Department of Defense Cyberspace Policy Report

A Report to Congress
Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934

November 2011

Preparation of this report/study cost the Department of Defense a total of Approximately $9,490 in Fiscal Years 2011-2012

RefID: 0-98AE431

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Defense Cyberspace Policy Report	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense ,1400 Defense Pentagon,Washington,DC,20301-1400**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**14**	

Contents

Introduction

This report is submitted in accordance with the requirements of Section 934 of the Ike Skelton National Defense Authorization Act (NDAA) for Fiscal Year 2011.

Cyberspace is a critical enabler to Department of Defense (DoD) military, intelligence, business and, potentially, civil support operations. While the development and integration of cyber technologies have created many high leverage opportunities for DoD, our increasing reliance upon cyberspace also creates vulnerabilities for both DoD and the Nation.

To more holistically capture these dynamic challenges and opportunities, the Department published the *Department of Defense Strategy for Operating in Cyberspace* (available at www.defense.gov/news/d20110714cyber.pdf), which identifies five distinct, but interrelated strategic initiatives to support DoD's cyberspace operations and its national security mission:

- Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential in its military, intelligence, and business operations;

- Employ new defense operating concepts, including active cyber defense, to protect DoD networks and systems;

- Partner closely with other U.S. Government departments and agencies and the private sector to enable a whole-of-government strategy and a nationally integrated approach to cybersecurity;

- Build robust relationships with U.S. Allies and international partners to enable information sharing and strengthen collective cybersecurity; and

- Leverage the Nation's ingenuity by recruiting and retaining an exceptional cyber workforce and enabling rapid technological innovation.

Section I: Description of Policy and Legal Issues

As described in the *Department of Defense Strategy for Operating in Cyberspace*, DoD is addressing the complex challenges and opportunities of cyberspace in an integrated manner. DoD is focused on the development and extension of all necessary policies and authorities for its cyberspace operations. As with all of the activities that DoD pursues in the physical world, cyberspace operations are executed with a clear mission and under clear authorities, and they are governed by all applicable domestic and international legal frameworks, including the protection of civil liberties and the law of armed conflict.

The Senate Report (S. Rept. 111-201) accompanying the Senate version of the Ike Skelton NDAA for Fiscal Year 2011 further identified thirteen specific questions on cyber policy for

both DoD and the U.S. Government. This report answers each of the thirteen questions posed in Senate Report 111-201.

1. *The development of a declaratory deterrence posture for cyberspace, including the relationship between military operations in cyberspace and kinetic operations. The Committee believes that this deterrence posture needs to consider the current vulnerability of the U.S. economy and government institutions to attack, the relatively lower vulnerability of potential adversaries, and the advantage currently enjoyed by the offense in cyberwarfare.*

The President's May 2011 *International Strategy for Cyberspace* states that the United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these national security and vital national assets as necessary and appropriate. When warranted, we will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we reserve the right to use all necessary means—diplomatic, informational, military, and economic—to defend our Nation, our Allies, our partners, and our interests. In doing so, we will exhaust all options prior to using force whenever we can; we will carefully weigh the costs and risks of action against the costs of inaction; and we will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support wherever possible. For its part, DoD will ensure that the U.S. military continues to have all necessary capabilities in cyberspace to defend the United States and its interests, as it does across all domains.

Deterrence in cyberspace, as with other domains, relies on two principal mechanisms: denying an adversary's objectives and, if necessary, imposing costs on an adversary for aggression. Accordingly, DoD will continue to strengthen its defenses and support efforts to improve the cybersecurity of our government, critical infrastructure, and Nation. By denying or minimizing the benefit of malicious activity in cyberspace, the United States will discourage adversaries from attacking or exploiting our networks. DoD supports these efforts by enhancing our defenses, increasing our resiliency, and conducting military-to-military bilateral and multilateral discussions.

In addition, the U.S. is working with like-minded nations to establish an environment of expectations, or norms of behavior, that increase understanding of cyber doctrine, and guide Allied policies and international partnerships. At the same time, should the "deny objectives" element of deterrence not prove adequate, DoD maintains, and is further developing, the ability to respond militarily in cyberspace and in other domains. Continuing to improve our ability to attribute attacks is a key to military response options.

