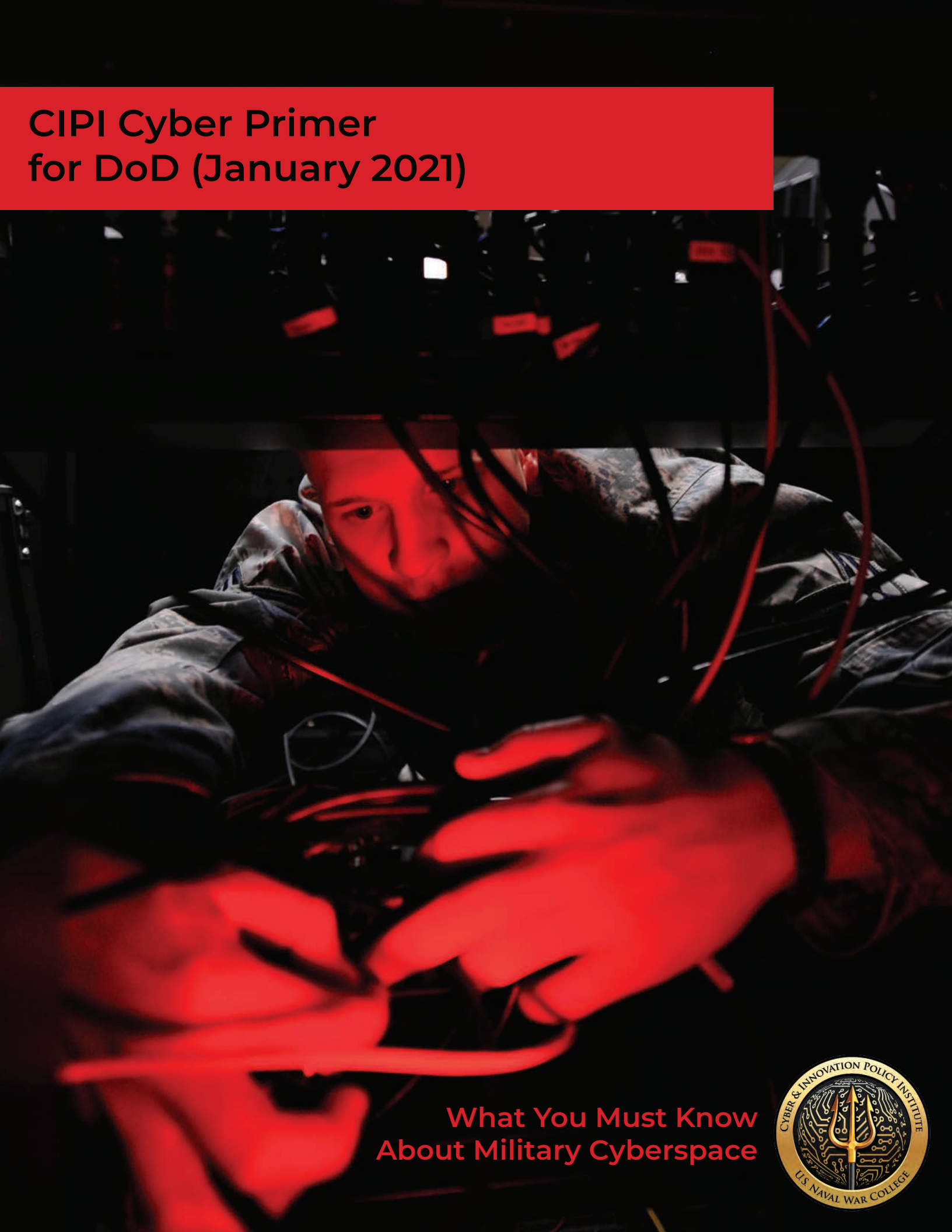
CIPI Cyber Primer for DoD (January 2021)



What You Must Know About Military Cyberspace

CYBER & INNOVATION POLICY INSTITUTE
U.S. NAVAL WAR COLLEGE

Contents

CYBER & INNOVATION POLICY INSTITUTE

U.S. NAVAL WAR COLLEGE

The Cyber & Innovation Policy Institute (CIPI) is the premier hub for cyber operations and strategy research at the U.S. Naval War College. The CIPI team is Frank Smith (director), Chris Demchak, Peter Dombrowski, Nina Kollars, Torey McMurdo, Ben Schechter, Paul Schmitt, Rachael Shaffer, and Sam J. Tangredi.

