomware attacks still occur frequently in the United States. While all major governments need strategic warning, this article focuses on the U.S. case because it is a major country about which a relatively large amount of cyber and warning information is publicly known. This article also adapts traditional U.S. strategic warning methods to cyber. Lessons herein can be adapted to some extent to other countries' situations. But, as with all other aspects of intelligence, no major "global" perspective useful for all countries is possible.

As governments struggled in recent years to define and address cybersecurity issues, firms stepped into the breach to meet immediate intelligence-related needs by monitoring ongoing attacks, offering defensive technical services to companies and governments on fee-generating bases, and attributing cyberactivities to specific perpetrators—often with considerable success. As Kris Oosthoek and Christian Doerr have written:

> In order to close this gap, the cybersecurity community established the field of Cyber Threat Intelligence (CTI). The primary objective of CTI is to realize a knowledge advantage over cyber threat actors. At the tactical and operational levels, CTI expedites early detection of malicious behavior, preferably before a malicious actor gains a foothold in the network. On a strategic level, CTI provides sense-making and insight into the relevant threat environment to decisionmakers. Effectively, CTI is the civilian, private-sector alternative to defensive counterintelligence executed by the established Intelligence Community (IC).[6]

This implicit mission statement does not, however, include strategic warning as it is usually defined. Neither monitoring an ongoing attack nor attribution of historical attacks are warning.

In this article, I define strategic warning in cyberspace traditionally as the alerting of senior national decisionmakers about the emergence of cyber-related threats of *major* national political, economic, or military importance. While other aspects of foreign government cyber operations—such as espionage and counterintelligence operations—are not as directly threatening, they are part of the array of cyber tools that states employ and help enable major attacks, meaning that strategic warning analysts must consider them as well. The boundary between threats of strategic and lesser importance as usual is blurred, but I consider a cyberattack that takes the entire U.S.

electricity grid offline for an extended period to be strategic in nature, while the May 2021 ransomware attack that temporarily shut the Colonial Pipeline Company and the July 2021 ransomware attack on Kaseya Limited, a software company, are of lesser importance.[7] If financial gain is the primary motive of an attack, it almost certainly is not strategic in nature. Like for other varieties of strategic warning, cyber warning messages must be clear, focused on relevant senior decisionmakers, and timely enough to enable effective deterrence, defense, or preparation for recovery from a major attack.

In the absence of dedicated strategic warning capacities, government agencies and private actors address warning aspects of cybersecurity in only slightly integrated ways. "Defenders" sometimes talk in ways that might be considered efforts to achieve tactical warning of impending cyberattacks, typically focusing on technical aspects of cyberactivities. While educating governments may help and cybersecurity firms identify some recurrent characteristics that might provide long-term indications of major national-level political and military threats, the firms do not seem to monitor integrated sets of the indicators consistently.[8] A clear recommendation in 2012 for establishment of a North Atlantic Treaty Organization (NATO) "early warning" capacity evidently had little effect.[9] The U.S. government does little strategic warning of any kind, and policymakers and intelligence officers rarely mention the term "strategic warning" or related concepts. "Anticipatory intelligence," a currently fashionable term in the IC, is *not* strategic warning. But because the offense in cyberconflict is generally seen as having major advantages over defense given the rapid development of offensive techniques and many vulnerabilities of potential victims of cyberattacks, identification of ways to anticipate important trends in the evolution of techniques, procedures, and goals of cyberattackers, and to detect plans for actual attacks, not contingency plans, is critical to achieving national-level cyber and other varieties of security.[10] Defensively oriented intelligence and security activities alone are likely to be only modestly effective.

The warning mission as defined above goes well beyond the IC's limited concept of cybersecurity, which makes good sense as far as it goes. For example, the National Counterintelligence and Security Center (NCSC), a component of the Office of the Director of National Intelligence (ODNI), defines its role concerning cyber in largely defensive and reactive terms that does not include strategic warning:

> The **cyber threat** is simultaneously a national & homeland security threat and a counterintelligence problem. State and non-state actors use digital technologies to achieve economic and military advantage, foment instability, increase control over content in cyberspace and achieve other strategic goals—often faster than our ability to understand the security implications and neutralize the threat.

> NCSC works with the U.S. Government cyber community and the IC, to provide the [counterintelligence] and security perspective on foreign intelligence and other threat actors' cyber capabilities and provides context and possible attribution of adversarial cyber activities.[11]

The ODNI has created an analytical "cyber threat framework," which may be useful for perceiving and discussing cyberthreats but also does not mention the warning function:

> The Cyber Threat Framework was developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. The Cyber Threat Framework is applicable to anyone who works cyber-related activities, its principle benefit being that it provides a common language for describing and communicating information about cyber threat activity. The framework and its associated lexicon provide a means for consistently describing cyber threat activity in a manner that enables efficient information sharing and cyber threat analysis, that is useful to both senior policy/decision makers and detail oriented cyber technicians alike.[12]

Yet despite the challenges and frequent failures, and the considerable attention devoted to tactical cyber issues, there have been some strategic cyber warning successes. For example, Estonia anticipated a major, politically motivated Russian cyberattack about two weeks before it occurred in 2007 by monitoring noncyber actions of protesters against the Estonian government's decision to move a monument to Soviet soldiers killed in World War II that long stood prominently in a square in Tallinn.[13] The monitoring of human activities enabled anticipation of a cyberthreat. But NATO headquarters did not get the word, generating surprise there. Political tensions between Georgia and Russia in 2008 were accompanied by low-level but increasing Russian cyberattacks before the main, primarily distributed denial-of-service attack that accompanied the kinetic war.[14]

This checkered history is not unique. The strategic warning function historically has, at best, a mixed record of success in detecting intended surprise conventional military attacks.[15] Difficulties long have included inadequate information, deception, failures of imagination, and a variety of cognitive biases, especially cognitive closure and confirmation bias. Cyber warning analysts face all of these and some unique technical factors, making the challenges still greater. This article therefore has a modest goal. Rather than propose a definitive warning method or methodology, it examines lesser questions: Is strategic warning of cyberattacks possible on a consistent basis even at a low level of success? If so, where might strategic warning professionals look for techniques that may improve abilities to identify impending threats? What new institutional mechanisms may be needed to address the more difficult challenges?

The article melds characteristics of cyberspace, institutional factors, and traditional strategic-level political and military motives for exploiting vulnerabilities in adversaries, thereby adapting to the cyber arena some of the concepts now in the strategic warning intelligence, foreign policy decisionmaking, psychological, and strategic studies literatures.[16] Although the ostensibly new cyber "domain"[17] of conflict is technically different from others in important respects—providing new venues for espionage, of attack, and for deception—the recurrent motives and frailties of national leaders and characteristics of adversary institutions remain key concerns of all varieties of strategic warning. Because states' conduct of strategically important intelligence and other operations in cyberspace is rapidly changing in both technical and operational terms and because key data are surely held in secure government spaces, I do not assert that the approaches suggested herein are complete, directly useful, or even novel. Rather, this article offers ideas that might be developed further by national intelligence services. Unbeknownst to me, some of these ideas may already be in use by the United States or other governments. I hope so.

