Airmen conduct cyber operations at Joint Base San Antonio–Lackland in support of command and control and network operations (U.S. Air Force/William Belcher)

Achieving Accountability in Cyberspace

Revolution or Evolution?

By John N.T. Shanahan

Consider three scenarios, all based on actual incidents, and consider how violations in cyberspace have effects far beyond the actual incidents.

Cross-domain Violation. During a crisis in the Arabian Gulf, a young Sailor working in an operations-intelligence cell on an aircraft carrier that is part of a U.S. Central Command (USCENTCOM) carrier strike group (CSG) is tasked to provide satellite imagery of a new base of operations used by the Iranian navy. The best imagery available is on an unclassified Web site. Due to the urgency of the situation, the Sailor disregards standard operating procedures for transferring data between networks and downloads the image to an unclassified thumb drive and inserts the thumb drive into a Secret Internet Protocol Router Network (SIPRNet) USB port to transfer the imagery in preparation for a briefing to the commander. Unfortunately, the thumb

Major General John N.T. Shanahan, USAF, is Commander of the Air Force Intelligence, Surveillance, and Reconnaissance Agency at Joint Base San Antonio–Lackland, Texas. His previous assignment was to the Pentagon as the J39 Deputy Director for Global Operations, Operations Directorate, Joint Staff.

drive is infected with treacherous malware, which is subsequently transferred to the ship's classified and unclassified networks through this cross-domain violation. Within hours, the malware propagates throughout both networks and begins to beacon to a site known for its state-sponsored cyberspace espionage activities. There is no choice but to shut down both the unclassified and the secret networks on the carrier, isolating it from the rest of the CSG and from higher headquarters ashore and leading to disastrous consequences for ongoing operations.

Network Protection Shortfalls. At a major Air Force installation in the United States, communications personnel in a tenant unit, whose primary unclassified operating network is neither owned nor operated by the installation host commander, fail to load a patch directed in a tasking order that is designed to close a significant vulnerability in the unit's network. A rogue cyberspace actor discovers and takes advantage of the well-known vulnerability using a socially engineered spear phishing email to inject malware throughout the network. Consequently, the entire network must be shut down for 2 weeks to clean up the infection, with major consequences for deployed personnel who rely extensively on the combat weather data provided by the tenant organization.

Cleared Defense Contractor (CDC) Shortcomings. A small CDC in San Diego that designs and builds critical components of a major weapons system fails to adequately protect its unclassified proprietary network. A known nation-state actor gains access to the company's network and begins to exfiltrate megabytes of data. The National Security Agency (NSA) teams up with the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) to detect and identify the perpetrators, but the company does not take the necessary steps to clean and safeguard its network even after notifying the CDC of the ongoing attack. Within a month the company loses almost all the information on its network relating to the sensitive weapons system components, not only providing the nation-state a major economic advantage in future business negotiations, but also giving the offending state a decade's head start in designing an indigenous system and allowing it to build countermeasures against the U.S. system.

Cascading Effects

In all three vignettes, actions in cyberspace led to cascading effects and debilitating consequences in multiple domains beyond cyberspace and affected operational readiness. A root cause analysis aimed at identifying the origin of the consequences quickly leads to hard questions about the fundamental issue of accountability. In the first case, should the CSG commander be held responsible? What about the Sailor's supervisors at every layer throughout his chain of command? And what happens to the individual who brought an unclassified thumb drive into secure spaces on the ship? In the second case, what should happen to the tenant unit commander? Should the host installation commander be held accountable for the tenant unit's mistake? What about the host installation's communications squadron commander? In the third scenario, should the CDC be barred from future business with the Department of Defense (DOD) or the U.S. Government? Should it be forced to clean and protect its network before it is allowed to continue operations?

These represent only a sample of the questions that must be answered to establish responsibility and mete out punishment. To help provide the framework required to identify the right questions and responses, it is useful to examine three disciplines that are already associated with longstanding robust cultures of accountability: nuclear operations, aviation mishap investigations, and, as simple as it may sound, driving a car.

Our adversaries and potential adversaries—nation-states, nonstate actors, criminals, hacktivists, and insider threats—are moving ever faster along the cyberspace continuum from exploitation to disruption to destruction. To counter the dangers we face in cyberspace today requires a more comprehensive approach than simply enhancing information assurance, improving automated defense tools, and creating more policies and procedures to deter substandard practices. There is a compelling need to establish meaningful accountability for actions or inaction affecting cyberspace operations. Establishing accountability for activities in and through cyberspace is now at least as important as attribution when striving to prevent or punish bad behavior whether that behavior is a result of friendly or adversary actions.

