MIT
POLITICAL SCIENCE

Massachusetts Institute of Technology
Political Science Department

Research Paper No. 2016-2

Perspectives on Cybersecurity:
A Collaborative Study

Massachusetts Institute of Technology:

Nazli Choucri
Chrisma Jackson
Lyla Fischer
Brooke Gier
Vivian Peron
Ben Ze Yuan
Liu Yangyue
Glenn Voelz

Do Not Cite or Circulate Without Permission from Authors

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

PERSPECTIVES on CYBERSECURITY
A Collaborative Study

Authors

Chrisma Jackson

Lyla Fischer

Brooke Gier

Vivian Peron

Ben Ze Yuan

Liu Yangyue

Glenn Voelz

Editors

Nazli Choucri

Chrisma Jackson

Department of Political Science

MIT

2015

Table of Contents

5. DoD Perspective on Cyberspace

Glenn Voelz

The emergence of threats from "cyberspace" present new national security challenges for state actors, particularly technology-dependent nations whose political, economic and military powers are reliant upon information technology and networked computer systems. For these countries, including the U.S., the exercise of military power increasingly demands uninterrupted access to globally interconnected command and control systems, communications, guidance and navigation systems, intelligence-gathering platforms, and logistics networks. Additionally, sensitive intellectual property and defense-related information residing in the Defense Industrial Base is vulnerable to these new forms of attacks, as well as industrial infrastructure and economic assets. In 2013, the Director of National Intelligence identified cyber attacks as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of 9/11.[78] These threats have grown in complexity as a wider range of actors engage in such activities, including "profit-motivated criminals, ideologically motivated hackers or extremists and variously-capable nation-states like Russia, China, North Korea and Iran," according to recent testimony by the Director of National Intelligence.[79]

Analysts generally agree that the cyber domain presents a unique set of challenges for U.S. national security, specifically due to the fact that the cyber domain affords adversaries unprecedented reach, speed, and anonymity. Additionally, the cyber domain is generally considered to offer tactical advantage to the offense.[80] These characteristics have increased the ability of state and non-state actors to use distributed computer systems for the purposes of espionage, crime, terrorism, and even physical attacks as part of larger conventional military campaigns.

5.1 Developing a Taxonomy of Cyber:

As a relatively new national security concern, there remains significant debate over the basic matter of taxonomy, specifically how to define and categorize these threats. A clear understanding of what constitutes an attack within this domain is a necessary prerequisite for developing appropriate policies and response options. For the purpose of this discussion, the term *cyberwarfare* generally refers to state-on-state actions, equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force.[81] Acts of *cyberterrorism* involve the "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." Distinct from these is the issue of *cybercrime*, involving "unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies." *Cyberespionage* is also considered a distinct activity involving the theft of "classified or proprietary information used by governments or private corporations to gain a

[78] U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: April 2015), 9.
[79] James R. Clapper, *Opening Statement to the Worldwide Threat Assessment Hearing*, Senate Armed Services Committee, February 26, 2015. http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee
[80] For elaboration of these concepts see Dakota L. Wood and Heritage Foundation, *Index of U.S. Military Strength: Assessing America's Ability to Provide for the Common Defense* (Washington DC: Heritage Foundation, 2015), 74.
[81] For overview see Catherine A. Theohary and John W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief* (Washington DC: Congressional Research Service, 2015), 1.

competitive strategic, security, financial, or political advantage."

Comparing Conventional Warfare versus Cyberwarfare[82]

	Conventional Warfare	**Cyberwarfare**
Political Context	Westphalian construct; conflicts waged by professional armies and state actors pursuing well-defined geo-political objectives. Grounded in conventional deterrence theories. Clear and well-established distinctions between warfare, terrorism, espionage and criminal behavior. Activities governed by established convention (law of war, Geneva, Hague, etc).	Extra-Westphalian; potentially involving both state and non-state actors pursuing financial, political or ideological causes, sometimes with ambiguous objectives. Uncertain rile for deterrence theories. Unclear distinctions between warfare, terrorism, espionage and criminal behavior. No clearly established norms for offensive cyber activities and use as a part of military campaigns.
Adversary Characteristics	Warfare waged by state armies and professional soldiers using doctrinal organized formations and functioning by depersonalized, bureaucratic logic. Adversaries are constrained by geographic space, logistics and industrial capacity.	Warfare waged by state as well as non-state entities. Some may use anonymity for operational advantage; use idiosyncratic tactics and organized around highly disaggregated networks. Adversaries are unconstrained by geography and distance. Power not directly linked to industrial capacity.
Operational Environment	Contested primarily in the conventional physical domains of war (land, sea, air, space) and waged in a contiguous linear battle-space; zone of conflict is defined by clear operational boundaries, fire and maneuver over geographic terrain. Conflict defined by measures conventional military power.	Contested primarily in the informational and cyber domain; spatially and temporally unbounded; defined by a merger of external and domestic security spheres of concern concerns. May include unconventional targets such as financial, infrastructure, private or pubic institutions.
Theories of War-Fighting	Influenced by tenets of maneuver warfare: mass, firepower, destruction of enemy forces and seizure of key terrain. Focus is on the operational level of war. Tactical advantage is to the Defense; however, cyber has also become a weapon of conventional warfare.	Influenced by technology theories and information warfare doctrines. Defined by unconventional approaches that do not align with traditional war-fighting theories. Tactical advantage is to the Offense.
Targeting Paradigm	Status-based targeting against legitimate military targets with focus on units, formations and equipment; Well-defined rules of engagement.	No clearly defined norms of targeting. Private and public interests, infrastructure, financial, informational, and military assets are all potential targeting. Ambiguous rules of engagement.