The article first outlines some key approaches used by strategic warning professionals; this refresher for some readers is designed to show that traditional warning techniques are adaptable to cyberspace. Next, it identifies scenarios that recur in cyberconflict and suggests variables that might be indicators that can distinguish specific scenarios as situations evolve toward becoming actual attacks. The next section discusses how the rapid pace of change in technology and operational practices, affected by significant learning and adaptation by many actors, may affect the warning function. The article then discusses deception in cyberspace. Finally, the article suggests some institutional changes that could better integrate warning assets and develop more effective strategic cyber warning practices. I conclude that somewhat better strategic cyber warning is possible, but it will occur in the United States only if intelligence services make important institutional changes and collectively get much smarter.

STRATEGIC WARNING: A FOUNDATION

Despite the distinctive technical characteristics of cyberattacks, they often display traits similar to those of traditional objects of strategic warning, which often are called "warning problems." Attackers frequently generate surprise based on technological or doctrinal innovations with political, military, economic, and even social origins.[18] Hence, technical aspects of cyber operations may make surprise easier but do not pose insurmountable challenges for strategic warning.

Although warning problems can be characterized in many ways, one variety is both common and useful. The U.S. Department of Defense in recent years has described warning problems as either “emerging” or “enduring.”[19] The first characterizes new issues that develop, or “emerge,” with little precedent, requiring rapid development of expertise and a quick and accurate determination of the nature of the issue at hand. Robert Gates, when he headed the analysis directorate of the Central Intelligence Agency (CIA) in the 1980s, described these as “over-the-horizon” problems.[20] One of his analysts’ jobs, he told them, was to warn decisionmakers about developing events they did not yet know would one day concern them greatly, to figure out new ways to see “over the horizon.” Expertise alone can address this challenge by identifying, for example, new ways to exploit previously unknown cyber vulnerabilities, the cyber-related ambitions of world leaders, or emerging patterns in the ways intelligence services use cyber proxies to work for them to provide plausible deniability. This is hard work. Many more surprises surely will occur as technologies evolve and actors learn and adapt.

In contrast, “enduring” problems are known threat situations that can be studied in detail. While specifics of established warning problems have never been publicly released by any country, to my knowledge, an example might be the chronic worry since 1953 that North Korea might again attack the Republic of Korea.[21] For such problems, the U.S. IC in the 1950s developed an analytic method known as “indications and warning” (I&W), which has proved its worth over time. The I&W method depends on establishment of scenarios and indicators whose trigger by receipt of new information, perhaps generated by cyber collection including social media data, might prompt a warning message to key decisionmakers.[22] Despite its short history and rapid evolution, cyberconflict displays patterns that make a slightly modified “enduring” warning approach feasible.

The Basic I&W Method

The I&W method is relatively simple in concept, but not in practice, when used for conventional military threat situations, which is its primary application, although it also has been used for other types of warning situations.[23] The process of developing an indicator-based warning problem is roughly as follows. First, analysts identify an importantly bad situation that might develop or already exists but could get worse and needs to be monitored systematically. In U.S. and NATO warning terminology, the bad situation of concern is an “end-state,” which is defined in general terms that specify only the basic nature of the potential situation that intelligence wants to monitor. For example, the prospect that some Country A might invade Country B might be formally established as the “Country A Invades Country B Warning Problem.”

Typically, a warning problem is assigned to one intelligence analytic unit, which often is the component that proposed the warning problem. Thus, in the warning system of the U.S. Department of Defense—the Defense Warning Network—a designated warning problem is "owned," from the bureaucratic standpoint, by the intelligence element of the regional combatant command responsible for actual or potential U.S. military activity in that country or region.[24] In NATO, a member state may propose a problem of national interest and take responsibility for monitoring it. The organization (or country) that "owns" the warning problem studies the situation, develops the analytic approach to be taken, monitors the situation, and issues status reports or formal warning messages as appropriate. U.S. combatant commanders typically set the alert status of their forces based on threat levels their intelligence staffs identify.

The frequently global and often nonmilitary nature of cyberthreats makes this method of assignment of organizational responsibilities for U.S. governmentwide cyber warning unworkable, however. Warning problems of the U.S. Cyber Command (USCYBERCOM), created in 2010, would help with technical knowledge but have three other problems: (1) alerts would not have the same clout with regional combatant commanders as assessments by their own staffs; (2) it is not clear that USCYBERCOM has adequate nonmilitary skills; (3) partly for the second reason, USCYBERCOM's messages would little reach or have credibility with nondefense parts of the government and the private sector. It also does not seem to be focused on strategic warning. Strikingly, USCYBERCOM's commander, General Paul Nakasone, in a seven-page posture statement before the U.S. Senate's Armed Services Committee on 5 April 2022, used a form of the term "warning" only once.[25] A proposed alternative institutional arrangement is discussed at the end of this article.

Warning analysts identify several *possible* ways that Country A might attack Country B, known as scenarios, which are then developed more fully. The scenarios are, in essence, testable hypotheses about the course of future events. Initially, analysts might be relatively unconstrained in their imagination, later settling on scenarios that are more *plausible*. At the end of a (preferably) substantial analytic process during which warning analysts develop considerable expertise about both countries, but especially Country A's leadership, military forces and doctrine, economic and social situations, and relationship with Country B, the warning organization formally establishes several (usually three to five) scenarios, which amount to fairly detailed hypotheses about how the "end-state" of concern might develop. The number of scenarios chosen is a judgment call; too many scenarios lose distinctiveness and are unmanageable, too few limit possibilities to the detriment of analytical completeness.

Military intelligence organizations sometimes identify "worst-case" scenarios, believing that such scenarios help by challenging conventional wisdom and enabling decisionmakers to scope responses appropriate to the gravest threats. Warning analysts generally should not make such scenarios, however, because they inappropriately prejudge likelihoods before analyses are complete.[26] This general practice also biases future analyses and the messages that intelligence sends to decisionmakers. Other negative effects include: financially costly but unnecessary responses; excessive responses that appear threatening to other actors, thereby precipitating "security dilemma"[27] situations; and the "cry wolf syndrome"—the tendency of decisionmakers to disregard repeated warning messages that are not exactly prescient even if the warning was accurate at one time but the warned-about event was called off or postponed, which damages the credibility of the warning function.[28] Moreover, worst-case scenarios sometimes become self-fulfilling prophesies. Alternatives to "worst-case" scenarios are "High-Impact-Low-Probability" (HILP) scenarios that analysts judge to be unlikely but serious if they were to occur.[29]

In the cyber realm a similar logic applies. There may be several "worst" cases or HILP scenarios, but analysts should not assume a major cyber-enabled kinetic attack when an actor may only be conducting counterespionage operations or trying to steal money. Largely unique to cyberspace, aggressive responses may damage or eliminate the future usefulness of cyber capabilities by altering adversaries' or targets' awareness of them, prompting copying of tools or possibly easy amelioration of vulnerabilities. This fact makes for chronic tension between organizations focused on conducting cyber operations and intelligence agencies intent on protecting sources and methods—not normally an issue for traditional warning problems.[30]

For each scenario, analysts hypothesize a path that could lead to the "end-state" of concern. The path for some Scenario 1 about a military end-state might involve variables such as manpower mobilization, a surge of industrial production, embassy evacuations, or propaganda campaigns that may be linked sequentially or causally in processes whose distinctive major events are designated as "indicators" of Scenario 1. Identification of political intent or a doctrinal requirement to use cyber to disrupt adversaries' military command and control communications networks might be a useful indicator in this scenario. Other scenarios would have (mostly) different indicators, which are needed to distinguish the actualization of the various scenarios, which is key to understanding the exact nature of threats, which in turn facilitates effective, tailored response decisions. Indicators should be expected to occur in specific ways or sequences as scenarios unfold—perhaps in causal relationships to each other—but should not be functionally directly linked to most other indicators. Diplomatic indicators should not be closely associated functionally with economic indicators, for example. Analysts do the same for all scenarios they identify. The indicators for each scenario also should be distinct from those of other scenarios in order to identify as precisely as possible the nature of a potential threat.