Ideas expressed in this document do not necessarily represent views of the U.S. Naval War College, the U.S. Navy, the U.S. Department of Defense, or the U.S. Government.

Graphic design: Kyle Victory

Images: https://www.flickr.com/photos/usairforce/4615586685 (cover)
https://www.flickr.com/photos/army-cyber/22224758158 (p.1)
https://www.flickr.com/photos/us7thfleet/36269793602 (p.9)

686 Cushing Road, Newport RI 02841

cipi_director@usnwc.edu

https://usnwc.edu/CIPI

@NWC_CIPI

Military Cyberspace: Essential, Different, Vulnerable

What does DoD need cyber for? Almost everything.
Cyberspace is more than merely an "enabler." It's essential. U.S. military operations in physical domains—land, sea, air, and space—increasingly depend on the cyber domain of networked information communication technology for command and control. So do other joint functions such as intelligence, fires, movement and maneuver, protection, and sustainment. Alternatives to cyber, such as analog communications, are poor substitutes for the speed, precision, and ease afforded by digital computer networks. Modern military power, like the modern economy , depends on cyberspace.

Cyberspace is integral to any credible theory of victory.

Cyber differs from land, sea, air, and space.
Unlike other global warfighting domains, cyberspace is a manmade environment created using digital electronics and the electromagnetic spectrum. Once networked in this way, the physical distances that define other domains become less relevant in cyberspace. Data in cyberspace can also be created, copied, and communicated, as well as corrupted, degraded, or destroyed. These cyber actions and effects have few apt analogies to military ations in physical domains. Attributing malicious action in cyberspace is also more difficult because of the volume, speed, and scale of cyber activity.

Its military utility differs as well. "Pwning" or owning an adversary's computer network doesn't mean the same thing as achieving air superiority or sea control, for instance. You can't just "sprinkle some cyber on" military operations in other domains. Nor can you just "bolt cyber on" after the fact to effectively analyze these operations through wargames, modeling, and simulation. Comprehension of different cyber actions and effects varies across the DoD workforce. If these differences aren't considered and baked into military planning, then cyber risks are ignored and misconstrued at considerable peril.

Military cyberspace is vulnerable.
All the capabilities that depend on cyberspace come at the cost of cyber vulnerability. Dependence on cyberspace is risky because this domain is vulnerable to error and attack. Information communication technology doesn't reduce the complexity of armed conflict or competition: It shifts when, where, and how complications manifest. Failure to account for this shift threatens to turn the U.S. military's technological advantages into dangerous liabilities.

Some of these vulnerabilities involve systemic risk. DoD depends on cyberspace outside of its control. Military cyberspace is intertwined with civilian, private, and foreign hardware, software, and data. Vulnerabilities outside the DoD can harm the armed services and military operations.

Some vulnerabilities are unique to DoD. The military's missions, capabilities, and personnel differ from other organizations. Its cyber vulnerabilities differ as well. DoD must balance tradeoffs between its specialized warfighting needs and general enterprise applications, as well as between the capabilities and vulnerabilities of military cyberspace. Fail to do so, and you court defeat.

Threat Environment: Cyberspace Is Contested

DoD does not—and cannot—dominate cyberspace. Control over this domain is distributed. Adversaries readily contest the U.S. military in and through it. Although cyber threats are longstanding, cybersecurity wasn't a top priority for DoD until recently. This legacy, combined with the complexity, scope, and rate of technological change, means that military cyberspace is not assured.

Threat actors range from states to non-state actors and individuals. They cause accidental and deliberate harm. Cybercrime threatens American prosperity and, with it, both the wealth that supports U.S. military power and the intellectual property that supports military technology. In addition, espionage is a primary objective for many state and state-sponsored hackers. Cyber espionage is a direct threat to DoD and a potential precursor to more destructive attacks. Information warfare and cyber harassment also threaten military readiness and unit cohesion.

Adversaries understand that the United States and its military rely on cyberspace. Examples of hacks that impact DoD include:

China (probably)

OPM hack: Between 2013 and 2015, this data breach at the U.S. Office of Personnel Management compromised sensitive records for more than 4 million government employees, putting U.S. military and intelligence personnel at risk.

