SCIENCE & GLOBAL SECURITY
2020, VOL. 28, NO. 1, 2–27
https://doi.org/10.1080/08929882.2019.1698126

Routledge
Taylor & Francis Group

Assessing Priorities towards Achieving Dependable and Secure Computing in the U.S. ICBM Force

Lauren J. Borja

School of Public Policy and Global Affairs, Liu Institute for Global Issues, University of British Columbia, Vancouver, Canada

ABSTRACT

This paper is an assessment of cybersecurity principles within the nuclear arsenal of the United States, specifically the nuclear-armed intercontinental ballistic missile forces. Ongoing modernizations will introduce new components, and potentially new vulnerabilities, into U.S. nuclear forces. The principles for achieving secure operations from the fields of computer security, dependable computing, and systems analysis, and the extent to which they are addressed within the management of U.S. nuclear intercontinental ballistic missiles is discussed. This paper then considers the types of vulnerabilities that may be overlooked during modernizations, followed by a critique of U.S. nuclear command and control policy choices that could make the consequences of these vulnerabilities more catastrophic.

ARTICLE HISTORY
Received 19 December 2018
Accepted 28 September 2019

Introduction

As cyberthreats to critical infrastructure have grown, many researchers inside and outside of the government have raised questions about the cybersecurity of nuclear weapon arsenals. In 2010, U.S. President Obama ordered a cyber vulnerability assessment of U.S. land-based nuclear missiles. The conclusions of that investigation, code-named "Red Domino," remain classified.[1] A 2013 report by the U.S. Defense Science Board (DSB) revealed that a full cyber inspection of the U.S. nuclear arsenal, beyond the land-based nuclear missiles, had yet to take place.[2] In 2017, another report from the DSB called for "immediate establishment of a program … to support cyber certification of U.S. nuclear forces and NC3 … including supply chain, insider threats, and physical sabotage or attack in addition to remote cyber attacks … "[3] In 2018, a report from the U.S. Government Accountability Office (GAO) on the cybersecurity of new weapon systems stated that "Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected, due in part to

CONTACT Lauren J. Borja lborja@stanford.edu Center for International Security and Cooperation, Stanford University, 616 Jane Stanford Way, Stanford, CA 94305, USA

basic issues such as poor password management and unencrypted communications."[4] While the report did not name specific weapon systems or describe faults in detail, its authors confirmed that the study included nuclear weapon systems.[5] Concerns about the cybersecurity of nuclear weapons have been raised by researchers outside of the government, who sound the alarm that, if left unaddressed, the systems were vulnerable to an accidental launch of nuclear weapons, the unauthorized launch of nuclear weapons, or inadvertent nuclear war.[6]

This uncertainty comes at a time when many of the states that possess nuclear weapons, including the United States, are modernizing their nuclear arsenals. These planned modernizations include updating existing or developing new nuclear weapons, nuclear weapons delivery vehicles, or command and control networks.[7] Modernizations in the Russian arsenal included the development of new nuclear missiles in response to U.S. missile defense systems.[8] The Chinese modernizations have increased the quality and quantity of its ballistic missile force.[9] In the 2018 "Nuclear Posture Review" written during President Trump's administration, the United States casts its modernization plans as a response to the deployment of "new" nuclear systems in other countries.[10] However, the United States has expanded the capabilities of its existing nuclear forces without deploying new weapon systems.[11]

The vulnerability of all weapon systems, including those that deliver nuclear bombs, is an anticipated and arguably unavoidable consequence of the rapid increase in computing capacity and its deployment into every aspect of society since the middle of the 20th century, including advanced military operations. But as computers become ubiquitous in the military environment, so too does the cyber threat. If the modernization of nuclear weapons follows a similar trajectory as other developments in weapon system technology,[12] modernization of the world's deadliest weapons will increase their vulnerability.

In the computer science literature, fundamental principles for creating secure computer systems exist. This paper attempts to assess the extent to which modernization of the U.S. nuclear arsenal follow these principles within its land-based intercontinental ballistic missile (ICBM) system, and which principles are prioritized over others. Based on these priorities, certain types of cyber vulnerabilities may be overlooked within the U.S. nuclear arsenal. Mitigating the threats from these vulnerabilities will require changes in U.S. nuclear weapons policy.

To discuss potential faults in the U.S. ICBM fleet, this paper uses the terminology from dependable computing to identify potential issues within the system. This paper advocates for a focus on dependable computing in addition to more traditional security measures to improve cybersecurity

within the U.S. ICBM force. Because of the potential for catastrophic consequences due to accidents within the nuclear arsenal, considering many different types of failures, not just those caused by malicious actors, is important. For this reason, insisting on the dependable and secure function of these systems is critical.

Identifying specific flaws, such as vulnerabilities in operating systems, is an important goal, but it is impractical for those without access to classified information. These specific faults are also properties of the system at a particular instance; if easily fixed, a specific fault may no longer threaten the security of a system. Identifying priorities, however, may be more instructive, potentially indicating where future oversight should be placed. Furthermore, the identification of systemic failures within the organization may be more useful in the prevention of catastrophic accidents, although certainly not a way to prevent them altogether.[13]

Importance of cybersecurity during modernization of the U.S. nuclear arsenal

Over the next 10 years, the United States plans to spend $263.8 billion on modernizing its nuclear arsenal, which includes developing new delivery systems, investing in stockpile management, and upgrading nuclear command and control infrastructure.[14] These estimates include plans to completely replace the currently deployed Minuteman ICBM system with a newly designed Ground-Based Strategic Deterrent.[15]

The design phase is the best time to incorporate cybersecurity principles. Like many other intensive engineering products, software and hardware go through phases of design, development, and testing before they are released. Implementing these principles after the design stage, such as during testing or after deployment, is not economical.

In a study released in 2012, the Software Engineering Institute, which is funded by the U.S. Department of Defense (DoD), performed a literature survey to develop best practices for creating software-reliant, safety-critical systems, such as aerospace vehicles.[16] The survey found that most of the errors in these systems were introduced during the design phase, but these design errors were not discovered until later phases of testing. Furthermore, the cost of correcting an error increased the longer the error remained undiscovered. The cost of fixing errors after the design was also identified in a recent report from the U.S. GAO on weapon system cybersecurity: “Bolting on cybersecurity late in the development cycle or after a system has been deployed is more difficult and costly than designing it in from the beginning.”[17]

In addition to being more costly, completely fixing certain errors is impossible for some operational products. The Specter hardware trojan demonstrates the challenges of fixing a design flaw after the product has been distributed and used widely. The Specter trojan, first identified in January 2018, is a class of vulnerabilities that exploits the way microprocessors, such as those used in almost all modern computers and smartphones, execute commands on various devices.[18] Intel, ARM and other microprocessor manufacturers struggled to release fixes because these chips were embedded in many different hardware products—from Apple laptops to Amazon servers. Many different software patches needed to be developed; however, none completely fixed the problem. An entire hardware replacement was not possible, because, at the time, all chips being sold in the market were vulnerable.[19] New methods of attack using the Specter vulnerability continued to be identified a year after its initial discovery.[20]

With these in mind, it is of utmost importance that the U.S. DoD focuses on cybersecurity during the modernization process. Failure to do so will not only increase costs but could lead to the deployment of nuclear weapon systems whose vulnerabilities cannot be remediated.

Dependable and secure systems analysis

Many different approaches to cybersecurity can be found in the technical literature. This section briefly summarizes work in the fields of computer security, dependable computing, and systems theory. These three fields have contributed to different types of cybersecurity analyses. Because this section provides a general overview, non-nuclear examples are given. A summary of this section can be found in Figure 1.