Indicators can be of many sorts, including military, political, economic, social, and technological factors, which include but are not limited to cyber-related variables.[31] Cyber indicators, like others, should help identify intent to act in specific ways in the future, not provide historical attribution.[32] I&W analysts should normally use a variety of functional and geographical indicators for each scenario to help ensure the independence of indicators and to enable various types of collection assets to provide relevant information about the status of indicators. There should be enough distinct scenarios to cover the plausible range of possibilities for realization of the "end-state." Historically, a major cause of warning failure has been an inability to identify all relevant scenarios. For example, Israeli intelligence identified two ways Egypt could attack Israel in 1973 but did not anticipate the way Egypt actually initiated the Yom Kippur War—a classic warning failure.[33] A lack of imagination about possible attack means, amplified by secrecy and deception, also seems to have been common in the early years of rapidly evolving cyberconflict. The broader range of possible cyberattacks than of conventional military attacks makes imagination and broad expertise in warning analysis even more important, and may make it necessary to build more scenarios per cyber warning problem than for others.

The intelligence analytic organization then tasks collection assets to gather information that enables timely recognition of events related to the actualization of each scenario. When events associated with an *indicator* change, analysts have an *indication* of possible movement toward (or away from) the "end-state," perhaps triggering a warning message.

Indicators should be predictive, diagnostic, unambiguous, and collectable. Indicators are *predictive* if they consistently, causally precede the "end-state" of warning concern.[34] They are *diagnostic* if their occurrence distinguishes the emergence of one scenario as more likely than other scenarios. Indicators are *unambiguous* if there is little possibility that experienced analysts will misinterpret received information. They are *collectable* if available collection assets can get information about the movement of indicators toward or away from a designated "end-state" on a consistent, timely basis.[35] Infrequent reporting renders even logically great indicators poor choices; there is no point in identifying reports from key regime insiders as an indicator if an intelligence service has no informants who can report such information or has contact with them sporadically. Israel long had good sources in Arab governments and reasonably therefore included such information in its indicator lists in 1973, but other states do not.[36] Hence, collection capabilities influence the selection of indicators, making analyst understanding of collection capabilities essential. This latter issue is a major challenge for traditional warning and may be even more important for cyber warning.

In cyberspace, collection assets include the monitoring of other parties' intrusions into one's own important networks, which are ones adversaries are most likely to target and that need strong defenses. Because of their sensitivity, states presumably monitor such networks by themselves or with very close allies. This is a variety of counterintelligence, defined by CIA counterintelligence specialist John Ehrman as "the study of the organization and behavior of the intelligence services of foreign states and entities, and the application of the resulting knowledge."[37] Hence, a strategic cyber warning unit must be part of a foreign-focused intelligence service, as opposed to a police or homeland security organization, even though historical events may sometimes be accurately assessed using public data.[38]

With good indicators chosen and collection assets in place, analysts monitor events for signs of change that might indicate an impending crisis, a relaxation of tensions, or a resolution of a problem that may suggest terminating the active monitoring of a warning problem. Good warning analysts typically recognize that their indicators are not equally important, and they identify "critical indicators" for special collection and analytical emphasis. They also know that indicators may change at different times and in different ways even if scenarios unfold roughly as they anticipate. Analysts weigh important indicators more highly than others in making decisions about whether to change warning status levels. Because warning problems vary significantly, no consistent quantities or qualities of indicators are necessary or sufficient to issue warning messages. Good judgment always is required. Appreciable movement of important indicators from one status level to another—in both directions and however defined—are reasons to issue warning messages. Focusing decisionmakers' attention on still emerging events of potential importance can help them take preliminary or incremental actions that deter observant prospective attackers who prefer to exploit undefended assets. In this latter respect, cyber and counterterrorism-related warning may be more similar than are cyber and conventional military warning problems.[39] Good analysts generally resist calls to create color-coded "stoplight charts" to indicate the status of a warning problem because the charts inherently are simplistic even though many intelligence consumers like them because they are visually appealing.[40]

Time Horizons

Strategic warning is designed to provide national decisionmakers with relatively long lead-time alerts about the development of issues of national importance that might require national-level responses. There has long been discussion about what constitutes adequate strategic warning measured in chronological time.[41] Temporal adequacy is determined by several factors, including: the nature and speed of evolving events; decisionmakers' receptivity and decisionmaking processes; and reaction times. Sometimes "adequate" times are substantial, although Israel before peace with Egypt was said to need only 72 hours of strategic warning in order to mobilize its reservists. Time horizons for strategic warning in recent years in the United States have been variously described as six months to two years.[42] Although some varieties of cyberattack, once launched, occur very rapidly, the histories of many attacks indicate that preparation times for major, sophisticated attacks often are measured in months or years, and some attacks are phased over months or years with victims sometimes not knowing they have been attacked for long periods of time.[43] For example, the embarrassing, evidently espionage-oriented attacks on the U.S. Office of Personnel Management in 2014 and 2015, apparently by China, occurred in three waves over a period of nearly a year before they were discovered.[44] This case is similar to other attacks in another respect: the cyber literature universally indicates that attribution of attacks by cybersecurity firms and governments to specific perpetrators often lags the discovery of cyberattacks by weeks or months. Hence, despite the weak performance of cyber warning to date, there frequently is plenty of time for effective strategic warning if intelligence services look in the right places and collect and analyze well.

