

AN ASSESSMENT OF THE DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE

Thomas M. Chen

As cyberspace has become increasingly important, the U.S. Government has issued a number of publications on national cyber security strategy leading up to the 2011 *Department of Defense Strategy for Operating in Cyberspace*. Some themes have reappeared consistently, such as the need for public/private sector partnerships and information sharing; reduction of vulnerabilities; more cyber security training; and international cooperation. Most recently, the 2011 *White House International Strategy for Cyberspace* aimed to promote a global cyberspace environment that is “open, interoperable, secure, and reliable” based on “norms of responsible behavior,” and emphasized the need for international cooperation and public/private sector partnerships.

Whereas the *International Strategy for Cyberspace* focuses on diplomacy, the *DoD Strategy for Operating in Cyberspace* may be considered a complementary strategy that is primarily interested in actions to ensure military superiority and protection of American assets. The unclassified *DoD Strategy for Operating in Cyberspace* outlines five strategic initiatives to address cyber security. The *DoD Strategy* is significant as an official recognition of the strategic importance of cyberspace to national security. However, the document is brief and often omits specific details. In the remainder of this article, each strategic initiative in the *DoD Strategy* is examined for clarity, comprehensiveness, and novelty.

Strategic Initiative 1.

DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential. This strategic initiative is an official declaration that cyberspace will be treated as the fifth operational domain in addition to air, land, sea, and space. The strategy states “DoD will organize, train, and equip for the complex challenges and vast opportunities of cyberspace.” Substantial changes have been made in organization such as establishment of the U.S. Cyber Command (USCYBERCOM) in 2009. As an example of training, cyber red teams conduct war games, e.g., Cyber Storm.

This initiative is a message to other government agencies as well as to foreign countries about the seriousness of cyber operations (and possibly military responses to cyber attacks). However, this “militarization of cyberspace” raises a few issues that are not addressed specifically in the *DoD Strategy*. First, what are the boundaries of cyberspace considered to be within military jurisdiction? Most critical network infrastructures are owned and operated by the private sector. Second, how will cyber attacks warranting a military response be differentiated from other malicious acts, such as cybercrime? For instance, spear phishing to install malware may be a tactic used in both cybercrime and military cyber espionage. Third, could cyber attacks escalate

unnecessarily into physical warfare? Clearly, rules need to be developed to guide appropriate responses to cyber attacks.

The strategic initiative calls for investment in more resilient and secure computer networks but is not specific about how investments will be made. There has been research in resilient networks, self healing, and intrusion tolerance for many years. These advanced technologies are fairly well understood, but implementation at the scale of DoD networks would be enormously costly.

Strategic Initiative 2.

DoD will employ new defense operating concepts to protect DoD networks and systems. This initiative identifies four specific actions: implement cyber hygiene best practices; address insider threats by strengthening workforce communications, accountability, and internal monitoring; implement active cyber defenses against external threats; and develop new defense operating concepts and computing architectures, such as secure cloud computing.

Generally, this strategic initiative has good ideas consistent with common sense, but the ideas are conventional. For instance, the initiative presumes that good hygiene can prevent most malicious acts. While certainly helpful, safe practices will not protect users against advanced attacks that often make use of sophisticated social engineering and zero-day exploits.

Perhaps most interestingly, the *DoD Strategy* makes a point to contrast “active” defense with traditional “passive” defense. Active defense seems to refer to real-time intrusion detection and prevention. This initiative could be interpreted as an implicit message aimed at adversaries saying that real-time retaliation is possible. On the other hand, active defense in practice is notoriously challenging. Intrusion detection has been researched for decades, but the accuracy of real-time detection (and hence prevention) is still an open question due to the continual inventiveness of skilled adversaries. The strategic initiative does not explain how active defenses will be carried out or who will provide the technology.

Strategic Initiative 3.

DoD will partner with other U.S. Government departments and agencies and the private sector to enable a whole-of-government cyber security strategy. This strategic initiative recognizes that a broad level of cooperation with other government departments and private companies is clearly necessary. A notable example of interdepartmental cooperation was a 2010 memorandum of agreement between DoD and the Department of Homeland Security (DHS) to coordinate efforts to protect critical infrastructures and jointly support the National Cybersecurity and Communications Integration Center. Whereas DoD is normally limited to defending military computer networks, the memorandum of agreement allows DoD’s cyber warfare expertise to be leveraged to help DHS protect domestic networks and critical infrastructure.

Public/private cooperation has been a recurrent theme in government publications on cyber security. This strategic initiative points to an example of the Defense Industrial Base (DIB) involving DoD, DHS, and 20 companies, including Internet service providers (ISPs) and defense contractors. Threat signature information is shared by USCYBERCOM and the National Security Agency (NSA) with the participating companies. Public/private cooperation is not easy due to conflicting interests. Companies have usually argued that they know their networks better and can adapt faster to new threats than government regulators. Consequently, the government is currently focused on voluntary actions, but it recognizes that incentives will be necessary.