Defending the Homeland is an important element of deterrence. DoD will use its significant capability and expertise in support of a whole-of-government approach to protect the Nation. The policy and legal authorities governing DoD's domestic activities – such as Defense Support to Civil Authorities – extend to cyber operations, as they would in any other domain. DoD will continue to work closely with its interagency partners, including the Departments of Justice and Homeland Security, to address threats to the United States from wherever they originate, through

a whole-of-government approach. The Department is dedicated to the protection of the Nation, and to the privacy and the civil liberties of its citizens.

Deterrence is a whole-of-government proposition. DoD supports the White House Cybersecurity legislative proposal to protect the American people, U.S. critical infrastructure, and our government's networks and systems more effectively. DoD is working closely with its interagency partners, including the Department of Homeland Security, to increase the cybersecurity of our critical infrastructure. Moreover, DoD continues to work with private sector partners through efforts like the Enduring Security Framework and the Defense Industrial Base Cybersecurity/Information Assurance programs to enhance cybersecurity, reduce vulnerabilities, and encourage the innovation necessary to protect and strengthen the U.S. economy. DoD is working with the Department of State to strengthen ties with our Allies and international partners to enhance mutual security.

2. *The necessity of preserving the President's freedom of action in crises and confrontations involving nations which may pose a manageable conventional threat to the United States but which in theory could pose a serious threat to the U.S. economy, government, or military through cyber attacks.*

The Department recognizes that a nation possessing sophisticated and powerful cyber capabilities could attempt to affect the strategic calculus of the United States. In this scenario, an adversary might act in ways antithetical to vital U.S. national interests and attempt to prevent the President from exercising traditional national security options by threatening or implying the launch of a crippling cyber attack against the United States.

Any state attempting such a strategy would be taking a grave risk. DoD recognizes the vital importance of maintaining the President's freedom of action. The Department is working, with our interagency partners, to ensure no future adversaries are tempted to pursue such a strategy. Our efforts focus on the following three areas:

- First, the Department, in conjunction with the Intelligence Community and Law Enforcement agencies, strives to secure the best possible intelligence about potential adversaries' cyber capabilities. These efforts are crucial because the United States needs to understand other nations' cyber capabilities in order to defend against them and to improve our ability to attribute any cyber attacks that may occur. Forensic analysis is a part of attributing attacks, but foreign intelligence collection and international law enforcement cooperation play a key role. In this regard, the co-location of the National Security Agency and United States Cyber Command (USCYBERCOM) provides benefits and efficiencies to the Department for its cyber operations. The National Security Agency's unique strengths and capabilities provide USCYBERCOM with critical cryptologic support for target and access development, enabling DoD cyberspace operations planning and execution.

- Second, the Department recognizes that strong cyber defenses and resilient information architectures, particularly those connected to critical infrastructure, mitigate the ability of

a future adversary to constrain the President's freedom of action. If future adversaries are unable to cripple our centers of gravity, they will be more likely to understand that the President has the full menu of national security options available.

- Finally, the President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include significant cyber attacks directed against the U.S. economy, government or military. As directed by the President, response options may include using cyber and/or kinetic capabilities provided by DoD.

3. *How deterrence or effective retaliation can be achieved in light of attribution limitations.*

The same technical protocols of the Internet that have facilitated the explosive growth of cyberspace also provide some measure of anonymity. Our potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage.

The Department recognizes that deterring malicious actors from conducting cyber attacks is complicated by the difficulty of verifying the location from which an attack was launched and by the need to identify the attacker among a wide variety and high number of potential actors. With this in mind, the Department actively seeks to limit the ability of such potential actors to exploit or attack the United States anonymously in three ways:

- First, the Department seeks to increase our attribution capabilities by supporting innovative research and development in both DoD and the private sector. This research focuses on two primary areas: developing new ways to trace the physical source of an attack, and seeking to assess the identity of the attacker via behavior-based algorithms. In the near future, the Department intends to expand and deploy applications that detect, track, and report malicious activities across all DoD networks and information systems on a near real-time basis. The ability to detect malicious activities quickly allows forensics experts to recover evidence during important windows of opportunity for attribution.