When dealing with our own personnel and organizations, providing explicit accountability guidelines is necessary to assure the confidentiality, integrity, and availability of "blue" cyberspace. We have not fully developed or implemented key tenets of cyberspace accountability throughout U.S. military operations even though we are beginning to grasp the magnitude of what happens when we ignore it or treat it lightly. If we accept the proposition that our military's approach to cyberspace accountability is inadequate, yet reject the canard that achieving accountability in cyberspace is a fool's errand, the next logical question is what it will take to fix the problem.

Because of the ubiquity of cyberspace, exceptionally low barriers to entry, ease of use, dizzying rate of change, and inherent complexity in both the interconnection of multiple systems and the internal functioning of individual systems, no single revolutionary action, policy, procedure, or pronouncement will fix our problem of accountability in cyberspace. However, we know from our experiences in other disciplines that certain fundamental conditions are necessary to enable a true and enduring *culture of accountability.* We do not need to create these elements from scratch in cyberspace. Instead we need a rapid, evolutionary transformation of current activities that focuses on fostering and maturing the culture of accountability that is based on education and training (and begins the moment one enters the military); establishment of clear chains of custody for all networks and systems; establishment of defined processes and procedures, as well as explicit guidance on acceptable behavior;

advanced methods for controlling access; and a standardized joint process for "cyberspace mishap investigations" that parallels the process used so successfully in military aviation safety over the past 30 years. The final and in many ways most important ingredient in the accountability soup is enforcement as a commander's program, as there is a direct and crucial link between accountability in cyberspace and operational readiness.

There are useful analogies between military nuclear weapons operations and cyberspace operations, and safety, more than any other attribute, exemplifies the concept of accountability in nuclear operations. The remarkable safety record accumulated over the past 60 years in Navy and Air Force nuclear activities has been directly attributable to an uncompromising approach to safety as well as unflinching scrutiny of mistakes, adoption of lessons learned, and enforcement actions. Honest mistakes are evaluated and corrected, and recommendations for improvement are applied quickly and consistently throughout the Services to prevent similar future mishaps. Intentional negligence or inattention to detail, on the other hand, is punished swiftly and unmercifully. To paraphrase one old-school Air Force general, when it came to punishing mistakes in nuclear operations, firing the responsible commander would be accompanied by the admonition, "I don't know if you are just unlucky or a bad leader, but I can't afford to waste any more time finding out."

Yet the differences between nuclear and cyberspace operations are stark enough to suggest that the solution to cyberspace accountability lies in a hybrid approach that not only includes some aspects of the nuclear enterprise but also recognizes that the unique nature of the environment demands other less narrow solutions. Nuclear operations are *special*, with access restrictions throughout every aspect of operations. We would not want it any other way and we cannot afford to have it any other way. In this country, every decision involving employment of a nuclear weapon emanates from one person: the President. In relative terms, only a very small percentage of U.S. military personnel are allowed access to nuclear command and control or to the weapons themselves. To receive such access requires undergoing a psychological and medical vetting process known as the Personnel Reliability Program (PRP), which remains in place as long as an individual maintains access to the nuclear enterprise. PRP involves multiple levels and layers of compartmentalization to ensure that only a tiny number of people are granted access to the entire nuclear decisionmaking ecosystem. There are many technical safeguards throughout the nuclear command and control communications process and with the nuclear weapons themselves to prevent accidental or unauthorized actions. The strategic consequences of one mistake can be enormous, so accountability must always remain at the heart of all nuclear operations. Accountability is the sine qua non of nuclear operations.

On the other hand, cyberspace is ubiquitous. It was designed that way from its inception, and it is exceedingly unlikely that we will ever turn back the clock with respect to access. In fact, the opposite is far more likely: as cyberspace is integrated more and more into everything we do, it is entirely possible that we will even stop thinking of it as a unique "thing." Our dependence on cyberspace is increasing exponentially every year. It is now an unassailable proposition that it will always be available, be as secure as the situation demands, allow nearly instantaneous communication, and be crucial to carrying out the quotidian functions of every household, business, academic institution, military organization, and so much more (though the military must continue to train and exercise to the worst-case scenario—a "day/week/month without cyberspace").

