~~FOR OFFICIAL USE ONLY~~

THE DEPARTMENT OF DEFENSE STRATEGY

FOR

COUNTERINTELLIGENCE IN CYBERSPACE

28 August 2009

~~FOR OFFICIAL USE ONLY~~

PREFACE

I approve this Department of Defense Strategy for Counterintelligence in Cyberspace and I endorse the mission and enterprise objectives set forth in this strategy as the path forward for building a comprehensive counterintelligence program that can engage, exploit, neutralize, and ultimately defeat foreign intelligence, international terrorist, and insider threats in cyberspace.

This strategy is consistent with the goals and objectives of the President's Comprehensive National Cybersecurity Initiative, the 2006 Quadrennial Defense Review, and other national security, defense, intelligence, and counterintelligence strategies. Development of the Strategy for Counterintelligence in Cyberspace was conducted in collaboration with the military departments, defense agencies, and combatant commands. In addition, it emphasizes the importance of collaboration between the defense counterintelligence enterprise and the information operations, information assurance, network defense, intelligence, and law enforcement communities. Finally, this strategy establishes goals and objectives for counterintelligence activities in the cyberspace domain, and is intended to justify resources for this priority effort.

I encourage the aggressive implementation of the mission and enterprise objectives laid out in this strategy. When implemented, this strategy will enhance the effectiveness of the Department of Defense counterintelligence program and will promote the integration of counterintelligence missions and functions in cyberspace.

James R. Clapper, Jr.
Under Secretary of Defense for Intelligence

FOREWORD

Land, sea, air, and space are all well-recognized operational environments. The Department of Defense (DoD) military departments, defense agencies, and combatant commands are strategically organized to accomplish their missions and functions in each of these domains in order to defeat our adversaries. DoD counterintelligence (CI) plays a critical role in each of these operational environments and is likewise organized in these areas to accomplish its mission to deter, exploit, and defeat the overt, covert, and clandestine intelligence activities[1] of our adversaries.

In recent decades, however, a new operational environment has emerged as evidenced by the increasing frequency and destructiveness of attacks and exploits launched against the United States through cyberspace.[2] In today's information-rich environment, computers are ubiquitous across DoD entities and across the U.S. defense industrial base. Large numbers of these computers are networked together to quickly transmit information to the warfighter. These computer systems hold crucial information, control critical systems, and are a primary communication mode for DoD, making them extremely attractive targets to our most capable adversaries.

DoD is developing new strategies to organize itself for success in this emerging cyberspace battlefield.[3] DoD CI is no exception. In August 2007, DoD established the Counterintelligence in Cyberspace Program to address the ongoing and ever increasing threat to DoD activities and information in cyberspace. The creation of the CI in Cyberspace Program was validated in the *National Military Strategy for Cyberspace Operations (NMS-CO) Implementation Plan*, which called for the formation of a "DoD Counterintelligence Cyber Program to manage the integration of Counterintelligence Cyber Strategy."[4]

The first step in fulfilling this requirement was to develop this DoD Strategy for CI in Cyberspace as a roadmap. It was crafted in coordination with the military departments, combatant commands, and defense agencies, all of which hold a critical stake in the integration of CI in cyberspace. This strategy aims to facilitate the creation of a professional CI force across DoD that will support the warfighter, protect DoD assets, safeguard U.S. person civil liberties, and carry out the CI mission to deter, exploit, and defeat the overt, covert, and clandestine activities of foreign intelligence and security services (FISS), international terrorists, and insider threats, in accordance with all applicable laws and presidential directives, thus ensuring U.S. military superiority in cyberspace.

[1] Department of Defense, *The Department of Defense Counterintelligence Strategy: Fiscal years 2008-2013* (Washington, D.C., 2008), v.

[2] The DoD Dictionary of Military and Associated Terms (12 April 2001, as amended through 17 March 2009) defines cyberspace as: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (pg 141).

[3] See the *National Military Strategy for Cyberspace Operations* (NMS-CO), the *NMS-CO Implementation Plan, Joint Publication 3-13: "Information Operations,"* and the *Trilateral Memorandum of Agreement among the Department of Defense and the Department of Justice and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitation Activities.*

[4] Department of Defense, *The National Military Strategy for Cyberspace Operations Implementation Plan* (Washington, D.C., signed October 1, 2007), A-26.