Strategic Initiative 4.

DoD will build robust relationships with U.S. allies and international partners to strengthen collective cyber security. This strategic initiative is aimed primarily at other nations to foster cooperation for “collective self-defense and collective deterrence” through information sharing, capacity building, training, and best practices. By conventional wisdom, strength in numbers could be an effective deterrent to

future cyber attacks. However, it is questionable whether deterrence is possible in cyber warfare in the same way that nuclear deterrence worked by fear of “mutually assured destruction.”

This strategic initiative raises two questions of practicality. First, can the United States forge treaties for effective international cooperation? New international treaties to cooperate in cyberspace would have to overcome considerable obstacles: competing interests; different attitudes toward cyber warfare; different definitions of malicious cyber acts (e.g., starting with “cyber warfare”); and difficult enforceability.

Second, can collective deterrence work in cyber security? To be effective, cyber deterrence must overcome a few practical obstacles. The first and obvious problem is attribution—identification of the real source of a cyber attack. Even if attribution can be solved, deterrence depends on credible capacity for destructive retaliation. Probably no one doubts the U.S. offensive capability, but it has not been demonstrated yet. In cyber warfare, there is no real reason to reveal “cyber weapons” unnecessarily.

Strategic Initiative 5.

DoD will leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation. This strategic initiative aims to maintain U.S. superiority through investment “in its people, technology, and research and development (R&D) to create and sustain the cyberspace capabilities.” The initiative does not propose revolutionary actions but does declare a message to two audiences: the private sector and foreign adversaries. To the private sector, the strategy conveys an intention to acquire new defense technologies and hire cyber professionals. To foreign adversaries, the message is DoD’s intention to achieve and maintain superiority in cyberspace.

The initiative is incomplete in addressing R&D. While the initiative aims for “technological innovation,” it gives much more attention to the DoD acquisition process than to investment in R&D. It is not clear how innovations will be stimulated. For example, nothing is mentioned

about investment in universities or scientific labs for basic research or how basic research will be translated into new products to acquire. The initiative is also highly dependent on defense funding.

Conclusions.

In conclusion, after reading the five strategic initiatives, some general observations about the unclassified *DoD Strategy for Operating in Cyberspace* can be made.

- The strategy focuses mostly on technology, resources, and cooperation; human resources are addressed only in the last initiative.
- The strategy emphasizes defense and prevention (the classified version of the strategy may obviously be different).
- The strategic initiatives mostly repeat themes that have appeared in previous government publications. The ideas are uncontroversial and sensible, but no novel ideas are really offered.
- Some of the actions are already in progress; in this sense, the *DoD Strategy* is mostly an affirmation of current initiatives.
- The strategy does not offer solutions to several practical challenges, such as how to implement advanced technologies for network resilience and robustness into DoD’s computer networks; how to accurately detect intrusions in real time; how to properly incentivize private sector information sharing; and how to effectively deter cyber attacks.
- No distinction is made between different types of adversaries: nation-states, foreign intelligence, hacktivists, criminals, hackers, or terrorists.
- The (unclassified) strategy neglects to address a few important issues: offensive cyber capabilities; attribution of cyber attacks; rules for proper response to cyber attacks; and metrics of progress toward implementation.

The ultimate question is whether the strategy is adequate to maintain DoD superiority in the face of existing and future cyber threats. The *DoD Strategy for Operating in Cyberspace* falls short in some ways. For example, it is not clear about priorities, futuristic vision, progress metrics, or enforcement and accountability. Future versions of the strategy could be improved by:

- expanding detailed plans of actions to take for each strategic initiative;
- explaining how to find solutions to practical challenges, such as how to implement advanced technologies for network resilience and robustness on a large scale; how to accurately detect and prevent intrusions in real time; and how to determine effective incentives for private sector information sharing;
- elaborating specific strategies to address different types of adversaries who have different capabilities, skills, and goals;
- elaborating specific mechanisms to stimulate technological innovations and translate research results into new defense products;
- including consideration of important issues, such as attribution, rules for proper

response to cyber attacks, and security metrics; and,

- proposing novel forward-looking ideas and new ways of thinking, i.e., effective cyber deterrence.

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute's homepage at www.StrategicStudiesInstitute.army.mil.

Organizations interested in reprinting this or other SSI and USAWC Press executive summaries should contact the Editor for Production via e-mail at SSI_Publishing@conus.army.mil. All organizations granted this right must include the following statement: "Reprinted with permission of the Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College."



This Publication



SSI Website



USAWC Website