Computer security

Computer security is defined as the protection of assets (for example, hardware, software or data) from threats, usually caused by attackers. To accomplish this, organizations develop a comprehensive security policy that addresses three main objectives: confidentiality, integrity, and availability.[21]

- Confidentiality refers to the protection of system data and users, including prevention of the unauthorized disclosure of data. If an electronic banking system were to disclose account numbers and balances to people other than account owners and authorized bank employees, it would no longer be confidential.
- Integrity comprises the prevention of changes to the system and its data as a result of unauthorized or inadvertent action. People use electronic

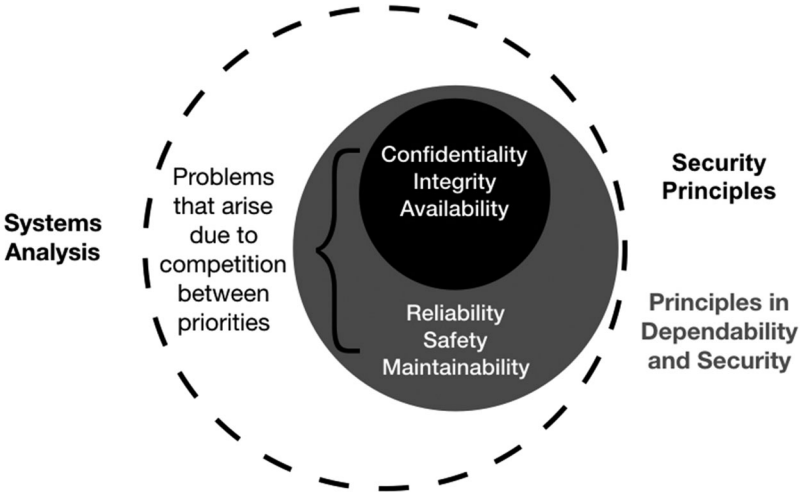

Figure 1. A schematic of the selected approaches to cybersecurity. This diagram highlights the distinctions between fields; however, these distinctions are not absolute.

banking services because the numbers they can view online reflect the balances in their accounts. The integrity of this system would degrade if these numbers could be changed by hackers or random system malfunctions.

- Availability is the property of a system that offers prompt service to authorized users. A system that lacks availability will experience intermittent outages in service, such as an electronic banking system that is only available during the business hours of its main branch location.

In addition to the three principles mentioned above, occasionally authenticity (users are legitimate, trusted) and accountability (users' actions can be traced through a system) are also included within security discussions.[22]

The field of computer security also suggests best practices for managing cybersecurity risk. Organizations should assign responsibilities to its members for upholding and enforcing aspects of the security policy. Risks are managed by continuously implementing security goals and policies for a particular system, assessing the extent to which the policies accomplish the goals, and improving upon either the policies or goals.[23] Within organizations, different levels of authentication may be necessary. As a result, computers must be able to isolate permitted actions for each privilege level.[24]

Another important aspect of cybersecurity is the classification of means and methods attackers use to compromise a system. Understanding the range of potential threats to a system is important for the successful implementation of a security policy. Examples of potential threats include insider or outsider attacks, information theft or data corruption. A full list of all

possible threats and vulnerabilities in the field of computer security is beyond the scope of this article,[25] but some discussion of potential attacks will be addressed in later sections.

Dependable and secure computing

Dependable and secure computing recognizes that computing systems are subject to faults beyond those carried out by malevolent actors and that certain predictable faults can be managed. Within dependability, the consequences of errors on the part of users of the system, including from incompetence or accidents, are also relevant.[26] To achieve dependability and security, three objectives must be considered, in addition to the confidentiality, integrity, and availability:

- Reliability is the ability of a system to offer the correct function. Systems that are not reliable will struggle to perform the intended service some of the time, such as an electronic banking system that occasionally transfers an incorrect amount of money.
- Safety refers to a system whose operation, intended or otherwise, does not cause harm. Unintended actions are also considered when assessing safety. If a user incorrectly electronically transfers money to a different account, this should not cause irreparable harm to the user. A system that fails in a manner that does not cause harm is considered fail-safe.
- Maintainability describes a system that can be repaired or updated. Systems that can only be updated during certain periods or under certain circumstances have poor maintainability. An electronic banking system would have poor maintainability if it could only be updated once per year when certain IT professionals are available.

In addition to recognizing similar attributes as the security field, dependable computing also prioritizes a taxonomy and description of possible faults. Within dependable computing texts, there is less of a focus on prescribing a policy than in security textbooks and a larger focus on the design process.[27] To achieve dependability, a system must have some ability to avoid, eliminate, tolerate, and forecast faults at various stages of development, testing, and fielding.[28]

Systems analysis

Systems theory, which is also important to the cybersecurity debate, is a way to analyze the performance of complex, highly technical systems. Originally conceived as a response to what its founders had identified as

shortcomings in the normal accident and high-reliability organization theories,[29] systems theory reframes safety or reliable operation of highly technical equipment as an emergent property of the system and its operating environment. The context within which the system will operate defines its safety requirements, which designers should be informed of when developing the system and specifying its functionality. This framing is useful when discussing accidents that occur when no one component is as fault.

The canonical example of this type of system failure is the loss of the Mars Polar Lander, whose problems could be traced back to improper communication of specifications.[30] In December 1999, the Lander crashed into the surface of Mars because the landing software mistook turbulence from the Martian atmosphere as confirmation that the Lander had reached the planet's surface. The software, performing according to its specifications, turned off the engines slowing the Lander's descent.[31] From a systems theory point of view, the software, which was accurately executing the code, has not failed. Instead, the process that engineered the system was at fault: the system did not properly communicate the requirements under which the software was expected to operate.

Systems theory can also be applied to cybersecurity problems. As the above example demonstrates, computers are often components in these complex systems. "The goal [of systems theory applied to computer systems]," according to a 2014 article in the *Communications of the ACM*, "is to ensure the critical functions and ultimately the services that the network and systems provide are maintained in the face of disruptions." Its authors advocate focusing on "top-down," "high-level strategies" instead of attempting to anticipate every vulnerability.[32] This form of analysis has produced an accident-assessment strategy (known as System-Theoretic Accident Model and Processes, STAMP)[33] and hazard assessment (System-Theoretic Process Analysis, STPA, which is based on STAMP).[34] Recently, an STPA analysis was performed on the Stuxnet cyberattack to assess vulnerabilities in Iranian centrifuges.[35]

Distinguishing between the three

Although there are clear distinctions between reliability, safety, and maintainability, the three have been and remain intertwined. It would be misleading to say that cybersecurity is not concerned with reliability. Furthermore, the definitions and language used within the fields have been fluid. For example, a conference paper from the 1978 National Computer Conference on cybersecurity defined "security" as "confidentiality" and "integrity," but also lists "reliability, availability and recovery" as a component of "defensiveness."[36] In

the 2018 handbook on information security provided by the U.S. National Institutes of Standards and Technology (NIST), "availability" is defined as "ensuring timely and reliable access to and use of information."[37]

In this paper, however, reliability and availability will be separated into two distinct categories. Certain pressures, such as production schedules or lack of funding for prolonged testing, can lead to situations where the reliability and availability of a product can be in conflict.

Recognition of the dangers of large, complex systems, whose faults can occur due to emergent properties beyond the failure of a single component, is also present within the discussions of security and dependability. For example, discussions on system theory have been included in textbooks on dependability in software engineering.[38] The overlap between the fields is also evident in documents produced by the U.S. government. For example, a NIST special publication on security engineering for systems, which adopts a systems theory approach, talks exclusively about cyber threats to critical infrastructure in its forward.[39]

Conflicting priorities within the U.S. nuclear ICBMs

To analyze how the principles of dependable and secure computing are addressed within the U.S. nuclear weapon system, the security of the land-based ICBM force is discussed. This leg of the U.S. nuclear triad consists of 400 nuclear warheads each deployed inside land-based ICBMs.[40] These ICBMs reside in hardened missile silos, which are controlled by a network of launch control centers. On average, each center is in direct, or primary control of about 10 missiles. A secondary launch control center monitors the commands sent by the primary center.[41] Inside the ICBMs is a missile guidance computer, which directs the nuclear-armed missile to its intended target.[42] Multiple target locations determined by the U.S. nuclear war plan are stored inside each missile's guidance computer.[43] To launch a nuclear missile, control centers specify both a target location and an execution order to launch a nuclear attack, by either selecting one of the pre-stored options or manually entering different information.[44]

Assessing the cybersecurity of the U.S. ICBM force using the previously described principles is a challenging process because of the confidential nature of such systems. However, one can indirectly assess this by examining measures of general security, if there is a clear indication that such factors have been accounted for. That being said, there are differences between physical- and cyber-security measures and the incorporation of security measures in the physical realm should not be taken as confirmation of these principles in the cyber realm.

