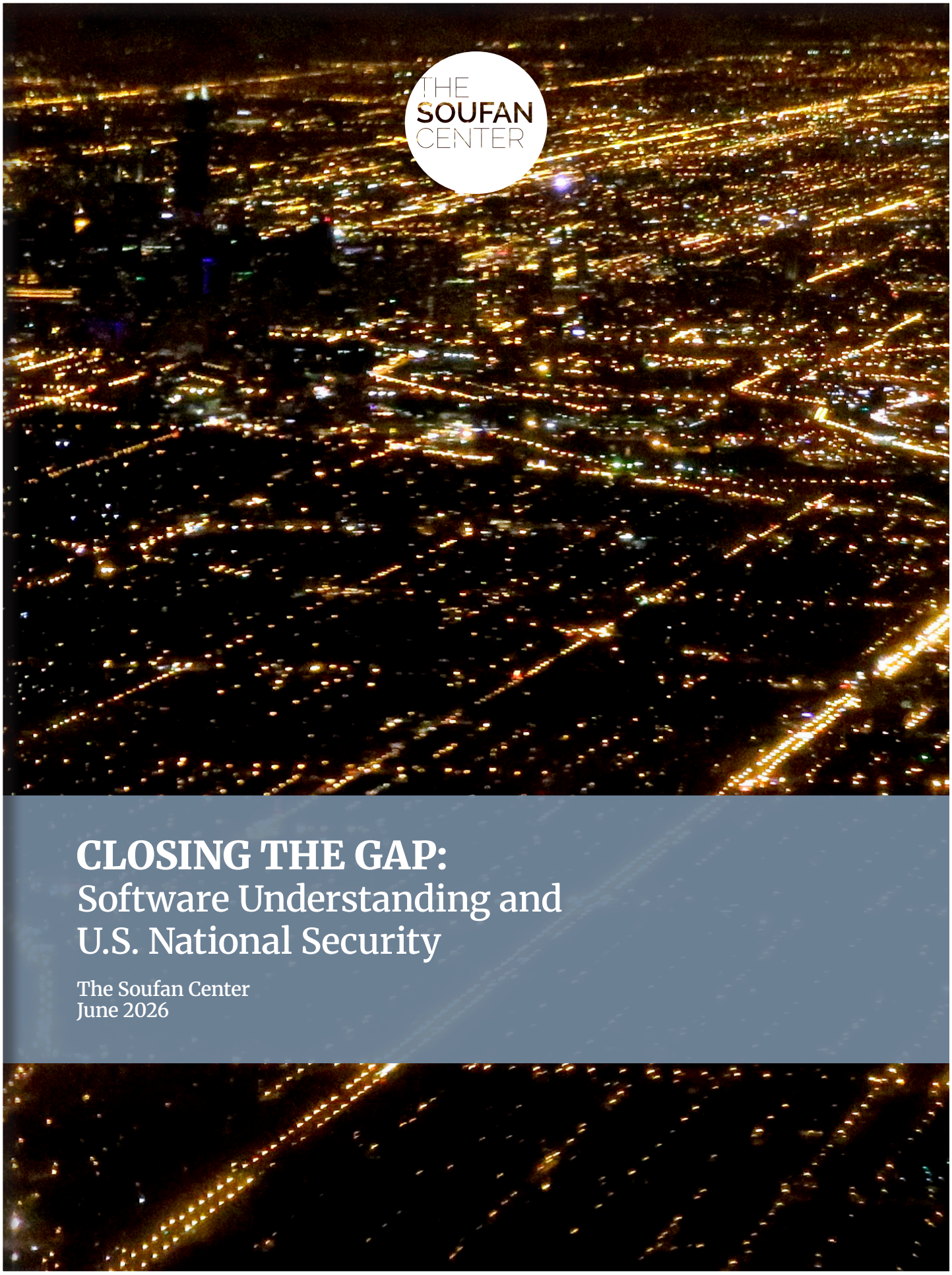

CLOSING THE GAP:
Software Understanding and U.S. National Security

The Soufan Center
June 2026

CLOSING THE GAP:
Software Understanding and U.S. National Security

The Soufan Center

June 2026

Cover Image: Associated Press

TABLE OF CONTENTS

Executive Summary

The Software Understanding Imperative

Software is an integral part of every dimension of U.S. national security and civil society. The United States' ability to project force and defend its interests depends on the proper and safe functioning of software-defined systems. Yet, our ability to understand, verify, and reason about software has been dramatically outpaced by its production and uptake. This has resulted in what is known as the *software understanding gap*. Because of the increasing prevalence and importance of software to U.S. national interests, and the risks associated with insufficient understanding of software-defined systems, closing this gap has become a national security priority. The U.S. Senate Armed Services Committee has recently directed the Department of War to develop a comprehensive strategy to transition formal methods research into production environments across the department, a concrete first step toward securing the software-defined systems that underpin U.S. national security. This report examines how the software understanding gap intersects with U.S. national security and the related implications. It concludes with a set of recommendations designed to close the software understanding gap and mitigate the challenges and risks identified in this report.

Expanded Risks

U.S. dependence on software-defined systems has given rise to national security risks across six dimensions, all of which have been exploited to varying degrees and in multiple ways by a range of actors, including Russia, Iran, the People's Republic of China (PRC), the Democratic People's Republic of Korea (DPRK), and an expanding set of non-state actors:

- **Ballooning Attack Surfaces**: A dramatic increase in the number of possible points of unauthorized entry and exploitation available to adversaries. For example, the PRC, through *Salt Typhoon,* infiltrated U.S. telecommunications provider systems for years, exploiting critical infrastructure in ways that would not have been possible only a generation ago.
- **Cascading Interdependencies**: Risk in one software-defined system leads to risk in multiple systems across domains. The *NotPetya* malware, initially deployed against Ukrainian government targets, spread global ly and crippled the Danish shipping giant Maersk, while disrupting the operations of the pharmaceutical company Merck, and the logistics firm FedEx.
- **Tyranny of Nearness**: Time and distance have effectively collapsed in the cyber domain which, in turn, has made defense, critical infrastructure, and civilian systems that were traditionally out of range now potential targets. Iran, a country with negligible conventional power projection capabilities has, through the exploitation of software-defined systems, been able to remotely infiltrate a water provider in a small town in Pennsylvania.
- **Tactical Becomes Strategic**: Low-level attacks can carry great strategic consequences. The PRC, through *Volt Typhoon*, pre-positioned itself within U.S. utilities and transportation hubs. Rather than causing immediate disruption, these kinds of penetrations are more likely precursors to a future, pre-positioned cyberattack in the event of a conflict over Taiwan.
- **Inured Blindness**: The scale and complexity of software-defined systems that underpin U.S. national security often hide intrusions for extended periods, granting adversaries the freedom to act strategically at the time of their choosing, before defenders are even aware a breach has occurred. Russia's *SolarWi nds* supply chain intrusion, which injected malicious code into third-party software updates distributed

to thousands of government agencies and private companies, went undetected for nearly a year, providing Russia with long-term covert access to sensitive systems.

- **Banality of Cybercrime and Cyber-espionage**: Unlike attacks in the physical domains, attacks on software-defined systems occur so frequently—because they are both low-risk and high-reward—that a normalization of cybercrime and cyber-espionage has emerged. China's systematic cyber-espionage campaigns have exfiltrated vast quantities of intellectual property, defense secrets, and personal data from U.S. government and private sector targets. North Korean cyber actors have stolen billions of dollars through cybercrime that has gone directly towards funding its weapons programs, while various non-state actors have developed new approaches to cybercrime that allow them to adapt and remain ongoing concerns.

Closing the Gap

Entire classes of risks can be mitigated if not eliminated altogether, through the application of improved software understanding across missions and systems critical to U.S. national security. However, closing the gap requires intentional, sustained investment and will be an uneven, long-term process that will inevitably lead to changes in threat actor behavior. As higher-priority targets are hardened, adversaries are likely to adapt by attacking lower-profile and more distributed targets. Nonetheless, these targets can also be hardened over time, through a sustained, well-structured and interagency approach to closing the gap.

Recommendations

An "Everyone and Everywhere Problem": The U.S. government must empower coordinated interagency software understanding advancement through a permanent body with real authority and resources, treat software understanding as a mission requirement integrated into operational planning and acquisition, and deploy formal methods for both forward and reverse software understanding.

Deferred Costs are Now Coming Due: Realign market incentives by tying rigorous security standards to government software acquisition requirements and employ formal verification techniques throughout the software development lifecycle.

Closing the Gap is Necessary but Not Sufficient: Take steps to reduce ambiguity and enforce accountability in the cyber domain at all levels and prepare for adaptive adversaries who will shift to lower-profile but higher-volume targets as major systems are hardened.

Abbreviations

AI	Artificial Intelligence
APT	Advanced Persistent Threat
C2	Command and Control
CCP	Chinese Communist Party
CISA	Cybersecurity and Infrastructure Security Agency
CVE	Common Vulnerabilities and Exposures
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DOD	Department of Defense
DOW	Department of War
DPRK	Democratic People's Republic of Korea (North Korea)
FBI	Federal Bureau of Investigation
FIS	Foreign Intelligence Service (*Sluzhba Vneshney Razvedki* or SVR) (Russia).
GRU	Glavnoye Razvedyvatelnoe Upravlenie (Main Directorate of the General Staff of the Armed Forces of the Russian Federation—Formerly the Main Intelligence Directorate) (Russia)
GAO	Government Accountability Office
ICS	Industrial Control Systems
IT	Information Technology
MOIS	Ministry of Intelligence and Security
NSA	National Security Agency
PRC	The People's Republic of China (China)
RGB	Reconnaissance General Bureau (North Korea)
SUNS	Software Understanding National Security
SUNSEC	Software Understanding National Security (Committee)
TTPs	Tactics, Techniques, and Procedures

Introduction

Software is ubiquitous in modern life and plays an essential role in the proper and secure functioning of national security apparatuses and the missions they support.[1] Ensuring that the software used for these purposes is functional, safe, and secure requires what the Cybersecurity and Infrastructure Security Agency (CISA), Defense Advanced Research Projects Agency (DARPA), the U.S. Department of Defense/War (DOD/DOW), and the U.S. National Security Agency (NSA) define as software understanding or, "the rigorous practice of constructing and assessing software-controlled systems to verify their functionality, safety, and security by design across all conditions—normal, abnormal, and hostile."[2] It is important to note that software understanding is not limited to identifying vulnerabilities. It also includes detecting malicious behavior, a distinct challenge since malicious code does not always resemble a technical flaw and what constitutes malicious behavior depends heavily on context. Because the pace of software development and its implementation in traditional national security spaces—and elsewhere—has outpaced our ability to comprehend software's characteristics across all these conditions, there now exists a software understanding gap.[3] (See Figure 1.) Given software's pervasiveness throughout and across all levels and dimensions of the national security ecosystem, this is an urgent problem that is growing rapidly. While difficult to quantify, the potential effects of this gap are catastrophic across all segments of national security and critical infrastructure; they are significant and urgent enough to have prompted the U.S. Senate Armed Services Committee to direct the Department of War (Defense) to develop a "comprehensive strategy for transitioning DARPA's formal methods research investments into production environments across the DOD" as a means of addressing the gap.[4] National security functions and systems are now deeply software-defined, and the risks posed by the software understanding gap are present and growing. Evaluating the potential and actual effects of the gap, while also developing policies (e.g., software development requirements), capabilities and practices (e.g., formal methods),[5] and procedures (e.g., data sharing agreements) to mitigate the effects of the gap, is not just prudent but of vital importance.

1 We define national security very broadly in this report because of the increasingly growing interrelationships and interdependencies amongst numerous sectors of importance to security in American society. We argue that many of these interdependencies are due to 1) the prevalence and predominance of software-defined systems in and to virtually all aspects of American life (creating interlinkages) and 2) because of software-defined systems' criticality to the pursuit and protection of U.S. national interests (creating mutual dependencies and vulnerabilities). We submit that it is increasingly difficult if not impossible to isolate various sectors or functions of society—even those that prima facie might seem relatively trivial, like local sewage and water treatment infrastructures—that conceivably are not or cannot be related to national security. The integrity and proper functioning of software-defined systems is the sine qua non of so many individual and collective aspects of American life—from defense and law enforcement to critical infrastructure to personal shopping and even recreation—that the interdependencies and vulnerabilities within and among these sectors cannot be disaggregated in a way that meaningfully isolates national security from various social functions that in a previous era may have been considered a subset of national interests but almost entirely unrelated to national security.

2 Closing the Software Understanding Gap, Washington, D.C.: Cybersecurity & Infrastructure Security Agency, Defense Advanced Research Projects Agency, U.S. Department of Defense, and the National Security Agency, January 16, 2025, p. 3. See also a comprehensive discussion of the software understanding gap and options for addressing this gap in Douglas Ghormley, Tod Amon, Christopher Harrison, and Tim Loffredo, SUNS: The National Need for Software Understanding: The Present Crisis, Technical Capability Gaps, and Path Forward, Albuquerque, New Mexico: Sandia National Laboratories, March 25, 2025.

3 Described as "a gap that exists because of our ability to build software greatly outstrips our ability to understand it." Douglas Ghormley, Tod Amon, Christopher Harrison, and Tim Loffredo, SUNS: The National Need for Software Understanding: The Present Crisis, Technical Capability Gaps, and Path Forward, Albuquerque, New Mexico: Sandia National Laboratories, March 25, 2025, p. 17.

4 U.S. Senate Committee on Armed Services, National Defense Authorization Act for Fiscal Year 2026, Report 119-39, Washington, D.C.: United States Senate Committee on Armed Services, July 15, 2025, p. 310. Several high-level reports and executive policy documents make this case. See, for instance, The White House, Back to the Building Blocks: A Path Toward Secure and Measurable Software, Washington, D.C.: The White House, February 2024.

5 Formal methods are "system design techniques that use rigorously specified mathematical models to build software and hardware systems. In contrast to other design systems, formal methods use mathematical proof as a complement to system testing in order to ensure correct behavior." Michael Collins, "Formal Methods," Pittsburgh, Pennsylvania: Carnegie Mellon University, 1998. As of March 5, 2026: https://users.ece.cmu.edu/~koopman/des_s99/formal_methods/.