SCENARIO DEVELOPMENT AND INDICATOR LISTS

The growing literature on cyberconflict—which evidently includes much of what cybersecurity firms know and smaller parts of what national intelligence services know and do—suggests that major governments now understand enough about the details of many cyberattacks to be able to identify recurring general patterns that can be developed into detailed scenarios of the enduring warning problem variety, at least for major actors who frequently employ cyber tools.[45] Details in the public domain are provided by cybersecurity firms such as CrowdStrike, which worked cases such as the Russian hack of the U.S. Democratic Party's computers in 2016, and the North Korean attack on the Sony film studio in 2014. Some events recur often enough in these accounts to constitute general indicators of some scenarios, subject to greater specification in new situations of interest. Hence, the process of identification of discriminating scenarios and key indicators of cyber warning problems is well underway. David Sanger, for example, suggested that cyberattacks come in five varieties—vandalism, burglary, thuggery, espionage, and sabotage—with the last two being the most worrisome.[46] Amy Zegart proposed five similar varieties but used different descriptors: stealing, spying, disrupting, destroying, and deceiving.[47] Ben Buchanan identified eight general steps in a hack, which also may provide hints helpful for identifying distinctive indicators.[48] M.A. Thomas proposed a "Cyber Effects model" that distinguishes cyberattacks according to the purposes intended by attackers.[49] Thomas' perspective was anticipated by Jason Healey and Leendert van Bochovan, who observed that it is important to delineate the importance of an attack and specified four axes of importance: purpose, target, context, and scale, which vary only slightly from traditional military measures of the severity of an armed attack.[50]

A frequently noted feature of the cyber realm is that preparations for various forms of attacks, which scenarios are designed to resemble, often have many technical traits in common. Indeed, it has been argued that the first 90% of a penetration of an adversary network can be used for many purposes, with the delivery of an attack payload occurring in the last 10% of the operation.[51] This "cyber kill chain" process can be anticipated and potentially disrupted, if intelligence is alert, perceptive, and understands useful reaction methods and effective timing.[52] This core characteristic of cyberspace may significantly inhibit the usefulness of some potential indicators, however, by making them less *diagnostic* and more *ambiguous* than is desirable in indicators, meaning the specification of technical indicators sufficiently precise to alone be adequate for warning analysis may be problematic.

Because of this difficulty, the process of deriving scenarios and indicator lists might usefully borrow from conventional warning problems by focusing more on variables associated with cyber operations that are not electronic in nature, including political, institutional, military, or other factors. Such nontechnical indicators helped produce Latvia's warning success in 2007.

Despite these challenges, and putting cyber history into warning terminology, at least six general scenarios recur that clearly are of ongoing strategic concern to states:

1. Cyber intrusions collect intelligence—espionage. This may be hard to distinguish from item 2 and is often a prelude to items 3 and 4. Major states evidently do a lot of this.
2. Cyber intrusions are functionally defensive in nature—they are aggressive (or "offensive") counterintelligence. This practice also appears to be fairly common.
3. Intelligence collection is a prelude to a possible military attack. This pattern has a long history in military intelligence during "peacetime." A Swedish official said in 2015 that he believed Russian intelligence collection activities against Swedish networks were preparations for military attacks on Sweden.[53]
4. Intrusions prepare for and then conduct attacks that physically damage infrastructure in target countries without an overt military attack. Examples include Stuxnet, the effort to damage Iranian nuclear centrifuges.[54] Iran's

attack on the Saudi Aramco oil company in 2012 caused a large amount of costly damage.[55]

5. Physically damaging infrastructure attacks accompany kinetic military actions, comprising another domain of armed conflict. The first case of this kind was Russia's short conflict against Georgia in 2008.[56] Many reports indicate that Russia used cyber before and during its major war against Ukraine in 2022. In these cases, traditional military mobilization and other processes occur, potentially providing conventional means of warning of cyberattacks that have supporting roles.
6. Cyber operations are designed to influence target countries politically, with or without other forms of information operations. These are at least two kinds: (1) covert influence operations, which are designed to destabilize targets politically[57] and (2) fairly obvious actions usually designed to intimidate specific targets and, by extension, others. Examples of the first sort include Russian interference with U.S. and French national elections in 2016 and 2017, respectively.[58] Examples of the second variety include: North Korea's attack on Sony in 2014, which was a warning to foreigners against disrespecting North Korea's leaders[59]; damaging Russian attacks on Ukraine over several years after 2014, including attacks on Ukraine's electrical infrastructure, which evidently were designed to both pressure Ukraine and deter third parties from dealing with Ukraine[60]; and retribution attacks on politically salient institutions such as the World Anti-Doping Agency, which banned Russian athletes from international competitions.[61]
7. Others, including variants of criminality. North Korea, for example, steals money from foreign banks to help meet its financial needs. These generally are not strategically important as individual acts, but it is important to identify when theft is a motive, if only to rule out other, more strategically significant scenarios.

Items 3, 4, and 5 qualify as strategic threats as traditionally defined, while political attacks are of growing strategic salience in many countries after Russian electronic interference in recent elections, which was consistent with the goals of the "active measures" campaigns of the Soviet Union. In early 2022, Sweden launched a Psychological Defence Agency,[62] which is designed to identify and help defend against information-based attacks. A similarly motivated but badly designed U.S. Disinformation Governance Board collapsed ignominiously in May 2022, soon after it was launched, largely due to congressional skepticism about its own objectivity.[63] Strategic warning of this sort has a new and different core audience—general citizenries of countries. Actions of all these types should be the primary focus of cyber warning analysts. Presumably the evolution of cyberattacks will produce other patterns in the future. If so, these need to be identified, evaluated, monitored, and responded effectively to, as appropriate.

Possible Indicators

Because penetrations of networks and surveillance of files therein often are consistent with several types of cyberattacks, and because final decisions to take specific actions may occur late in the preparation for an operation or after all preparations have been completed, identification of technical indicators that can provide indications of a unique scenario is likely to be difficult. Stated differently, cyber penetrations give actors numerous options of widely varying strategic importance, hindering early determination of the operation that might actually occur. Evaluation of institutional factors that shape the procedures and practices of many cyber operations could lead to development of reliable, longer-term indicators, as Ned Moran suggested in 2010.[64]

State-run cyber operations, as opposed to the cyberpranks of teenagers or solely criminal acts, are organized activities of groups of people. Because they reflect the characteristics of leaders, organizational structures and cultures, and standard operating procedures also used in the physical world, bureaucratic processes may provide hints about the identity of cyberactors (the much focused-on "attribution" problem) and clues about planned future cyber operations.[65] For example, some hackers as both solo actors and leaders of organizations cultivate distinctive online persona, and they often communicate in personally identifiable ways.[66] Government cyber organizations often act like other government bureaucracies in that they develop routine practices and procedures that are observable. Students of hacking have noted that some attacks coincide with standard daytime work hours in Shanghai and St. Petersburg, which are homes of prominent Chinese and Russian hacker groups, respectively. Sanger observed that North Korea used very similar technical and procedural means to attack the Sony film studio in the United States, several South Korean targets, and Channel 4 television in the United Kingdom over a period of several years in the 2010s.[67] Buchanan noted that cyber operations develop institutional "momentum," suggesting that identification of types of momentum and their implications for intentions and/or timing of attacks may be useful.[68] Such patterns can be easily modified as a deception technique—and need to be monitored as such.

Cyber operations often are connected to entities that have narrowly defined responsibilities, limiting their operational cyber possibilities for bureaucratic or political reasons. For example, the Chinese People's Liberation Army's (PLA's) cyber operation, as a large entity operating within bigger Chinese communist party and government structures, has intragovernmental connections that commercial cybersecurity firms have traced. In addition, some states, including Russia and China, use energized volunteers as "patriotic hackers."[69] In 2014, China was said to have over 200,000 members of its cyber "militia."[70] To the extent that states control or less directly encourage groups of volunteers or opinion leaders to act in state-desired ways, their activities and communications may contain hints about future state-perpetrated cyber operations and may be relatively easy to monitor.