- Availability: United States ensures that its ICBMs always remain available through redundant measures. For example, presidential launch orders can be communicated to the launch control centers via different telephone, satellite, and radio networks. Launch control centers can establish communication with an entire squadron of fifty ICBMs so that if one control center fails, another can control its missiles.[45]
- Reliability: In addition to missile test launches conducted at Vandenburg Air Force Base, U.S. ICBMs undergo operational testing while deployed in their silos. These tests include simulated electronic launches, which test the electronics necessary to initiate a missile launch up until the point of ignition, and tests of the software used inside the launch control centers to command the missiles.[46]
- Safety: The United States targets its ICBMs into the ocean as a safety measure, which is said to "ensure that in the very unlikely event of an accidental launch [U.S. missiles] could not and would not strike another nation."[47] This policy has been described as "little more than public relations," because "[with remote retargeting capabilities] switching from ocean targeting to wartime targeting is like changing television channels."[48] Safety against accidental launches is not the same, however, as safety against the deliberate and possibly unauthorized launch.
- Integrity: many unique authorization codes are needed to arm, target, and launch U.S. ICBMs. Those inside the launch control centers do not have access to all the codes needed to launch the missiles under their watch. The presidential authorization code is allegedly only contained in physical form and is not stored on a computer.[49]
- Confidentiality: details about the susceptibility of U.S. ICBMs to cyber-attacks remain classified.[50]
- Maintainability: of the six principles, maintainability is the most challenging for the U.S. ICBM force, because it can reduce the number of missiles available to target certain locations. Maintenance occurs on a tight schedule, with upgrades and testing planned weeks to months in advance.[51] During maintenance, missiles require higher degrees of safety, such as activation of additional pins or manual switching to prevent it from being launched.[52] As a result, the target of the missile could be reassigned to another missile if it considered a high priority. To do this, "maintenance scheduling determines the total number of days required [for the procedure] and requests relief from priority assignments … " This request is forwarded up the chain to U.S. Strategic Command. "Typically, these scheduled actions occur 45 days prior to the needed targeting [change]. The ICBM Strike Team then begins building a monthly targeting package for the entire ICBM fleet" of all these monthly requests.[53]

There are conflicts between these principles. For example, the United States could use additional physical launch-inhibiting methods only employed during maintenance procedures on a daily basis to increase the safety of its ICBM force.[54] These procedures, however, would need to be manually deactivated by a maintenance team in each deployed missile before any of the missiles could be launched. Because missiles are stored in dispersed locations typically without crewmembers onsite, this task would take minutes to hours to achieve, depending on the available manpower. This would change the missile launch availability: again, safety and availability conflict.

Dealing with faults within the nuclear arsenal

The handling of faults within computer systems is another aspect of dependable computing. Because these errors cannot be completely eliminated, organizations should have procedures to mitigate their danger. Yet the history of faults within the U.S. nuclear arsenal demonstrates that more attention should be paid to these aspects of cybersecurity. As in the last section, this analysis focuses on the U.S. ICBM force. Without the ability to successfully prevent, tolerate, and forecast faults, the dependability in the ICBM force could degrade due to minor malfunctions in hardware or software.

The computer science industry and academic experts suggest that an organization must have procedures to deal with faults within a computer system to keep the system secure.[55] These can be separated into three categories. First, an organization should have procedures in place to prevent faults from happening. These could include debugging during the initial design and testing phase for new software or hardware. Second, faults in one subsystem should not bring system-wide failure. This can be accomplished by building redundant paths or isolating certain subsystems to keep a fault from infecting the entire system. Third, organizations should be able to predict how many faults remain in their system. Models exist for quantitative error-prediction in software and hardware. These models depend on various characteristics of the software or hardware, such as lines of code or its complexity, and can be verified against data from system testing.

One example illustrates the ICBM's force inability to both prevent and tolerate faults. Launch control center is normally in constant communication with nuclear missiles. On 23 October 2010, all five launch control centers at Warren Air Force Base in Wyoming lost communications with all fifty nuclear missiles in their purview.[56] Even if orders, such as target changes, are not being sent by the launch control centers, the missiles must constantly report their status and check-in with the launch control centers.

During the 2010 incident, this communication channel was jammed; the launch control centers could only observe "down" status from the missiles themselves. Remote cameras used for silo security revealed that the missiles had not been launched, but for a little under an hour the launch control centers struggled to regain control and communications.

One analysis of the incident traced the fault to the displacement of a single circuit card within one of the computers responsible for monitoring the nuclear missiles inside one of the launch control centers.[57] Launch control centers routinely establish communication with each other in a round-robin fashion. When the circuit card was not seated properly, however, it jammed this communication channel, effectively paralyzing all connected launch control centers. As a result, the squadron lost communication and control with its nuclear missiles.

This incident has been described as more than just a loss in communications but also a degradation in nuclear command and control.[58] During the time when communications the launch control centers were severed, the missiles could have responded to launch orders received via radio antenna. This redundant communication method is used by the Airborne Launch Control System (ALCS),[59] which is an airplane-based launch control center used by the Air Force to launch nuclear land-based missiles if the control centers on the ground are incapacitated. During normal operations, the ground-based launch control centers continuously inhibit commands from the ALCS.[60] The launch control centers were unable to provide these crucial inhibit commands during the 2010 incident. If someone had successfully replicated and broadcasted the launch command used by the ALCS, there would have been nothing the launch control centers could have done to prevent it.

Even more troubling was the fact that this incident could have been prevented. The official report about the 2010 incident mentioned an incident in 1998 where similar communications problems were traced to a different loose circuit card in the same type of launch control center computer system.[61] The 1998 report recommended modifications to the installation procedure for the circuit cards and an investigation into potential hardware modifications are proposed.[62] According to the 2010 report, "Some of the recommendations coming out of the 1998 incidents were never implemented and may have been successful in preventing or at least mitigating the severity and duration of this event."[63] In 2011, the Air Force spent over $10 million to implement hardware to detect jamming of this launch control center communication line, update operations software, and to add "mechanical insertion/inspection hardware necessary to ensure cards are properly installed and remain fully seated."[64]

This incident illustrates that the Air Force experiences serious faults within the ICBM force and struggles to prevent their occurrence. It is perhaps unrealistic to expect that no problems should or could occur within the U.S. nuclear weapons arsenal. These problems, however, should not lead to degradation the command and control of nuclear forces. Furthermore, known vulnerabilities should be fixed.

Finally, methods for fault prediction used to assess reliability in the nuclear arsenal lag industry best practices and have led to newer systems being fielded with faults. A study by the National Research Council on reliability in defense applications critiqued established military reliability practices. Their report stated that the DoD had allowed contractors to rely on identifying failures by primarily testing new systems after the design phase. According to the report, "fixes incorporated late in development often cause problems in interfaces, because of a failure to identify all the effects of a design change, with the result that the fielded system requires greater amounts of maintenance and repair."[65] The report went on to recommend eliminating entirely the military's current method for assessing failure rates, because of its "fail[ure] to accurately predict electronic component reliabilities, as has been shown by a number of careful studies, including on defense systems . . . .[and] poor ranking of the predicted reliabilities of the defense systems in development."[66]

A specific example of poor fault prediction within the nuclear arsenal can be found in the 2015 operational testing for the Family of Advanced Beyond Line-of-Sight Terminals (FAB-T).[67] The FAB-T are a series of ground and aircraft computer terminals that interface with military satellite communication systems for disseminating nuclear and non-nuclear war plans.[68] Operational testing identified problems in the reliability models used by the FAB-T program to predict faults in the system. As a result, substantial problems were traced back to the hardware and software of the terminals. These problems were great enough that nuclear emergency messages sent and received over the FAB-T "were either not received or contained corrupted content. Missing or inaccurate reproduction of the original message can cause significant problems in the command and control of nuclear assets during operations."[69] Problems were also noted in the analysis used by the program manager to predict the remaining faults in the FAB-T system. Testers recommended updating these prediction methods to guide testing. The operational testing report from the following year found that while the reliability prediction methods had improved, failures in the system prevented realistic testing and, therefore, realistic data for the models was not available.[70]

These incidents are prescient during the United States' planned nuclear modernization. These incidents make it likely that similar problems will

exist within the U.S. nuclear arsenal. Explicitly, the United States could field nuclear systems with many errors that it would then struggle to find and correct.