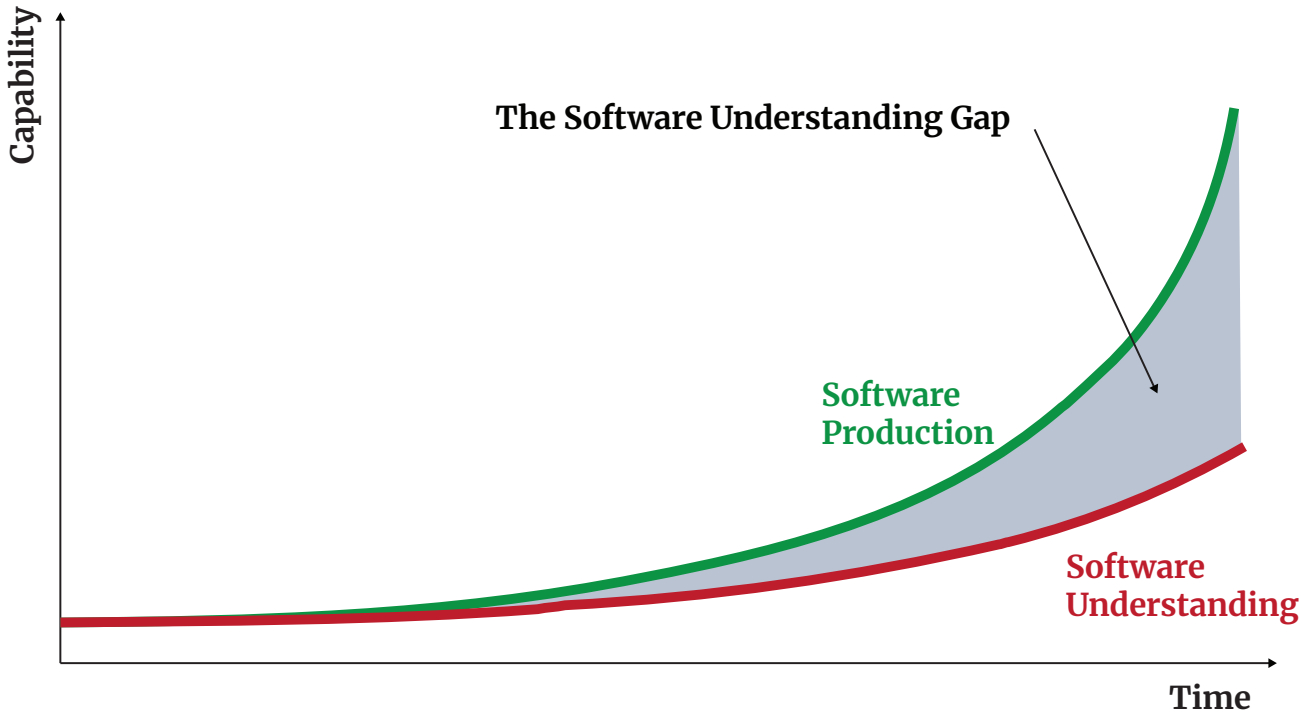

Figure 1. The Software Understanding Gap

Note: This is a conceptual representation of the software understanding gap, where "the ability to produce software has outstripped our ability to adequately understand it." The gray space between "software understanding" in red and "software production" in green, is the graphical representation of the software understanding gap.

Source: Douglas Ghormley, Tod Amon, Christopher Harrison, and Tim Loffredo, SUNS: The National Need for Software Understanding—The Present Crisis, Technical Capability Gaps, and Path Forward, Albuquerque, New Mexico: Sandia National Laboratories, March 25, 2025, p. 17.

To explore this topic and expose the intricacies and nuances of these relationships further, we leveraged a range of data sources including expert interviews, primary and secondary literatures, and a set of cases that are topical, of central value, and considered high-risk to U.S. national security. Our central research question—how does the software understanding gap intersect with U.S. national security?—guided our interview questions and our examination of literature and helped us frame our supporting research questions. Answering our first research question (how does software fit within the larger national security apparatus?) (it is ubiquitous) helped us to develop our subsequent research questions (See Table 1).

Central Research Question	**How does the software understanding gap intersect with U.S. national security?**
Supporting Research Question #1	**How does software fit within the larger national security apparatus?**
Supporting Research Question #2	**To what degree is national security dependent on the integrity and proper functioning of cyber-physical systems and how has this dependency unfolded/grown?**

Supporting Research Question #3	**How has dependency on cyber-physical systems affected or altered traditional conceptions of or approaches to national security, i.e., what notable changes have emerged, and what are their implications?**
Supporting Research Question #4	**How do the effects of cyber-physical system dependency manifest in salient geopolitical contexts?**
Supporting Research Question #5	**What are the policy implications of these manifestations/how do we resolve the software understanding gap?**

Table 1. Research Questions

Our second question was to what degree is national security dependent on the integrity and proper functioning of cyber-physical systems, and how has this dependency unfolded/grown? (it is entirely dependent). Answering this unveiled a process by which successive decisions further deepened U.S. national security dependence on cyber-physical systems while limiting options to reverse course.

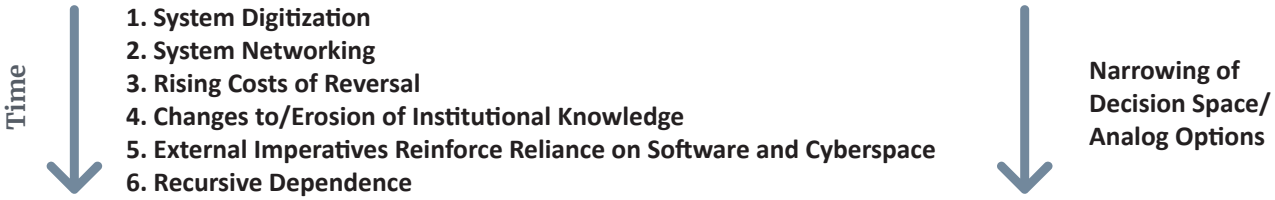

Figure 2. Process and Dimensions of Crossing the Cyber-Rubicon

Source: The Soufan Center analysis.

Exploring the range of possibilities raised by our third question (how has dependency on cyber-physical systems affected or altered traditional conceptions of or approaches to national security, i.e., what notable changes have emerged, and what are their implications?) exposed numerous risks relating to cyber-physical systems, which have led to greater complexity, uncertainty, and instability within the national security ecosystem.

Our fourth question (how do the effects of cyber-physical system dependency manifest in salient geopolitical contexts?) required us to examine how major U.S. adversaries (Russia, Iran, the People's Republic of China (PRC), the Democratic People's Republic of Korea (DPRK), and several non-state actors) engage in cyber-related activities and then project the effects of closing the software understanding gap on these activities. It should be noted that one of these activities stands out for its perniciousness in the cyber domain: pre-positioning, which comprises gaining access to a network or system to be used for future malicious activity. While pre-positioning has analogues in the physical domain, the inscrutability of software makes detecting it vastly more difficult, and the cost and risk to the adversary are incomparably lower. This asymmetry makes cyber pre-positioning uniquely dangerous, particularly in pre-crisis or crisis situations, where an attacker can cause unforeseen destabilizing effects on a range of targets. Knowing that this is possible (it has been demonstrated by several countries, including those examined in this report) can give a defender pause, disrupt planned responses in a contingency, or even deter an actor (loss of confidence in systems or fear of the unknown, causing a change in escalatory calculations). Compounding this, cyber activities are not always attributable, as a clever malicious intrusion can be indistinguishable from poor-quality code, leaving defenders uncertain whether they face an adversary or their own system's failures.

Answering our final question (what are the policy implications of these manifestations/how do we resolve the software understanding gap?) helped us identify three major and outstanding issues and develop associated recommendations:

Issue 1: The Software Understanding Gap is an "Everyone" and "Everywhere" Problem and Must be Resolved to Help Reduce U.S. Cyber Risk and Improve its National Security Posture.

- Recommendation 1.1: Establish Interagency Coordination, Identify Stakeholders, and Prioritize Efforts to Address the Software Understanding Gap.
- Recommendation 1.2: Treat Software Understanding Capabilities as a Mission Requirement.
- Recommendation 1.3: Implement Forward and Reverse Software Understanding Capabilities Using AI-enabled Formal Methods.
- Recommendation 1.4: Enable Zero-Friction Sharing to Promote Grassroots Solutions and Cooperation.
- Recommendation 1.5: Establish Software Understanding Interoperability Agreements with International Partners.

Issue 2: The Way Software Development Evolved was Premised on a Market Model and Incentives that Deferred Costs that are Now Coming Due.

- Recommendation 2.1: Create the Conditions to Realign Incentives Across Relevant Sectors.
- Recommendation 2.2: Employ Formal Verification Techniques in Software Development and Analysis.
- Recommendation 2.3: Conduct Cost Scoping that Accounts for the Value of Mission Success, the Mission Risk from Software Vulnerabilities, and Upfront Investments in Software Understanding Capabilities.

Issue 3: Closing the Software Understanding Gap is Necessary but Does Not Entirely Eliminate Risk.

- Recommendation 3.1: Take Steps that Reduce Ambiguity and Enforce Accountability in the Cyber Domain, at All Levels.
- Recommendation 3.2: Prepare for Adaptive Adversaries, Particularly Non-State Actors that Will Attack Low-Hanging Fruit.
- Recommendation 3.3: Establish Mechanisms to Continuously Monitor Evolving Risks, Operational Conditions, and Adversary Behavior Across the Cyber Domain.

The United States has enjoyed a degree of relative economic and technical dominance for decades, and because of this has also held and maintained a position of preeminence in geopolitics and manifold areas of importance to national and international security, particularly in the four physical operational domains of air, land, sea, and space. U.S. preeminence now, however, relies increasingly on the fifth domain of cyberspace and related capabilities, all of which have advanced in tandem with the exponential growth and use of software. Throughout the post-Cold War period, the United States has been able—across all segments of society—to accrue the benefits of the low material costs and rapid production rates of software and software-defined systems. However, the rapid incorporation of software into national security and critical infrastructure systems occurred before a full understanding had emerged regarding the scale, persistence, and strategic implications of software risk. Now, the bill for this is coming due. Vulnerabilities that could have been accepted as a cost of doing business in previous periods can no longer be treated as such—not because the risks were fully understood and consciously accepted at the time, but because our collective understanding of these risks has evolved significantly, as has the adver-

sary's ability and willingness to take advantage of them. The cause for this is clear: the United States has crossed a cyber-Rubicon and it is now dependent on the cyber domain—and its attendant peculiarities and risks—for the pursuit of its national interests and security.[6] The depth of this dependence and its implications are drastic as the challenges posed in and through cyberspace are compounded by a lack of software understanding commensurate with its importance to the plurality of national interests.

The objective of this report is to help inform policymakers of the implications of the software understanding gap in U.S. national security and to make recommendations that help maintain U.S. dominance across all operational domains and in all geopolitical contexts.[7] It identifies six general risks of dependence on software-defined systems and how these risks manifest in specific geopolitical situations. The report concludes with an identification of major issues and recommendations for how to mitigate these issues.

6 It should also be noted that "historically, the U.S. military achieved and maintained a dominant C3 [command, control, and communications] technological advantage, but peer competitors and adversaries have closed the gap." U.S. Department of Defense, DOD Command, Control, and Communications (C3) Modernization Strategy, Washington, D.C.: U.S. Department of Defense, September 2020, p. i.

7 In respect to all geopolitical contexts and given the nature of cyberspace and the interdependent vulnerabilities inherent to the domain, there is an argument to make regarding software understanding and potential shared vulnerabilities among allies and other partners. While we do not make this argument here, it should be noted that where there is an imbalance or unevenness in cyberspace interoperability among allies, shared vulnerabilities will also be present to varying degrees. That is, even were the United States to close the software understanding gap (or vice versa, if its allies were to do so), it could still potentially suffer from those cyberspace vulnerabilities that its allies possess; this could occur directly (a partner connected to a shared network) or indirectly (a partner losing necessary or useful capabilities in other domains because of cyber vulnerabilities).

Expanded Risks of Software-Defined Systems

U.S. dependence on software-defined systems has led to an expanded set of risks.[8] The exposure of these risks has modified how we conceive of conflict and how it is practiced—chiefly, what is targetable, when it is targetable, who is doing the targeting, and the range of potential effects achievable through an attack. In the following sections, we evaluate these risks from three different angles. First, we discuss six general but salient geopolitical risks that have emerged from or grown out of U.S. dependence on software-defined systems. Second, we place these risks in context by evaluating specific cases and instances where each has manifested in real-world conditions and by discussing their implications on U.S. (and international) security. Third, we discuss how we expect these risks to change and evolve (second and third order effects) once the United States begins to close the software understanding gap. Because closing the software understanding gap is not a "silver bullet," we wanted to extrapolate from our cases and examples and provide policymakers with a grounded roadmap of expected adversary and competitor adaptations and behaviors.

General Geopolitical Risks

Ballooning Attack Surfaces

An attack surface is the range of possible vulnerabilities or vectors in a system that can be exploited or attacked. As software-defined systems have proliferated, the attack surface has expanded, resulting in three significant changes. First, the democratization of possible targets in and through software that is embedded in civilian life (what would have been termed countervalue targets in a previous era, inclusive of critical infrastructure but also many elements of civil society and everyday life). These targets are not only more plentiful than their military counterparts, but also "softer" and constitute a more diverse range of functions and capabilities. Second, not only has the number of civilian (and military) targets subject to attack grown, but they are also more frequently "in range"; that is, devices, systems, weapons, sectors, and so forth, that in previous eras would not have been subject to an attack can now be attacked stealthily, by numerous actors, and from long distances. Until just a few decades ago, many activities and functions (e.g., civilian banking functions) were effectively insulated from military attack, while others could only be targeted when within the range of a kinetic weapon (e.g., artillery or other battlefield systems). Outside of general war, strategic weapons, or direct battlefield exchanges, such systems were not realistically targetable. Third, even if adversaries' capabilities do not increase in the cyber or physical domains, their ability to exploit U.S. vulnerabilities will grow nonetheless as critical infrastructure, military systems, and economic functions become increasingly software-defined. As a result, not only are more assets targetable, but they are also subject to multiple forms of attacks from different actors and at varying distances. Further, cyber effects are not always attributable and are far more deniable than kinetic attacks, lowering the potential cost to adversaries and complicating U.S. response options. Taken together, this can have an adverse psychological impact: a vast attack surface that cannot be fully secured or understood means that not just military planners but also civilians cannot have full certainty that a software-defined system is not presently or might not in the future be compromised.

Cascading Interdependencies

Because the pervasiveness of cyber-physical systems across national security apparatuses is proportional to their criticality, the risk of failure in the cyber domain is potentially cascading, comprehensive, and catastrophic. Complex interconnections of software (e.g., transitive dependencies) and the continued search for efficiencies in software production have created vulnerabilities throughout cyber-enabled systems that are subject to attack, accident,

8 We acknowledge that because there is overlap and interlinkages between these effects, the following lists should not be considered as mutually exclusive (nor exhaustive) and are broken into constituent parts here for the sake of analysis and discussion.

and degradation or failure.[9] And when these systems are not working properly, operations in the other domains will be substantially degraded as well. A prolonged power outage, for instance, cascades rapidly into banking, emergency response, and transportation failures. Attackers can also exploit these interconnections deliberately, as when an adversary compromises a peripheral networked device such as a residential climate control system to pivot into core information technology (IT) infrastructure. This kind of dependency is unique insofar as disruptions in other non-cyber operational domains will neither necessarily nor directly cause similar cross-domain effects.

