CYBER SAFETY IN THE E

BY ROBERT S. METZGER

Cyber has been rising for years in public consciousness. Recent events place us on the brink of a new era where nation-states execute open and attributable cyberattacks targeting homeland infrastructure and the fabric of our electronically enabled society. In such an era, public safety may come to dominate how security professionals address cybersecurity.

Much of the emphasis of recent years has been on the protection of information and connected systems against attacks. Should ours be the era where cyber warfare comes to occupy a foreground role in nation state conflicts, "safety" of connected systems, and those who depend upon them, may rise above all other considerations, even while other objectives include the integrity and availability of systems as well as the confidentiality of information stored on networks and devices.

We must contemplate a world where the geopolitical dimension of cybersecurity becomes a fixture in foreign affairs and national defense policy. In such a world, diverse attacks of varying severity are not extraordinary but expected. Government and industry leaders must accept that the best of present defenses may only drive adversaries to aggression directed where defenses are weak or absent. In such an environment, "voluntary" measures will not suffice for much of government and industry. Businesses who fail to invest in and sustain truly effective security will accept peril to their enterprise existence. When nation-state-directed cyber challenges become a constant for America, today or in the near future, public safety will demand profound changes in policy, law, regulation and enterprise operations. Current headlines instruct us to plan ahead.

AN ASCENDING HISTORY OF VULNERABILITIES, ATTACKS, AND CONSEQUENCES

Cyberattacks are hardly news. But there are so many, on a continuous basis, it is easy to lose track of the particular actors, methods, and consequences. The trend line of recent years, even before we take the Iran crisis into consideration, warns us of what may lie ahead.

One constant is that attack types both proliferate and repeat. There have been numerous reported attacks on networks and servers to compromise personal information. Back in 2015, China was thought to have breached the information system of the federal Office of Personnel Management to steal approximately 21.5 million records, including the sensitive security clearance files of millions of U.S. individuals. Yet companies of all sizes continue to suffer involuntary transfer—"exfiltration," or theft—of their valuable IP and trade secrets. China has dominated such thefts for years, with little sign of either abatement or denial of the gains they have sought and accomplished through this unwelcome knowledge transfer.

There is a plethora of evidence that for years adversaries, principally China, have continued to exploit weaknesses in the cyber protection of U.S. and international companies to mount economic espionage campaigns of mind-boggling scope – and success. As far back as 2012, then-NSA Chief Gen. Keith Alexander said that cyber theft of industrial data and IP was "the greatest transfer of wealth in human history." Late in 2019, Maj. Gen. Thomas Murphy, Director of the Protecting Critical Technology Task Force (PCTTF), a special Pentagon Task Force established to protect industrial security, affirmed that foreign nations steal billions per year in technology from the United States. The need remains acute today to better protect the information security of defense contractors.

A different kind of attack, directed against infrastructure and industrial operations, seeks not to steal data so much as to corrupt it, or host systems, and damage or deny the utility, or safety of physical assets operated through computer instruction or network connection. A well-known example of such a "cyber-physical" attack is the NotPetya malware attack in 2017 that crippled Maersk shipping and impaired the operations of the Merck pharmaceutical giant, which are among many consequences to companies in Europe and elsewhere.

NotPetya is a prominent example of a supply chain attack, but it is hardly unique. Supply chain attacks can be accomplished through hardware, software, and even service providers. As concerns hardware, in 2018 the Bloomberg news service published a sensational story that motherboards produced by a widely respected supplier harbored a malicious microchip inserted by manufacturing subcontractors in China, which in theory could compromise widely installed servers and other computing systems. A high impact software attack was experienced by Equifax, in 2017, resulting in the compromise of sensitive credit information of an estimated 147 million Americans. How did this happen? Well-intentioned security researchers found and published a web server vulnerability in open source Apache Struts software. Attackers were able to exploit the known vulnerability before Equifax acted to install the recommended patch. With respect to attacks through the service

RA OF CYBER WARFARE

provider sector, Target suffered a breach in 2013, which was accomplished by theft of network credentials from a third-party heating and ventilation contractor. Between 70 and 110 million customer records were compromised, at a reported cost to Target of $202 million.