Defense contractor hacks: For more than a decade, terabytes of data have been stolen from the defense industrial base on weapons that range from the F-35 Joint Strike Fighter and Patriot missile to undersea warfare systems.

Russia (probably)

2016 U.S. election interference: After hacking the computer accounts of American politicians, stolen data was published to interfere with the presidential election. Active measures also provoked political discord through social media. Defending elections from foreign hacking subsequently became a top priority at U.S. Cyber Command (USCYBERCOM).

2020 SolarWinds breach: This hack planted malware in the supply chain of trusted software, gaining access to hundreds of U.S. government agencies and corporations. A private firm reported the breach before the Department of Homeland Security (DHS) or DoD.

Policy Challenges

Cyber threat assessment is difficult. DoD is at risk. But how credible is risk analysis when uncertainty is high and information sharing is limited? Is cyber net assessment useful when idiosyncratic factors such as the skill and luck of individual users can impact the vulnerability of military systems?

Few cyber attacks are spectacular, but many are corrosive. The threat to date does not resemble a "cyber Pearl Harbor" or "cyber 9/11." How can DoD respond accordingly when computer code doesn't explode and yet adversaries use cyberspace to erode U.S. military capabilities?

States are only part of the problem. Non-state actors threaten the U.S. military through cyber intrusions and attacks, as well as through gaps, errors, and weaknesses in the information technology supply chain. How does DoD address friendly as well as hostile groups and individuals, including insider threats?