The Tyranny of Nearness

For millennia, one of the principal constraints of warfare has been the geographic distance separating warring forces and their societies. Distance influences command and control, logistical support, weapon-system effectiveness, and a host of other factors of import to hostile parties. Over time, the constraints imposed by distance were reduced by various mechanical inventions and advances in telecommunications.[10] As a result, by the early to mid-20th Century, command and control over forces at great distances and across vast areas became the norm: these forces could move further and faster and attack targets at longer range and with greater speed and effect than ever before. The advent of the intercontinental ballistic missile and advanced guidance systems, as well as satellite communications and imagery, further reduced these constraints and put a wide range of targets within reach, not just at long (or short) range but also at incredible speed.[11] The cyber domain radically changes this calculus—time and distance have, in essence, collapsed in this domain as targets connected to software-defined systems can conceivably be reached in seconds,[12] regardless of the distance between the attacker and the target. Furthermore, if a network penetration is persistent, an attacker can "loiter" in a defender's space for long periods without having to consider the logistical constraints inherent in operations conducted at a distance in the physical operational domains.

The Tactical Becomes the Strategic

One consequence of ballooning attack surfaces, cascading interdependencies, and the collapsing of traditional physical constraints in cyber-enabled conflict is the elevation of what once might have been considered tactical or low-level/low-consequence events to strategic importance.[13] Consider, for instance, the malfunctioning or loss of command over various industrial control systems (ICS)[14] in critical infrastructure or communications networks. Normally, such failures might cause disruptions that could be controlled or otherwise mitigated, but during a national emergency, these disruptions could prove catastrophic. In both instances, software-defined systems can conceivably enable an attacker[15] to disrupt these systems across broad geographies, in a way that the disruption might not even register as an attack. In either event, scenarios that might not have even been considered in pre-

9 As a Hoover Institution report notes, "As complexity hides interdependence(s), ergo complexity is the enemy of security." Daniel E. Geer, Jr., "A Rubicon," Aegis Series Paper No. 1801, Stanford, California: Hoover Institution, 2018, p. 1.

10 Including mechanized vehicles, variously powered ships, air transport, and a variety of long-range terrestrial and space-based communications capabilities.

11 Estimates for the U.S. Minuteman III land-based missile give it a range of 6,000 miles and a top speed of 15,000 miles per hour, meaning that it can hit targets in other continents within about 25-30 minutes from launch with devastating effects. See, "How Far Can Nukes Travel? Missile Ranges Explained," ScienceInsights, March 7, 2026. As of March 8, 2026: https://scienceinsights.org/how-far-can-nukes-travel-missile-ranges-explained/.

12 This of course assumes a vector, discovered vulnerability, exploit, and means for delivering a payload.

13 For instance, while the security of traffic lights or other commonplace transportation control mechanisms might seem unimportant when considering the broader national security landscape, there are certain potential quick-response contingencies where a widespread loss of command over these kinds of mundane functions might delay or confuse a national response just long enough to make the event a fait accompli.

14 See, for instance, the discussion of attacks on supervisory control and data acquisition systems in Isaac R. Porche III, Jerry M. Sollinger, and Shawn McKay, A Cyberworm that Knows no Boundaries, Santa Monica, California: RAND Corporation, 2011, p. 1.

15 The attacker(s) in this case might be a state or another actor as offensive capabilities are now available for purchase. See, Jen Roberts and Emma Schroeder, "Makings of the Market: Seven perspectives on offensive cyber capability proliferation," Atlantic Council, March 1, 2023. As of March 8, 2026: https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/makings-of-the-market-seven-perspectives-on-offensive-cyber-capability-proliferation/.

vious strategic contingency planning—because they were not possible—are now at least imaginable and could prove significant if numerous tactical attacks are conducted at scale simultaneously.[16]

Inured Blindness

The scale and complexity of modern software-defined systems have created a form of strategic blindness in which states and organizations may not fully understand what is at risk within their own systems until it is far too late. High (and low) profile attacks that would have been prosecuted through the physical domains in a previous era—and accordingly detected and attributed quite easily—can now occur without warning and might even go undiscovered for quite some period. Many of these threats remain undiscovered because malicious activity can blend into the immense volume of routine activity occurring within the system. The potential value of these ubiquitous and seemingly benign cyber-physical systems can be enormous. If compromised, these systems can provide adversaries with sensitive information and access to higher-value networks that previously would have required costly or high-risk operations to obtain.

The Banality of Cybercrime and Cyber-espionage

Cyber-crime and cyber-espionage have become relatively commonplace and affect not just government organizations but also corporations, small businesses, and individuals. Both are low-risk, high-reward activities that allow criminals to exploit simple vulnerabilities while remaining largely anonymous in the process. While cyberattacks are generally never ignored (if discovered), they occur so frequently and, for the most part, have been treated passively. These activities are conducted by state and non-state actors alike and can be highly disruptive. In some cases, the motive is profit and in others it is the value of the information that is obtainable through software-defined systems. What separates these activities from their counterparts in the physical domains is the relative ease with which they can now be conducted and the volume of highly sensitive information that can be stolen or manipulated quickly and at relatively low cost through software-defined systems—neither of which would have been possible if conducted through physical means.

Specific Geopolitical Risks (Russia, Iran, the PRC, the DPRK, and Non-State Actors)

This section examines how the six risks we identified in the previous section have unfolded in specific contexts of high relevance to U.S. national security (i.e., Russia, Iran, the PRC, the DPRK, and non-state actors). The following analyses are meant to paint a sober and balanced picture of what can be expected in the absence of software understanding based on the empirical record as opposed to hypothesizing or speculating about worst-case scenarios that are difficult at best to divine from the range of possibilities, which seem nearly infinite based on the complexity of the cyber domain, specifically, and of conflict in general. It should be noted that the examples provided are not necessarily mutually exclusive and should therefore not be considered in isolation. For instance, attacks on software-defined systems and intrusions into cyber-physical systems might take advantage of ballooning attack surfaces, which then lead to disruptions caused by cascading interdependencies, resulting in tactical attacks or intrusions with strategic effects.

16 This recalls an adversarial version of Krulak's strategic corporal, except in this case a complex environment combined with cyber capabilities enables various actors to deliberately engage in tactical attacks with the potential to create strategic effects. See discussion in Franklin Annis, "Krulak Revisited: The Three-Block War, Strategic Corporals, and the Future Battlefield," Modern War Institute at West Point, February 3, 2020. As of March 23, 2026: https://mwi.westpoint.edu/krulak-revisited-three-block-war-strategic-corporals-future-battlefield/.

Ballooning Attack Surfaces

The consequence of ballooning attack surfaces is that a greater number of targets of more types can be rapidly attacked by more actors in more ways than would otherwise be possible. In practice, this often, but not solely, leads to "soft-underbelly" attacks or intrusions into civilian cyber-physical systems affecting tens of thousands of organizations and potentially millions of individuals. The exploitation of these risks has been highly consequential and has resulted in cyber-physical system compromises, data loss and exposure, criminal extortion, and numerous other malign consequences.

Case/Country	Examples and Discussion
Russia	The *SolarWinds* intrusion of 2019 by Russia's Foreign Intelligence Service (FIS or SVR) compromised the systems of private companies and U.S. federal government agencies by using a software product of a trusted U.S. third-party network management vendor to breach and gain a foothold into thousands of downstream networks.[17] Russia has also targeted Western logistics and technology companies that have ties to the war in Ukraine, exploiting common vulnerabilities and exposures (CVEs), internet-facing infrastructure, and credential weaknesses in the systems of these companies.[18] **Implications**: ***Russia has exploited weaknesses in software-defined systems to support its objectives in ways that would not be possible through the physical operational domains, including the interdiction of aid to Ukraine, data exfiltration, and pre-positioning specifically for future exploitation during kinetic conflicts or other times of crisis.***
Iran	The Iran-linked *CyberAv3ngers* campaign has exploited ICS vulnerabilities to attack critical infrastructure, to include a 2023 attack on the Aliquippa, Pennsylvania water authority[19] and attacks on computer systems and fuel gauges at gas stations across the United States.[20] **Implications**: ***These attacks allow Iran to engage in behaviors that would not otherwise be possible—at least not to the same extent or at such a low cost—in the physical domains: signaling its capability, extracting valuable data, and reinforcing deterrence, at least insofar as it continues to demonstrate an ability to quickly respond to U.S. activities it views unfavorably with cyber-enabled attacks on U.S. critical infrastructure.***

17 U.S. Government Accountability Office, Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents, Washington, D.C.: U.S. Government Accountability Office, January 2022.

18 "Russian GRU Targeting Western Logistics Entities and Technology Companies," Cybersecurity & Infrastructure Security Agency, May 21, 2025. As of April 10, 2026: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a.

19 Erika Stanish, "Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group," CBS News, November 26, 2023. As of April 17, 2026: https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/.

20 See, Dan Gooding, "Iran may be hacking tank readers at US gas stations: Report," Newsweek (Undated). As of May 16, 2026: https://www.msn.com/en-us/news/us/iran-may-be-hacking-tank-readers-at-us-gas-stations-report/ar-AA23jkyx?ocid=BingNewsSerp.

PRC	The PRC has conducted numerous attacks and intrusions targeting U.S. critical infrastructure and public and private sector actors. *Volt Typhoon*[21] focused on utilities and transportation hubs and was conducted in a way designed to avoid detection for as long as possible. In addition, the PRC launched *Salt Typhoon* (made public in 2024), which was also directed against telecommunications companies (including those located near U.S. military bases)[22] and enabled the PRC to collect data on millions of Americans.[23] It is widely believed that the threat posed by *Salt Typhoon* is ongoing.[24] **Implications**: ***The possible benefits of these kinds of intrusions are manifold: complex surveillance and intelligence, psychological operations, countermeasure detection, or even future strategic disruption enabled by pre-positioning. As some analysts have concluded, the "PRC may attempt to launch large-scale cyberattacks against lifeline sectors to slow U.S. military mobilization in response to a conflict involving the U.S. and China, particularly over Taiwan."***[25]
Other Actors	The *WannaCry* ransomware attacks of 2017, attributed to the DPRK and its Reconnaissance General Bureau (RGB), spread globally for months after exploiting a Microsoft Windows operating system vulnerability. The self-propagating worm has infected over 300,000 computers around the world.[26] **Implications:** ***This incident demonstrated how expanded attack surfaces enable state-backed actors to project asymmetric power through low-cost cyber operations, capable of inflicting disproportionate global disruption.***[27]

Table 2: Ballooning Attack Surfaces

Cascading Interdependencies

The consequence of cascading interdependencies is that specified attacks (e.g., on critical infrastructure software-defined systems) can affect multiple systems, causing domino effects across multiple domains simultaneously. In some cases, this can present vertically (e.g., across an industry from production through distribution or through multiple service providers sharing common infrastructure) or horizontally (e.g., across closely related segments of an industry or service provider). Because modern cyber-physical systems rely on shared infrastructure, the exploitation of a single vulnerability can lead to effects on multiple related or even unrelated systems, causing substantial immediate and downstream effects.

21 See discussion in, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," Microsoft Threat Intelligence, May 24, 2023. As of April 21, 2026: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques and New Jersey Cybersecurity & Communications Integration Cell and "Volt Typhoon," New Jersey Cybersecurity & Communications Integration Cell. As of April 21, 2026: https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure/volt-typhoon.

22 David E. Sanger and Julian E. Barnes, "China's Hacking Reached Deep Into U.S. Telecoms," The New York Times, November 21, 2024. As of April 21, 2026: https://www.nytimes.com/2024/11/21/us/politics/china-hacking-telecommunications.html.

23 "The Chinese cyber-attack that could have stolen data from every American," BBC, April 17, 2026. As of April 21, 2026: https://www.bbc.com/audio/play/w3ct8m8l.

24 Derek B. Johnson, "FBI: Threats from Salt Typhoon are 'still very much ongoing'," Cyberscoop, February 19, 2026. As of April 21, 2026: https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026.

25 New Jersey Cybersecurity & Communications Integration Cell, "Volt Typhoon," New Jersey Cybersecurity & Communications Integration Cell. As of April 21, 2026: https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure/volt-typhoon.

26 Bill Chappell and Scott Neuman, "U.S. Says North Korea 'Directly Responsible' For Wannacry Ransomware Attack," NPR, December 19, 2017. As of May 16, 2026: https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack.

27 See, "Cybercrime-as-a-Service, Explained," Microsoft, October 9, 2025. As of April 15, 2026: https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/stories/what-is-caas/?msockid=10bea85dba48683e31fbbf61bb3d6995; United Nations Office of Counter-Terrorism, Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks, New York: United Nations Office of Counter-Terrorism, 2024; The White House, 2023 White House Strategy to Combat Transnational Organized Crime, Washington, D.C.: The White House, December 2023; and, "Criminal groups engaging in cyber organized crime," United Nations Office on Drugs and Crime. As of April 14, 2026: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html.