States have formal or de facto doctrines that may be analytically helpful, including political and economic policies, practices, plans, and strategies. Major cyber states—including Russia, China, North Korea, and Iran—have made clear in the past that they have goals that instruments of national power, including cyber assets, will support. These four countries conducted 77% of all identified cyber operations from 2005 to March 2022, according to the Council on Foreign Relations' "Cyber Operations Tracker" website.[71] All are hostile to Western interests, making them priorities for study. For example, North Korea protects the image and reputation of the Kim dynasty as a high priority. Ben Buchanan argued that the pattern of North Korean attacks on the United States and South Korea, as well as its financially motivated attacks, seem to be part of a larger strategic plan.[72] Russian President Vladimir Putin by many accounts focuses substantially on Russia's reputational status in the world and a perceived need to restore Russia's standing as a great power—a fixation demonstrated graphically again by his invasion of Ukraine in 2022.[73] The oft-referenced "Gerasimov doctrine," named for Russia's chief of general staff General Valery Gerasimov, prominently includes information operations, broadly defined to include cyber, in Russia's package of political–military "hybrid warfare" tools.[74] Buchanan argued that the Chinese PLA's Unit 61398 focuses its intelligence collection on industrial sectoral priorities in China's five-year economic plan.[75] Given the importance of China's "four modernizations" campaign to communist party leaders, this document may offer useful hints about where to look for new PLA cyber operations.[76] Other countries have different cyber-related civilian and military doctrines. Such information also seems likely to be fairly easy to collect. Hence, it should be possible to identify goals of potential adversaries that cyber operations can usefully help enable, which should aid in refining indicators related to the use of cyber operations to support achievement of these goals. Sophisticated political and/or economic expertise is needed for such work.

Jason Healey identified ten characteristics that sequentially indicate growing state involvement in cyberattacks—as opposed to individual or criminal actions. While his intent was to identify ways of generating accurate attribution for attacks, the characteristics could also be useful for warning.[77] It may be that states allocate nuisance or criminal attacks mainly to proxies while doing important projects themselves. Or there may be other patterns.[78]

"Zero days," or the identification of previously unknown, exploitable vulnerabilities in a potential target, are key assets in cyberspace.[79] Sometimes actors learn of adversaries' inventory of "zero days," perhaps providing hints about future uses of valuable assets. Analysts can ponder the capabilities these assets convey or suggest, given likely targets' vulnerabilities, and correspondingly identify uses that are possible or expected from each such asset based on the anticipated objectives of potential attackers. Here again, an ability to assess such issues implies a need for expertise on political, military, and/or economic characteristics of potential aggressors, as well as their technical abilities and target vulnerabilities. Because they are valuable but can erode as technologies change and knowledge of the changes spreads, keeping zero days in inventory may suggest an important anticipated future use.

Especially if cyber operations complement military activities, there will be vertical command and control relationships with senior leaders and horizontal communications between functional units. These may be vulnerable to monitoring.

Aggressors are most likely to attack individuals and institutions against whom they think they can be successful, meaning monitoring actors' assessments of potential adversaries' technical abilities, psychological makeup, institutional vulnerabilities, and victims' likely responses makes good sense. This has been an issue for years in conventional and irregular political/military conflicts.[80] It seemingly is now in cyberspace as well. For example, President Barack Obama is widely seen as having been reluctant to act against attackers, prompting widespread belief that on his watch cyberattacks on American interests posed little risk of meaningful U.S. retaliation.[81] They thus were inexpensive by many definitions, effectively encouraging more attacks. The situation does not seem to have improved much since. Indeed, General Nakasone, commander of USCYBERCOM and director of the National Security Agency (NSA), said in 2018 that U.S. adversaries "do not fear us" in cyberspace.[82]

One of the points made repeatedly by observers of cyberconflict is the apparent attempt by perpetrators to keep the conflict "below" the level at which aggression would be considered an act of war that requires a military response. A key intelligence question therefore is: What are prospective attackers' and victims' perceptions of that threshold? The answer may put a cap on the magnitude of activities actors' are willing to conduct, or tolerate, in the absence of conditions of general warfare, thereby influencing selections of some scenarios and indicators.

RAPID CHANGE AFFECTS THESE PROCESSES

The speed of cyber-related technological change, rapid learning through chronic interactions between hackers and defenders, and similarity of antecedent actions for a range of types of cyberattacks mean that developing strategically important warning indicators is likely to be harder than for traditional warning of military attacks. This difficulty puts a premium on understanding factors that motivate cyberattacks, perhaps including strategic cultures of national states, basic national geopolitical orientations, leaders' psychological and political propensities, and undoubtedly others. Such understanding might enable appreciation of the range of cyberactivities consistent with differing national goals, enabling better warning. But acquisition of such knowledge is not a sure thing, and it almost certainly will require deeper understanding of political, economic, military, and social factors in key states—and their evolutionary trends—than has traditionally been the case in even dedicated U.S. warning analysts, who have mainly been line analysts on rotational assignments to warning offices, making them warning amateurs for much or all of their tours. What is certain is that conventional analytical approaches such as use of structured analytic techniques and the current U.S. reliance on line analysts who primarily work on other issues cannot cope with the challenges of cyber warning.[83]

Rapid change makes frequent reassessment of indicators, scenarios, and even entire warning problems essential. One of the historical dangers of enduring warning problems is that their monitoring becomes routine and they are not reassessed often enough, meaning what once were sound judgments become unchallenged assumptions that are wrong. Perhaps the most prominent example is Israel's reliance on its "Concept" of Egyptian war plans that is widely seen as the primary cause of its failure to anticipate the Yom Kippur War of October 1973. In fact, the "Concept" was Egypt's actual war plan until President Sadat changed it in late 1972.[84] Israeli military intelligence did not accept and internalize accurate new reporting on Egypt's war plans, leading to a strategically important warning failure less than a year later.

DECEPTION IN CYBER OPERATIONS

The points above imply that some aspects of what traditionally has been called denial and deception (D&D) activities that accompany surprise attacks will be easier to achieve in cyberspace than in the tangible world. Deception clearly is a key part of some cyberattacks. For example, Russia's NotPetya attack on Ukraine in 2017 had an appreciable deception element; while apparently designed to damage Ukrainian infrastructure, it was made to look like a ransomware attack.[85] Understanding and to some extent modifying the insights of deception specialists to both offensive and defensive aspects of cyber operations may be especially useful for cyber warning. Barton Whaley was particularly insightful, in my view, and his writings are worth special study.[86] Other useful sources include works by Donald C. Daniel and Katherine L. Herbig[87] and by Cynthia Grabo.[88]

Learning lessons from the history and practice of deception is essential.[89] Whaley, like other warning and deception specialists, observed that "stratagem," which he defined as the study and practice of deception and surprise in war, could be learned but not taught.[90] Whaley described the "best" stratagem as one that

> generates a set of warning signals susceptible to alternative, or better yet, optional interpretations, where the intended solution is implausible in terms of the victim's prior experience and knowledge while the false solution (or solutions) is plausible. If the victim does not suspect the possibility that deception may be operating he will be guiled.[91]

Robert Gates similarly observed that the best way to ensure surprise is to do something that appears to others to be self-destructive.[92] A historical example is the U.S. amphibious landing at Inchon in 1950, well behind North Korean lines, which evidently was successful largely because the North Koreans believed such an operation was too risky for the Americans to seriously consider. Because imagination, creativity, determination, and perhaps a bit of deviousness are desirable in warning personnel, career warning specialists like the well-respected Cynthia Grabo are needed. They should be carefully chosen. Not every good intelligence analyst is also a good warning analyst, especially when doing warning on a part-time basis. Putting the point differently, Richard K. Betts once observed that while "normal theory" often usefully informs intelligence analysts, "exceptional thinking" may be needed to identify adversaries' unusual situations, especially ones designed to be deceptive.[93] There is no formula for identifying these unusual situations; experience and aptitude are clearly critical, however.