While the specific physical, administrative, and technical controls used in nuclear operations may not be directly transferrable to operations that depend on maximizing access to cyberspace, the combined application of all three types of controls and the rigid enforcement of compliance with those controls offer insights into the critical elements of a cyberspace accountability culture.

The Social Compact of Trust

In addition to activities undertaken to ensure safety in nuclear operations, an approach similar to that used in military aviation safety over the past 50 years, especially since the early 1980s when Class A incident rates began to decrease dramatically after an alarming spike in the 1960s and 1970s, can be particularly useful for cyberspace operations. Serious aircraft mishaps are normally followed by two related but distinct safety investigations, each only 30 days long. The first is a safety investigation board (SIB). It focuses on identifying and correcting the root causes of a mishap and relies on a candid exchange of information. This offers the equivalent of immunity from punishment for admitting to failing to follow procedures or breaking rules in return for providing privileged information (which is never released to the public) deemed crucial to avoiding future similar mishaps. The second, an accident investigation board (AIB), is used inter alia to determine culpability and accountability *throughout every level of the chain of command*, potentially leading up to loss of aviation rating and even nonjudicial punishment. Applying the same level of formality and discipline inherent in aviation safety investigations to serious cyberspace mishaps will be instrumental in enhancing cyberspace accountability.

Likewise, trust and confidence are important to cyberspace accountability. Driving 50 mph down Arlington Boulevard, one can be less than 2 feet away from traffic approaching in the opposite lane at 50 mph. One small mistake would result in a 100 mph collision. Why is it we do not drive in perpetual fear of collision with our hands clutching the wheel in a death grip and our eyes locked firmly on the road? We *trust* that the driver in the other vehicle will not veer into us. We *trust* that his lifelong combination of training and experience has rendered him as interested in and capable of avoiding us as we are of avoiding him. The probability that he will veer into us is never zero, but it is so low that we essentially disregard this danger when we drive.

Students answer questions during Joint Cyber Analysis Course at Center for Information Dominance (U.S. Navy/Jessica Gaukel)

This mutual trust on the road rests on two pillars. The first revolves around minimum standards and the certification process that bestowed driver's licenses on both drivers, plus the benefits accrued by years of experience on the road. The second is constructed around a shared understanding of accountability along with confidence in the consequences of failure to abide by the rules of the road ranging from pecuniary penalties, to insurance rate increases, to loss of one's driver's license, to causing major damage to one's vehicle, and on up to jail time and even death. We need to engender similar trust and confidence in cyberspace to drive the kind of self-interested compliance that allows us to operate without fear. But how?

In recognition of the prominence of safety and trust, while also borrowing critical tenets from the U.S. military nuclear enterprise, we must focus on five critical areas to develop and inculcate the proper degree of accountability for individual or organizational activities in cyberspace.

First and foremost, we must *educate and train*. The ubiquity of cyberspace is not an excuse for failing to emphasize the importance of basic cyberspace protection at every opportunity; to the contrary, cyberspace's ubiquity demands lifelong attention to norms of behavior. Within the Air Force, the Nuclear Weapons Surety Program ensures that personnel are trained and certified on specified functional tasks whenever they hold positions that could affect nuclear operations. It includes initial nuclear surety training as well as recurring training for as long as they perform such duties. In the Navy, the principles inculcated into every nuclear propulsion operator are designed to provide protection through proper operations (the nuclear propulsion principles are integrity, level of knowledge, procedural compliance, forceful backup, questioning attitude, and formality). Applying similar standards to cyberspace means protection training should begin literally in elementary school and receive an appropriate emphasis throughout one's entire career to include all military professional schools (such as Service academies), Service and joint professional developmental education, and technical training. Unfortunately, there are hundreds of real-world case studies to help drive home the costs and risks of bad cyberspace practices in our education and training courses. Despite substantial differences between nuclear and cyberspace operations, when it comes to developing a culture of accountability the nuclear analogy reigns supreme and should be viewed as the gold standard when devising cyberspace protection training at every level.

Next, we should establish an explicit *chain of custody* for every network at every installation and facility throughout the military (and associated CDCs). There cannot be any ambiguity regarding who is ultimately responsible for

every system and every network on any given installation. As a wing commander of a major Air Force installation, I did not "own" every network on my base, and more often than not I was not even aware of what was happening with several major networks and associated systems that were owned and operated by tenant units. While I was partly to blame for this lack of awareness (because I never asked all the right questions), the fact that there were so many different systems under different ownership is symptomatic of the chaotic network environment that exists across DOD today (entropy would be an understatement). This is precisely why senior leaders are advocating forcefully for the Joint Information Environment (JIE), which will eventually collapse thousands of DOD enclaves into a more defensible, secure, and standardized architecture that will simplify worldwide cyberspace operations and improve the ability to establish accountability. This is also a crucial step toward changing how we view DOD networks—that is, as mission-critical warfighting platforms rather than utilities we take for granted.