Case/Country	Discussion
Russia	In 2017, a Russian malware attack on Ukrainian government institutions and businesses caused infected systems to become inoperable and, seemingly unintentionally, spread globally: Danish shipping company Maersk experienced extreme disruptions across all its operating ports while Merck, a pharmaceutical company, as well as the logistics giant, FedEx, fell victim to similar operational disturbances.[28] Russia's 2015 and 2026 cyberattacks on Ukraine's power grid translated into the loss of electricity for at least 230,000 consumers.[29] **Implications:** ***These kinds of attacks can produce failures that affect kinetic, industrial, and logistical operations across entire industries and vast geographies.***
Iran	In 2012, the Iran-linked *Shamoon* malware wiped at least 30,000 computers of Aramco, the national oil company of Saudi Arabia.[30] This forced Aramco into manual fallback operations across its physical extraction and refinement operations. In 2026, during the Iran War, Iran-linked threat actors employed a wiper attack on Stryker, a U.S. medical technology company.[31] Although the attack was identified and halted relatively quickly, it nonetheless resulted in significant immediate and downstream damage ranging from corporate operations disruptions and significant data loss to supply chain effects and damage to hospital operations, including the cancellation of surgeries and the delay of custom medical implants for some patients.[32] **Implications:** ***In these examples, Iran was able to attack adversary corporate interests quickly and with substantial primary and secondary effects, many of which would be difficult to plan for without prior knowledge of countless system risks and a thorough understanding of what would happen if these systems were corrupted or disabled.***
PRC	*Volt Typhoon* was a pre-positioning operation conducted by the PRC that targeted and penetrated U.S.-based utilities and transportation hubs which, if compromised, could translate into the distributed loss of electricity, clean drinking water, or other public services. **Implications:** ***Conceivably, the PRC could (and likely would) use pre-positioned access to these systems and infrastructures to complicate and slow U.S. military responses in the case of heightened tensions between the two countries like that which would occur during a Taiwan Strait contingency. Former U.S. officials have suggested that the goal of these intrusions is to undermine U.S. efforts to defend Taiwan by enabling the PRC to initiate a series of infrastructure failures to disrupt U.S. mobilization efforts and cause civil unrest, thereby reducing both the capacity and public appetite for U.S. operations in the defense of Taiwan.***
Other Actors	The 2021 ransomware attack on the Colonial Pipeline by *DarkSide*,[33] a Russia-based non-state criminal organization, had the immediate effect of disrupting corporate billing operations and the downstream effects of substantially disrupted pipeline operations, reduced and delayed flight operations in the eastern United States, and fuel shortages at U.S. filling stations across multiple southern U.S. states. **Implications:** ***Despite being a ransomware attack and causing no discernable damage to cyber-physical operational equipment, this attack resulted in significant security concerns, uncertainty, and a loss of confidence in system integrity, ultimately leading to the follow-on effects of distribution delays and stoppages.***

Table 3: Cascading Interdependencies

28 See discussion of NotPetya in, Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018. As of May 16, 2026: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

29 Jakub Przetacznik and Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks," Brussels: European Parliamentary Research Service, June 2022, p. 3. As of April 22, 2026: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

30 See, "Shamoon (2012)," NATO Cooperative Cyber Defence Centre of Excellence. As of April 16, 2026: https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012) and Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," The New York Times, October 23, 2012. As of April 17, 2026: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

31 Emily Otto, "Shamoon To Stryker: Iran Wields Wiper Attacks," Center for European Policy Analysis, March 16, 2026. As of April 17, 2026: https://cepa.org/article/shamoon-strikes-stryker-iran-wields-wiper-attacks/.

32 Ike Swetlitz and Miquéla V. Thornton, "Stryker Cyberattack Delays Surgeries for Some Patients," Bloomberg, March 18, 2026. As of April 17, 2026: https://www.bloomberg.com/news/articles/2026-03-18/stryker-cyberattack-delays-surgeries-for-some-patients.

33 Joye Purser, "Five Years Later: Lessons Learned From Colonial Pipeline Ransomware Attack," Infosecurity Magazine, May 6, 2026. As of May 16, 2026: https://www.infosecurity-magazine.com/opinions/lessons-learned-from-colonial/. See also, U.S. Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," U.S. Department of Justice, June 7, 2021 and Nicole Perlroth, "Colonial Pipeline paid 75 Bitcoin, or Roughly $5 Million, to Hackers," The New York Times, May 13, 2021. As of May 16, 2026: https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html.

Tyranny of Nearness

The tyranny of nearness results in targets always being within the range of an adversary and the possibility of various, rapidly launched, and often repeatable targeted effects across broad geographies, irrespective of distance and with minimal resource use. It enables sophisticated information operations campaigns, espionage, crime, and pre-positioning that would otherwise not be possible or would consume enormous amounts of resources if conducted through the physical operational domains.

Case/Country	Discussion
Russia	The nominally independent but Russian state-sanctioned group *Noname*[34] has been responsible for thousands of attacks on European states and entities providing support to Ukraine, including public authorities and arms manufacturers. Despite being a non-state or sometimes semi-state actor, this group is capable of quickly responding to events with targeted Distributed Denial of Service (DDoS) attacks that create varying effects, depending on the targets chosen. Russian state services have also employed DDoS attacks as a prelude to kinetic activity (e.g., Georgia in 2008) and in parallel to kinetic actions (e.g., *Sandworm* in Ukraine in 2022). **Implications:** ***Strategic and operational disruptions can be executed responsively and at a distance, and when necessary, in coordination with tactical troop movements and other operations in the physical domains.***
Iran	Iran has engaged in attacks on Israel and the United States as well as Saudi Arabia for the purposes of retribution but also for the targeting of individuals and intelligence gathering activities. Iranian cyber actors conduct persistent intrusion campaigns into critical infrastructure sectors, often for cyber espionage or later operational use. *APT33*, for example, has targeted various companies with ties to Saudi Arabia's aviation sector, apparently seeking insight into Saudi military aviation capabilities.[35] *APT35*, also known as *Charming Kitten*, has proven highly adept at targeting political dissidents, human rights organizations, and Iran scholars to extract intelligence.[36] *APT34*, also known as *OilRig* and linked to the Iranian Ministry of Intelligence and Security (MOIS) is known to conduct longer-duration espionage against government and private sector targets across the Middle East for the dual purposes of intelligence collection and disruptive operations.[37] **Implications:** ***Iran has limited capability to conduct military operations beyond its immediate vicinity except through proxies or cyber operations. With Iran's conventional military decimated after months of war against the United States and Israel, Tehran could likely shift more resources to asymmetric means in the aftermath, including cyber operations, to exact revenge and attempt to restore a modicum of deterrence.***

34 U.S. Department of Justice, "Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups," U.S. Department of Justice, December 9, 2025. As of April 10, 2026: https://www.justice.gov/opa/pr/justice-department-announces-actions-combat-two-russian-state-sponsored-cyber-criminal and James Coker, "Pro-Russian Hacktivist Group Claims 6600 Attacks Targeting Europe," Infosecurity Magazine, December 5, 2024. As of April 10, 2026: https://www.infosecurity-magazine.com/news/pro-russian-hacktivist-attacks/.

35 Jacqueline O'Leary, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," Google Cloud, September 20, 2017. As of April 17, 2026: https://cloud.google.com/blog/topics/threat-intelligence/apt33-insights-into-iranian-cyber-espionage/.

36 "Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society," Cybersecurity & Infrastructure Security Agency, May 14, 2024. As of April 17, 2026: https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf.

37 "OilRig: Iran's Persistent Espionage Arm in Cyberspace," BRANDEFENSE, December 24, 2025. As of April 17, 2026: https://brandefense.io/blog/oilrig-apt-2025/.

PRC	The PRC engages in prolific economic espionage, which is focused mainly on stealing intellectual property, typically industrial and defense technologies that can be used to support its commercial and military objectives. According to Former Director of the Federal Bureau of Investigation (FBI), Christopher Wray, the PRC "is engaged in the largest and most sophisticated theft of intellectual property and expertise in the history of the world, leveraging its most powerful weapons, starting with cyber."[38] These operations are coordinated across cyber, human, and corporate channels.[39] In 2010, cyber actors successfully stole portions of Google's source code[40] and *Operation Cuckoobees*, beginning in 2019 and executed by China-linked *APT41*, exfiltrated "hundreds of gigabytes of intellectual property from companies, much of it linked to Made in China 2025 national science and technology goals."[41] **Implications:** ***Although it is difficult to gauge what the PRC might do in the absence of these kinds of capabilities, it is certain that the competition that the PRC is engaged in against the United States is decidedly helped by its ability to exfiltrate industrial and technological secrets that would otherwise take the country decades to develop on its own.***
Other Actors	The cyber domain and software-defined systems afford non-state actors greater reach without crossing actual borders, which conveniently allows them to take advantage of local, more controlled conditions while exploiting limitations on cross-border law enforcement.[42] Non-state actors use cyberspace to conduct traditional criminal activities (e.g., dealing drugs over the internet) or to facilitate new crimes (e.g., hacking into financial institutions for the purpose of committing fraud).[43] **Implications:** ***With software-defined systems at their disposal, organized crime groups and terrorist organizations can reduce their reliance on physical proximity to carry out their objectives.***[44]

Table 4: Tyranny of Nearness

The Tactical Becomes the Strategic

The consequences of intrusions into software-defined systems are no longer limited to large-scale attacks: even singular, covert intrusions into previously overlooked systems can lead to deterrent and other strategic effects, necessitating their inclusion in contingency planning and crisis management. Intrusions and attacks of this nature amplify an attacker's capabilities and cause effects that could not otherwise be achieved at a similar pace or scale, ultimately creating additional instability and uncertainty.

38 U.S. Federal Bureau of Investigation, "Director Wray's Remarks at the Vanderbilt Summit on Modern Conflict and Emerging Threats," FBI, April 18, 2024. As of April 21, 2026: https://www.fbi.gov/news/speeches-and-testimony/director-wrays-remarks-at-the-vanderbilt-summit-on-modern-conflict-and-emerging-threats.

39 Darren E. Tromblay, "From Outside Assaults to Insider Threats: Chinese Economic Espionage," Information Technology & Innovation Foundation, November 3, 2025. As of April 21, 2026: https://itif.org/publications/2025/11/03/from-outside-assaults-to-insider-threats-chinese-economic-espionage/.

40 Kim Zetter, "Report: Google Hackers Stole Source Code of Global Password System," Wired, April 20, 2010. As of April 21, 2026: https://www.wired.com/2010/04/google-hackers.

41 Benjamin Jensen, "How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy," Center for Strategic & International Studies, October 19, 2023. As of April 21, 2026: https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy.

42 The White House, 2023 White House Strategy to Combat Transnational Organized Crime, Washington, D.C.: The White House, December 2023, p. 19.

43 Sankul Kabra and Saira Gori, "Drug trafficking on cryptomarkets and the role of organized crime groups," Journal of Economic Criminology, Volume 2, December 2023. As of April 14, 2026: https://www.sciencedirect.com/science/article/pii/S294979142300026X/.

44 "Criminal groups engaging in cyber organized crime," United Nations Office on Drugs and Crime. As of April 14, 2026: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html.

Case/Country	Discussion
Russia	Russia has used cyberattacks to create significant operational disruption, notably its attack on Viasat during the 2022 invasion of Ukraine. The attack was intended to restrict the flow of on-the-ground information about the invasion by limiting communications and preventing the broadcast of footage while also disrupting Ukraine's command and control (C2) of its armed forces. The attack destroyed thousands of modems in Ukraine and had a longer-term effect than the DDoS attacks used in previous conflicts with Estonia and Georgia. As a result, Ukraine was forced to switch to alternative communication systems, notably SpaceX's Starlink terminals, which arrived four days after the attack. In the longer term, Viasat worked with Ukrainian officials to ship and install thousands of new modems. While the effect of this attack had an operational impact, some analysts have claimed that "there is no evidence that the attack yielded any tangible military benefits to the Russian invasion. Furthermore, by replacing the Viasat systems with Starlink, Ukraine's military and government not only restored pre-invasion capacity but improved military-specific functions of their satellite communications."[45] **Implications:** ***Similar attacks could vastly compromise tactical and strategic communications architectures in future conflicts. Where time is of the essence, even short disruptions could result in substantial operational setbacks or defeats.***
Iran	Iran has used cyber operations as a tool of retaliation, often in response to geopolitical developments. Intrusions into water systems and infrastructure disruptions have demonstrated some capability without crossing thresholds that might trigger large-scale retaliation. It also serves domestic purposes: showing that the state can and does respond to perceived aggression or unfavorable geopolitical developments. The attack on Las Vegas Sands—seemingly in response to its owner's stance on the Middle East—is illustrative.[46] **Implications:** ***These kinds of retributive attacks, which would have been very difficult and perhaps impossible to carry out a generation ago, and certainly not at long distances, are not only costly but could under certain circumstances lead to escalatory reprisals.***
PRC	Former CISA Director Jen Easterly told the U.S. House of Representatives Select Committee on the Chinese Communist Party (CCP) in 2024 that the goal of PRC pre-positioning within U.S. critical infrastructure was to "crush American will for the U.S. to defend Taiwan in the event of a major conflict there," which she described as an "'everything, everywhere, all at once' scenario."[47] The extent of such an attack could be massive and the implications severe, with the potential for public utilities, banking systems, healthcare, and all trappings of modern society grinding to a halt for a period of days, weeks, or longer. This challenge is further compounded by the difficulty of removing pre-positioned threats, even when found: it has been publicly stated that expelling the actors responsible for *Salt Typhoon* would require significant investment and the replacement of countless routers and other hardware.[48] **Implications:** ***Pre-positioning in U.S. critical infrastructure serves two purposes: potential disruption and deterrence. Past high-profile successful penetrations of U.S. critical infrastructure are likely to give pause to decision-makers in the event of hostilities, as they will have to assume and account for the likelihood of PRC-led disruptions to critical services.***

45 Alexander Kott, George (Yegor) Dubynskyi, Andrii Paziuk, Stephanie E. Galaitsi, Benjamin D. Trump, and Igor Linkov, "Russian Cyber Onslaught was Blunted by Ukrainian Cyber Resilience, not Merely Security," Computer, Volume 57, Number 8, pp. 82-89. p. 83.

46 While this incident did not have a widespread, immediate effect, the attack demonstrated that cyber operations could be used to punish individuals for comments made by targeting their businesses. Benjamin Elgin and Michael Riley, "Nuke Remark Stirred Hack on Sands Casinos That Foreshadowed Sony," Bloomberg Technology, December 10, 2014. As of April 17, 2026: https://web.archive.org/web/20170518141232/https://www.bloomberg.com/news/articles/2014-12-11/nuke-remark-stirred-hack-on-sands-casinos-that-foreshadowed-sony.

47 Nathaniel Mott, "Changelog: U.S. cyber leaders warn of China threat," README_, February 1, 2024. As of April 21, 2026: https://readme.synack.com/changelog-u.s.-cyber-leaders-warn-of-china-threat.

48 David DiMolfetta, "GAO mulls cost evaluation of nationwide telecom hardware replacement," NEXTGOV, January 6, 2025. As of April 23, 2026: https://www.nextgov.com/cybersecurity/2025/01/gao-mulls-cost-evaluation-nationwide-telecom-hardware-replacement/401963/.

Other Actors	Two examples, both involving North Korea, stand out when considering how a "tactical" engagement could lead to strategic results: the 2014 North Korean attack on Sony Pictures before the release of *The Interview* and the instance when an American who was angered by North Korean hacking decided to take down North Korea's internet on his own in 2022.[49] In the former case, a hacker group sponsored by or affiliated with North Korea not only launched attacks against a company headquartered in the United States but also threatened terrorist attacks against theaters in the United States.[50] In the latter case, Alejandro Caceres managed by himself to identify that the North Korean internet was "fragile" and determined that he wanted to send a message after being targeted and angered by North Korean actions in cyberspace and his disappointment in the U.S. response to these actions.[51] **Implications:** ***In neither case were the attackers legitimate parties to any conflict and yet they not only were able to but did engage in actions that could have led to serious consequences among two nation-states.***

Table 5: The Tactical Becomes the Strategic

Inured Blindness

Common and otherwise innocuous software-defined devices have been commandeered for strategic purposes, including espionage and intelligence gathering, pre-positioning, and in support of information operations.