Whaley suggested that a good defense involves not trying only to identify deception, or purposefully false signals, but rather finding signals that indicate the true intent of an attacker.[94] He noted that one of the best ways to achieve surprise is to generate false starts, which lead to "cry wolf syndrome" situations that damage the credibility of warning in the view of opposing decisionmakers. Another good way to produce deception is to build many options into one's plan, a task made easier by the inherent characteristics of cyber operations.[95] It is deception, Whaley averred, not security, which history demonstrates is the best guarantee of successful surprise attacks.[96]

This pattern in cyberspace is even more complicated. While potential attackers often develop multiple options by surveilling target networks, they know that their actions may be noticed by defenders and therefore may add technical features to their surveillance that further hide their intent or suggest options they do not intend to use. Conversely, "defenders" employing counterintelligence per John Ehrman's concept may learn enough about an intruder's actions and apparent motives to add or delete files or structures or take other actions subject to adversary surveillance that are designed to mislead the surveillants.[97] Given the timeframes involved, there may be long periods of dynamic interaction between intruders and defenders that feature elements of mutual deception. Cyberwarfare practitioners and cyber warning analysts both need to know this logic and history—and be able to translate evolving best practices to new situations quickly and effectively in order to improve warning, not perfect it. These characteristics mean that, contrary to the view of Healey and van Bochovan, strategic cyber warning is not easy.[98]

NEEDED INSTITUTIONAL CHANGES

This analysis suggests a need for highly skilled warning personnel and a dedicated cyber warning organization, which should combine characteristics of at least three historical American intelligence institutions and, importantly, additional abilities the IC has never had.[99] First, the IC needs to restore the position of the national intelligence officer for warning (NIO/W) function (1979–2011), which combined in a small office several important capabilities: (1) a senior officer charged with being the final warning authority in the IC and warning's interface with senior national-level decisionmakers; (2) a small staff of analysts who worked with line analytic units to draw warning-related insights from them, who addressed warning issues not covered by others, and who learned warning history and practiced established warning techniques; and (3) a responsibility to develop new warning methods as needs changed and alternative analytic approaches appeared to be useful. These characteristics required specialized expertise. But Director of National Intelligence James Clapper unwisely abolished the position of NIO/W in 2011, assigning warning duties broadly to all analysts, the national intelligence managers, and other national intelligence officers. These people have plenty of other things to do, which means, by many accounts, that warning gets short shrift. This dispersion of responsibility also means that no one is in charge of the warning function broadly; individual warning messages are slowed, watered down, and unfocused; and the development of warning techniques is virtually impossible.

Second, because denial, in the form of cyber defenses, and deception are such important parts of cyberconflict, an element dedicated to understanding evolving trends in cyber-related D&D, including the favorite tricks of specific foreign actors and their blind spots, is needed. An organization devoted to D&D was established within the National Intelligence Council in the 1980s but recently has languished.[100] It needs reinvigoration and a more prominent cyber focus.

Third, because many cyber operations evidently involve espionage or counterespionage, or both, a significant counterintelligence component is needed. Following the recommendation of counterintelligence specialist Ehrman, this element should be primarily an analytic unit devoted to the study of the characteristics of foreign cyber institutions, broadly defined, and development of recommendations for operations to exploit that knowledge.[101]

Fourth, while training can help warning analysts, a better approach is to more carefully select cyber warning analysts, looking for innate abilities of the sort Grabo and Whaley noted in analysts who are genuine experts in primary countries of interest, including likely targets of potential attackers. This latter skill is a traditional weakness of American analysts, who have excessively worried about being accused of "spying" on their own government. A dedicated career warning track would also be helpful—if leaders can figure ways to reward excellent warning analysts even though they produce few current intelligence publications.

These capabilities should work together in team efforts, but this combination does not rest logically within any IC agency or the office of the current national intelligence officer for cyber issues. Placement in the CIA or the Federal Bureau of Investigation or the NSA all have some advantages but major drawbacks, most obviously including bureaucratic objections by agencies that do not possess the center. Therefore, I suggest placement of such a unit within the ODNI—either as a new organization or within a significantly restructured NCSC. In either case, it should have senior leadership and enough multiagency participation to have immediate access to, and credibility with, all IC agencies, USCYBERCOM, the Office of the Secretary of Defense, the Department of Homeland Security, the White House, and the general public. Maintaining credibility with the citizenry may be a special challenge given the rocky, short life of the Disinformation Governance Board and the legacy of the IC's politicization of intelligence against President Trump in recent years.[102] The office should have a budget to sponsor research on relevant technologies and warning techniques. The office also should interact as feasible with liaison partners, starting with the Five Eyes intelligence alliance. Such new skills presumably will help identify emerging as well as enduring warning issues sooner and more accurately. If these abilities are achieved, it would resemble the Watch Committee and National Indications Center of the 1950s—an excellent warning organization of a very different era.[103]

CONCLUSION

While cyberconflict differs from traditional military operations in some technical ways, basic motives and many associated kinetic forms of conflict are similar. Timeframes of strategic importance still are appreciable in many cases, and scenarios and indicators can be identified. Hence, strategic warning appears to remain viable, although in practice it seems likely to be harder than before, when success rates were modest. This challenge can be met to some extent by a renewed focus on the study of warning as an analytic discipline, on D&D as a specialized discipline, on cyber-focused counterintelligence, and on research on cyberactors and scenarios of special importance. This means one or more new institutions is needed in the IC, and may also be needed in other states' intelligence services. By doing such work, the "batting average" of strategic cyber warning can be increased.[104] But given the strong aversion to the warning function that the U.S. IC has shown for over a decade and the slow progress the U.S. government as a whole has made in addressing cyberthreats, the most difficult challenge may be making a decision to do things differently.

REFERENCES

[1] For an early, rare discussion of strategic warning regarding information operations, see Lou Anne deMattei, "Developing a Strategic Warning Capability for Information Defense," *Defense Intelligence Journal*, Vol. 7, No. 2 (1998), pp. 81–121.

[2] John P. Carlin, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (New York: PublicAffairs, 2018); Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (New York: Oxford University Press, 2016), pp. 159–160; David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), pp. 145–146, 181, 191–192, 235, 237–238.