Potential threats and vulnerabilities

Based on current operational priorities, this section broadly outlines areas where vulnerabilities may be introduced. Vulnerabilities are discussed from a high-level perspective. This approach may be more valuable than a list of specific technical deficiencies, because it may indicate where future attention needs to be paid, instead of tallying a current state of the system.

Furthermore, from this list of vulnerabilities, no one plan would give an attacker the ability to retarget said missile and launch a U.S. ICBM. That this remains opaque is certainly an attribute of not just the high level of secrecy around such systems but also the layered approach to security. However, these vulnerabilities could allow attackers to obtain significant data or information on U.S. ICBM operations, which would be the first step in a sophisticated cyberattack. These barriers are greatly reduced if attackers are aided by people working inside the U.S. ICBM force,[71] who may or may not be aware of their participation in the attack (i.e., malicious or inadvertent cyber insiders).[72]

Connections can penetrate air gaps

The trend in weapons systems of all types is to increase networking and add functionality. Much of this change is enabled by computers. Many of these systems are "air-gapped" or physically isolated from the Internet. For many years, this was considered enough, but more recently there is recognition that air gapping alone is insufficient against many cyberattacks.

Illustrating this threat, certain malware programs can cause air-gapped computers to leak classified information through the acoustic signals created by the infected computer's internal cooling fans.[73] Viruses have also infected air-gapped U.S. military networks. In 2008, a computer virus known as the agent.btz worm was discovered on both secret and top-secret military computer networks within the Pentagon. According to U.S. military officials, this infection was likely due to an authorized user inserting an infected universal serial bus (USB) into a computer connected to the classified networks, which is technically prohibited. To remove the worm from the classified networks, the Pentagon banned USB drives on all networks for over a year.[74]

Air-gapped computers have also been the targets of sophisticated government cyberattacks. In 2010, the notorious Stuxnet virus was discovered. It

was allegedly developed by the Israeli and U.S. governments to disrupt centrifuge machines in the Iranian Nantaz uranium enrichment facility.[75] As of 2013, United States had not fully verified that the computer networks associated with its nuclear weapons system were resilient to similar threats.[76] A more recent report in 2017 advocates for "an annual assessment of the cyber resilience of the U.S. nuclear deterrent … against a top tier cyber threat."[77]

Today, there is a recognition that air gaps are far from sufficient in protecting military weapons systems. From a report on weapons systems cybersecurity from the U.S. GAO, "any exchange of information is a potential access point for an adversary. Even "air-gapped" systems that do not directly connect to the Internet for security reasons could potentially be accessed by other means, such as USB devices and compact discs (CD). Weapon systems have a wide variety of interfaces, some of which are not obvious, that could be used as pathways for adversaries to access the systems"[78] As has been said before, the report did not mention any specific weapon, later news reports confirmed that nuclear systems were included.[79]

One such pathway into the U.S. nuclear ICBM arsenal is through nuclear early warning systems, such as the Space-Based Infrared System (SBIRS). The SBIRS is a series of satellites and ground-based support systems that detect missile launches and nuclear detonations using a series of infrared sensors.[80] SBIRS relies on software algorithms to take data from the various satellites in the SBIRS constellation and construct object trajectories that provide the starting location and point of impact of an identified object.[81] If the object is identified as a ballistic missile, targeted at the United States, policies are in place to initiate a U.S. nuclear retaliatory attack before the missile arrives.[82]

This policy places a large amount of stress on the sensors, algorithms, computers, and people that comprise SBIRS. As a result of this policy, the time for deciding whether objects detected by SBIRS are false alarms, inherent software problems, or a malicious cyberattack is severely constrained. SBIRS detects multiple infrared events per day, the majority of which are false alarms. According to SBIRS ground controllers, of the 8,000 annual infrared "events," only 200 can be assigned to missile launches.[83] In addition to false alarms, SBIRS has had numerous software and cybersecurity issues during its development and fielding.[84] Most of the information produced from operational testing of the SBIRS remains classified, but documentation released in 2016 revealed that cybersecurity concerns were found and that vulnerability assessments and penetration tests have never been completed.[85] Based on this limited information, significant questions should be raised regarding the susceptibility of the SBIRS system to cyber-attacks.

The vulnerability of legacy systems

Another potentially overlooked vulnerability to the U.S. nuclear weapons, such as those on ICBMs, could arise due to their reliance on older technology. Much of the nuclear arsenal relies upon legacy equipment. For example, a 2016 report from the U.S. GAO reported that the nuclear arsenal currently uses information technology that is over 50-years-old. Many of the technologies, which included 8-inch floppy disks, are now obsolete and increasingly hard to replace. The report said that the DoD planned to replace the system by the end of fiscal year 2017.[86]

According to military officials, the security benefits of using legacy equipment outweighs the inconvenience of using outdated technology. On numerous occasions, generals in charge of the nuclear arsenal or associated with its modernization have made claims about its security based on its age. According to these military officials, cybersecurity problems do not affect the nuclear arsenal: floppy discs cannot be hacked and systems in the arsenal lack modern connectivity.[87] When incidents occur within the nuclear arsenal, this narrative is also repeated to the media and public: "old machines offer almost maximum cybersecurity by virtue of their age."[88]

The age of a component is not related to its resiliency to cyber-attacks, and this includes floppy drives of all sizes.[89] Certain factors make hacking via floppy drive more challenging, but none of these challenges rise to the level of making such an attack impossible. Floppy drives are harder to procure and have less storage space than more common devices, such as CDs and USB drives. The limited storage capability of floppy discs restricts the size and potentially the sophistication of the code in the malicious attack, while also making the malicious code easier to detect because it cannot be hidden amongst other files and programs. Unlike CDs and USBs, computers do not automatically recognize and run programs found on floppy drives, making them a less effective way to spread malware.[90] These obstacles, however, are not insurmountable. The first case of ransomware was distributed via floppy drive in 1989.[91] Furthermore, the size of malware viruses has remained relatively constant over time and could easily fit on a floppy drive.[92]

Moreover, legacy systems can strain dependability and security. Certain system standards might not have been required when the equipment was initially installed, and it may not be clear how to assess older equipment against these new standards. Organizations, such as NASA, have attempted to assess the risk associated with the continued use of antiquated technologies in current environments.[93] Software security experts have pointed out that newer devices connected to older networks with insufficient security lead to hackers gaining access to older networks with relative ease. Older

networks were not designed to protect against current and evolving threats.[94]

Agencies responsible for testing military equipment operations have also discussed the security vulnerabilities introduced by legacy equipment. While such reports contain little details on the testing performed on nuclear systems, their statements on the limited testing of the cybersecurity of legacy systems are certainly relevant. Recent reports reveal that "preliminary assessments of systems and networks that had been developed and fielded several decades ago, and which were widely believed to be safe from current-era cyber-attacks … identified technology updates that were not part of the original design or security plan and which could provide avenues for a cyber-attack."[95] Clearly, legacy equipment is not, by definition, secure and overlooking such concerns can lead to significant vulnerabilities.

Switch to COTS components

Modernization also increases the probability that commercial off-the-shelf (COTS) products will be used in the command and control system. COTS components are typically less expensive, offer improved functionality and availability, and require less testing and resources over components built from scratch. Using products developed in-house and COTS products present security concerns, but each type presents a set of unique concerns. Because the nuclear arsenal has traditionally relied on products designed in-house, problems could arise as COTS equipment is incorporated.