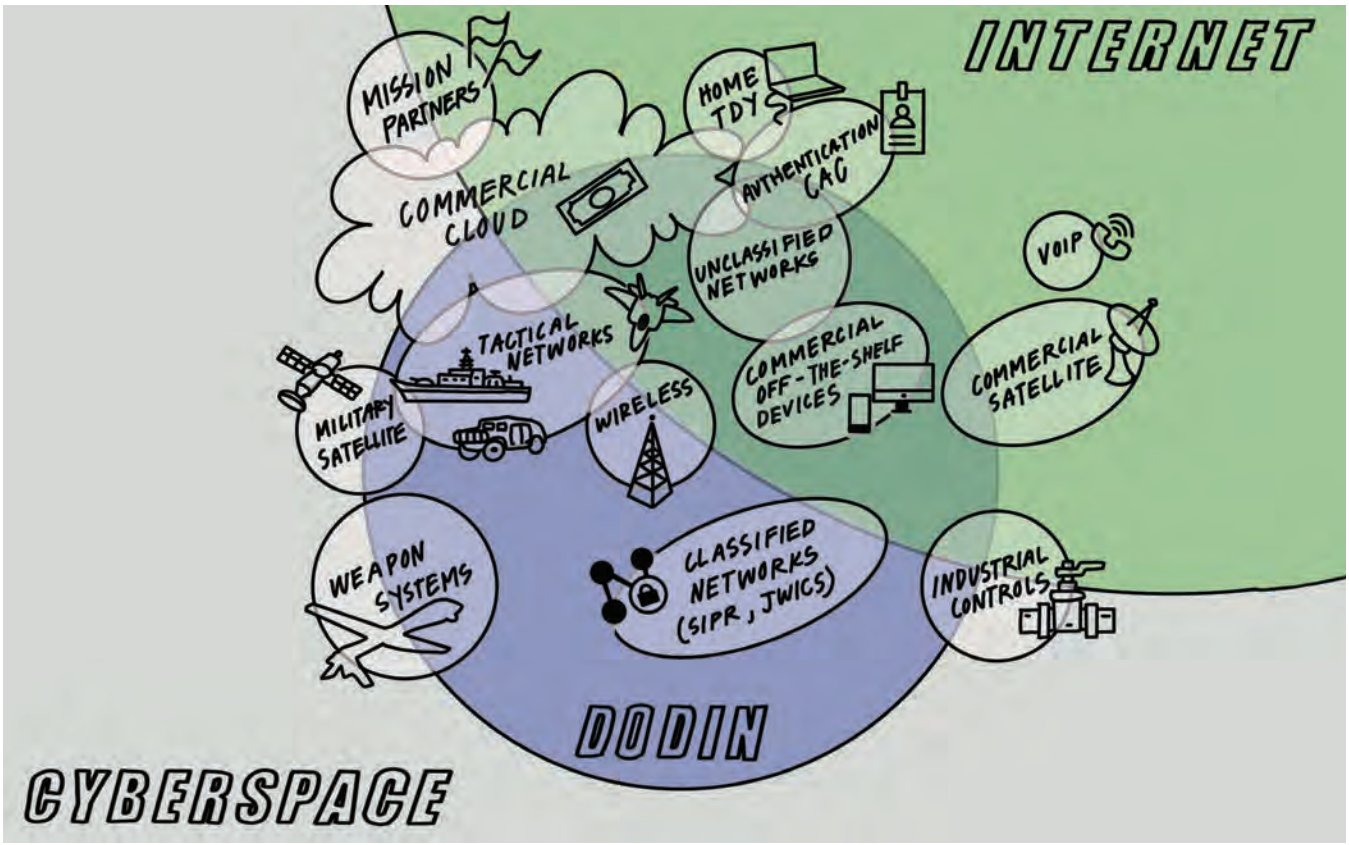
Structure of DoD Cyberspace

DoD cyberspace is the DODIN, namely, the Department of Defense Information Network.

The DODIN is a complex, global system. It consists of dozens of gateways, hundreds of data centers, thousands of information systems, and millions of devices connected through countless networks, segments, enclaves, and clouds. Some of the infrastructure is physical, including cables, cell towers, and satellites. Some is virtual. It's a vast attack surface. The DODIN includes the U.S. military's classified and unclassified computer networks, as well as the networked hardware and software in its weapon systems, industrial control systems, and telecommunications. It extends from the tactical edge to back office equipment in the Pentagon.

DoD often relies on shared and commercial cyber infrastructure

The U.S. military uses the DODIN in almost every mission, command, and area of responsibility. However, this "network of networks" is not built, owned, or operated entirely by DoD. DODIN infrastructure is a mix of military and civilian, public and private, old and new, foreign and domestic. As a result, U.S. military cyberspace isn't an exclusively military space, or exclusively American. The warfighting domain overlaps with the broader Internet. Cyber conflict and competition can occur through everyday infrastructure.



Defend Forward: DoD Cyber Strategy

The *2018 DoD Cyber Strategy* is derived from the *2018 National Defense Strategy*. The *2018 DoD Cyber Strategy* seeks to build a more lethal force, compete and deter in cyberspace, strengthen alliances, reform the Department, and cultivate talent.

The most important shift from past thinking is competition. To compete, DoD's cyber posture changed from holding its forces in reserve as a deterrent threat to defending forward.

Defend Forward is the strategic concept implemented by USCYBERCOM: The functional, Unified Combatant Command for cyberspace operations. This concept includes offensive and defensive operations that are conducted outside DoD networks and below the threshold of armed conflict.

A supporting concept is **Persistent Engagement,** whereby USCYBERCOM proactively targets adversaries to impose costs. Competition is continuous and prioritized as much as deterrence and warfighting.

This approach assumes that tactical and operational gains and losses in cyberspace accumulate to strategic effect—victory or death by a thousand cuts. It also involves allies and partners. For example, USCYBERCOM conducts "hunt forward" missions at the invitation of foreign partners to help defend friendly government networks.

Policy Challenges

Unintended consequences: "Those who live in glass houses should not throw stones." DoD depends on cyberspace. So, is an assertive (if not offensive) approach advantageous or shortsighted? Either way, how should DoD manage second- and third-order effects, including blowback and escalation risks, in friendly, neutral, and hostile networks?

Metrics of success or failure: How do you know if this strategy is working? Cyber actions often lack physical effects. So how are they measured? What outcomes are evidence of cyber initiatives that advance U.S. national security, and how does the return on investment compare with other tools?

Organization for information environments: What is the best way to organize cyber forces? The same commander leads USCYBERCOM and the National Security Agency (NSA). Is this an effective structure for military and intelligence missions, as well as for coordination with DHS and other agencies? Are the authorities, roles, and responsibilities appropriate and sufficient? How about oversight and integration with other capabilities?

Cyber Operations

Cyber operations combine several tactical engagements to achieve strategic objectives. These campaigns require coordination across time and space. Few targets in cyberspace are static: Hardware and software are updated and patched. Users learn and change. Thus, planning cyber operations requires a concerted effort across multiple teams and services. Integrating them with other kinetic and non-kinetic operations compounds the coordination challenges.