Case/Country	Discussion
Russia	The most consistent Russian cyber activity is sustained, long-duration espionage targeting U.S. and Western interests. These operations include past efforts like *Moonlight Maze* and more recent campaigns such as the *SolarWinds* supply chain intrusion, all of which have demonstrated a breadth of tactics, techniques, and procedures (TTPs) used to compromise systems. For example, since 2022, CISA has tracked a Russian Intelligence or *Glavnoye Razvedyvatelnoe Upravlenie* (GRU)-linked cyber espionage campaign targeting Western logistics and IT companies that leverages a combination of credential guessing, CVE exploitation, internet-facing infrastructure, and spear phishing.[52] Russia has proven itself adept at both brute-force and more sophisticated espionage campaigns. **Implications:** ***Espionage campaigns of these sorts take advantage of unsecured systems that contain troves of information that might otherwise seem innocuous but could be used in innovative ways by an adversary, either in preparation for or in the event of hostilities.***

49 See Andy Greenberg, "North Korea Hacked Him. So He Took Down Its Internet," Wired, February 2, 2022. As of March 26, 2026: https://www.wired.com/story/north-korea-hacker-internet-outage/. See also, discussion of escalation in Chris Blattman, "Cyber Warfare Is Getting Real," Wired, December 17, 2022. As of March 26, 2026: https://www.wired.com/story/cyberwar-security/.

50 Alex Fitzpatrick, "These Are the Theaters That Have Pulled The Interview after Threat," Time, December 17, 2014. As of March 26, 2026: https://time.com/3637565/interview-theaters-cancel/.

51 Shreyas Reddy, "Why a private US citizen decided to take down North Korea's internet on his own," Interview, NK News, May 7, 2024. As of March 26, 2026: https://www.nknews.org/2024/05/why-a-private-us-citizen-decided-to-take-down-north-koreas-internet-on-his-own/.

52 "Russian GRU Targeting Western Logistics Entities and Technology Companies," Cybersecurity & Infrastructure Security Agency, May 21, 2025. As of April 10, 2026: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a.

Iran	During the 2019 period of Gulf tanker attacks, Iranian cyber actors attempted to collect intelligence and disrupt maritime logistics, port authority networks, and shipping companies' operations.[53] Iran has not demonstrated the real-time integration of cyber operations with operations in the physical domains as has been seen in Russia's operations in Ukraine, nor is Tehran believed to have capabilities on par with China. The operations seen so far tend to run in parallel with, rather than be synchronized with, kinetic action. Nonetheless, the 12-Day War in June 2025 marked an inflection point. According to the Director-General of Israel's National Cyber Directorate, Iran was able to penetrate Israeli parking and street cameras to not only track senior officials' movements, but also to conduct battle damage assessments.[54] It has conducted similar successful cyber intrusions since the start of the 2026 Iran War.[55] **Implications:** ***Whereas Iran's operational and strategic capabilities in the physical domains are limited, it is nonetheless able to gather strategically valuable information through the infrastructure put in place and maintained by its adversaries.***
PRC	The PRC has collected millions of records on U.S. (and other countries') government personnel and citizens through various cyber-enabled operations. Through *Salt Typhoon*, the PRC gained access to the metadata of more than one million U.S. residents, including the contents of wiretap request logs and, in some cases, audio recordings of senior political figures and national security officials. In 2024, it was revealed that PRC-linked hackers "might have held access to network infrastructure used to cooperate with lawful U.S. requests for communications data."[56] Information about such requests may have tipped off PRC officials to compromised programs or sources identified by U.S. law enforcement agencies. **Implications:** ***Among other purposes, this kind of information can be used to disrupt foreign espionage operations.***
Other Actors	Non-state actors use software-defined systems to cheaply and remotely gather information generally (e.g., through hacking databases) or on specific targets (e.g., against antithetical groups and individuals, especially those investigating their activities).[57] This information can be used to facilitate transactions, gather and disclose sensitive information,[58] or target opponents. One drug trafficking group was able to use hackers to get into a system providing information on port operations and containers in Antwerp.[59] Mexican cartels have reportedly purchased spyware to surveil all manner of targets, hacked into government databases to extract information, and collected real-time cellphone geolocation data on targets.[60] Mexican cartels also gained access to Mexico City's camera systems for general surveillance and for target movement and tracking purposes.[61] **Implications:** ***Because of the risks of software-defined systems, various non-state actors are able to mimic if not realize capabilities that were once largely monopolized by nation-state actors and their proxies.***

Table 6: Inured Blindness

53 "Cyber interference against vessels in the Persian Gulf and Gulf of Oman (2019)," NATO Cooperative Cyber Defence Centre of Excellence. As of April 17, 2026: https://cyberlaw.ccdcoe.org/wiki/Cyber_interference_against_vessels_in_the_Persian_Gulf_and_Gulf_of_Oman_(2019)

54 Yonah Jeremy Bob, "Iran has attacked every Israeli citizen multiple times, new cyber chief Yossi Karadi says," The Jerusalem Post, December 9, 2025. As of April 19, 2026: https://www.jpost.com/israel-news/defense-news/article-879689.

55 Anat Peled, "Iranian-Linked Groups Hacked Into at Least 50 Security Cameras in Israel," The Wall Street Journal, March 30, 2026. As of April 19, 2026: https://www.wsj.com/livecoverage/iran-war-news-updates/card/iranian-linked-groups-hacked-into-at-least-50-security-cameras-in-israel-dwrn3Wa3K-cI3NfbGiHJl.

56 Sarah Krouse, Dustin Volz, Aruna Viswanatha, and Robert McMillan, "U.S. Wiretap Systems Targeted in China-Linked Hack," The Wall Street Journal, October 5, 2024. As of April 21, 2026: https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

57 "Criminal groups engaging in cyber organized crime," United Nations Office on Drugs and Crime. As of April 14, 2026: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html.

58 Congressional Research Service, Cybersecurity: Selected Cyberattacks, 2012-2024, Washington, D.C.: Congressional Research Service, January 8, 2025, p. 17.

59 This has occurred at several ports in Europe and elsewhere. See, Paul May and Pavla Holcova, "Inside Job: How a Hacker Helped Cocaine Traffickers Infiltrate Europe's Biggest Ports," Organized Crime and Corruption Reporting Project, February 14, 2020. As of April 19, 2026: https://www.occrp.org/en/project/narcofiles-the-new-criminal-order/inside-job-how-a-hacker-helped-cocaine-traffickers-infiltrate-europes-biggest-ports.

60 Daniel Blanco Paz, "Cyber Warfare Capabilities of Mexican Cartels," grey dynamics, July 31, 2024. As of April 14, 2026: https://greydynamics.com/cyber-warfare-capabilities-of-mexican-cartels/.

61 Nuray Taylor, "Fueling Cartels' Cybercrime," The Cyber Edge, October 1, 2025. As of April 14, 2026: https://www.afcea.org/signal-media/cyber-edge/fueling-cartels-cybercrime.

Banality of Cybercrime and Cyber-espionage

Both cybercrime and cyber-espionage are incredibly common and enormously damaging not only in terms of resources and information stolen (or compromised) but also in respect to the costs of remediating affected systems. Cybercrime and cyber-espionage are both low-cost, low-risk, and high-reward activities that give a variety of actors outsized capabilities, many of which can lead to unpredictable effects. During crisis situations, commonly occurring cybercrime and cyber-espionage *have the potential to* escalate and engender different responses than what typically obtains during periods of relative peace.

Case/Country	Discussion
Russia	The first major cyber-espionage campaign launched by the Russians (*Moonlight Maze*) persisted for over three years, while the more recent *SolarWinds* intrusions were active for months. In April 2026, a large-scale cyber-espionage campaign attributed to *APT28* (linked to the GRU) was revealed. The campaign exploited routers to infiltrate and collect information on governments, militaries, and critical infrastructure.[62] **Implications:** ***Because their efforts are covert, it is difficult to assess the efficacy of Russian espionage. However, it is safe to assume long-term access to sensitive and even classified information has likely enabled many Russian strategic objectives. There is a substantial imbalance between the relative ease of these efforts and the potential strategic payoff when they are successful.***
Iran	The campaigns by *OilRig* (targeting Arab Gulf state governments and energy and finance sectors) and *MuddyWater* (targeting adversary governments, military, and critical infrastructure) are representative of multi-month and multi-year Iranian intrusions into networks containing sensitive information. While it is publicly known that many of these espionage campaigns have focused on government ministries, militaries, the telecom sector, and diplomatic organizations, it is unclear to what extent actual sensitive or classified data has been accessed or extracted. **Implications:** ***These intrusions have been problematic in at least two ways. First, Iran was able to rather easily infiltrate highly valuable systems largely unfettered and at low cost (but at high cost to the entities attacked). Second, despite eventually being uncovered, the full effect of these intrusions is unknown as the intent of these activities cannot be discerned merely by identifying the target(s) of the penetrations.***
PRC	The PRC has been able to extract enormous amounts and types of data from its targets, including highly relevant and economically important information on technologies of economic value. According to former NSA chief Keith Alexander, cyber espionage has led to "the greatest transfer of wealth in history."[63] The multiyear *Operation CuckooBees,* for example, is said to have exfiltrated hundreds of gigabytes of intellectual property and sensitive data from technology and manufacturing companies in North America, Europe, and Asia.[64] The U.S. economy is losing between $200 billion and $600 billion a year as a result of these operations.[65] **Implications:** ***The exact effect of this kind of espionage on the PRC's military power is unclear, although it is likely that the CCP funnels relevant commercial innovations into PRC military research and development. What is clear is that even if these intrusions were costly in dollar terms to the PRC, the returns on investment are enormous as they have enabled rapid military and economic growth that would otherwise not be attainable, resulting in a narrowing of the capability gap between the PRC and its competitors.***

62 Veronika Melkozerova, "Russian spooks hack Wi-Fi routers to spy on West," Politico, April 8, 2026. As of April 10, 2026: https://www.politico.eu/article/russias-gru-hacked-hundreds-of-wi-fi-routers-world-wide/.

63 Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history'," Foreign Policy, July 9, 2012. As of April 21, 2026: https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

64 Nicole Sganga, "Chinese hackers took trillions in intellectual property from about 30 multinational companies," CBS News, May 4, 2022. As of April 21, 2026: https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies.

65 Stavros Atlamazoglou, "The U.S. Economy is Losing as Much as $600 Billion a Year in Intellectual Property from Chinese Espionage," The National Interest, May 11, 2024. As of April 23, 2026: https://nationalinterest.org/blog/buzz/us-economy-losing-much-600-billion-year-intellectual-property-chinese-espionage-210956.

Other Actors	The DPRK has developed highly deliberate programs to conduct cyber espionage. Through the RGB, it sponsors a range of groups, including *Andariel*, *Onyx Sleet*, *DarkSeoul*, *Silent Chollima*, and *Stonefly/Clasiopa*. These groups primarily target "defense, aerospace, nuclear, and engineering entities to obtain sensitive and classified technical information and intellectual property to advance the regime's military and nuclear programs and ambitions."[66] North Korea also operates programs designed to embed North Korean IT specialists in foreign firms[67] for espionage and financial gain through blackmail, successfully placing these workers in hundreds of Fortune 500 companies.[68] Various non-state actors also engage in sophisticated cybercrime and cyber-espionage activities. Criminal organizations such as Camorra and 'Ndrangheta facilitate and participate in internet gambling rings[69] while other organized crime groups use ransomware and "high-value business email compromise schemes" to generate funds by targeting U.S. citizens with cyber fraud.[70] Cybercrime is a multi-billion-dollar-per-year industry, and some estimates suggest that globally, cybercrime—including the destruction of data, lost productivity, and other secondary and tertiary effects of an attack—will cost $12.2 trillion annually by 2031.[71] **Implications:** ***For North Korea, cybercrime serves as a means of offsetting the effects of international sanctions***[72] ***and as a funding source for sustaining and expanding its cyber capabilities. The cyber group Andariel has used funds extorted from U.S. and South Korean victims to finance "attack infrastructure," subsequently used in espionage operations targeting government agencies, military organizations, armed forces, and firms involved in missile, aerospace, and uranium-processing technologies. More broadly, software-defined systems have enabled both state and non-state actors to conduct surveillance and gain intelligence in ways previously only available to nation-states. These expanded capabilities allow criminal and proxy groups to expand their operational reach, giving rise to international instability and tensions between the states from which these actors operate and those most affected by their activities.***

Table 7: Banality of Cybercrime and Cyber-espionage

Risks to software-defined systems alter how adversaries can pursue their geopolitical objectives. Overall, the software understanding gap often makes adversaries' pursuit of these objectives cheaper, less risky, more scalable, and sometimes as or more effective than actions in the physical domains.

Russia: Exploiting these risks directly supports its objective of weakening Europe and the alliance system it views as intruding on its sphere of influence. Weaknesses in U.S. and allied software-defined systems enable long-term network pre-positioning and intelligence collection, which can be activated in moments of crisis, as seen in Ukraine, Estonia, and elsewhere. Because software-defined systems are often deeply interconnected, even limited intrusions can produce significant operational effects, allowing Russia to amplify the impact of its military actions. This aligns with its approach of synchronizing cyber operations with conventional conflict, exploiting risks not only for long-term espionage but also to enable short-term tactical and operational military objectives. Overall, risks in software-defined systems have given Russia an additional avenue to pursue its geopolitical objectives, primarily centered on influencing its western flank.

Iran: The same risks in software-defined systems serve a different geopolitical purpose: enabling a weaker pow-

66 "North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs," Cybersecurity & Infrastructure Security Agency, July 25, 2024. As of April 12, 2026: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a. See also, Matthew Ha and Sophie McDowell, "North Korea's Cybercrime Threat Is Growing in Both Size and Sophistication," Foundation for Defense of Democracies. As of April 13, 2026: https://www.fdd.org/analysis/2025/11/12/north-koreas-cybercrime-threat-is-growing-in-both-size-and-sophistication/.

67 Jakob Bund, "Hand and Glove: How Authoritarian Cyber Operations Leverage Non-state Capabilities," Stiftung Wissenschaft und Politik, June 26, 2025. As of April 13, 2026: https://www.swp-berlin.org/10.18449/2025C30/.

68 Matt Kapko, "North Korean operatives have infiltrated hundreds of Fortune 500 companies," Cyberscoop, April 30, 2025.

69 "Criminal groups engaging in cyber organized crime," United Nations Office on Drugs and Crime. As of April 14, 2026: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html.

70 The White House, 2023 White House Strategy to Combat Transnational Organized Crime, Washington, D.C.: The White House, December 2023, p. 9.

71 David Braue, "Cybercrime to Cost the World $12.2 Trillion Annually by 2031." Cybercrime Magazine, May 28, 2025. As of April 15, 2026: https://cybersecurityventures.com/official-cybercrime-report-2025/.