Third, we should provide defined *processes and procedures*, as well as *explicit guidance on behavior*, for cyberspace operations. The concept of "positive control" in nuclear operations is applicable to cyberspace because there must be clearly specified standards of performance and behavior. These standards prevent inappropriate interpretations or assumptions regarding what to do and how to act. While this may initially appear to impose onerous restrictions on the use of "wide open" cyberspace (and as such are anathema to those who are convinced that cyberspace should be no more restricted than the air we breathe), the concept of positive control is reflected in the road signs and traffic controls we live by when driving vehicles anywhere in the world. Absent well-defined guidelines, there will be too much room for misinterpretation or questionable behavior by anyone who touches cyberspace in any capacity.

Fourth, accelerating development of *advanced methods for controlling access* to networks or the information resident on them—such as credential-based access controls, boundary-layer controls, better forensics, and trustworthy computing platforms—is crucial. While one of the principal advantages to cyberspace is the ability to share information nearly instantly and globally, at every level of classification, and with one person or millions, there is no "unalienable right" to unfettered access to all systems and all information. As the U.S. Government learned the hard way in the Private Bradley Manning WikiLeaks incident, in certain cases access to cyberspace must be treated as a privilege, not a right. History teaches that regardless of the domain involved, the "insider threat" remains the greatest danger. That is even truer in cyberspace, demanding innovative ways to minimize the damage caused by the Private Mannings of the world. We must recognize that—analogous to the history of highway safety—the fault does not always lie solely with the operator. We need systems engineered to be used responsibly by people with a reasonable amount of training. Otherwise, we may be asking for unreasonable levels of proficiency on the part of the operator and not enough on the network administrator or software engineer.

Finally, we must *establish a formal DOD-wide "cyberspace mishap" investigation process.* We must treat network/system mishaps the same way we treat military aviation mishaps, for instance, by establishing categories such as Type 1/2/3 cyberspace mishaps analogous to Class A/B/C aircraft mishaps. A *Type 1 cyberspace mishap* would be defined using the criteria of loss of life, significant damage, or major impact to mission resulting in a requirement for formal general officer-led SIB- and AIB-like investigations. Type 2 and 3 mishaps would also require investigations but at lower levels and with varying degrees of reporting requirements.

The Commander's Program

We create the foundation for accountability in cyberspace by training personnel, establishing a chain of custody, providing explicit guidance, improving our methods to control access, and developing a formal investigative process. The other action that must overlay all of those activities is enforcement as a commander's program, to include publication of the implications of failure to obey the rules of the road in cyberspace and a demonstrated commitment to adhere to it. The commander's program for cybersecurity should receive the same emphasis as safety, to include a requirement that commanders at all levels continuously highlight "cyberspace protection" and "cyberspace safety" while also incorporating cyber security into all training, exercise, and inspection programs. Discussing it during periodic safety "down days" is important but hardly sufficient. On one hand, we should not expect a "zero-mistake" cyberspace force. Indeed, it is even more unrealistic to demand a zero-mishap culture in cyberspace than it is in any other domain. On the other hand, there are substantial differences between acts of omission and acts of commission. The former can be ameliorated through a focus on training, but there can be no quarter for the latter because it can easily put entire networks and weapons systems at risk. Still, unless and until the consequences of failure are stated explicitly and adhered to, there will always be room for misinterpretation and lax enforcement of punitive measures.

Along with training and certification and establishing cyberspace chains of custody, explicitly specifying the consequences of failure to follow the rules will build the necessary level of mutual trust and, similar to driving on our nation's roads without the steering-wheel death grip, allow us to operate more safely and securely in cyberspace. We must also strengthen and enforce existing agreements with CDCs. While there will be new financial and administrative costs associated with meeting more stringent DOD cyberspace accountability requirements, CDC chief executive officers, chief information security officers, and chief information officers must understand that the ultimate price for ignoring the rules is debarment from future business with the U.S. Government. While this will be extremely challenging politically,

it is essential in halting the egregious exfiltration of sensitive information and intellectual property from CDCs across the United States and globally.