DODIN Operations
The first line of defense, DODIN operations protect DOD cyberspace. They are proactive and threat agnostic, mitigating vulnerabilities and maintaining military infrastructure.

Defensive Cyberspace Operations
Defensive operations address specific threats. These operations include threat hunting, active countermeasures, and incident response. They are conducted in DoD and specified non-DoD cyberspace. Some missions may damage or destroy enemy systems.

Offensive Cyberspace Operations
Offensive operations attack adversaries in and through cyberspace. Targets range from hardware, software, and data to physical infrastructure, weapon systems, and command and control in other domains. These operations aim to create immediate effects, including damaging or destroying enemy systems.

Cyber attacks are conducted in hostile or third-party networks. In theory, they are related but distinct from cyber exploitation, which includes intelligence collection and battlespace preparation. Whether target audiences accept this distinction is another question.

Examples of offensive operations include:

Stuxnet: Origin unknown, but widely reported to involve the United States and Israel. This cyber campaign targeted Iran's uranium enrichment facilities. The attack was discovered in 2010.

Glowing Symphony: Operation conducted by USCYBERCOM Joint Task Force Ares to disrupt, degrade, and destroy the Islamic State's activity in cyberspace, starting in 2016. This campaign reportedly involved interagency deconfliction, cyber targeting outside Syria and Iraq, and coordination with kinetic operations.

Policy Challenges

Timelines: Cyber ≠ fast. Amateur hackers can launch simple distributed denial of service attacks with a few clicks of the mouse. But valuable targets may be hard targets that require exquisite exploits, which take months or years to develop. How should lead-time be factored into operational planning?

Tradeoffs: Cyber operations are costly and often involve intelligence gain/loss. Destroying a target or alerting an adversary that they've been detected threatens the intelligence otherwise gained from monitoring the target or intrusion. Quieter operations are more difficult. Even preparing for offense by stockpiling cyber vulnerabilities runs the risk that the knowledge and exploits will perish, leak, or backfire. How are these costs and benefits weighed?

Scale: It isn't easy or automatic to increase the scale of cyber fires. Successfully attacking one enemy weapon system, or defending against one intrusion, doesn't mean that the same capabilities apply to other targets. What military effects result from single use operations, and what effects are replicable at scale?

Cyber Tactics

Cyber tactics are the steps taken to attack and defend specific parts of cyberspace. Offense and defense are both technical and social: Hacking computers as well as hacking users' behavior. The tactics involved are often described in terms of the "cyber kill chain," namely, the step-by-step sequence of a hack illustrated below. Offensive tactics link these steps together to produce cyber effects. Defensive tactics aim to break the chain.

Tactical defense

You defend what's valuable. That includes the confidentiality, integrity, and availability of DoD cyberspace, without which the U.S. military risks tactical defeats that cost blood and treasure. Recall that the DoD cyber strategy of Defend Forward also assumes that tactical losses aggregate into strategic threats to the Nation.

Cyber defense is difficult. Every new user, new device, and new line of code changes the domain. Defending it depends on discriminating between legitimate and malign behavior: No mean feat when the structure and contents of cyberspace are in flux and attribution in this domain is difficult.

Cyber defense is not impossible, however. You use defensive tactics every day. For example, passwords and encryption both impede adversaries, even if you're sketchy on the details of how they work. Other tactical tools include access controls, firewalls, filters, and virtual private networks that help protect DoD cyberspace; antivirus, logs, audits, and intrusion detection systems that help monitor malware and hacking; honeypots that distract, redirect, or reveal hacks; plus backups and segregated environments that help limit damage. There is no silver bullet or quick fix. But defensive tactics reduce the risks.

Tactical offense

Offensive tactics are purposeful. They aim to deceive, degrade, deny, disrupt, or destroy. Examples range from phishing that tricks users into revealing confidential information and ransomware that locks their files to remote access tools that manipulate, exfiltrate, or destroy hardware, software, and data from afar.

Offensive tactics are flexible. They can be tailored for different effects. Cyber espionage may be quiet and persistent, for instance, employing tactics that are difficult to detect and uproot. In contrast, cyber attacks that destroy computer systems and networked equipment may be easily detected once executed. Attackers—be they states, terrorists, or criminals—can build, buy, and borrow a variety of exploits and expertise. Since the tools and knowledge get repurposed and reused, proliferation is a problem.