Table of Contents

MISSION AND VISION

MISSION

DoD CI will detect, identify, assess, exploit, penetrate, degrade, and counter or neutralize intelligence collection efforts, other intelligence activities, sabotage, espionage, sedition, subversion, assassination, and terrorist activities directed against the Department of Defense, its personnel, information, materiel, facilities, and activities, or against U.S. national security in the cyberspace domain.

VISION

The integrated application of DoD CI activities will neutralize or exploit, and ultimately defeat the intelligence activities of individuals, organizations, international terrorists, and FISS operating against DoD personnel, facilities, programs, information, and operations in the cyberspace domain.

EXECUTIVE SUMMARY

The DoD Strategy for CI in Cyberspace aligns with the National Military Strategy for Cyberspace Operations, the Department of Defense Counterintelligence Strategy 2008-2013, the President's Comprehensive National Cybersecurity Initiative and the United States Government-Wide Cyber Counterintelligence Plan 2008.

While some of these documents define counterintelligence in cyberspace as encompassing a very broad mission set that includes critical infrastructure protection and supply chain risk management, this strategy focuses on the conduct of counterintelligence in cyberspace, and recognizes that future iterations may expand into these additional areas.

The DoD Strategy for CI in Cyberspace contains five strategic objectives: two mission objectives and three enterprise objectives. Mission objectives are outcomes. They identify the strategic results DoD CI strives to achieve. Enterprise objectives are capabilities. They represent organizational goals that will help to achieve desired outcomes. Each mission and enterprise objective contains sub-objectives that describe how the mission and enterprise objectives will be achieved, resources permitting.

Mission Objectives (Outcomes)

1. Deny intelligence activities targeting U.S. and DoD interests in cyberspace.
    - Deter, detect, identify, assess, neutralize, or exploit adversaries in cyberspace.
    - Support the protection of information and technology.
    - Protect the integrity of DoD intelligence and CI activities.
2. Conduct CI activities in cyberspace in support of DoD efforts to shape the choices of countries at strategic crossroads.
    - Dissuade foreign governments from threatening U.S. interests.
    - Cooperate with foreign partners to achieve DoD CI in Cyberspace objectives.

Enterprise Objectives (Capabilities)

1. Achieve unity of effort in cyberspace.
    - Synchronize and deconflict CI activities in cyberspace.
    - Standardize DoD CI tactics, techniques, and procedures (TTP) in cyberspace.
2. Develop, increase, and improve DoD CI in cyberspace force readiness.
    - Enhance recruitment, mentoring, and retention of the CI force.
    - Develop CI in cyberspace professional standards.
3. Mold and shape a DoD CI enterprise for cyberspace.
    - Prioritize resources to combat threats.
    - Exploit emerging scientific and research advances.

THE STRATEGY

Background

The United States is increasingly under attack in cyberspace. The National Counterintelligence (CI) Strategy states, "The cyber environment provides unprecedented opportunities for adversarial activities and is particularly vulnerable because of the nation's reliance on information systems. The cyber networks that businesses, universities, and ordinary citizens use every day are the object of systematic hostile activities.[5]

The Department of Defense (DoD) is a high-priority target for some of the nation's most capable cyberspace adversaries who not only threaten DoD systems, but also critical infrastructure, such as the defense industrial base and other private sector and defense contractor entities and organizations. Each of these elements is a critical component of the nation's infrastructure that supports the warfighter.

Network defense and information operations are well-established disciplines that play a critical role in DoD cyber . strategy. The CI mission in cyberspace complements the overarching missions of the network defense, information operations (IO), and information assurance (IA) communities by providing unique capabilities that specifically target Foreign Intelligence and Security Service (FISS) and international terrorists without encroaching upon the distinct responsibilities held by IO and IA. CI activities in cyberspace provide another level of "defense in depth" that actively seeks to mitigate, exploit, and otherwise thwart the ability of FISS to use cyberspace as a means of intelligence collection or as an operational arena.

The DoD Strategy for CI in Cyberspace establishes strategic mission and enterprise objectives for developing a DoD CI Program and a professional CI force capable of countering FISS, international terrorists, and insider threats operating in cyberspace. The strategy also establishes objectives for synchronizing and coordinating CI activities with those of information operations, network defense, and human intelligence (HUMINT) cyber operations.

The DoD CI in Cyberspace Program focuses the five traditional CI functions (investigations, operations, collections, analysis and production, and functional services) to address the adversary threat in cyberspace.