5.2 Evolution of DoD Cyber Strategy:

In response to these new challenges, the DoD has gradually developed a strategy framework for understanding the nature of these threats, development appropriate policies for dealing with them,

[82] Chart by author, Glenn Voelz

and organizing the national security apparatus to support a range of possible responses. Much of the progress in this area has been reactive in nature, triggered by specific events serving to highlight the increasing complexity of the threat environment. Some of the more notable examples in recent years include:

- The 2007 attacks against the Estonian parliament, banks, ministries, newspapers, and media outlets, purportedly originating from Russia, that raised the question of whether NATO member countries would respond collectively to the DDoS attacks.

- A series of intrusions from 2007-2008 into defense contractor information systems, reportedly ex-filtrating several terabytes of data related to F-35 design information.

- A 2008 incident involving malicious computer code uploaded onto a Central Command classified network via flash drive placed by a foreign intelligence agency - a turning point in U.S. cyber-defense strategy and led, in part, the formation of U.S. Cyber Command.

- A 2015 North Korean attack on Sony Pictures, considered one of the most destructive cyber-attacks on a U.S. entity to date. This attack fueled an ongoing national discussion about the nature of the cyber threat and the need for improved cyber-security cooperation between government and the private sector.

These events, among others, have led to new policy initiatives and organizational changes within the DoD focused on cyber defense, network protection and DoD support to critical infrastructure security. More recently, this has included the explicit integration of offensive cyber capabilities into military doctrine and national security strategy. Several notable milestones in this evolution include:

- In 2006, the Joint Chiefs of Staff published the first National Military Strategy for Cyberspace Operations focused specifically on cyber security. The document characterized the cyberspace domain, identified threats and vulnerabilities, and proposed a strategic framework to assure U.S. military superiority in cyberspace.

- In 2007, the DoD launched the Defense Industrial Base (DIB) Cyber Security and Information Assurance program designed to increase the protection of sensitive information relating to defense technologies, weapons systems, policy and strategy development, and personnel.

- In 2009, Defense Secretary Gates ordered consolidation of the various DoD cyber task forces into a single four-star command, the U.S. Cyber Command, which began operations in May 2010 as part of the U.S. Strategic Command.

- In 2011, the DoD issued its first Strategy for Operating in Cyberspace. This strategy was significant as a policy document by outlining DoD's overall initiatives for cyber space, and the recognition that DoD would treat cyberspace as a distinct operational domain (equivalent to air, land, maritime, and space) and organize, train, and equip forces so DoD could take full advantage of cyberspace's potential. However, this strategy document was vague on the use of offensive cyber capabilities and non-specific in the actors posing the greatest threats to U.S. interests.

- In 2015, the DoD issued an updated version of its Cyber Strategy, for the first time explicitly discussing the circumstances under which cyber-weapons could be used against an attacker. The document also explicitly named several countries presenting the greatest threat to U.S. interests in the cyber domain, including China, Russia, Iran and North Korea.

5.3 Overview of the 2015 DoD Cyber Strategy

The updated version of DoD's Cyber Strategy, released in 2015, outlined the evolving threats to U.S. interests, clarified the role of the DoD in countering these threats, and more clearly presented the range of possible policy responses to these threats. This has included an explicit statement describing a potential role for offensive cyber operations as part of a wider range of military response options. Several key points of the updated strategy document include:

- Highlighting that the nature of the threat and noting that "a disruptive, manipulative, or destructive cyber-attack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected."

- Clarifying bureaucratic roles and noting that the DoD, in concert with other agencies, is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace.