Effects vary. The efficacy of offense depends on the technology and skill used to defend the target. Again, valuable targets may be hard targets. Cyber attacks don't always succeed. Nor do they always have the intended effect. Your confidence in these tactics should vary accordingly.

Allies and Partners

Alliances and partnerships are integral to DoD cyber strategy, operations, and tactics. The U.S. military can't do cyber alone. DoD depends on foreign and domestic relationships. These relationships depend on trust, and trust is social– It can't simply be coded or hardwired into software and hardware.

Domestic

Critical relationships inside the government include military and intelligence services, evident in the dual hatted leadership of USCYBERCOM and NSA. DoD relationships with civilian authorities are critical as well, particularly with the Cybersecurity & Infrastructure Security Agency in DHS and the National Cyber Investigative Joint Task Force run by the Federal Bureau of Investigation.

Interagency cooperation is necessary but not sufficient, however. The military must also work with the private sector, which owns much of the critical infrastructure that DoD depends on. It must work with the defense industrial base as well, which DoD must help defend against cyber intrusions and attacks.

In addition, DoD must work with companies in Silicon Valley and elsewhere that focus on commercial markets. It must engage as a large but nevertheless minority player in the global marketplace for information technology. The same is true for academic partnerships. DoD needs interdisciplinary talent and expertise from higher education for military cyber.

Foreign

Cyberspace is global. International partnerships provide competitive advantages. Many allies and partners have advanced cyber capabilities. These capabilities complement our own through trusted relationships (e.g., the Five Eyes alliance and NATO). Capacity building can also create new opportunities for combined cyber operations and collective cybersecurity.

Policy Challenges

Operational partnerships: Collaboration is easier said than done. Military cyber depends on authorities, responsibilities, and capabilities that are spread—but not always shared—across public and private sectors at home and abroad. How can DoD work more effectively through the interagency? How can it manage clashes in culture with non-traditional defense contractors, as well as tensions between commercial interests in profit and liability protection versus public interests in cybersecurity?

Information sharing & interoperability: Information technology enables information sharing. Yet information sharing about cyber threats remains limited. So is interoperability. How can DoD share and receive more timely and useful information? How can it interoperate effectively with diverse allies and partners?

Secrecy: Some cyber capabilities must be classified and compartmentalized to be effective. But over-classification can blunt information sharing and military innovation, as well as risk assessment and oversight. How can DoD protect sensitive information without handicapping itself with counterproductive information controls?

Laws and Norms

Military cyberspace and cyber operations are governed by numerous laws, regulations, and policies. Domestic laws are most important. But DoD also has a stake in international laws and norms for cyberspace.

Domestic

Important rules that govern U.S. military cyber operations include, among others:

National Defense Authorization Act (NDAA) for FY2012, SEC. 954: Authorizes DoD to conduct offensive cyber operations but doesn't specify if they count as covert action under Title 50, SEC. 3093.

NDAA FY2019, SEC. 1632: Specifies that, under certain conditions, cyber operations are traditional military activities and thus exempt from constraints on covert action.

NDAA FY2019, SEC. 1692: Authorizes DoD to disrupt, defeat, and deter active, systematic, and ongoing attack campaigns by Russia, China, North Korea, or Iran. This provides the legal backbone for Defend Forward.

2018 National Security Presidential Memoranda 13 (NSPM-13): Classified guidance that reportedly allows for the delegation of authorities to DoD for offensive cyber operations.

Along with the rules for cyber operations are laws governing electronic surveillance, such as the Foreign Intelligence Surveillance Act. For law enforcement, the U.S. Department of Justice had used the Computer Fraud and Abuse Act to indict Chinese, Russian, and Iranian nationals for hacking, among other charges. Additional regulations require DoD contractors to secure covered defense information and report cybersecurity incidents. Compliance with the Cybersecurity Maturity Model Certification likewise attempts to protect the defense industrial base and supply chain.

Military norms and culture are also influential in cyberspace. Not all norms are good. Nor are they fixed. For example, the U.S. military normally focuses on kinetic force, but cyber options may change the standards for appropriate behavior.

International

Some international laws apply to cyberspace. The Budapest Convention, for instance, is an international treaty on cybercrime. The Tallinn Manual, a non-binding study for NATO, argues that the law of war and international humanitarian law apply to cyber warfare as well.