Ultimately, the purpose of this strategy is to establish a set of strategic mission and enterprise objectives that ensure U.S. military strategic superiority in cyberspace.

[5] National Counterintelligence Executive, *The National Counterintelligence Strategy of the United States* (Washington, D.C., 2007), 7.

Mission Objectives

Mission Objective 1: Deny intelligence activities targeting U.S. and DoD interests in cyberspace.

The DoD CI Strategy states "the business of DoD CI is denying intelligence activities that target U.S. and DoD interests."[6]

In cyberspace, network and computer security alone are insufficient to keep U.S. and DoD interests secure and to ensure the warfighter has the tools needed for success. DoD CI offers a unique set of capabilities that are an important complement to information assurance and information operations, providing another layer of "defense in depth" that will be brought to bear against our adversaries in cyberspace.

Deter, detect, identify, assess, and neutralize or exploit adversaries in cyberspace.

The DoD CI Strategy states that "to deter and defeat intelligence adversaries, the DoD CI Community must sustain its defensive capabilities, advance offensive CI, and ensure the DoD CI enterprise is positioned to meet current and future challenges."[7]

FISS efforts to access sensitive data from U.S. cyberspace systems and to spot, assess, and recruit individuals under the authority of, or associated with, the DoD are well documented. Adversaries and allies alike look to exploit our vulnerabilities, and we must be vigilant in our efforts to mitigate or defeat these threats.

FISS efforts are directed at DoD cyberspace assets, the defense industrial base, and other critical infrastructure systems that contain science, technology, and other data critical to support the warfighter.

International terrorists are also a threat to DoD assets in cyberspace. Every international terrorist attack is preceded by intelligence operations and planning. Often, international terrorists use cyberspace to communicate and may direct and control international terrorist activities through cyberspace. Cyberspace can also be a target that international terrorists may exploit or attack directly with potentially devastating effects on our critical infrastructure.

International terrorists and FISS, however, are not the only threats. Trusted insiders can threaten our cyberspace systems because they have the access necessary to defeat multiple layers of security. An insider threat is an individual with access to DoD resources, which includes cyber-systems, networks, information, facilities, and operations, who are acting for or on behalf of a foreign power or international terrorists.[8]

To defeat the efforts of our adversaries in cyberspace the DoD CI community will increase its efforts to aggressively deter, detect, identify, assess, and neutralize or exploit adversary intelligence activities as described in the 2007 National Counterintelligence Strategy: "The counterintelligence community will conduct aggressive, strategically-directed

[6] Department of Defense, *The Department of Defense Counterintelligence Strategy - Fiscal Years 2008 – 2013* (Washington, D.C., 2008), 1.

[7] Ibid.,

[8] Department of Defense, *Department of Defense Insider Threat Implementation Plan* (Approved on 2 October 2007 by USD(I)) (Washington, D.C., 2008), 5.

operations against priority intelligence targets around the world using the full range of operational means."[9]

The DoD CI in Cyberspace Program, established to comply with task CI/LE.4 of the National Military Strategy for Cyberspace Operations Implementation Plan, will accomplish this by significantly increasing the number of CI personnel that make up the professional CI force, and by providing them with the policy, guidance, doctrine, technical tools, training, and tradecraft that enable them to accomplish this mission in the cyber domain.

DoD CI will conduct offensive activities in cyberspace that seek to identify and defeat national security threats from FISS, international terrorists, and insider threats. CI components will accomplish this by extending traditional methodologies into the cyber domain, by leveraging the latest technology, and by creating innovative and proactive cyber tactics, techniques, and procedures.

Support Information and Technology Protection.

Information regarding U.S. commercial and government science and technology, as well as military plans, procedures, and communications, is contained in open, proprietary, and secure information systems. FISS and international terrorists, collect this information in an effort to gain political, military, and economic advantage.

DoD CI will implement measures to support the protection of this information and to increase offensive action against FISS and international terrorist collectors in cyberspace.

Protect the integrity of DoD intelligence and CI activities.

The DoD CI Strategy states that "DoD decision-makers and warfighters rely on the integrity of intelligence and CI activities."[10]

The integrity of DoD intelligence and CI sources, methods, and operations must be rigorously protected. DoD decision-makers depend on the reliability of our intelligence sources, yet our adversaries use denial and deception practices to undermine our understanding of their intentions, knowledge, capabilities, actions, as well as the operating environment.