- Second, the Department has significantly improved its cyber forensics capabilities over the past several years. The Intelligence Community and U.S. Cyber Command continue to develop a highly skilled cadre of forensics experts. Additionally, DoD has been the primary supporter of an innovative and effective center of excellence for forensics capabilities at the Defense Cyber Crime Center. This unique organization provides an important nexus of support to both defense and law-enforcement communities, as well as to private sector companies who support DoD.

- Third, in partnership with the Department of Homeland Security, DoD is expanding its international partnerships to increase shared situational awareness, warning capabilities and forensics efforts. The ability to share timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors enables advance

deterrence of malicious activity. Equally important are efforts to work with international partners to bolster cyber forensics capabilities.

4. *To the extent that deterrence depends upon demonstrated capabilities or at least declarations about capabilities and retaliatory plans, how and when the Department intends to declassify information about U.S. cyber capabilities and plans or to demonstrate capabilities.*

Effective deterrence in cyberspace is founded upon both the security and resilience of U.S. networks and systems, and ensuring that the United States has the capability to respond to hostile acts with a proportional and justified response. The *International Strategy for Cyberspace* provides a clear statement that the United States reserves the right to use all necessary means—diplomatic, informational, military, and economic—to defend our Nation, our Allies, our partners, and our interests in cyberspace.

The dynamic and sensitive nature of cyberspace operations makes it difficult to declassify specific capabilities. However, the Department has the capability to conduct offensive operations in cyberspace to defend our Nation, Allies and interests. If directed by the President, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict.

5. *How to maintain control of or manage escalation in cyberwarfare, through, for example, such measures as refraining from attacking certain targets (such as command and control and critical infrastructure).*

The unique characteristics of cyberspace can make the danger of escalation especially acute. For instance, the speed of action and dynamism inherent in cyberspace, challenges of anonymity, and the widespread availability of malicious tools can compound communications and increase opportunities for misinterpretation. As a result, DoD recognizes the clear importance of steps such as the development of transparency and confidence building measures, in addition to further development of international cyberspace norms, to avoid escalation and misperception in cyberspace. DoD and the Department of State are actively engaged with Allies, partners, and other states to build transparency and confidence with traditional adversaries.

The Department also seeks to prevent dangerous escalatory situations by following the same policy principles and legal regimes in its cyberspace operations that govern actions in the physical world, including the law of armed conflict. DoD's cyberspace operations are subject to careful coordination and review, including the use of cyberspace for intelligence operations. Intelligence, military, and political implications are carefully considered for cyberspace operations as elsewhere.

In collaboration with other U.S. Government agencies, Allies and partners, DoD pursues bilateral and multilateral engagements to develop further norms that increase openness, interoperability, security, and reliability. International cyberspace norms will increase stability and predictability

of state conduct in cyberspace, and these norms will enable international action to take any required corrective measures.

Finally, the Department believes that increased transparency minimizes the likelihood that a cyber incident will escalate to a dangerous or unintended level. DoD continues to pursue opportunities for the facilitation and expansion of transparency among key international actors with regard to their command and control, doctrine, and deployment of cyber capabilities. DoD works with international partners to develop confidence building and risk reduction measures to decrease the chance of miscommunication and escalation in cyberspace.

6. ***The rules of engagement for commanders at various command echelons for responding to threats to operational missions and in normal peacetime operating environments, including for situations in which the immediate sources of an attack are computers based in the United States.***

DoD has implemented rules of engagement for the operation and defense of its networks. In current operations that occur in designated Areas of Hostilities, specific rules of engagement have been approved to govern and guide DoD operations in all domains. DoD's cyber capabilities are integrated into planning and operations under existing policy and legal regimes.