[3] For example, Sommer Brokaw, "FBI Disrupts Russian State-Controlled Network of Hacked Computers," UPI News, 7 April 2022, https://www.msn.com/en-us/news/other/fbi-disrupts-russian-state-controlled-network-of-hacked-computers/ar-AAVYS1i?ocid=msedgntp&cvid=dee7551befd04273806ae268f28c89b6

[4] U.S. National Intelligence Strategy (2019), p. 13, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

[5] David V. Gioe, "Cyber Operations and Useful Fools: The Approach of Russian Hybrid Intelligence," *Intelligence and National Security*, Vol. 33, No. 7 (2019), pp. 954–973.

[6] Kris Oosthoek and Christian Doerr, "Cyber Threat Intelligence: A Product without a Process?" *International Journal of Intelligence and CounterIntelligence*, Vol. 34, No. 2 (2021), pp. 300–315.

[7] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, "The Colonial Pipeline Cyber Incident," https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[8] For example, Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, DC: Georgetown University Press, 2020), pp. 149–154.

[9] Jason Healey and Leendert van Bochovan, "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO," Atlantic Council (2012), https://www.files.ethz.ch/isn/155419/NATO%20Cyber%20Warning%202012.pdf

[10] Amy B. Zegart, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton, NJ: Princeton University Press), p. 259; Buchanan, *The Cybersecurity Dilemma*.

[11] NCSC website, https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-cyber-security (accessed 6 April 2022).

[12] ODNI website, https://www.dni.gov/index.php/cyber-threat-framework (accessed 6 April 2022).

[13] Jason Healey, "A Brief History of US Cyber Conflict," in *A Fierce Domain: Conflict in Cyberspace, 1986–2012*, edited by Jason Healey (Washington, DC: CCSA, 2013), p. 70.

[14] *Ibid*., p. 71.

[15] John A. Gentry and Joseph S. Gordon, *Strategic Warning Intelligence: History, Challenges, and Prospects* (Washington, DC: Georgetown University Press, 2019).

[16] For example, Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (Athens: University of Georgia Press, 2018), pp. 125–156.

[17] Some military people think of military operational "domains" in geographic terms, as land, air, sea, and space.

[18] Richard K. Betts, "Surprise Despite Warning: Why Sudden Attack Succeeds," *Political Science Quarterly,* Vol. 95, No. 4 (1980–1981), pp. 551–572.

[19] John A. Gentry and Joseph S. Gordon, "U.S. Strategic Warning Intelligence: Situation and Prospects," *International Journal of Intelligence and CounterIntelligence,* Vol. 31, No. 1 (2018), pp. 31–32.

[20] Personal experience.

[21] For a description of a warning exercise, see Diane M. Ramsey and Mark S. Boerner, "A Study in Indications Methodology," *Studies in Intelligence,* Vol. 7, No. 3 (1963), pp. 75–94.

[22] Gregory F. Treverton, "An American View: Hybrid Threats and Intelligence," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, edited by Mikael Weissmann et al. (London: I.B. Tauris, 2021), p. 40.

[23] The discussion in this section draws heavily from Gentry and Gordon, *Strategic Warning Intelligence*, Chapter 6.

[24] The U.S. Defense Department divides the world into segments that are the responsibility of specific regional military commands, which have primary Department of Defense responsibility for any military action the United States is taking, or may take. Hence, commands' intelligence directorates closely follow events in their areas of responsibility. The U.S. government evidently does not yet have similar organizational coherence in the cyberdomain.

[25] General Paul M. Nakasone, Posture Statement, 5 April 2022, https://www.armed-services.senate.gov/imo/media/doc/5%20Apr%20SASC%20CYBERCOM%20Posture%20Statement%20(GEN%20Nakasone)%20-%20FINAL.pdf

[26] For good critiques of "worst case" scenarios, see Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics,* Vol. 31, No. 1 (1978), pp. 65–66, 74–75, 88; Michael I. Handel, "Intelligence and the Problem of Strategic Surprise," *Journal of Strategic Studies*, Vol. 7, No. 3 (1984), pp. 247–248; Michael Herman, "Intelligence and the Assessment of Military Capabilities: Reasonable Sufficiency or the Worst Case?," *Intelligence and National Security*, Vol. 4, No. 4 (1989), pp. 773–782.

[27] In a “security dilemma,” one state’s efforts to improve security by increasing its armaments precipitates a countering response by another, leading to an arms race that does not improve either state’s security. See Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics,* Vol. 30, No. 2 (1978), pp. 167–214.

[28] Barton Whaley, *Strategem: Deception and Surprise in War* (Boston: Artech House, 2007), p. 99.

[29] Jack Davis, “Strategic Warning: Intelligence Support in a World of Uncertainty and Surprise,” in *Handbook of Intelligence Studies*, edited by Loch K. Johnson (London: Routledge, 2007), p. 181.

[30] Jon R. Lindsay, “Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem,” *Intelligence and National Security*, Vol. 36, No. 2 (2021), pp. 260–278.

[31] Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Lanham, MD: University Press of America, 2004), pp. 51–76.

[32] Florian J. Egloff and Max Smeets, “Publicly Attributing Cyber Attacks: A Framework,” *Journal of Strategic Studies* (forthcoming).

[33] Israeli military intelligence identified two scenarios—a large-scale effort to conquer the Sinai or pinprick border attacks—neither of which were worrisome. Egyptian President Anwar Sadat chose another approach—a limited war associated with political goals.

[34] Academic analysts see requirements for indicators similarly. For example, see Handel, “Intelligence and the Problem of Strategic Surprise,” pp. 229–281; Gregory F. Treverton, *Intelligence for an Age of Terror* (New York: Cambridge University Press, 2009), pp. 42–45.

[35] Australian Defence Warning System brochure.

[36] Uri Bar-Joseph, “A Question of Loyalty: Ashraf Marwan and Israel’s Intelligence Fiasco in the Yom Kippur War,” *Intelligence and National Security*, Vol. 30, No. 5 (2015), pp. 667–685.

[37] John Ehrman, “What are We Talking about When We Talk about Counterintelligence?” *Studies in Intelligence*, Vol. 53, No. 2 (Extracts) (2009), p. 6. See also Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), pp. 112–117.

[38] Treverton, “An American View,” p. 40.

[39] John P. Sullivan and James J. Wirtz, “Terrorism Early Warning and Counterterrorism Intelligence,” *International Journal of Intelligence and CounterIntelligence*, Vol. 21, No. 1 (2008), pp. 13–25.

[40] Healey and van Bochovan, “Strategic Cyber Early Warning,” p. 6.

[41] Cynthia M. Grabo, “Strategic Warning: The Problem of Timing,” *Studies in Intelligence,* Vol. 16, No. 2 (1972), pp. 79–92.

[42] Gentry and Gordon, *Strategic Warning Intelligence*, pp. 122–126.

[43] Buchanan, *The Cybersecurity Dilemma*, p. 42; Zegart, *Spies, Lies, and Algorithms*, p. 254.

[44] Carlin, *Dawn of the Code War,* pp. 352–360.