72 Congressional Research Service, North Korean Cyber Capabilities: In Brief, Washington, D.C.: Congressional Research Service, August 3, 2017.

er to engage in asymmetric deterrence and retaliation that would otherwise be far less likely. Lacking the conventional capabilities of the United States, Iran relies on exploitable weaknesses in, for example, ICS and other "softer" targets to harass its adversaries and signal its capabilities. It also provides an additional avenue for Iran to impose costs on the United States, since Iran cannot compete with it in a conventional military engagement. The breadth of risks in software-defined systems allows Iran to conduct responsive attacks tied to geopolitical events, often below the threshold that would normally prompt a direct kinetic confrontation. In this way, systemic risks in software-defined systems provide Iran the opportunity to operate on a near-equal footing with many of its adversaries.

PRC: The PRC's objectives in this regard are more strategic and align with its overarching objectives in its competition with the United States. Rather than prioritizing immediate disruption, the PRC exploits the complexity and risks of software systems to conduct sustained espionage and embed itself within critical networks for potential future contingencies, specifically Taiwan. In this context, the PRC's ambitions and exploitation of risk to software-defined systems are less concerned with immediate gains and targeted more toward enabling the gradual accumulation of strategic advantage, whether through intellectual property theft or by collecting massive amounts of data on U.S. government employees and citizens.

Others: For the DPRK, risks in software-defined systems enable the objective of regime survival through financial gain. The DPRK has been able to conduct large-scale cybercrime, generating profit to prop up its isolated economy and expand its technical capabilities. Because distances have collapsed in the cyber domain, the ruling regime has been able to generate revenue and exert influence globally despite its economic and geographic isolation. Violent and criminal non-state actors similarly benefit by being able to generate funding streams that could not otherwise be realized and by being able to conduct operations at a distance, thus avoiding normal methods of detection and interdiction.

The Effects on National Security of Closing the Software Understanding Gap

The empirical record demonstrates that the risks of software-defined devices and cyber-physical systems have lowered barriers to behaviors and engagements that otherwise would be unlikely to happen and have expanded the targets available to states and non-state actors alike. The risks of software-defined devices have indeed created a new—or more accurately, evolved—arena for conflict, competition, and crime as well as new vectors by which each can be conducted, and have done so in ways that enable malign behavior by state and non-state actors alike. The proliferation of artificial intelligence (AI) is likely to serve as a force multiplier in this regard, but the advantage will not be evenly distributed. Attackers need only find a single exploitable flaw, while defenders must identify and remediate all of them. AI accelerates both tasks, but the attacker's is fundamentally easier, giving them a structural advantage.

However, because these risks and challenges result from issues that are largely resolvable with the coordinated application of existing and new capabilities and techniques, it is possible to obviate many of these consequences and effectively tighten the software understanding gap, resulting in a closer merger of the red and green curves shown in Figure 1. We caution that success in this regard will breed adaptation: competitors and adversaries alike will respond in ways that mimic the malign behaviors charted in the previous sections. Nonetheless, these risks can also be addressed over time as additional targets are progressively hardened against cyberattacks and intrusions.

First-Order Effects if the Software Understanding Gap is Closed

The six risks identified in the previous sections (to include downstream effects and costs), stemming from the increasing reliance on software-defined systems across domains, would be significantly redressed ***if the software understanding gap were closed***. The following analyses project what would happen if U.S. civilian and military software-defined devices and cyber-physical systems are verified for their function, safety, and security by design across all conditions, whether hostile or non-hostile, before their deployment.

- **Ballooning Attack Surfaces**—Entire classes of software vulnerabilities will be eliminated. Counterforce and countervalue targets will be rendered far less vulnerable to distant and anonymous attacks, and confidence in system integrity and performance will be improved.
- **Cascading Interdependencies**—Critical paths will be identified and mathematically proven, which will enable timely and targeted risk mitigation. The risk of single-point failures causing chain reactions across sectors and domains will be substantially reduced.
- **Tyranny of Nearness**—System resilience is enabled, regardless of the attacker's identity or geographic proximity. This will push the defensive perimeter outwards and make attacks not only more difficult to conduct but also far more resource-consuming than they would otherwise be.
- **The Tactical Becomes the Strategic**—The ability of localized or lower-level intrusions to generate outsized strategic effects will be limited by enabling more predictable and verifiable system behavior. The number of actors capable of conducting these intrusions will be substantially limited, and thus more identifiable and subject to interdiction.
- **Inured Blindness**—By improving visibility into system behavior and dependencies, epistemic uncertainty will be reduced. This will also enable an attenuation of the prevailing signal-to-noise ratio in the cyber domain, allowing better tailored defenses, responses, and resource applications.
- **Banality of Cybercrime and Cyber-espionage**—Reducing easily exploitable vulnerabilities and strengthening systemic resilience will raise the cost, complexity, and technical barriers associated with persistent cybercrime and cyber-espionage. This will reduce the volume of these activities and limit the financial, technical, or other rewards available to state and semi-state or independent criminal actors.

Second- and Third- Order Effects if the Software Understanding Gap is Closed

Because the software understanding gap is pervasive and the solutions proposed in this report are not a "silver bullet," we must assume that the process of closing the software understanding gap will take time and proceed unevenly across sectors (i.e., from higher-value national security systems to more mundane corporate and consumer software-supported systems). The incentives for and urgency to close the gap will vary across different sectors of society as varying organizational dynamics, market incentives, and onerous regulatory regimes will result in an uneven closing of the software understanding gap in non-defense industries. Second, if the software understanding gap is closed, it is unlikely to be closed for everyone (to include adversaries but also allies and other partners) and certainly not with anything approaching simultaneity. Accordingly, we do not expect the activities, risks, and challenges identified and discussed in this report to disappear but instead to responsively be pushed down/out to more vulnerable institutions, organizations, and individual systems over time (e.g., from defense and critical infrastructure to corporate and other civilian systems and devices). That is, as improvements in the security

of higher-value national security and critical infrastructure systems are made, we expect malicious activity to be displaced to softer and more distributed targets, in ways that are a logical extension of malign activities already occurring today. We should also expect adversaries to continue inimical actions in and through the cyber domain, while adapting to changing circumstances by developing new TTPs.

The following is a hypothesized general list of interrelated and mutually reinforcing changes we expect to occur if the United States begins to close the software understanding gap and progressively lessens the risks prevalent to software-defined and cyber-physical systems.

High-Value Systems Will Become More Difficult to Compromise Directly.

- Nation-states may empower proxies to engage in lower-level cybercrimes and cyber-espionage (e.g., to avoid detection and go after less-secure and less-valuable but more plentiful targets). This could enable a shift from cyberattacks on, for example, defense networks and instead to criminal intrusions, but enabled with the sophisticated capabilities of a state. We are also likely to see more higher-risk and proximal attacks on cyber-physical systems using social engineering tools and crafted devices (e.g., Stuxnet).[73]

Shrinking Cyber Targets Will Compel Adversaries to Shift Targets

- As traditional attack surfaces shrink, there will be fewer exposed entry points and exploitable pathways available to malicious actors. Many targets will become progressively inaccessible except for close, inside, or extremely sophisticated cyber-physical attacks. Vigilance will be required to minimize other behaviors that enable penetrations and attacks.
- Adversaries are therefore likely to adapt, identify, and exploit weak links, infiltrate vulnerable seams in supply chains, and attempt to gain access to critical infrastructure and other high-value systems in different (and unexpected) ways. Softer targets (e.g., non-institutional, individual, or otherwise less secure) will increasingly be subject to cyberattacks until they are similarly secured.
- The shift to softer targets (both domestic and foreign) will be difficult to monitor and track (the volume of targets is likely to paradoxically rise as state and non-state actors develop new TTPs and apply these to broader and more plentiful but lower-profile targets). However, securing high-profile targets (e.g., critical infrastructure) and associated networks will progressively limit the possibility of causing mass or cascading effects and/or critical disruptions.

Deterrence Will Be Reinforced as Attribution Rates Increase.

- The concept of deterrence relies on involved parties understanding and being confident that actions will result in consequences. Closing the software understanding gap reinforces deterrence by denial by making software-defined systems more difficult to penetrate, disrupt, or exploit successfully. Improved resilience raises the costs and uncertainty facing attackers while reducing the expected return on investment of malicious activity. As a result, adversaries are more likely to redirect their efforts toward softer targets that offer a higher probability of success at lower cost.
- Attribution rates will rise as behaviors and identities are more easily and quickly tracked and exposed through software understanding capabilities. Attacks on high-profile national security assets will become more difficult to execute and will consequently yield fewer rewards. Fewer actors (or their proxies) will

73 Stuxnet was introduced directly to the affected systems via USB drives as opposed to remotely via the internet.

be able to conduct sophisticated cyberattacks without fear of discovery. When cyberattacks do occur (or are attempted), they should thus be more detectable (triggering or permitting quicker and more accurate targeting and response). Given that in the long run there will be fewer actors capable of conducting effective cyber operations and fewer available targets, the likelihood of attributing and/or interdicting a cyberattack will increase.

Predictability Will Increase, Allowing for Better Resource Tailoring and Application.

- Unpredictability will initially ebb and flow as adversaries develop responsive TTPs but should subside over time as risks and vulnerabilities are sequentially reduced in scale and scope. As the software understanding gap narrows, cyber risks and attack pathways should become more legible and traceable, reducing uncertainty and improving strategic planning and response.
- Cyberattacks will still be most likely to occur at the outset of a conflict, but the targets will be reduced substantially, and cyberattacks, or other actions, will more closely track operations in the physical domains.
- Risk assessments will be able to focus more on known vulnerabilities through observable risks, and less on speculation about potential adversary capabilities. This will enable more accurate assessments of adversary capabilities and system vulnerabilities, while also improving the allocation of resources for intelligence gathering, monitoring, and defense.

Adversaries Will Be Forced to Shift Back to Attacks and Intrusions in the Physical Domains

- While a longer-term and less direct effect, as software-defined devices and cyber-physical systems are progressively secured, we can expect to see actors resorting to what might be termed as “pre-cyber” or “analog” behaviors. That is, as it becomes gradually more difficult for these actors to exploit software-defined devices directly (e.g., to target vulnerable systems and processes) and indirectly (e.g., as a vehicle enabling other illicit activities by piggybacking on other actors’ poorly regulated or largely unsecure software-defined infrastructure), they will nonetheless still require funding sources to support their activities, and will still need to engage in malign activities to survive. We can thus expect those states and non-state actors that presently disproportionately accrue asymmetric benefits from malign cyber activities to adapt and revert to illicit actions in the physical domains. The more an actor relies on activities in the cyber domain to achieve its objectives (e.g., less powerful states and non-state actors), the more likely it is to shift its operational foci to illicit physical domain activities.

U.S. Adversaries Will Seek to Similarly Close the Software Understanding Gap and Take Advantage of Any Asymmetries

- As the United States closes the software understanding gap across higher-value national security and civilian infrastructure and software-defined systems, other states will do the same. We can expect that hostile competitors will seek to disrupt this process as possible, either by corrupting software-defined goods imported into the United States or through other inimical actions targeting complicated supply chains.

Issues, Discussion, and Recommendation

Our recommendations are meant to address the challenges identified in this report and promote a restored position of assured dominance in software development, with the United States able to harness its creativity and technological advantages unencumbered by the software understanding gap, while simultaneously allowing for the exploitation of its adversaries' vulnerabilities. Although this problem is uniquely complex and manifests in ways that transcend technological, organizational, and policy boundaries, it is largely resolvable with emerging and available capabilities.

Issue 1: The Software Understanding Gap is an "Everyone" and "Everywhere" Problem and Must be Resolved to Help Reduce U.S. Cyber Risk and Improve its National Security Posture.

Discussion: Because software is indispensable to the proper functioning of government and military agencies, critical infrastructure, commercial organizations, and civil society, the range of potential national security risks posed by software-defined systems is nearly inestimable: it is a problem that affects every organization and everyone. However, because of substantial resources needed, bureaucratic, legal, and other constraints, this problem cannot be resolved everywhere simultaneously. This poses several challenges. First, although by no means simple, the federal government (as well as state and local governments) can determine and mandate how subordinate organizations will approach this problem and who will serve as the proponent or lead agency for supporting efforts. Accordingly, the federal government must develop software understanding capabilities that critical infrastructure operators and other non-governmental entities will need, as it cannot reasonably hold these entities accountable for a gap they lack the tools to close. Second, there exists a significant triage and sequencing issue for all organizations in respect to where to start and how to prioritize their efforts to close the software understanding gap. Third, there is a bureaucratic problem of how organizations will work with other organizations where interdependencies exist, even when these organizations share a "parent" organization and mutual interests in closing the software understanding gap. While this might seem *relatively* straightforward for hierarchical governmental organizations like the DoW and its subordinate headquarters and organizations, the same cannot be said for those organizations responsible for managing public-private critical infrastructure or commercial entities, including foreign commercial entities that are responsive to differing regulatory frameworks.

Recommendation 1.1: Establish Interagency Coordination, Identify Stakeholders, and Prioritize Efforts to Address the Software Understanding Gap—Building on the 2023 Software Understanding for National Security (SUNS) initiative, the federal government should formalize and empower the Software Understanding National Security Committee (SUNSEC) as a permanent interagency coordination body for closing the software understanding gap. The SUNS initiative convened experts from 18 federal agencies and produced foundational work such as *The Need for Software Understanding,* which examined the software understanding challenge for national security and critical infrastructure and called for a coordinated national effort to advance software understanding capabilities. Just as the National Cancer Program coordinates research across institutions rather than funding disparate efforts in isolation, SUNSEC should provide a coherent, coordinated research agenda for software understanding across the federal government. Rather than creating a new entity, the federal government should provide SUNSEC with the authorities, resources, and institutional support necessary to continue and expand this work.

Recommendation 1.2: Treat Software Understanding Capabilities as Mission Requirements–Mission success increasingly depends on secure, reliable and resilient software-defined systems, particularly in hostile environments. Software understanding capabilities should therefore be integrated directly into operational planning, mission engineering, acquisition, and mission execution processes rather than being treated as isolated technical or compliance functions. Software understanding requirements should derive from mission owners and operational expectations first, ensuring that such capabilities are aligned to mission context and risk.