As it continues to build and develop its cyber capabilities and organizational structures, the Department is addressing operational needs by modifying its standing rules of engagement for commanders to enable required decisions and take appropriate actions to defend critical information networks and systems. Due to the interconnectedness and speed that defines cyberspace, these standing rules of engagement will reflect: the implications of cyber threats; the operational demands of DoD's continuous, worldwide operations; and the need to minimize disruption from collateral effects on networked infrastructure.

DoD recognizes the unique challenge presented by malicious activity coming from within the United States. The Department will support domestic agencies and departments, using its significant capability and expertise in support of a whole-of-government approach to protect the Nation. The policy and legal authorities governing DoD's domestic activities – such as Defense Support to Civil Authorities – extend to cyber operations, as they would in any other domain. DoD will continue to work closely with its interagency partners, including the Departments of Justice and Homeland Security, to address threats to the United States from wherever they originate, through a whole-of-government approach. The Department is dedicated to the protection of the Nation, and to the privacy and the civil liberties of its citizens.

7. ***How the administration will evaluate the risks and consequences attendant to penetrations of foreign networks for intelligence gathering in situations where the discovery of the penetration could cause the targeted nation to interpret the penetration as a serious hostile act.***

Espionage has a long history and is nearly always practiced in both directions. For the U.S. and many other states, traditional espionage has been a state-sponsored intelligence-gathering function focused on national security, defense, and foreign policy issues. The United States

Government collects foreign intelligence via cyberspace, and does so in compliance with all applicable laws, policies, and procedures. The conduct of all U.S. intelligence operations is governed by long-standing and well-established considerations, to include the possibility those operations could be interpreted as a hostile act.

Classified material pertaining to this section is available in the separate Classified Annex.

8. ***How DoD shall keep Congress fully informed of significant cyberspace accesses acquired for any purpose that could serve as preparation of the environment for military action.***

The Department has been working closely with Congress to improve the reporting schemes for cyberspace operations. DoD will provide quarterly cyber briefings to appropriate Members of Congress and their congressional staff in fulfillment of notification requirements. For sensitive operations that may require out-of-cycle reporting, DoD will ensure that appropriate Members of Congress and their congressional staff receive any necessary additional briefings.

9. ***The potential benefit of engaging allies in common approaches to cyberspace deterrence, mutual and collective defense, and working to establish norms of acceptable behavior in cyberspace.***

The President's *International Strategy for* Cyberspace makes clear that hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners, and DoD has been working actively to clarify those expectations within our alliances.

To implement that vision, the *Department of Defense Strategy for Operating in Cyberspace* emphasizes the importance of building robust relationships with U.S. Allies and partners to strengthen the deterrence of malicious cyberspace activity and to build collective cyber defenses. Through shared warning, capacity building, and joint training activities, international engagement provides opportunities for an exchange of information and new ideas to strengthen U.S. and allied cyber capabilities. DoD continues to coordinate amendments to the National Disclosure Policy that will ensure detailed cyber operations discussions with Allies and international partners.

DoD is actively deepening its engagement on cyber issues with its Allies and international partners. The Department continues to have both senior-level and expert coordinating activities with Australia, Canada, New Zealand, and the United Kingdom. DoD has worked closely with its NATO Allies on cyber issues, including the revised NATO Cyber Policy and associated action plan approved at the June 2011 Ministerial. In further development of our treaty relationships, DoD is strengthening its relationships with Japan and the Republic of Korea. DoD and its Allies and international partners can maximize cyber capabilities, mitigate risk, and deter malicious activities in cyberspace.

The United States is actively engaged in the continuing development of norms of responsible state behavior in cyberspace, making clear that as a matter of U.S. policy, long-standing

international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace's unique aspects may require clarifications in certain areas.

10. ***The issue of third-party sovereignty to determine what to do when the U.S. military is attacked, or U.S. military operations and forces are at risk in some other respect, by actions taking place on or through computers or other infrastructure located in a neutral third country.***

The nature of the DoD response to a hostile act or threat is based upon a multitude of factors, but always adheres to the principles of the law of armed conflict. These responses include taking actions short of the use of force as understood in international law.