Interpretations of international laws and norms for cyberspace are contested, however. Disputes over rival interpretations are one way that competition plays out in the United Nations and other fora. Trust between the United States, China, and Russia is low.

Technical standards, protocols, and infrastructure are also sites for international competition that impact DoD. Fear about Chinese dominance of 5G wireless infrastructure is one example. Others include commercial encryption standards and internet protocols. Standards competitions are policy choices with winners and losers. The outcomes are consequential: They lay the foundation for building and leveraging power—including military power—in cyberspace.

Adjacent Capabilities & Emerging Technologies

So many military functions depend on cyberspace that it's easy to confuse or conflate different information related capabilities. It's also dangerous. Cyber operations are related but distinct from electronic warfare, for instance. So are space operations, cryptology, and military information support operations. The psychological, social, and political expertise needed to influence foreign audiences through cyberspace differ from the technical expertise needed to hack foreign networks. The U.S. military needs each of these capabilities: One doesn't substitute for the other.

It's likewise dangerous to conflate competition and lethality, particularly in cyberspace. Cyber competition below the threshold of armed conflict is related but distinct from a high intensity, kinetic fight. The U.S. military needs to prevail in both. DoD cannot afford to gloss over the differences.

Cyber Dependent, But Different

You've heard the hype: Artificial intelligence! Blockchain! Quantum! Emerging technologies are often described as if they'll disrupt the military and revolutionize warfare. Perhaps they will. Perhaps not. It's difficult to predict the future. Technology hype can mask important gaps between imagined and actual performance. It can also draw attention away from less flashy but more significant technological change.

Artificial intelligence: AI depends on trusted "big data" and algorithms that are created, communicated, processed, and stored in cyberspace. Data is a strategic asset. But datasets and algorithms created for civilian applications may be biased or inapplicable to military AI. Artificial or not, "intelligence" depends on context.

Blockchain: Distributed ledger technologies are software applications that use decentralized architectures and cryptography for database management—here again, through cyberspace. Potential military applications range from improving data integrity to supply chain management. But potential vulnerabilities aren't well specified.

Quantum technologies: The special properties of quantum mechanics can be used to build new kinds of computers, ciphers, and sensors. However, quantum information systems still depend on digital information systems and thus cyberspace: They aren't a replacement. In theory, powerful quantum computers threaten public key encryption and authentication. In practice, it's uncertain if or when such machines will ever be built.

Research and development depend on policy choices. Military applications aren't inevitable. Nor is U.S. military leadership. Whereas the Internet was born in the USA and cyberspace came of age during a peak in American power, times have changed. DoD must now reckon with allies, adversaries, and third parties with far more sway over emerging technologies and how they're used in competition and conflict.

Want To Know More? Recommended Reading

There's a lot written about cyber. Some of it's useful. While by no means a complete list, the following reading provides a starting point for additional insight into cyber conflict and military cyberspace.

Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (2017). A geopolitical perspective on the uses and misuses of cyber power during the 2010s.

Nigel Inkster, *China's Cyber Power* (2016). Accessible description of how the People's Republic of China seeks to shape cyberspace to its advantage at home, abroad, and on the battlefield.

Martin Libicki, *Cyberspace in Peace and War* (2016). Comprehensive overview that connects technical content with key policies, operational concepts, strategies, and norms for cybersecurity.

Rebecca Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* (2016). Critical analysis of Stuxnet, challenging the widespread belief that offense has the advantage in cyberspace.

Josephine Wolff, *You'll See This Message When It Is Too Late* (2018). A rare analysis of what happens after data breaches in the public and private sectors, as well as the lessons to learn in the aftermath.

Additional References

Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017). Renowned study of legal regimes that apply to cyber operations above and below the threshold of armed conflict.

Joint Chiefs of Staff, *Cyberspace Operations, Joint Pub 3-12* (2018). Doctrine that provides authoritative guidance on the organization and function of U.S. military cyber operations.

U.S. Department of Defense, *Summary of the DoD Cyber Strategy* (2018). Unclassified overview of the current strategic approach.

The White House, *National Cyber Strategy of the United States of America* (2018).

Angus King and Mike Gallagher, *Cyberspace Solarium Commission* (2020). Bipartisan, consensus report on how to reform the U.S. national cybersecurity policy.


CYBER & INNOVATION POLICY INSTITUTE
U.S. NAVAL WAR COLLEGE