The computer industry has warned about the use of COTS components in safety-critical applications.[96] Because COTS components typically lack documentation on the design or safety standards used to produce them, incorporating them into safety-critical application designs is risky. Even if documentation exists, the design or safety standards might not be applicable if the device is used outside of the design conditions specified by the manufacturer. COTS products can also require periodic maintenance or updates from the supplier, which may conflict with the operation of safety-critical systems.

The ongoing globalization of the supply chain for COTS computer components also makes it harder to ensure their security. Today's computer components are often designed, fabricated, and assembled in different countries. Even if a country has set up in-house fabrication facilities, it is likely that these will use parts or machinery produced elsewhere. Using equipment from multiple countries increases the possibility that malicious design features or hardware components might be covertly embedded into

devices. Once they have been built in, these covert features are almost impossible to detect.[97]

An example of how the U.S. DoD is struggling with the changes necessitated by COTS equipment, a heavily redacted 2018 report from the U.S. DoD's Office of the Inspector General found that multiple programs overseen by the Air Force Space Command could contain supply chain vulnerabilities. Certain procedures for mitigating supply chain risk were not followed in three programs listed by the report. Of the three programs named, two participate in either nuclear early warning and or command and control: the SBIRS and the FAB-T, which are a series of ground and mobile terminals that provide nuclear-survivable communications. "As a result, an adversary has the opportunity to infiltrate the Air Force Space Command supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the critical hardware, software, and firmware."[98]

The cybersecurity of the nuclear arsenal is also challenged by the lifecycle of modern computer components, which require more frequent updates and replacement. For computer systems used in everyday life, these updates are an inconvenience, but most people realize that undertaking these routine updates offers an improved defense against malware and viruses. Weapon systems are different and incorporating such updates in a timely fashion might be difficult because of various constraints. For example, U.S. nuclear missiles are expected to be in continuous use and, as a result, missile maintenance requires prior approval by higher authority.[99] As a result,

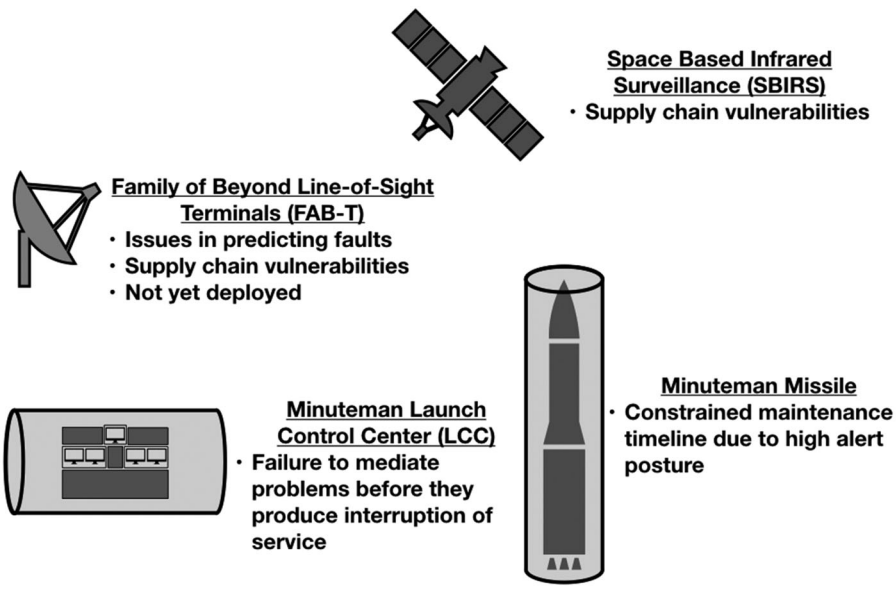

Figure 2. A schematic of potential vulnerabilities discussed in this paper.

known vulnerabilities will likely persist much longer in weapon systems than in other systems that can be updated more frequently.

These known vulnerabilities, summarized in Figure 2, will continue to compromise security. The WannaCry ransomware attack, which crippled the British National Health Services, illustrated the dangers of infrequent software updates. The attack used a vulnerability that affected systems that had not been updated with the most recent Microsoft patch.[100]

Each task is challenging, and the U.S. DoD is certainly not the only organization to be challenged by them. Clearly, a degree of risk lies with any technology within the U.S. nuclear arsenal. Reducing this risk, therefore, requires more than just a technical solution.

Policy choices increase the danger of cybersecurity problems

United States' nuclear weapons policy exacerbates baseline cybersecurity vulnerabilities and those caused by modernization. The stated policy of the United States is that the President can launch nuclear weapons against another country if data from the U.S. early warning system identifies an incoming attack. The launch can be commanded before the arrival of attacking missiles, within a few minutes of notification from the early warning system. The guarantee of retaliation, in theory, decreases the value of a hypothetical first strike.

To comply with the short window for decision-making that is required for rapid launch, the United States configures its nuclear forces for quick use. This policy, however, increases the risk of accidental or inadvertent launch. For example, storing nuclear warheads inside missiles that are fueled with combustible materials leads to the potential for accidental explosions.[101] An accidental leak of liquid propellant from a U.S. ICBM in 1980 led to an explosion that ejected parts of the missile and nuclear warhead from their reinforced silo.[102] Even though nuclear warhead did not detonate, this example illustrates the dangers of storing nuclear warheads with their delivery vehicles.

The potential for inadvertent or accidental nuclear war due to computer malfunction is not necessarily new; earlier generations of computerized systems have brought the United States close to the brink of launching nuclear weapons. On 3 June 1980, a computer screen in a command post of the U.S. Strategic Air Command indicated an incoming Soviet-launched ballistic missile, with more missiles appearing within a few seconds.[103] Bomber pilots were notified to start their engines on the tarmac and U.S. ICBMs were prepared for launch. Fortunately, people realized that something was amiss because the number of incoming missiles fluctuated wildly with no clear pattern of attack. The spurious signals were dismissed in a threat

assessment conference, and the nuclear bombers and missiles were de-alerted. An investigation revealed that a computer chip failure had led to the erroneous readings.[104] However, if the spuriousness of the warning had not been realized within the roughly 30 minutes it takes for a missile to fly from the Soviet Union to the United States, the U.S. President might have decided to launch missiles at the Soviet Union.

Today, the strain on early warning systems due to false alarms has only increased. Ballistic missile technology continues to proliferate to new countries, even if they do not possess nuclear weapons. "Every day, [early-warning detection] events occur, often involving civilian or military missile launches, that require a look by the early-warning crews at [various] Air Force bases."[105] As stated before, numbers from just one early-warning system, the SBIRS, state that there are roughly 8,000 detection events annually; only 200 correspond to actual missile launches.[106] For each of these, early-warning ground crews have less than five minutes to determine if the event will be reported to higher command. Even though there are many steps between event detection and notification of the president,[107] there have been cases where the U.S. president has been notified of an "ambiguous imminent threat."[108]

Conclusion

This paper identifies growing cybersecurity concerns that many nuclear arsenals will face based on issues that have occurred in the past two decades, after the end of the Cold War era. These concerns will only increase as modernization programs continue. Using the United States again as an example, some organizations might need to revisit their priorities and reassess how well each system addresses best-practice cybersecurity principles. Evidence indicates that the U.S. ICBM force is not well structured to mitigate certain future cybersecurity threats.

When countries structure their nuclear command and control systems to comply with the short decision-making times necessary for launch on warning policies, they create systems that have alarming low margins of error. Storing nuclear warheads mated with their delivery vehicles, such as land-based missiles, significantly increases the risk that a problem within either system could lead to a nuclear detonation. These policies increase the risk that small errors could lead to an inadvertent nuclear war. The fact that the U.S. ICBM force can be launched, without the possibility of recall, after receiving launch orders that are less than 200 characters long contributes to this risk.[109] United States has put alerts into effect, readying nuclear-armed bombers and missiles for launch, before messages from its early warning system can be fully verified.

Cases already exist of errors within the U.S. and Russian nuclear systems. As more digital components are built into the nuclear command and control network and the weapons themselves, the potential for problems similar to the above example will increase. New problems will also present themselves as more components become digital or older components are modernized. Computer components introduce more uncertainty into the already complex task of controlling and directing nuclear forces. When combined with the short timescales for decision making put into place by launch on warning policies, problems introduced by digital components could lead to unpredictable accidents with catastrophic consequences.[110] Knowing that modern technology increases the risk of errors, it is important to take steps to ensure that these malfunctions do not lead to catastrophic failure. Eliminating these policies is one step that could reduce the lethality of computer failures in nuclear command and control.