DoD adheres to well-established processes for determining whether a third country is aware of malicious cyber activity originating from within its borders. In doing so, DoD works closely with its interagency and international partners to determine:

- The nature of the malicious cyber activity;
- The role, if any, of the third country;
- The ability and willingness of the third country to respond effectively to the malicious cyber activity; and
- The appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstances.

11. ***The issue of the legality of transporting cyber "weapons" across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of "overflight rights."***

There is currently no international consensus regarding the definition of a "cyber weapon." The often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult. Most of the technology used in this context is inherently dual-use, and even software might be minimally repurposed for malicious action.

The interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains. The law of armed conflict and customary international law, however, provide a strong basis to apply such norms to cyberspace governing responsible state behavior. Significant multinational work remains to clarify the application of norms and principles of customary international law to cyberspace.

As the President recognized in the *International Strategy for Cyberspace*, the development of norms for state conduct does not require a reinvention of customary international law nor render

existing norms obsolete. Rather, the principled application of existing norms must be developed with our partners and Allies. DoD, in conjunction with other U.S. Government departments and agencies, will continue to work with our partners and Allies to build consensus on the applicability of norms in cyberspace to develop customary international law further.

12. ***The definition or the parameters of what would constitute an act of war in cyberspace and how the laws of war should be applied to military operations in cyberspace.***

The phrase "act of war" is frequently used as shorthand to refer to an act that may permit a state to use force in self-defense, but more appropriately, it refers to an act that may lead to a state of ongoing hostilities or armed conflict. Contemporary international law addresses the concept of "act of war" in terms of a "threat or use of force," as that phrase is used in the United Nations (UN) Charter. Article 2(4) of the UN Charter provides: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state." International legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the physical domains (i.e., sea, air, land, and space), also apply to the cyberspace domain.

As in the physical world, a determination of what is a "threat or use of force" in cyberspace must be made in the context in which the activity occurs, and it involves an analysis by the affected states of the effect and purpose of the actions in question.

The particular attributes of cyberspace can make this determination especially difficult, including the detection of the activity, political and/or technical attribution, and a determination if the particular activity is part of a larger military operation, although these are challenges present in the "real world" as well.

Without question, some activities conducted in cyberspace could constitute a use of force, and may as well invoke a state's inherent right to lawful self-defense. In this context, determining defensive response to even presumptively illegal acts rests with the Commander-in-Chief.

13. ***What constitutes use of force in cyberspace for the purpose of complying with the War Powers Act (Public Law 93-148).***

The requirements of the War Powers Resolution apply to "the introduction of United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations."

Cyber operations might not include the introduction of armed forces personnel into the area of hostilities. Cyber operations may, however, be a component of larger operations that could trigger notification and reporting in accordance with the War Powers Resolution. The Department will continue to assess each of its actions in cyberspace to determine when the requirements of the War Powers Resolution may apply to those actions.

Section II: Decisions of the Secretary of Defense

By approving the *Department of Defense Strategy for Operating in Cyberspace*, the Secretary of Defense has set out comprehensive guidance for the Department's cyberspace activities in defense and support of U.S. national interests. The strategy also provides clear objectives and policies for DoD to take advantage of cyberspace's potential, while recognizing the continued growth of both cyberspace threats and vulnerabilities.

DoD has also worked closely with the Administration to develop its Cybersecurity Legislative Proposal. DoD supports the Administration's efforts to improve cybersecurity for the American people, our critical infrastructure, and the U.S. Government's networks and systems. DoD relies upon U.S. critical civilian infrastructure for its operations. The theft of sensitive information and intellectual capital erodes DoD's effectiveness and the economic vitality upon which our military strength depends.

Section III: National Military Strategy for Cyberspace Operations

The Joint Staff does not intend to modify the National Military Strategy for Cyberspace Operations at this time. To guide the Department's activities in cyberspace, the Secretary of Defense has approved the *Department of Defense Strategy for Operating in Cyberspace*.

Section IV: Current Use of Cyber Modeling and Simulation

Cyber modeling and simulation technologies are rapidly evolving in scope and sophistication. As the size and complexity of networks continue to grow, the need for capabilities to understand and study them has become increasingly apparent. In DoD, the use of these tools and technologies varies greatly depending upon the unique requirements and mission sets of component organizations.