Not to be neglected, of course, are attacks executed by manipulation of social media. The U.S. intelligence community found that Russian hackers pursued an "influence campaign" to manipulate the 2016 national elections. Such malignant mischief has hardly abated. Russia has not confined its social media disinformation campaigns to the United States. It is recently reported that Russia is trying a new Facebook election tampering tactic in the Ukraine. While Russia remains a dominant perpetrator of social media manipulation, a recent study found that political disinformation campaigns were evident in 70 countries—more than twice the figure from two years before.

THE IRAN CRISIS REDEFINES CYBER RISKS

Even before the events of January 2020, where some feared that Iran and the U.S. stood at the brink of war, Iran had shown itself to be a motivated and capable cyber adversary that has explored many varieties of cyber activity intended to harm the United States and our allies.

- Former Director of National Intelligence (DNI) James Clapper accused Iran of a cyberattack upon an American casino corporation in February 2014 in which hackers stole customer data: credit card data, Social Security numbers, and driver's license numbers.
- In March 2016, the Department of Justice indicted seven Iranians—allegedly working on behalf of Iran's Revolutionary Guards Corps—of conducting distributed denial of service (DDOS) botnet attacks upon dozens of major financial institutions.
- The Department of Justice subsequently accused Iran, again said to be acting through its Revolutionary Guards Corps, of attempting an attack in 2016 on a flood control dam in New York State. Had this attack been successful, it could have caused flooding.
- Subsequently, in 2017, Iran was said to be responsible for the industrial sabotage cyberattack made upon Aramco oil facilities in Saudi Arabia.
- Atlanta, in 2018, suffered a massive ransomware attack, causing over $30 million in losses, leading the Justice Department to indict two Iranian hackers. Public systems have been held hostage to ransomware.

These and other examples of Iran cyber activity all transpired before the United States took the provocative step of using unmanned aerial systems to kill a top Iranian leader, General Qasem Soleimani. When this occurred, many leading analysts asked whether this attack would cause a threshold to be crossed where cyber warfare comes out of the shadows and into the open. Such a concern is not novel. Events in January 2020, however, prompted a widely publicized discussion, with much media attention, that cyber was a plausible if not likely vector of retaliation. In this sense, nation-state cyber threats "graduated" from the realm of the possible to a level of threat that generated concern among the general public. As such, this threat received the attention of Congress and calls for a considered response at a national level. Indeed, with the warning, or perhaps the experience, of the crisis with Iran in January 2020 comes an obligation to consider a conflict landscape, as may be upon us imminently, in which cyber is a dominant and overt method to "retaliate," or otherwise influence or injure opposing parties.

CYBERATTACKS: OUT FROM THE SHADOWS?

Although the history of cyber conflict is brief, in relative terms, a prevailing condition has been that attackers always seek deniability or doubt. While their victims may *suspect* who is behind the handiwork or even *accuse* individuals and nation states of responsibility, real-time attribution with high confidence is difficult. It can take months, even years, to complete and make public the forensic work behind allegations of responsibility. This "attribution condition" has complicated national policy in both civilian and military domains.[1]

Attacks may have nation-state sponsors, leverage nation-state resources, or proceed with nation-state assent. But, for all their public notoriety and sometimes widespread consequences, most historical cyber-delivered attacks have occurred in the shadows of obscurity and uncertainty—"gray zones" where the attacker neither identifies itself nor announces its purpose.

Further, for all the injury done, few cyberattacks have intentionally sought to wreak damage, even to public

infrastructure and key industries, that results in massive destruction of property as well as injury and death in the civilian populace. (NotPetya is the closest to these consequences, but it is an open question whether Russia, believed to have initiated the attack, either intended or controlled its spread, breadth, and outcome.)