Recommendation 1.3: **Implement Forward and Reverse Software Understanding Capabilities Using AI-enabled Formal Methods**—Formal methods are not new and have been a *potential* solution to the software understanding problem for quite some time.[74] We highlight the word "potential" because while effective, formal solutions have generally been too resource-intensive to employ at scale. Three factors plagued the use of formal methods for software understanding in the past: there were not enough practitioners available; the work was costly to perform; and the process took extensive amounts of time to complete—all of which made the exercise enormously costly in manpower and dollar terms. However, the prevailing calculus of leveraging formal methods has changed with the advent and use of AI, leading to substantial reductions in the time and resources required to gain software understanding for reverse- (old software and processes) or forward-looking (new or not yet produced software) purposes. Whereas rigor and speed used to be trade-offs in the formal methods process, AI has made them complementary factors. Additionally, and critically, there is a growing body of evidence to suggest that U.S. adversaries are or will soon be using AI for similar defensive but also offensive purposes, creating what appears at the outset to be the genesis of an AI (and software understanding) competition, where maintaining a healthy lead will be requisite to a host of security applications.[75]

Recommendation 1.4: Enable Zero-Friction Sharing to Promote Grassroots Solutions and Cooperation—Closing the software understanding gap will require a whole-of-society approach. However, there is neither a standardized nor efficient mechanism in place for these organizations to quickly and coherently collaborate and collect and share insights, best practices, or other data relevant to this effort. Because this effort will be so large and will occur unevenly across various sectors, pre-approved sharing agreements and data-sharing infrastructure—designed to minimize hurdles and enable information flows—will be requisite. The federal government should establish shared infrastructure and streamlined cross-agency approval processes that enable personnel from different agencies to collaborate on software understanding capabilities, removing the bureaucratic barriers that currently fragment these efforts. Also, because many private sector and non-government organizations will play a role in closing the software understanding gap, consideration should be given to mechanisms and processes that maximize their inclusion while limiting their exposure to post hoc liabilities that naturally (and legally) limit their willingness to share information.[76]

Recommendation 1.5: Establish Software Understanding Interoperability Agreements with International Partners—Because the software understanding gap is not limited by borders and can affect U.S. national security interests both directly (e.g., allies involved in collective security or established through treaty) and indirectly (e.g., partners engaged in security activities that tangentially support U.S. interests), the United States should work with its international partners to develop programs and standards for establishing software understanding in relevant areas (e.g., shared information or weapon systems or critical infrastructure where interoperability is requisite).

---

74 For instance, see Kathleen Fisher's discussion of High Assurance Cyber Military Systems in "DARPA PM Kathleen Fisher, High Assurance Systems," (Video) YouTube, March 14, 2012. As of May 27, 2026: https://www.bing.com/videos/riverview/relatedvideo?q=DARPA+HACMs&mid=7D81986191A41583BF6C7D81986191A41583BF6C&churl=https%3a%2f%2fwww.youtube.com%2fchannel%2fUCOIHBHRbvncMo7Bf0Vx1zEQ&FORM=VIRE.

75 See, Z.Z. Ren, Zhihong Shao, Junxiao Song, Huajian Xin, Haocheng Wang, Wanjia Zhao, Liyue Zhang, Zhe Fu

Qihao Zhu, Dejian Yang, Z.F. Wu, Zhibin Gou, Shirong Ma, Hongxuan Tang, Yuxuan Liu, Wenjun Gao

Daya Guo, and Chong Ruan, "DeepSeek-Prover-V2: Advancing Formal Mathematical Reasoning via Reinforcement Learning for Subgoal Decomposition," github. As of April 20, 2026: https://github.com/deepseek-ai/DeepSeek-Prover-V2. See also Sheera Frenkel, Paul Mozur, and Adam Satariano, "Mutually Automated Destruction: The Escalating Global A.I. Arms Race," The New York Times, April 12, 2026. As of April 20, 2026: https://www.nytimes.com/2026/04/12/technology/china-russia-us-ai-weapons.html?smid=nytcore-ios-share.

76 See discussion, variously, in Douglas Ghormley, Tod Amon, Christopher Harrison, and Tim Loffredo, SUNS: The National Need for Software Understanding: The Present Crisis, Technical Capability Gaps, and Path Forward, Albuquerque, New Mexico: Sandia National Laboratories, March 25, 2025.

Issue 2: The Way Software Development Has Evolved is Premised on a Market Model and Incentives that Deferred Costs that are Now Coming Due.

Discussion: The economics of software development and use have long incentivized speed of development and functionality over security. As the software understanding gap has expanded alongside U.S. dependence on cyber-physical systems, these tradeoffs have become increasingly untenable. However, since the costs of generating software understanding and creating secure software are likely[77] to decrease with the application of AI to formal methods, software can now be secured in a way that still promotes speed of development and complexity of function but without as many negative externalities (e.g., consumers who have no ability to fix software when it malfunctions, a system where security largely comes in the form of post hoc responses based on the compliance model of cybersecurity). While this process is not cost-free, it is in practice—according to Boehm's Law[78]—radically cheaper to fix a software defect early rather than later in the development cycle. Incidentally and of substantial import, the difficult-to-calculate costs borne by the national security apparatus due to the risks posed by insecure software generally are also ipso facto reduced when incentives change, and costs and risks are appropriately accounted for and remedied prior to implementation.

Recommendation 2.1: Create the Conditions to Realign Incentives Across Relevant Sectors—The potential financial costs of the software understanding gap have not been realized historically in a way that prompted changes in how software is made because the actual costs of unsecured software were not well understood but were apparently lower than what would be necessary to produce an organic shift in the market. This historical experience has produced a substantial lag in threat perception (and market response)—what was true in respect to software-defined device risks 20 or even 10 years ago is changing rapidly with the exponential growth of the software understanding gap and U.S. dependence on cyber-physical systems. In the absence of perceptible costs being incurred more immediately (compelling producers and consumers to make rapid changes organically), changes will have to be made to encourage different approaches to how software is produced (and repaired). First, commercial software development and acquisition should continue but should also be subject to rigorous security standards, particularly as AI-enabled formal methods will likely reduce the costs historically associated with implementing higher-assurance software practices. These standards should be incorporated directly into acquisition requirements for programs of record and other government initiatives, using procurement and contracting mechanisms to help realign incentives across the software market. The federal government should invest in building software understanding capabilities sufficient to analyze supply-chain software and prefer solutions with fewer vulnerabilities. This would create a meaningful market incentive for vendors to invest in formal methods during development–benefits that are currently invisible to government buyers and therefore go unrewarded. Software-defined systems imported from abroad should similarly meet these standards. Second, benchmarks for secure software design should take advantage of market forces and add prestige to producers that meet specified industry requirements.[79] Such "gold standards"[80] can help drive commercial competitions where other inducements are neither practical nor enforceable.

Recommendation 2.2: Employ Formal Verification Techniques in Software Development and Analysis—Software producers should adopt formal verification and higher assurance practices throughout the software development lifecycle, including testing and verification. These methods can reduce resource investments in terms of time and human capital, promote speed of development with far fewer unexpected vulnerabilities, improve system reliability and resilience, and strengthen confidence in software-defined systems while reducing long-term costs. This is particularly important for national security missions with changing parameters, which require iteration and rapid

77 Although not yet proven, this is expected to occur over time.

78 See, "Boehm's Law." As of May 27, 2026: https://rnjn.in/glossary/boehms-law/.

79 Gopal Sarma and Kathleen Fisher, "Tipping the Cyber Balance: How AI Benchmarks Could Make Software Safer," RAND Corporation, February 3, 2026. As of March 8, 2026: https://www.rand.org/pubs/commentary/2026/02/tipping-the-cyber-balance-how-ai-benchmarks-could-make.html.

80 See "Closing: HON. Emil Michael, Under Secretary of Defense for Research and Engineering," (Video) YouTube. As of May 27, 2026: https://www.youtube.com/watch?v=ROZv0G-6zxs.

formal verification.

Recommendation 2.3: Conduct Cost Scoping that Accounts for the Value of Mission Success, the Mission Risk from Software Vulnerabilities, and Upfront Investments in Software Understanding Capabilities—Developing metrics that accurately account for and assign value to software vulnerabilities will help to appropriately scope the problem posed to U.S. national security by the software understanding gap. Asking questions like "what is the cost to national security if this software or the system and mission it supports fails?" should be normalized and taken into consideration when balancing benefits and risks. This kind of accounting will also help to demonstrate how up-front investments in software understanding will produce downstream benefits that might otherwise go uncalculated (upfront costs, especially when considering national security requirements, should be only a small portion of overall production and use costs, and are likely infinitesimal when compared to the costs associated with the potential failure of strategic, front-line defense and intelligence systems).

Issue 3: Closing the Software Understanding Gap is Necessary but Does Not Entirely Eliminate Risk.

Discussion: Software-defined systems will continue evolving faster than our ability to fully understand, secure, and verify them. Even if the United States narrows the software understanding gap, strategic competition, malicious activity, and cyber conflict will persist. We can expect that state-based adversaries and non-state actors will respond to improved U.S. software assurance—especially if the accompanying rollout is uneven across sectors—by adapting their operations, progressively from hardened targets to "softer" but not necessarily less valuable targets (e.g., non-government sectors of the economy, small businesses, and other less secure or "lower hanging fruit"). Existing cybersecurity mechanisms, including, but not limited to, cyber hygiene, vulnerability management, and layered defenses, will remain essential. Efforts to narrow the software understanding gap should be understood as complementary to, and mutually reinforcing of, broader cybersecurity and resilience efforts.

Recommendation 3.1: Take Steps that Reduce Ambiguity and Enforce Accountability in the Cyber Domain, at All Levels—While closing the software understanding gap can improve prevention and resilience, it does not eliminate the need for broader cybersecurity practices or accountability regimes. Investments in software understanding should complement core practices such as vulnerability management, patching, monitoring, and incident response. In addition, the United States should continue to develop policies and procedures that treat malign cyber domain activities more like activities in the physical domains, i.e., with policies designed to increase transparency and enforce standards of behavior to improve deterrence. This is especially true for cybercrime and cyber-espionage, the responses to which seem to be disproportionately relaxed compared to what we would expect in the event of a state-sponsored or non-state physical raid on a government building or private business.

Recommendation 3.2: Prepare for Adaptive Adversaries, Particularly Non-State Actors that Will Attack Low-Hanging Fruit—If/when the United States improves its software understanding posture and hardens higher-value targets, adversaries, especially non-state actors, are likely to shift toward less protected entities and higher-volume, lower-profile attacks. Accordingly, the United States should be prepared to dedicate resources to detecting, disrupting, and prosecuting lower-level cybercrime and other opportunistic malicious cyber activities that collectively impose significant societal and economic costs. As major targets become harder to penetrate, adversaries will increasingly seek advantages and shelter in less-protected areas of the cyber domain.

Recommendation 3.3: Establish Mechanisms to Continuously Monitor Evolving Risks, Operational Conditions, and Adversary Behavior Across the Cyber Domain—In conjunction with Recommendation 1.1, the U.S. government should create a task force or some similar organization charged with gathering and organizing lessons learned during the closing of the software understanding gap (for use and implementation beyond defense and security organizations) to include: monitoring changes to and trends in cyber-related activities during peace, conflict, and for criminal purposes; developing doctrine based on adversary behavior that affects all sectors of society; and, hosting red-teaming and wargaming efforts to divine what is likely next in adversary exploitations of software-defined devices and cyber-physical systems. The principal point of this organization is to document (friendly) actions and (adversary) reactions as the United States closes the software understanding gap and to ensure that these lessons are available to stakeholders and other interested parties. In this regard, this organization would be

analogous to the U.S. Marine Corps Center for Lessons Learned, the U.S. Army Center for Lessons Learned, or the Joint Lessons Learned Program. This is important insofar as closing the software understanding gap is going to be an uneven process and occur over a long period across many sectors of society—failing to specify an agency or organization for these purposes makes it more likely that information sharing will not occur and lessons learned and best practices identified will be poorly implemented, not implemented at all, or lost.[81]

Acknowledgments

We would like to thank all of our interviewees for graciously donating their time to help us better understand the software understanding gap, the policy challenges associated with closing the gap, and other salient issues discussed in this report. Our acknowledgment of these individuals does not imply any expressed endorsement of this report by either them or their employers or other organizations with which they are affiliated: the opinions and findings contained herein are those of the research team alone, as are any errors that might be present.

The Soufan Center would like to thank Atalanta for their support of this report. The findings and conclusions presented in this report are solely those of the research team and do not necessarily reflect the views of The Soufan Center or its supporters.

Supported by

Atalanta

81 This is not meant to replace or even duplicate efforts of U.S. Cyber Command, the service cyber commands, intelligence agencies, or law enforcement, but instead to complement these efforts and act as a repository that can work with industry and other partners in closing the software understanding gap.

Bibliography

"Boehm's Law." As of May 27, 2026: https://rnjn.in/glossary/boehms-law/.

"Closing: HON. Emil Michael, Under Secretary of Defense for Research and Engineering," (Video), *YouTube*. As of May 27, 2026: https://www.youtube.com/watch?v=ROZv0G-6zxs.

"Criminal groups engaging in cyber organized crime," *United Nations Office on Drugs and Crime*. As of April 14, 2026: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html.

"Cyber interference against vessels in the Persian Gulf and Gulf of Oman (2019)," *NATO Cooperative Cyber Defence Centre of Excellence*. As of April 17, 2026: https://cyberlaw.ccdcoe.org/wiki/Cyber_interference_against_vessels_in_the_Persian_Gulf_and_Gulf_of_Oman_(2019).

"Cybercrime-as-a-Service, Explained," *Microsoft*, October 9, 2025. As of April 15, 2026: https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/stories/what-is-caas/?msockid=10bea85dba48683e31fbbf61bb3d6995.

"DARPA PM Kathleen Fisher, High Assurance Systems," (Video) *YouTube*, March 14, 2012. As of May 27, 2026: https://www.bing.com/videos/riverview/relatedvideo?q=DARPA+HACMs&mid=7D81986191A41583BF6C7D81986191A41583BF6C&churl=https%3a%2f%2fwww.youtube.com%2fchannel%2fUCOIHBHRbvncMo7Bf0Vx1zEQ&FORM=VIRE.

"How Far Can Nukes Travel? Missile Ranges Explained," *ScienceInsights*, March 7, 2026. As of March 8, 2026: https://scienceinsights.org/how-far-can-nukes-travel-missile-ranges-explained/.

"Mexican cartels turn to bitcoin, internet, e-commerce," *Associated Press*, March 10, 2022. As of April 14, 2026: https://apnews.com/article/business-caribbean-mexico-crime-drug-cartels-1bb5ebf84fbf71baf6a845648bad4990.

"Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society," *Cybersecurity & Infrastructure Security Agency*, May 14, 2024. As of April 17, 2026: https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf.

"North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs," *Cybersecurity & Infrastructure Security Agency*, July 25, 2024. As of April 12, 2026: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a.

"OilRig: Iran's Persistent Espionage Arm in Cyberspace," *BRANDEFENSE*, December 24, 2025. As of April 17, 2026: https://brandefense.io/blog/oilrig-apt-2025/.

"Russian GRU Targeting Western Logistics Entities and Technology Companies," *Cybersecurity & Infrastructure Security Agency*, May 21, 2025. As of April 10, 2026: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a.

"Shamoon (2012)," *NATO Cooperative Cyber Defence Centre of Excellence*. As of April 16, 2026: https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012).