Exploration and refinement of tactics, techniques, and procedures used to defend DoD networks are a key application of modeling and simulation. The use of "test ranges" allows the military to increase awareness, adjust planning, improve resiliency of its networks and systems, and train personnel. DoD's cyber workforce can use these capabilities to increase proficiency through realistic, practical application of techniques and procedures to hone skills for better identification of vulnerabilities and improved remediation response. In addition to new technologies and their application, the use of ranges allows DoD to explore and develop new concepts for its operations in a contained but realistic environment.

The Defense Intelligence Agency (DIA) and several Combatant Commands are developing and using methodologies, analytic techniques, and tools to identify potential cyber vulnerabilities. Modeling and simulation are some of the tools used, but they are still at early stages of development. Including methodologies and modeling in structural analytic techniques provides DoD with a framework to test assumptions and explore the interaction between networks. For instance, the Cyber Operations Research Environment (CORE) provides data necessary to perform predictive strategic analysis on the impact of potential cyber threats. This work

provides the information necessary to prioritize mitigation efforts, increase network security, and preserve the ability of particular systems to perform military missions.

DoD is also pursuing revolutionary approaches to modeling and simulation, such as the National Cyber Range (NCR). The NCR will create a new state-of-the-art capability for large-scale cyber testing. This ability to evaluate cyber technologies, policies, and procedures will be a critical asset to the development of future operations. By enabling testing and analysis under real word conditions, DoD will be able to refine, research, and develop capabilities that can strengthen cyber defenses and revolutionize cybersecurity. The NCR will allow testing of current cyber environments, and it will be the foundation of future modeling and simulation capabilities.

Classified material pertaining to this section is available in the separate Classified Annex.

Section V: Application of Cyber Modeling and Simulation

The application of cyber modeling and simulation capabilities can improve current defense and future development activities. These lessons will allow DoD to develop improved architectures and increase the sophistication of its cyber defenses. New capabilities such as the NCR will provide vast improvements in DoD's ability to model and simulate a variety of networks quickly and at scale. DoD continues to innovate and explore new initiatives that improve our cyberspace strategies and programs.

As cyber technologies and their applications continue to evolve, DoD is exploring the use of modeling and simulation technologies to test and evaluate new cyberspace concepts, policies, and capabilities. These efforts will enable DoD to develop new ideas and adapt to technological trends. Improved modeling and simulation capabilities will further DoD's efforts to understand and integrate more effectively policy, legal, operational, and technical trends in cyberspace that will allow the Department to identify vulnerabilities, address them, and ensure that the U.S. military continues to have the capability to fulfill its national security mission in defense of the Nation.

Classified material pertaining to this section is available in the separate Classified Annex.

ANNEX A: FULL TEXT OF SECTION 934 OF THE NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2011

SEC. 934. REPORT ON THE CYBER WARFARE POLICY OF THE DEPARTMENT OF DEFENSE.

> (a) REPORT REQUIRED.—Not later than March 1, 2011, the Secretary of Defense shall submit to Congress a report on the cyber warfare policy of the Department of Defense.
>
> (b) ELEMENTS.—The report required under this section shall include the following:

(1) A description of the policy and legal issues investigated and evaluated by the Department in considering the range H. R. 6523—203 of missions and activities that the Department may choose to conduct in cyberspace.

(2) The decisions of the Secretary with respect to such issues, and the recommendations of the Secretary to the President for decisions on such of those issues as exceed the authority of the Secretary to resolve, together with the rationale and justification of the Secretary for such decisions and recommendations.

(3) A description of the intentions of the Secretary with regard to modifying the National Military Strategy for Cyberspace Operations.

(4) The current use of, and potential applications of, modeling and simulation tools to identify likely cybersecurity vulnerabilities, as well as new protective and remediation means, within the Department.

(5) The application of modeling and simulation technology to develop strategies and programs to deter hostile or malicious activity intended to compromise Department information systems.

(c) FORM.—The report required under this section shall be submitted in unclassified form, but may include a classified annex.