Fortunately, we are not starting from scratch in establishing our culture of cyberspace accountability. Training programs exist for operators and users of DOD cyberspace, to include annual information assurance and protection training. Similarly, the beginning of a chain of custody already exists with the certification and accreditation process, which requires approvals to both operate and connect systems. The standards for the training and certification and accreditation process, in addition to required security controls and a host of other processes and procedures, are documented in a large number of DOD issuances. Moreover, U.S. Cyber Command and the Services regularly perform Command Cyber Readiness Inspections of military organizations and CDCs, though these inspections cover only a small percentage of those eligible to be inspected because of a lack of capacity. JIE and similar initiatives demonstrate a commitment to advancing our security technology. Activities such as the Air Force's Operational Review Board already provide a framework for a cyberspace mishap investigation process.

Despite these ongoing efforts, we still lack the culture of accountability we aspire to, and we see the result in daily intrusions and in network exploitation. Once again, our experience from other disciplines that have figured this out over time offers a simple explanation: our commanders must make cyber security a priority. This will be reflected in the results of inspections, evaluations of unit and personnel performance, and disciplinary action when failures warrant it.

Similar to the accountability we seek to establish for our own cyberspace operations, these principles also apply to development of international norms of behavior in cyberspace. Turning from the tactical and operational to the strategic level, accountability is equally important when considering options to deny objectives or impose costs against cyberspace attacks that threaten our critical infrastructure and key resources. Nation-states, for example, must be held accountable for attacks they allow to originate from or pass through their sovereign territory, even if a nonstate actor or another nation is ultimately responsible for creating and launching the attack. As Microsoft's David Aucsmith puts it, "We must shift our discussion of doctrine away from attribution and towards accountability. People, organizations, and states should have an obligation to assist in cyberspace investigations where their property or jurisdiction is involved. Noncooperation should be viewed as a sign of culpability."[1] Accountability must be linked to the concept of cyberspace deterrence; that is, our political leaders should form an explicit link between establishing culpability for a cyberspace attack and the substantial costs that will be imposed for disregarding formal warnings. And, of course, this requires following up with actions to match the rhetoric. To do otherwise would completely undermine one of the core tenets of accountability.

Implementation of the processes and procedures throughout the five focus areas outlined above suggests alternate endings for the three vignettes that open this article. The first incident never occurred because of the cyberspace protection training the Sailor received throughout his life and early in his Navy career, because the ship's network defenses prevented insertion of a thumb drive into a SIPRNet computer, and because he knew via the commander's intent that his commander would not tolerate the violation of rules prohibiting the use of the thumb drive. In the second scenario, the tasking order was implemented automatically, and even if it was not, there were only a small handful of different networks on the installation, allowing a recently established regional JIE Enterprise Operations Center to quickly identify and patch the vulnerability remotely. Finally, thanks to new Federal Acquisition Regulations and comprehensive cybersecurity legislation, the CDC in the third scenario was contractually and legally forced to shut down its network within the first hour after NSA/FBI/DHS identification of the nation-state exploitation operation. When the CDC subsequently refused to expend the funds necessary to fix its network defenses, it was barred from future business with the U.S. Government.

Conclusion

The cyberspace genie cannot be put back in the bottle. To the contrary, cyberspace genies are proliferating by the millions, so an evolutionary rather than revolutionary approach to accountability is called for. The perfect cyberspace defense will never exist. While the offense-defense pendulum will continue to swing in both directions, the advantage will reside perennially with the cyberspace attacker and the inside threat. Moreover, the wars of the future will be network-enabled, and we ignore this simple fact at our peril. In this game of highly complex four-dimensional chess, the side that can maintain and control its own networks while continuously adapting to a chaotic, fluid information environment will gain a distinct advantage. To develop and mature the necessary degree of accountability in cyberspace—a domain in which, more than any other save the nuclear enterprise, one tactical misstep may have grave strategic consequences—we must rely on the combination of the five focus areas described here with the view that their implementation is a commander's responsibility. Unless and until commanders place and foster the necessary and equal level of emphasis in all five core areas within their personnel—analogous to adhering to the principles of nuclear propulsion—the requisite culture of accountability in cyberspace will never take root. **JFQ**

Note

[1] David Aucsmith, "The Technology and Policy of Attribution," in *#Cyber Doc: No Borders—No Boundaries*, ed. Timothy R. Sample and Michael S. Swetnam, 14 (Arlington, VA: Potomac Institute Press, 2012).