"The Chinese cyber-attack that could have stolen data from every American," *BBC,* April 17, 2026. As of April 21, 2026: https://www.bbc.com/audio/play/w3ct8m8l.

"Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," *Microsoft Threat Intelligence,* May 24, 2023. As of April 21, 2026: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques.

Annis, Franklin, "Krulak Revisited: The Three-Block War, Strategic Corporals, and the Future Battlefield," *Modern War Institute at West Point,* February 3, 2020. As of March 23, 2026: https://mwi.westpoint.edu/krulak-revisited-three-block-war-strategic-corporals-future-battlefield/.

Atlamazoglou, Stavros, "The U.S. Economy is Losing as Much as $600 Billion a Year in Intellectual Property from Chinese Espionage," *The National Interest,* May 11, 2024. As of April 23, 2026: https://nationalinterest.org/blog/buzz/us-economy-losing-much-600-billion-year-intellectual-property-chinese-espionage-210956.

Blattman, Chris, "Cyber Warfare Is Getting Real," *Wired*, December 17, 2022. As of March 26, 2026: https://www.wired.com/story/cyberwar-security/.

Bob, Yonah Jeremy, "Iran has attacked every Israeli citizen multiple times, new cyber chief Yossi Karadi says," *The Jerusalem Post*, December 9, 2025. As of April 19, 2026: https://www.jpost.com/israel-news/defense-news/article-879689.

Braue, David, "Cybercrime to Cost the World $12.2 Trillion Annually by 2031." *Cybercrime Magazine*, May 28, 2025. As of April 15, 2026: https://cybersecurityventures.com/official-cybercrime-report-2025/.

Bund, Jakub, "Hand and Glove: How Authoritarian Cyber Operations Leverage Non-state Capabilities," *Stiftung Wissenschaft und Politik*, June 26, 2025. As of April 13, 2026: https://www.swp-berlin.org/10.18449/2025C30/.

Chappell, Bill and Scott Neuman, "U.S. Says North Korea 'Directly Responsible' For Wannacry Ransomware Attack," *NPR*, December 19, 2017. As of May 16, 2026: https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack.

Closing the Software Understanding Gap, Washington, D.C.: Cybersecurity & Infrastructure Security Agency, Defense Advanced Research Projects Agency, U.S. Department of Defense, and the National Security Agency, January 16, 2025.

Coker, James, "Pro-Russian Hacktivist Group Claims 6600 Attacks Targeting Europe," *Infosecurity Magazine*, December 5, 2024. As of April 10, 2026: https://www.infosecurity-magazine.com/news/pro-russian-hacktivist-attacks/.

Collins, Michael, "Formal Methods," Pittsburgh, Pennsylvania: Carnegie Mellon University, 1998. As of March 5, 2026: https://users.ece.cmu.edu/~koopman/des_s99/formal_methods/.

Congressional Research Service, *Cybersecurity: Selected Cyberattacks, 2012-2024*, Washington, D.C.: Congressional Research Service, January 8, 2025.

-----, *North Korean Cyber Capabilities: In Brief*, Washington, D.C.: Congressional Research Service, August 3, 2017.

DiMolfetta, David, "GAO mulls cost evaluation of nationwide telecom hardware replacement," *NEXTGOV*, January 6, 2025. As of April 23, 2026: https://www.nextgov.com/cybersecurity/2025/01/gao-mulls-cost-evaluation-nationwide-telecom-hardware-replacement/401963/.

Elgin, Benjamin and Michael Riley, "Nuke Remark Stirred Hack on Sands Casinos That Foreshadowed Sony," *Bloomberg Technology*, December 10, 2014. As of April 17, 2026: https://web.archive.org/web/20170518141232/https://www.bloomberg.com/news/articles/2014-12-11/nuke-remark-stirred-hack-on-sands-casinos-that-foreshadowed-sony.

Fitzpatrick, Alex, "These Are the Theaters That Have Pulled The Interview after Threat," *Time*, December 17, 2014. As of March 26, 2026: https://time.com/3637565/interview-theaters-cancel/.

Frenkel, Sheera, Paul Mozur, and Adam Satariano, "Mutually Automated Destruction: The Escalating Global A.I. Arms Race," *The New York Times*, April 12, 2026. As of April 20, 2026: https://www.nytimes.com/2026/04/12/

technology/china-russia-us-ai-weapons.html?smid=nytcore-ios-share.

Geer Jr., Daniel E., "A Rubicon," Aegis Series Paper No. 1801, Stanford, California: Hoover Institution, 2018.

Ghormley, Douglas, Tod Amon, Christopher Harrison, and Tim Loffredo, *SUNS: The National Need for Software Understanding: The Present Crisis, Technical Capability Gaps, and Path Forward*, Albuquerque, New Mexico: Sandia National Laboratories, March 25, 2025.

Gooding, Dan, "Iran may be hacking tank readers at US gas stations: Report," *Newsweek* (Undated). As of May 16, 2026: https://www.msn.com/en-us/news/us/iran-may-be-hacking-tank-readers-at-us-gas-stations-report/ar-AA23jkyx?ocid=BingNewsSerp.

Greenberg, Andy, "North Korea Hacked Him. So He Took Down Its Internet," *Wired*, February 2, 2022. As of March 26, 2026: https://www.wired.com/story/north-korea-hacker-internet-outage/.

-----, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018. As of May 16, 2026: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Ha, Matthew and Sophie McDowell, "North Korea's Cybercrime Threat Is Growing in Both Size and Sophistication," *Foundation for Defense of Democracies*. As of April 13, 2026: https://www.fdd.org/analysis/2025/11/12/north-koreas-cybercrime-threat-is-growing-in-both-size-and-sophistication/.

Jensen, Benjamin, "How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy," *Center for Strategic & International Studies,* October 19, 2023. As of April 21, 2026: https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy.

Johnson, Derek B., "FBI: Threats from Salt Typhoon are 'still very much ongoing'," *Cyberscoop,* February 19, 2026. As of April 21, 2026: https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026.

Kabra, Sankul and Saira Gori, "Drug trafficking on cryptomarkets and the role of organized crime groups," *Journal of Economic Criminology*, Volume 2, December 2023. As of April 14, 2026: https://www.sciencedirect.com/science/article/pii/S294979142300026X/.

Kapko, Matt, "North Korean operatives have infiltrated hundreds of Fortune 500 companies," *Cyberscoop*, April 30, 2025.

Kott, Alexander, George (Yegor) Dubynskyi, Andrii Paziuk, Stephanie E. Galaitsi, Benjamin D. Trump, and Igor Linkov, "Russian Cyber Onslaught was Blunted by Ukrainian Cyber Resilience, not Merely Security," *Computer*, Volume 57, Number 8, pp. 82-89.

Krouse, Sarah, Dustin Volz, Aruna Viswanatha, and Robert McMillan, "U.S. Wiretap Systems Targeted in China-Linked Hack," *The Wall Street Journal,* October 5, 2024. As of April 21, 2026: https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

May, Paul and Pavla Holcova, "Inside Job: How a Hacker Helped Cocaine Traffickers Infiltrate Europe's Biggest Ports," *Organized Crime and Corruption Reporting Project*, February 14, 2020. As of April 19, 2026: https://www.occrp.org/en/project/narcofiles-the-new-criminal-order/inside-job-how-a-hacker-helped-cocaine-traffickers-infiltrate-europes-biggest-ports.

Melkozerova, Veronika, "Russian spooks hack Wi-Fi routers to spy on West," *Politico*, April 8, 2026. As of April 10, 2026: https://www.politico.eu/article/russias-gru-hacked-hundreds-of-wi-fi-routers-world-wide/.

Mott, Nathaniel, "Changelog: U.S. cyber leaders warn of China threat," *README_,* February 1, 2024. As of April 21, 2026: https://readme.synack.com/changelog-u.s.-cyber-leaders-warn-of-china-threat.

New Jersey Cybersecurity & Communications Integration Cell, "Volt Typhoon," *New Jersey Cybersecurity & Communications Integration Cell.* As of April 21, 2026: https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure/volt-typhoon.

O'Leary, Jacqueline, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," *Google Cloud*, September 20, 2017. As of April 17, 2026: https://cloud.google.com/blog/topics/threat-intelligence/apt33-insights-into-iranian-cyber-espionage/.

Otto, Emily, "Shamoon To Stryker: Iran Wields Wiper Attacks," *Center for European Policy Analysis*, March 16, 2026. As of April 17, 2026: https://cepa.org/article/shamoon-strikes-stryker-iran-wields-wiper-attacks/.

Paz, Daniel Blanco, "Cyber Warfare Capabilities of Mexican Cartels," *grey dynamics*, July 31, 2024. As of April 14, 2026: https://greydynamics.com/cyber-warfare-capabilities-of-mexican-cartels/.

Peled, Anat, "Iranian-Linked Groups Hacked Into at Least 50 Security Cameras in Israel," *The Wall Street Journal*, March 30, 2026. As of April 19, 2026: https://www.wsj.com/livecoverage/iran-war-news-updates/card/iranian-linked-groups-hacked-into-at-least-50-security-cameras-in-israel-dwrn3Wa3KcI3NfbGiHJl.

Perlroth, Nicole, "Colonial Pipeline paid 75 Bitcoin, or Roughly $5 Million, to Hackers," *The New York Times*, May 13, 2021. As of May 16, 2026: https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html.

-----, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2021. As of April 17, 2026: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Porche III, Isaac R., Jerry M. Sollinger, and Shawn McKay, *A Cyberworm that Knows no Boundaries*, Santa Monica, California: RAND Corporation, 2011.

Przetacznik, Jakub and Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks," Brussels: European Parliamentary Research Service, June 2022, p. 3. As of April 22, 2026: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

Purser, Joye, "Five Years Later: Lessons Learned From Colonial Pipeline Ransomware Attack," *Infosecurity Magazine*, May 6, 2026. As of May 16, 2026: https://www.infosecurity-magazine.com/opinions/lessons-learned-from-colonial/.

Reddy, Shreyas, "Why a private US citizen decided to take down North Korea's internet on his own," Interview, *NK News*, May 7, 2024. As of March 26, 2026: https://www.nknews.org/2024/05/why-a-private-us-citizen-decided-to-take-down-north-koreas-internet-on-his-own/.

Ren, Z.Z, Zhihong Shao, Junxiao Song, Huajian Xin, Haocheng Wang, Wanjia Zhao, Liyue Zhang, Zhe Fu, Qihao Zhu, Dejian Yang, Z.F. Wu, Zhibin Gou, Shirong Ma, Hongxuan Tang, Yuxuan Liu, Wenjun Gao, Daya Guo, and Chong Ruan, "DeepSeek-Prover-V2: Advancing Formal Mathematical Reasoning via Reinforcement Learning for Subgoal Decomposition," *github*. As of April 20, 2026: https://github.com/deepseek-ai/DeepSeek-Prover-V2.

Roberts, Jen and Emma Schroeder, "Makings of the Market: Seven perspectives on offensive cyber capability proliferation," *Atlantic Council*, March 1, 2023. As of March 8, 2026: https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/makings-of-the-market-seven-perspectives-on-offensive-cyber-ca-

pability-proliferation/.

Rogin, Josh, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history'," *Foreign Policy,* July 9, 2012. As of April 21, 2026: https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

Sanger, David E. and Julian E. Barnes, "China's Hacking Reached Deep Into U.S. Telecoms," *The New York Times,* November 21, 2024. As of April 21, 2026: https://www.nytimes.com/2024/11/21/us/politics/china-hacking-telecommunications.html.

Sarma, Gopal and Kathleen Fisher, "Tipping the Cyber Balance: How AI Benchmarks Could Make Software Safer," *RAND Corporation*, February 3, 2026. As of March 8, 2026: https://www.rand.org/pubs/commentary/2026/02/tipping-the-cyber-balance-how-ai-benchmarks-could-make.html.

Sganga, Nicole, "Chinese hackers took trillions in intellectual property from about 30 multinational companies," *CBS News,* May 4, 2022. As of April 21, 2026: https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies.

Stanish, Erika, "Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group," *CBS News*, November 26, 2023. As of April 17, 2026: https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/.

Suárez, Amanda, "Why Mexican Cyber-Cartels Threaten U.S. National Security," *Geopolitical Monitor*, June 24, 2021. As of April 14, 2026: https://www.geopoliticalmonitor.com/why-mexican-cyber-cartels-threaten-u-s-national-security/.

Swetlitz, Ike and Miquéla V. Thornton, "Stryker Cyberattack Delays Surgeries for Some Patients," *Bloomberg*, March 18, 2026. As of April 17, 2026: https://www.bloomberg.com/news/articles/2026-03-18/stryker-cyberattack-delays-surgeries-for-some-patients.

Taylor, Nuray, "Fueling Cartels' Cybercrime," *The Cyber Edge*, October 1, 2025. As of April 14, 2026: https://www.afcea.org/signal-media/cyber-edge/fueling-cartels-cybercrime.

The White House, *Back to the Building Blocks: A Path Toward Secure and Measurable Software*, Washington, D.C.: The White House, February 2024.

-----, *2023 White House Strategy to Combat Transnational Organized Crime*, Washington, D.C.: The White House, December 2023.

Tromblay, Darren E., "From Outside Assaults to Insider Threats: Chinese Economic Espionage," *Information Technology & Innovation Foundation,* November 3, 2025. As of April 21, 2026: https://itif.org/publications/2025/11/03/from-outside-assaults-to-insider-threats-chinese-economic-espionage/.

United Nations Office of Counter-Terrorism, *Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks*, New York: United Nations Office of Counter-Terrorism, 2024.

U.S. Department of Defense, *DOD Command, Control, and Communications (C3) Modernization Strategy*, Washington, D.C.: U.S. Department of Defense, September 2020.

U.S. Department of Justice, "Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups," *U.S. Department of Justice*, December 9, 2025. As of April 10, 2026: https://www.justice.gov/opa/pr/justice-department-announces-actions-combat-

-----, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," *U.S. Department of Justice*, June 7, 2021.

U.S. Federal Bureau of Investigation, "Director Wray's Remarks at the Vanderbilt Summit on Modern Conflict and Emerging Threats," *FBI*, April 18, 2024. As of April 21, 2026: https://www.fbi.gov/news/speeches-and-testimony/director-wrays-remarks-at-the-vanderbilt-summit-on-modern-conflict-and-emerging-threats.

U.S. Government Accountability Office, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, Washington, D.C.: U.S. Government Accountability Office, January 2022.

Zetter, Kim, "Report: Google Hackers Stole Source Code of Global Password System," *Wired,* April 20, 2010. As of April 21, 2026: https://www.wired.com/2010/04/google-hackers.

The Soufan Center is a 501c3 non-profit organization

THE SOUFAN CENTER

156 W 56th Street
New York, NY
10019

Phone
+1 646-248-6486
Email
info@thesoufancenter.org
Website
www.thesoufancenter.org