Even with such a background of many actual and attempted incursions, and despite the accusations by U.S. authorities informed by the National Security Agency (NSA) and other government entities, Iran has not until present times taken an overt act of cyber warfare intending to cause substantial damage to critical infrastructure or U.S. defense assets. Its response to the assassination of General Soleimani may break the pattern. We must contemplate the real possibility—even if it does not become an actuality *this time*—that Iran, or some other nation-state, will engage in *open cyber warfare* where it intends that the victim nation know both who did it and how it was done—and where it intends severe civilian consequences. At a national level, we must conclude, just as the United States did with nuclear weapons in August of 1945, that nation states have reached a level of maturation of Cyber Conflict where Iran, or another adversary nation, may determine to enroll "cyberattacks" as part of its overt geopolitical arsenal for use when in conflict with another nation-state adversary. The nation then responded to the emergence of atomic weapons, as a new form of weaponry, with new doctrines, with investment in measures to deter and defend against nuclear attack, and through regimes of international agreement evolved to encompass nuclear threats. The maturity of nation-state cyber threats calls for similar national initiatives and global actions to reduce threats and mitigate harm.

LESSONS FROM "DELIVER UNCOMPROMISED": CROSS-DOMAIN, COORDINATED ATTACKS

The MITRE Corporation's Report, "Deliver Uncompromised," released to the Secretary of Defense in 2018, warned that adversaries could engage in asymmetric warfare using "blended operations" that exploit multiple attack vectors, such as networks, industrial systems and infrastructure, supply chains, and social media. Asymmetric warfare is especially attractive to an adversary who cannot or chooses not to confront the United States in areas where we enjoy dominance—such as conventional military forces able to deliver kinetic power. Iran may appraise itself to be in such a condition today, even if it seeks to retaliate by conventional military means and notwithstanding its martial bluster[2].

It is unlikely that Iran could duplicate the precision drone attack that killed General Soleimani. Iran has some, but only limited, conventional military capability to attack the regional bases or assets employed by the U.S. to mount the attack on General Soleimani. Iran could carry out or sponsor proxy military attacks on the U.S. assets and forces in the Middle East, or those of our allies. Iran may be deterred from such kinetic attacks by risk of a disproportionate and overwhelming military response of the U.S. and its allies, who possess kinetic superiority.

In just this kind of scenario, the MITRE Report anticipates that a hostile power, such as Iran, will resort to cyber-enabled attacks against the United States or allies. In the worst case, a "cyber-physical" attack upon control systems can destroy physical assets, producing costly damage. Iran has learned this lesson in the 2010 Stuxnet attack, which savaged uranium enrichment centrifuges at Iran's Natanz nuclear facility. It is widely reported that the United States was an author of Stuxnet.

If Iran chooses to limit its fight in the areas where the United States enjoys clear military dominance, and determines to carry the attack outside of its region to the homeland of the United States, it may attack using cyber-physical means. It would avoid well-defended U.S. military systems and those civil and commercial systems that are well-protected. Unfortunately, the target array is vast, as many systems of both government and industry remain relatively undefended and non-resilient. Iran may make an attack, either covert or attributable, both to injure and to warn that it could do worse. Even if Iran is restrained by concern about escalation consequences, it may believe it can do a great deal of harm within the U.S. homeland. The consequences of such attacks, if successful, could range from inconvenience and disruption of public services, on the one hand, to the destruction of infrastructure, great property damage, and injury, even death, to civilians.[3]

One may wonder whether the U.S. national command authority fully considered these risks in ordering the lethal attack upon General Soleimani. Regardless, that attack is fact. Now, U.S. military leaders and policymakers must confront the questions of how to protect our homeland as well as overseas assets should Iran, or some other aggrieved local power, resort to cyber as its means to retaliate. Very soon, we may find that the past scenarios of analysts have become brutal realities in today's headlines. Should that occur, a "national reckoning" may follow. Measures to defend and recover from cyber-physical attacks could move from "recommended" to "essential." New laws or national policy may require demonstrable and sustained cybersecurity to protect a wide range of public sector functions, industries, and services.