Without access to classified data, it is difficult to prescribe specific steps that can increase the overall safety of the system. However, one can argue that general measures to enhance safety, even if it comes at the cost of availability, are desirable from the viewpoint of reducing the chances of accidental or inadvertent nuclear weapons use.

Notes and References

1. Kevin Hartnett. "What's Wrong with Our Nuclear Phones," *Politico*, August 3, 2015, https://www.politico.com/agenda/story/2015/08/whats-wrong-with-our-nuclear-phones-000181; Bruce G. Blair, "Why Our Nuclear Weapons Can Be Hacked," *The New York Times*, January 20, 2018, https://www.nytimes.com/2017/03/14/opinion/why-our-nuclear-weapons-can-be-hacked.html.
2. James R. Gosler, and Lewis Von Thaer, Resilient Military Systems and the Advanced Cyber Threat (Washington, D.C.: Defense Science Board, 2013), 7, http://www.dtic.mil/docs/citations/ADA569975.
3. Lewis Von Thaer, and James R. Gosler, Defense Science Board (DSB) Task Force on Cyber Deterrence (Washington, D.C.: Defense Science Board, 2017), 24, https://apps.dtic.mil/docs/citations/AD1028516.
4. Cristina T. Chaplain, Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities (Washington, D.C.: Government Accountability Office, October 2018), 2, https://www.gao.gov/assets/700/694913.pdf.
5. David E. Sanger, and William J. Broad, "New U.S. Weapons Systems Are a Hackers' Bonanza, Investigators Find," *The New York Times*, October 10, 2018, https://www.nytimes.com/2018/10/10/us/politics/hackers-pentagon-weapons-systems.html.
6. Jason Fritz, Hacking Nuclear Command and Control (International Commission on Nuclear Nonproliferation and Disarmament, 2009), http://www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.pdf; Bruce G. Blair, Global Zero on Nuclear Risk Reduction: De-Alerting and Stabilizing the World's Nuclear Force Postures (Global Zero, 2015), https://www.globalzero.org/get-the-facts/nuclear-risk-reduction; Andrew Futter, Hacking the Bomb: Cyber Threats and Nuclear Weapons (Washington D.C.: Georgetown University Press, 2018), 208, http://press.georgetown.

edu/book/georgetown/hacking-bomb; Beyza Unal, and Patricia Lewis, Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences (Research Paper, The Royal Institute of International Affairs Chatham House, 2018), https://www.chathamhouse.org//node/33714; Page O. Stoutland, and Samantha Pitts-Kiefer, Nuclear Weapons in the New Cyber Age (Nuclear Threat Initiative, 2018), https://www.nti.org/analysis/reports/nuclear-weapons-cyber-age/; M. V. Ramana, and Mariia Kurando, "Cyberattacks on Russia—the Nation with the Most Nuclear Weapons—Pose a Global Threat," *Bulletin of the Atomic Scientists* 75(2019): 1, 44–50, doi:10.1080/00963402.2019.1556001.

7. Hans M. Kristensen, and Robert S. Norris, "Russian Nuclear Forces, 2018," *Bulletin of the Atomic Scientists* 74(2018): 3, 185–195, doi:10.1080/00963402.2018.1462912; Hans M. Kristensen, and Matt Korda, "Indian Nuclear Forces, 2018," *Bulletin of the Atomic Scientists* 74(2018): 6, 361–366, doi:10.1080/00963402.2018.1533162; Hans M. Kristensen, Robert S. Norris, and Julia Diamond, "Pakistani Nuclear Forces, 2018," *Bulletin of the Atomic Scientists* 74 (2018): 5, 348–358, doi:10.1080/00963402.2018.1507796; Hans M. Kristensen, and Robert S. Norris, "Chinese Nuclear Forces, 2018," *Bulletin of the Atomic Scientists* 74(2018): 4, 289–295, doi:10.1080/00963402.2018.1486620; Hans M. Kristensen, and Robert M. Norris, "United States Nuclear Forces, 2018," *Bulletin of the Atomic Scientists* 72(2018): 4, 120–131, doi:10.1080/00963402.2018.1438219.
8. Pavel Podvig, "Russia's Current Nuclear Modernization and Arms Control," *Journal for Peace and Nuclear Disarmament*, 1(2018), 1–12, doi:10.1080/25751654.2018.1526629.
9. Gregory Kulacki, China's Nuclear Force: Modernizing from Behind (Washington, D.C.: Union of Concerned Scientists, 2018), https://www.ucsusa.org/sites/default/files/attach/2018/01/modernizing-from-behind.pdf.
10. James Mattis, Nuclear Posture Review (Washington, D.C.: Office of the Secretary of Defense, 2018), https://www.defense.gov/News/Special-Reports/NPR-2018.
11. "U.S. Nuclear Modernization Programs," Arms Control Association, Last reviewed August 2018, https://www.armscontrol.org/factsheets/USNuclearModernization.
12. Chaplain, Weapon Systems Cybersecurity.
13. Charles Perrow, Normal Accidents: Living with High-Risk Technologies, Revised ed. (Princeton, NJ: Princeton University Press, 1999), https://www.amazon.com/Normal-Accidents-Living-High-Risk-Technologies/dp/0691004129.
14. John Pendleton, and David C. Trimble, Nuclear Weapons: Ten-Year Budget Estimates for Modernization Omit Key Efforts, and Assumptions and Limitations Are Not Fully Transparent, (Washington, D.C.: Government Accountability Office, 2014), https://www.gao.gov/products/GAO-14-373.
15. Ryan Snyder, "The Future of the ICBM Force: Should the Least Valuable Leg of the Triad Be Replaced?" Policy White Paper, Analysis of Weapons-Related Security Threats and Effective Policy Responses (Washington, D.C.: Arms Control Association, 2018), https://www.armscontrol.org/sites/default/files/files/PolicyPapers/PolicyPaper_RS_2018_0319.pdf.
16. Peter H. Feiler et al., Reliability Validation and Improvement Framework (Pittsburgh, PA: Software Engineering Institute, Carnegie-Mellon University, 2012), https://apps.dtic.mil/docs/citations/ADA610905.
17. Chaplain, Weapon Systems Cybersecurity.
18. Paul Kocher et al., Spectre Attacks: Exploiting Speculative Execution, (Research paper: Cornell University, 2018), http://arxiv.org/abs/1801.01203.