[45] Troy Mattern, John Felker, Randy Borum, and George Bamford, “Operational Levels of Cyber Intelligence,” *International Journal of Intelligence and CounterIntelligence*, Vol. 27, No. 4 (2014), pp. 702–719.

[46] Sanger, *The Perfect Weapon,* p. 2.

[47] Zegart, *Spies, Lies, and Algorithms*, pp. 261–269.

[48] Buchanan, *The Hacker and the State,* pp. 108–125.

[49] M. A. Thomas, "Distinguishing Cyberattacks by Difficulty," *International Journal of Intelligence and CounterIntelligence*, Advance Online Publication. doi: 10.1080/08850607.2021.2018565

[50] Healey and van Bochovan, "Strategic Cyber Early Warning," p. 4.

[51] Zegart, *Spies, Lies, and Algorithms*, p. 270.

[52] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research*, No. 1 (2011), p. 80.

[53] Buchanan, *The Cybersecurity Dilemma*, p. 26.

[54] Brantly, *The Decision to Attack*, pp. 97–98, 115.

[55] Sanger, *The Perfect Weapon*, pp. 51–54.

[56] Buchanan, *The Hacker and the State*, p. 166.

[57] *Ibid*., p. 213.

[58] Alfred Ng, "NSA Chief: US Alerted France to Russian Election Hacking," *Cnet News*, 9 May 2017, https://www.cnet.com/news/privacy/nsa-warned-france-russia-election-hacking-mike-rogers/

[59] Buchanan, *The Hacker and the State*, pp. 180–181; Sanger, *The Perfect Weapon*, p. 124.

[60] Sanger, *The Perfect Weapon,* pp. 152–170.

[61] Buchanan, *The Hacker and the State*, p. 315.

[62] Emma Woollicott, "Sweden Launches Cyber Defense Agency to Counter Disinformation," *Forbes*, 5 January 2022, https://www.forbes.com/sites/emmawoollacott/2022/01/05/sweden-launches-psychological-defense-agency-to-counter-disinformation/?sh=31c09cc44874

[63] Rebecca Shabad, "Disinformation Head Nina Jankowicz Resigns after DHS Board is Paused," *NBC News*, 19 May 2022, https://www.nbcnews.com/politics/white-house/dhs-disinformation-head-resigns-board-paused-rcna29578

[64] Ned Moran, "A Cyber Early Warning Model," in *Inside Cyber Warfare: Mapping the Cyber Underworld*, edited by Jeffrey Carr (Sebastopol, CA: O'Reilly Media, 2010), pp. 180–188.

[65] Carlin, *Dawn of the Code War*, p. 51; Buchanan, *The Cybersecurity Dilemma*, p. 42.

[66] Carlin, *Dawn of the Code War*, pp. 297, 302, 304; Sanger, *The Perfect Weapon,* pp. 296–298, 328–329.

[67] Sanger, *The Perfect Weapon*, pp. 124–128, 133–138, 287.

[68] Buchanan, *The Cybersecurity Dilemma*, p. 43.

[69] For some proposed political and "patriot hacker"–oriented indicators, see Healey and van Bochovan, "Strategic Cyber Early Warning," pp. 5–6.

[70] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), p. 114.

[71] Council on Foreign Relations, "Cyber Operations Tracker," https://www.cfr.org/cyber-operations/

[72] Buchanan, *The Hacker and the State*, p. 278.

[73] Sanger, *The Perfect Weapon,* pp. 175–177.

[74] *Ibid.*, pp. xviii, 154, 157.

[75] Buchanan, *The Hacker and the State*, p. 95; Sanger, *The Perfect Weapon*, p. 109.

[76] Sanger, *The Perfect Weapon,* p. 130.

[77] Jason Healey, "Concluding Assessment," in Healey, *A Fierce Domain*, pp. 265–278.

[78] Egloff and Smeets, "Publicly Attributing Cyber Attacks," pp. 8–11.

[79] Buchanan, *The Cybersecurity Dilemma*, pp. 172–173; Sanger, *The Perfect Weapon,* p. 181.

[80] John A. Gentry, "Warning Analysis: Focusing on Perceptions of Vulnerability," *International Journal of Intelligence and CounterIntelligence*, Vol. 28, No. 1 (2015), pp. 64–88; John A. Gentry, "The Instrumental Use of Norms in War: Impact on Strategies and Strategic Outcomes," *Comparative Strategy*, Vol. 37, No. 1 (2018), pp. 35–48.

[81] Sanger, *The Perfect Weapon,* pp. 141, 146, 191–192; Carlin, *Dawn of the Code War.*

[82] Cited in Sanger, *The Perfect Weapon,* p. 295.

[83] Oosthoek and Doerr, "Cyber Threat Intelligence"; Gentry and Gordon, "U.S. Strategic Warning Intelligence," pp. 32–34.

[84] Ephraim Kahana, "Early Warning versus Concept: The Case of the Yom Kippur War 1973," *Intelligence and National Security,* Vol. 17, No. 2 (2002), pp. 81–104.

[85] Buchanan, *The Hacker and the State*, pp. 295–296; Sanger, *The Perfect Weapon,* pp. 153–156.

[86] Whaley, *Strategem.*

[87] Donald C. Daniel and Katherine L. Herbig (eds.), *Strategic Military Deception* (Oxford: Pergamon, 1982).

[88] Cynthia Grabo with Jan Goldman, *Handbook of Warning Intelligence* (Lanham, MD: Rowman & Littlefield, 2015).

[89] Whaley, *Strategem*, pp. 4–5.

[90] *Ibid.*, p. xiv.

[91] *Ibid.*, pp. 74–75.

[92] Christopher Andrew, *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (New York: HarperPerennial, 1995), p. 538.

[93] Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007), pp. 55–62.

[94] Whaley, *Strategem*, p. 77.

[95] *Ibid.*, pp. 119–120.

[96] *Ibid.*, p. 127.

[97] Terry C. Quist, "The Changing Profile of Counterintelligence," conference paper, International Studies Association, 2 April 2022, p. 6.

[98] Healey and van Bochovan, "Strategic Cyber Early Warning," p. 6.

[99] For another view, see Jacqueline Poreda, "Intelligence After Next: Building a Counterintelligence Analytic Cadre," MITRE Corporation, February 2021,

https://www.mitre.org/publications/technical-papers/intelligence-after-next-building-a-counterintelligence-analytic-cadre

[100] James B. Bruce, "Countering Denial and Deception in the Early 21st Century: An Adaptation Strategy When All Else Fails," *American Intelligence Journal,* Vol. 32, No. 2 (2015), pp. 17–28.

[101] Ehrman, "What Are We Talking About When We Talk about Counterintelligence?"

[102] John A. Gentry, "The New Politicization of the U.S. Intelligence Community," *International Journal of Intelligence and CounterIntelligence,* Vol. 33, No. 4 (2020), pp. 639–665.

[103] Cynthia M. Grabo, "The Watch Committee and the National Indications Center: The Evolution of U.S. Strategic Warning, 1950–1975," *International Journal of Intelligence and CounterIntelligence,* Vol. 3, No. 3 (1989), pp. 363–385.

[104] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, Vol. 31, No. 1 (1978), p. 85.