SECURITY AND SAFETY IN THE NEW ERA

It is time to be realistic about what has been accomplished by cyber exertions thus far, and where we have fallen short. There is much to protect. There are areas relatively well secured, but many less so, and some not at all. The "defense industrial base" is where the federal government has devoted its most sustained regulatory attention and imposed the greatest requirements upon its contractors. Even there, security accomplishments rate no better than "mixed," and this is to protect just information security against hostile exploitation. Present security requirements do little to protect against threats to industrial operational technology (ICS, SCADA, PLCs, and the like) and little to protect against supply-chain threats deliverable through any of the hardware, software, or service provider vectors. Protection of connected systems informed by IoT devices and communicating through 5G networks is in its infancy.

Security is costly, higher security is difficult, and agile security to respond to determined foes in a dynamic environment is harder still. Yet there is no sanctuary from the actual threat environment. A significant cyber-physical attack may impact our populace, our government, our industry, and, indeed, our way of life. No one will argue *then* that it is everyone's business to adapt and respond to this new, contested world. Our dependencies upon electronic systems won't go away unless they are disrupted or removed by force. While many cyberattacks will be network-delivered, security is more than discrete cells of protection of information on particular information systems. And security cannot be an "elective" that businesses or critical infrastructure operators consider but do not deliver. Relying upon "market forces," or trusting in the good intentions of "prudent business," may fall woefully short, with a heavy price that we pay.

A case in point is presented by the present Cybersecurity Maturity Model Certification (CMMC) of the Department of Defense. The basic concept is to replace an approach that relies upon contractor "self-attestation" of security with a system of assessment and validation against defined technical processes and expected enterprise policies. From the comments of Maj. Gen. Murphy of the PCTTF, referenced above, there can be little doubt that the uniformed military, and senior civilian leadership of the Pentagon, are dissatisfied with the failures of present methods to secure controlled technical information of the defense industrial base.

Still, many in the defense industry remain resistant to the investments required to achieve credible resilience at the entity and industry levels, and there are many sources of doubt whether all the ambitions of CMMC can be realized within the aggressive timetable set by its leadership. CMMC is a very ambitious undertaking. No doubt, its rollout will be turbulent, and there will be much frustration and uncertainty. Every effort should be made to reduce the "shock" and the burden to industry. To this end, special measures may be required to enable smaller businesses and non-traditional government contractors (often key innovators) to meet necessary CMMC levels. There should be no disagreement, however, that CMMC is necessary, and those in the security community should help to achieve its goals.

Industry should appreciate that CMMC today is the base for other initiatives to come in the future. The structure now proposed by DoD incorporates the CMMC assessment of capacity to protect data as a proxy for the larger "supply chain security" of assessed organizations. But at the end of the day, the present CMMC tool only addresses the ability to protect sensitive data; it lacks standards and practices as well as assessment criteria directed at overall supply chain security. The initial CMMC maturity levels are focused on protection of information on premises systems. CMMC does not yet take on other cyberattack vectors, such as operational technology, or the discrete components of supply chain security. These are on the radar of DoD's CMMC program leadership, as they should be, however.

There are some difficult questions ahead on how the relationship between government and industry might change to reflect and respond to the contemporary cyber environment. In many areas, cooperation is encouraged, but voluntary. Even though there are statutes that encourage voluntary event sharing, many companies refrain from sharing sensitive data about their information systems and their security experience. This may need to be rethought, and new forms of "safe harbor" may be needed to overcome industry resistance to fulsome reporting.

Reporting of cyber incidents is an essential element of effective information security. In the defense area, DoD needs to know, and promptly, what has been lost, so that it can determine the impact of compromise and how best to respond. Today, DoD relies upon contractors to report compromising activities. Excepting some contractors cleared to do classified work, DoD neither mandates nor facilitates the use of automated systems of event monitoring. If in place, such systems would greatly accelerate the act of informing government and industry of attacks, thereby expediting effective and timely response. The contemporary approach, in contrast, relies upon the particular resources of individual contractors and the discretion of their management. Event reporting results, inevitably, are unresponsive to the speed of the attack.