19. Lily Hay Newman, "Meltdown and Spectre Fixes Arrive—But Don't Solve Everything," *WIRED*, January 6, 2018, https://www.wired.com/story/meltdown-and-spectre-vulnerability-fix/.
20. Peter Bright, "Spectre, Meltdown Researchers Unveil 7 More Speculative Execution Attacks," *Ars Technica*, November 14, 2018, https://arstechnica.com/gadgets/2018/11/spectre-meltdown-researchers-unveil-7-more-speculative-execution-attacks/.
21. William Stallings, and Lawrie Brown, Computer Security: Principles and Practice, 4th ed. (New York, NY: Pearson, 2018).
22. M. Andrews, and J. A. Whittaker, "Computer Security," *IEEE Security Privacy* 2(2004): 5, 68–71, doi:10.1109/MSP.2004.66.
23. Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri, "An Introduction to Information Security," NIST Special Publication (Washington, D.C.: National Institute of Standards and Technology, 2017), https://doi.org/10.6028/NIST.SP.800-12r1.
24. J. H. Saltzer, and M. D. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE* 63(1975): 9, 1278–1308, doi:10.1109/PROC.1975.9939.
25. See the following for a more detailed discussion and classification of potential risks: Nieles, Dempsey, and Pillitteri, "An Introduction to Information Security"; Stallings and Brown, Computer Security: Principles and Practice.
26. A. Avizienis et al., "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing* 1(2004): 11–33, doi:10.1109/TDSC.2004.2; John Knight, Fundamentals of Dependable Computing for Software Engineers (London, U.K.: Chapman and Hall/CRC, 2012), doi:10.1201/b11667.
27. For example, compare the table of contents for both Knight, Fundamentals of Dependable Computing for Software Engineers; Matt Bishop, Computer Security, 2nd edition (Boston, MA: Addison-Wesley Professional, 2018). The latter has many chapters devoted to different types of implementation policies. There is also no discussion of encryption, nor does it appear as a topic in the index, in the former.
28. Avizienis et al., "Basic Concepts and Taxonomy"; Knight, Fundamentals of Dependable Computing for Software Engineers.
29. Nancy Leveson et al., "Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems," *Organization Studies* 30(2009): 227–249, doi:10.1177/0170840608101478.
30. Nancy Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, (Cambridge, MA: MIT Press, 2017), https://mitpress.mit.edu/books/engineering-safer-world.
31. Keith Cowing, "NASA Reveals Probable Cause of Mars Polar Lander and Deep Space-2 Mission Failures," *SPACEREF*, March 28, 2000, http://www.spaceref.com/news/viewnews.html?id=105.
32. William Young, and Nancy G. Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory," *Communications of the ACM,* 57(2014): 32, doi:10.1145/2556938.
33. Leveson, Engineering a Safer World.
34. Nancy G. Leveson, and John P. Thomas, STPA Handbook (Published by authors, 2018), http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.
35. Arash Nourian and Stuart Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet," *IEEE Transactions on Dependable and Secure Computing* 15(2018): 2–13, doi:10.1109/TDSC.2015.2509994.

36. Peter G. Neumann, "Computer System Security Evaluation," in *Conference Proceedings of National Computer Conference (NCC)* (American Federation of Information Processing Societies, 1978), 1088, doi:10.1109/AFIPS.1978.53.
37. Nieles, Dempsey, and Pillitteri, "An Introduction to Information Security," 3.
38. Knight, Fundamentals of Dependable Computing for Software Engineers.
39. Ron Ross, Michael McEvilley, and Janet Carrier Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Vol 1," Special Publication (Washington, D.C.: National Institute of Standards and Technology, 2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.
40. Amy F. Woolf, U.S. Strategic Nuclear Forces: Background, Developments, and Issues (Washington, D.C.: Congressional Research Service, 2018), https://fas.org/sgp/crs/nuke/RL33640.pdf.
41. Bruce Blair, Strategic Command and Control, 1st edition (Washington, D.C.: Brookings Institution Press, 1985).
42. TRW Systems ICBM Prime Team, Minuteman Weapons System History and Description (Intercontinental Ballistic Missile (ICBM) System Program Office (SPO), 2001), http://minutemanmissile.com/documents/MinutemanWeaponSystemHistoryAndDescription.pdf.
43. Bruce G. Blair, "Mad Fiction," *The Nonproliferation Review* 21(2014): 239–50, doi:10.1080/10736700.2014.924711.
44. Minuteman Systems Engineering, WS-133A-M Upgrade Wing III and V: Integrated Minuteman Command and Control Systems (Seattle, WA: Boeing Aerospace Company, 1978).
45. ICBM Prime Team, Minuteman Weapons System History and Description.
46. Commander of the Air Force Global Strike Command, "Intercontinental Ballistic Missile (ICBM) Operational Test and Evaluation (OT&E)," Test and Evaluation (Air Force, 2011).
47. Bureau of Arms Control, Verification, and Compliance, "U.S. Nuclear Force Posture and De-Alerting," *U.S. Department of State*, December 14, 2015, https://2009-2017.state.gov/t/avc/rls/250644.htm.
48. Bruce G. Blair, "Mad Fiction." 249, doi:10.1080/10736700.2014.924711.
49. Bureau of Arms Control "U.S. Nuclear Force Posture."
50. Hartnett, "Our Nuclear Phones."
51. Commander of the Air Force, "Intercontinental Ballistic Missile (ICBM)."
52. See rules 15, 19, and 20 in Secretary of the Air Force, "Safety Rules for the Intercontinental Ballistic Missile Systems," Safety, Washington, D.C., 2006, https://cdn.theatlantic.com/static/mt/assets/politics/procedures.pdf.
53. Lt. Col. Andrew S. Kovich, "ICBM Strike Planning," *AAFM Newsletter*, June 2007, 10.
54. According to experts, turning the key in a simple switch for each missile would prevent ignition and offer a simple de-alerting solution for the U.S. ICBMs. See Bruce Blair, "De-Alerting Strategic Forces," in Reykjavik Revisited: Steps toward a World Free of Nuclear Weapons (Stanford, CA: Hoover Institute, 2008), 25–31, http://media.hoover.org/sites/default/files/documents/Drell_Goodby_Schultz_Reykjavik_Revisited_25.pdf; Union of Concerned Scientists, A Simple Method For Taking US Land-Based Nuclear Missiles Off High Alert (Cambridge, MA: Union of Concerned Scientists, 2015), https://www.ucsusa.org/sites/default/files/attach/2015/04/safing-us-nuclear-missiles.pdf.

55. Avizienis et al., "Basic Concepts and Taxonomy" 11–33, doi:10.1109/TDSC.2004.2.
56. Keegan Hamilton, "The Plan to Make America's Nukes Great Again Could Go Horribly Wrong," *VICE News*, April 20, 2017, https://news.vice.com/en_us/article/a3j9mg/the-plan-to-make-americas-nukes-great-again-could-go-horribly-wrong.
57. Ed Heath, "LCC B-01 Command and Control Communications Anomaly Analysis," Hill AFB, UT 84056-5990, Air Force, November 15, 2010, 3, http://speakingtruthtopower.org/Extraction%2017.pdf.
58. John Reed, "Keeping Nukes Safe from Cyber Attack," *Foreign Policy*, September 25, 2012, https://foreignpolicy.com/2012/09/25/keeping-nukes-safe-from-cyber-attack/.
59. Capt. Cory Kuehn, "ALCS 50th Anniversary: Celebrating a Proud Heritage," *AAFM Newsletter*, March 2017.
60. Secretary of the Air Force, "Intercontinental Ballistic Missile Systems."
61. Heath, "LCC B-01 Command and Control Communications Anomaly Analysis."
62. SELECT Integrated Product Team, "WSP CMPG-B Card Anomaly Investigation," Ogden Air Logistics Center, Air Force, published September 1998, http://speakingtruthtopower.org/Extraction%208.pdf.
63. Ibid.
64. "ICBM - EMD FY2013," Exhibit R-2, RDT&E Budget Item Justification, Air Force, published February 2012, 19–20, http://www.dtic.mil/descriptivesum/Y2013/AirForce/stamped/0604851F_5_PB_2013.pdf.
65. National Research Council, Reliability Growth: Enhancing Defense System Reliability (Washington, D.C.: The National Academies Press, 2015), 64, https://doi.org/10.17226/18987.
66. Ibid.
67. Robert F. Behler, "Family of Advanced Beyond Line-of-Sight Terminals (FAB-T)," Annual Report FY2015 (Washington D. C.: The Office of the Director, Operational Test and Evaluation (DOT&E), 2016), http://www.dote.osd.mil/pub/reports/fy2015/pdf/af/2015fab-t.pdf.
68. Mike Gruss, "Raytheon Tops Boeing for FAB-T Production Contract," *SpaceNews.Com*, June 2, 2014, https://spacenews.com/40777raytheon-tops-boeing-for-fab-t-production-contract/.
69. Behler, "Family of Advanced Beyond Line-of-Sight Terminals (FAB-T)," January 2016, 336.
70. Ibid.
71. Matthew Bunn and Scott D. Sagan, eds., Insider Threats, 1st edition (Ithaca, NY: Cornell University Press, 2017).
72. The potential vulnerabilities introduced by inadvertent insiders to computer networks in various commercial and government sectors is addressed in Michael Theis et al., "Common Sense Guide to Mitigating Insider Threats, Sixth Edition" (Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, 2018), https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644.
73. It should be noted that most of these methods would require an insider to collect these leaked transmissions. See Andy Greenberg, "Air Gap Hacker Mordechai Guri Steals Data With Noise, Light, and Magnets," *WIRED*, February 7, 2016, https://www.wired.com/story/air-gap-researcher-mordechai-guri/.
74. Ellen Nakashima, "Cyber-Intruder Sparks Response, Debate," *Washington Post*, December 8, 2011, https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_print.html?noredirect=on.

75. Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair*, March 2011, https://www.vanityfair.com/news/2011/03/stuxnet-201104.
76. James R. Gosler, and Lewis Von Thaer, "Resilient Military Systems and the Advanced Cyber Threat."
77. Thaer. and Gosler, Defense Science Board (DSB) Task Force on Cyber Deterrence. 24.
78. Chaplain, Weapon Systems Cybersecurity.
79. Sanger and Broad, "New U.S. Weapons Systems Are a Hackers' Bonanza."
80. Theresa Hull, Air Force Space Command Supply Chain Risk Management of Strategic Capabilities (Washington, D.C.: Department of Defense, Office of the Inspector General, 2018), https://media.defense.gov/2018/Aug/16/2001955109/-1/-1/1/DODIG-2018-143_REDACTED.PDF.
81. Justin Ray, "Advanced Missile Detection Satellite for Early-Warning Alerts Awaits Liftoff," *SPACEFLIGHT NOW*, January 16, 2017, https://spaceflightnow.com/2017/01/16/advanced-missile-detection-satellite-for-early-warning-alerts-awaits-liftoff/.
82. Jeffrey Lewis, "Is Launch Under Attack Feasible?" *NTI*, August 24, 2017, http://www.nti.org/analysis/articles/launch-under-attack-feasible/.
83. Ray, "Advanced Missile Detection Satellite."
84. Jon Ludwigson, DOD Space Acquisitions: Including Users Early and Often in Software Development Could Benefit Programs (Washington, D.C.: Government Accountability Office, March 2019), https://www.gao.gov/assets/700/697617.pdf.
85. J. Michael Gilmore, FY16 Air Force Programs, Space-Based Infrared System Program, High Component (SBIRS HIGH) (Washington, D.C.: Office of the Director, Operational Test & Evaluation, December 2016), https://www.dote.osd.mil/pub/reports/FY2016/pdf/af/2016sbirs.pdf.
86. "Information Technology: Federal Agencies Need to Address Aging Legacy Systems," U.S. Government Accountability Office, Published on May 25, 2016, https://www.gao.gov/products/GAO-16-468.
87. Maj. Gen. Garrett Harencak, The Requirements and Contributions of Nuclear Deterrence (speech, Air Force Association, National Defense Industrial Association and Reserve Officers Association Capitol Hill Forum, Washington D.C., 2015), http://higherlogicdownload.s3.amazonaws.com/AFA/6379b747-7730-4f82-9b45-a1c80d6c8fdb/UploadedImages/Events/Heussy/051315afaharencakfinal.pdf; Sandra Erwin, "Q&A: Air Force Gen. John Hyten Says U.S. Space Strategy, Budget Moving 'down the Right Path,'" *SpaceNews.Com*, April 3, 2018, http://spacenews.com/qa-air-force-gen-john-hyten-says-u-s-space-strategy-budget-moving-down-the-right-path/.
88. Hamilton, "The Plan to Make America's Nukes Great Again Could Go Horribly Wrong."
89. Over the years, a variety of floppy drive sizes have been introduced. Newer floppy drives tend to be smaller and have more storage space than older drives, like those found in certain nuclear command and control systems (see David A. Powner, Information Technology: Federal Agencies Need to Address Aging Legacy Systems, U.S. Government Accountability Office, Published on May 25, 2016, https://www.gao.gov/products/GAO-16-696T) Security concerns are similar for all floppy drives, regardless of size.
90. Chris Hoffman, "How AutoRun Malware Became a Problem on Windows, and How It Was (Mostly) Fixed," *How-To Geek*, https://www.howtogeek.com/203522/how-autorun-malware-became-a-problem-on-windows-and-how-it-was-mostly-fixed/.
91. Joseph Cox, "The World's First Ransomware Came on a Floppy Disk in 1989," *Motherboard*, 12 April 2017, https://motherboard.vice.com/en_us/article/nzpwe7/the-worlds-first-ransomware-came-on-a-floppy-disk-in-1989.

92. A DARPA analysis in 2011 found that the size of most malware since the 1980s is about 125 lines of code. See Dan Kaufman, An Analytical Framework for Cyber Security (Colloquium on Future Directions in Cyber Security, Arlington, VA, 7 November 2011), http://www.dtic.mil/dtic/tr/fulltext/u2/a552026.pdf.
93. Janice Hill and Rhoda Gaggs, "Software Safety Risk in Legacy Safety-Critical Computer Systems," in Proceedings 2007 IEEE SoutheastCon (SoutheastCon 2007, Richmond, VA: IEEE Publishing, 2007), 229–232, doi:10.1109/SECON.2007.342891.
94. This was the case when hackers used various medical devices to penetrate and remove data from hospital networks: Alan Grau, "Hackers Invade Hospital Networks Through Insecure Medical Equipment," *IEEE Spectrum: Technology, Engineering, and Science News*, June 12, 2015, https://spectrum.ieee.org/view-from-the-valley/biomedical/devices/hackers-invade-hospital-networks-through-insecure-medical-equipment.
95. Robert F. Behler, "FY18 Cybersecurity," DOT&E FY2018 Annual Report (Washington, D.C.: Office of the Director, Operational Test & Evaluation, 2018), 231, https://www.dote.osd.mil/pub/reports/FY2018/pdf/other/2018cybersecurity.pdf.
96. Felix Redmill, "The COTS Debate in Perspective," in *Computer Safety, Reliability, and Security* (SAFECOMP 2001, Budapest, Hungary: Springer, 2001), 119–129, https://dl.acm.org/citation.cfm?id=724850.
97. S. Bhasin, and F. Regazzoni, "A Survey on Hardware Trojan Detection Techniques," in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2015: 2021–2024, doi:10.1109/ISCAS.2015.7169073.
98. Hull, "Air Force Space Command Supply Chain Risk Management of Strategic Capabilities," ii.
99. Commander of the Air Force, "Intercontinental Ballistic Missile (ICBM) Operational Test and Evaluation (OT&E)."
100. Chris Graham, "NHS Cyber Attack: Everything You Need to Know about 'biggest Ransomware' Offensive in History," *The Telegraph*, 13 May 2017, https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.
101. Zia Mian, M. V. Ramana, and R. Rajaraman, "Plutonium Dispersal and Health Hazards from Nuclear Weapon Accidents," *Current Science* 80(2001): 1275–1284.
102. Eric Schlosser, Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety, Reprint edition (New York, NY: Penguin Books, 2014).
103. David E. Hoffman, "Review: The Fear Factor," *Foreign Policy*, July 8, 2010, https://foreignpolicy.com/2010/07/08/the-fear-factor-2/.
104. Geoffrey Forden, "False Alarms in the Nuclear Age," *NOVA PBS*, November 6, 2001, http://www.pbs.org/wgbh/nova/military/nuclear-false-alarms.html.
105. See reference 15 in Bruce Blair, "Strengthening Checks on Presidential Nuclear Launch Authority," *Arms Control Today*, January 4, 2018, https://www.armscontrol.org/act/2018-01/features/strengthening-checks-presidential-nuclear-launch-authority#endnote15.
106. Ray, "Advanced Missile Detection Satellite."
107. Michael D. Wallace, Brian L. Crissey, and Linn I. Sennott, "Accidental Nuclear War: A Risk Assessment," *Journal of Peace Research* 23(1986): 9–27, doi:10.1177/002234338602300102.
108. Blair, "Checks on Presidential Nuclear Launch Authority."
109. Dave Merrill, Nafeesa Syeed, and Brittany Harris, "To Launch a Nuclear Strike, President Trump Would Take These Steps," *Bloomberg*, January 20, 2017, https://www.bloomberg.com/politics/graphics/2016-nuclear-weapon-launch/.
110. Perrow, Normal Accidents: Living with High-Risk Technologies.