- Presenting clear strategic goals focused on building capabilities for effective cyber-security and cyber operations to defend DoD networks, systems, and information; defend the nation against cyber-attacks of significant consequence; and support operational and contingency plans.

- Outlining five strategy goals for cyberspace missions, including:
  1. Build and maintain ready forces and capabilities to conduct cyberspace operations.
  2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.
  3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence.
  4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.
  5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

- Describing the structure of the "Cyber Mission Force" (CMF) within the DoD, comprised of nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components.

- Acknowledging the challenge of deterrence in cyberspace, noting that due to the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behavior.

- Noting that attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups, thus requiring strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution.

- The strategy also clearly states that if directed, "DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities."

While the 2011 defense cyber strategy was primarily defensive in focus, the updated 2015 version offers a more aggressive posture, noting that "during heightened tensions or outright hostilities, DoD must be able to provide the President with a wide range of options for managing conflict escalation. If directed, DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities."[83] With regard to offensive cyber operations in the military context, recent legislation under Title 10 of the United States Code has supported this position and affirmed that "the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution."[84]

The updated strategy goes on to state that "there may be times when the president or the secretary of defense may determine that it would be appropriate for the U.S. military to conduct cyber-operations to disrupt an adversary's military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber-operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests."[85] However, it still remains somewhat unclear how the U.S. might respond to cyber attacks from non-state actors against private corporations or individual U.S. citizens.

Publication of the 2015 document marks a significant evolution from previous DoD strategy.

[83] U.S. Department of Defense, *The Department of Defense*, 14.

[84] See Section 954, in the 2012 National Defense Authorization Act

[85] U.S. Department of Defense, *The Department of Defense.*

The most significant change is the explicit acknowledgement that offensive cyber operations have a clear role as part of U.S. military strategy. Furthermore, the language suggests that these capabilities could even be used in a preemptive manner or in a shaping role "during heightened tensions or outright hostilities." This broadened scope of utility suggests a potential role for cyber operations as part of a conventional military conflict, where capabilities could be directed against an adversary's command and control networks, military-related critical infrastructure, and weapons system. The document also provides greater detail on the bureaucratic structure of the government's evolving cyber force and how these entities work to protect military assets, economic interests, and critical infrastructure.

While the threats depicted in the strategy are significant, at least one knowledgeable analyst has suggested that the new strategy reflected a more sober estimate of the potential impact from such attacks, describing something less catastrophic than an imminent "cyber Pearl Harbor."[86] Despite greater clarity in the new strategy, some questions remain with regard to how this construct will be applied in specific scenarios, as well as thresholds for the use of offensive cyber weapons. For instance, how does the new strategy clarify the distinctions between various forms of cyber attack, such as between cyber-war, cyber-espionage, cyber-terrorism and cyber-crimes? Furthermore, how would the distinctions between these actions be relevant in determination of appropriate responses, either by conventional military instruments or by cyber weapons? Finally, under what scenarios could an adversary's cyber attack escalate into a conventional kinetic response? The answers to many of these questions are likely unknowable until confronted and clearly would vary depending upon specific circumstances, the impacts of the attacks, and the parties involved. For this reason, strategies are not expected to provide an exhaustive menu of response options for every conceivable scenario; however, they should generate planning scenarios and serve as a catalyst for developing a flexible range of policy options for decision-makers, including the capabilities and response tools necessary for dealing with an unpredictable set of contingencies. In this sense, the new strategy appears to offer forward movement in the policy debate on cyberwarfare based on serious consideration of how the U.S. might respond against a realistic range of threats.

[86] Herb Lin, "Two Observations About The New DOD Cyber Strategy," Lawfare Blog (blog), April 24 2015, www.lawfareblog.com/2015/04/two-observations-about-the-new-dod-cyber-strategy/.

References

Clapper, James R. 2015. Opening Statements to the Worldwide Threat Assessment Hearing. Senate Armed Services Committee, February 26. http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee.

Lin, Herb. 2015. "Two Observations About The New DOD Cyber Strategy," *Lawfare Blog* (blog), April 24, 2015, www.lawfareblog.com/2015/04/two-observations-about-the-new-dod-cyber-strategy/.

Theohary, Catherine A. and John W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief*. Washington DC: Congressional Research Service. http://fas.org/sgp/crs/natsec/R43955.pdf.

U.S. Department of Defense. 2015. *The Department of Defense Cyber Strategy*. Washington, D.C.: April. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Wood, Dakota L. and Heritage Foundation. 2015. *Index of U.S. Military Strength: Assessing America's Ability to Provide for the Common Defense*. Washington, DC: Heritage Foundation. Available at http://ims-2015.s3.amazonaws.com/2015_Index_of_US_Military_Strength_FINAL.pdf.