There are different technologies and methods available to greatly improve the knowledge and response of industry at all sizes. For example, automated security information and event management (SIEM) is widely accepted as a key means by which sophisticated companies respond and recover from attacks. Too little of U.S. industry applies this capability, increasing the exposure of the smaller companies to potentially devastating attacks – and jeopardizing their customers. Very few smaller companies have the financial resources or technical expertise to host a SIEM. The answer is not to leave them vulnerable. The security community should consider how the federal government can provide the necessary resources that are unreachable to much of domestic industry, in a way that protects IP rights and assures the private sector that they will benefit from use of government-hosted or supplied security measures.

THE NEW ERA: PROTECT, BUT EXPECT ATTACK AND PLAN TO RECOVER

Cyber has been a tool of state actors, to be sure, among many other instigators. But rarely, if ever, has a nation chosen to take an overt aggressive cyber-delivered act against a country with an intent to cause physical destruction and injury or death to persons. The January 2020 events with Iran warn us that this paradigm may change. A new era may be upon us – where cyberattacks are a principal rather than collateral form of warfare.

Should this be so, we may be on the verge of a true "quantum change" in how cyber and related threats are perceived, by the general public, and in what is demanded of our government to defend the public against such threats.

Undoubtedly, there will be consequences as governments act at the federal, state, and local levels. Lawyers who service the public sector, international organizations, as well as those who advise commercial entities should begin now to think about what changes to recommend and how such changes will affect the landscape of law and regulation, as well as their clients.

This is where cyber "safety" should have higher priority. Adversaries tend to have the advantage of initiative, a condition likely to continue. We must assume, therefore, that today's good defense will not always succeed against tomorrow's novel attacks. DoD now conducts increasingly challenging exercises to test its key military systems to enable resiliency and provide for rapid recovery. The future cyber battleground, unfortunately, is not limited to military platforms or Pentagon assets. Beyond existing security process and practice, an orientation of "test, assess, respond and recover" needs to be at the core of both government and business as we approach the time of open cyber warfare. Few targets, if any, are out of reach. Oceans and geographic distances mean nothing to a determined, skillful cyber adversary.

Robert S. Metzger, an attorney in private practice, heads the Washington, D.C. office of Rogers Joseph O'Donnell, PC. He is a co-author of the 2018 MITRE "Deliver Uncompromised" Report and served on the 2017 Defense Science Board Task Force that produced the "Cyber Supply Chain" report. This article presents the personal views of Mr. Metzger and should not be attributed to any organization with which he is or has been affiliated.

ENDNOTES

1. To some, this attribution "dead zone" carries a collateral benefit of an ambiguity that is also embedded in the prevailing construct of "Cyber Conflict" as an element of Customary Law of Armed Conflict. There is a curious preference of many in the national security community to maintain that ambiguity as to definition and boundaries of cyber events, which permits the U.S. to condemn the cyber act of an adversary one day and execute an identical act in retaliation the next, with relative impunity under existing international legal constructs. Such a paradoxical position, with the risks it can be employed by us as well as against us, itself argues for multi-national efforts to update the laws of war to better address issues of cyber conflict.

2. Such blended kinetic attacks and cyberattacks have long been of concern; a DHS-hosted Red Team exercise in 2004 involving 100 U.S. corporate C-suite leaders found that the dominant fear they harbored was an attack against U.S. assets that blended cyber and kinetic vectors against their facilities and communities.

3. Recent history of response and recovery times after natural disasters should provide little comfort to U.S. planners of what could result from a cyberattack directed against civilian infrastructure. That history evidences vulnerability to secondary infrastructure impacts of long duration in areas such as the electric power grids and other essential service. Adverse consequences could become catastrophic if cyberattacks produce regional population dislocations, evacuations of the scale of Hurricane Katrina, or an epidemic outbreak of an infectious disease, for illustration.