DoD CI will penetrate our adversaries' intelligence operations to assess their tradecraft, source networks, and leadership structures, while validating the reliability of our own sources and methods. These activities will help protect the integrity and reliability of DoD intelligence and CI activities and information.

[9] National Counterintelligence Executive, *The National Counterintelligence Strategy of the United States* (Washington, D.C., 2007), 1.

[10] Department of Defense, *The Department of Defense Counterintelligence Strategy - Fiscal Years 2008 – 2013* (Washington, D.C., 2008), 2.

Mission Objective 2: Conduct CI activities in cyberspace in support of DoD efforts to shape the choices of countries at strategic crossroads.

The DoD CI in Cyberspace Program supports the strategic requirements of the Quadrennial Defense Review Report[11] (QDR), where "Shaping the Choices of Countries at Strategic Crossroads" is a critical priority identified by senior civilian and military leaders. The QDR further states "the choices that major and emerging powers make will affect the future strategic position and freedom of action of the United States, its allies and partners. The United States will shape these choices in ways that foster cooperation and mutual security interests."[12]

Offensive DoD CI activities can influence key decisions of U.S. adversaries, help resolve conflicts before they escalate, and provide strategic advantage in cyberspace.

To shape the choices of countries at strategic crossroads, DoD CI will:

- Conduct CI activities to dissuade foreign governments from threatening U.S. interests.
- Enhance cooperation with foreign partners to achieve DoD CI in Cyberspace Program objectives.

Dissuade foreign governments from threatening U.S. interests.

The National Defense Strategy asserts, "We will work to dissuade potential adversaries from adopting threatening capabilities, methods, and ambitions, particularly by sustaining and developing our key military advantages."[13]

In order to implement the objectives laid out in the DoD CI Strategy, the DoD CI Enterprise will actively engage intelligence organizations, international terrorists, and insider threats by influencing their risk/gain calculations, by manipulating their relationships with foreign governments, and by distorting their perceptions of the operating environment and the intelligence they collect.

Enhance cooperation with friendly foreign partners.

The QDR recognizes that "alliances are clearly one of the nation's greatest sources of strength."[14]

CI partnerships with cooperative foreign intelligence/CI services afford access to foreign expertise and information. Where possible, the DoD CI community will coordinate, synchronize, and deconflict CI activities with allies to build capacity and develop mechanisms to share the risks and responsibilities of today's challenges.

[11] Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C., 6 February 2006), 27.

[12] Ibid.

[13] Department of Defense, *The National Defense Strategy of the United States of America* (Washington, D.C., 2005), 9.

[14] Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C., 6 February 2006), 6.

Enterprise Objectives

Enterprise objectives relate to our capacity to maintain a competitive advantage over states and forces that threaten the security of the nation. Objectives are achieved through the coordination, collaboration, and synchronization of efforts across DoD, with other cyber disciplines, agencies of government, and the private sector.

Enterprise Objective 1: Achieve unity of effort in cyberspace.

The National Intelligence Strategy stresses "transformation of the Intelligence Community will be driven by the doctrinal principle of integration."[15]

To meet these challenges, the DoD CI in Cyberspace Program will focus on greater coordination, collaboration, synchronization, and deconfliction of all cyberspace activities throughout the DoD elements, the Intelligence Community, and the law enforcement community, and with other cyber disciplines, thus ensuring greater unity of effort.

Synchronize, coordinate, and deconflict CI activities in cyberspace.[16]

Synchronization and coordination among DoD elements and other members of the Intelligence Community operating in cyberspace will greatly facilitate deconfliction of sources, methods, tactics, and resources, and will promote information sharing, lessons learned, and best practices.

Coordination with the law enforcement community on computer-related investigations within the military services, defense agencies, and combatant commands will facilitate information-sharing that will significantly enhance the effectiveness of such investigations.

Coordination with network operations, network security, network warfare, and joint task force operations will provide valuable information and operational support to CI activities. These functions complement one another in helping to accomplishing the DoD cyber mission along with DoD CI in cyberspace objectives.

Standardize DoD CI in Cyberspace TTP.

DoD is expanding and standardizing the CI in Cyberspace Program and allocating the professional resources to successfully implement the program. Developing the Program requires expanding the recruiting, staffing, and training of the CI professional work force, and developing standardized

[15] Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America, Transformation through Integration and Innovation* (Washington, D.C., October 2005), 4.

[16] Guidelines for deconfliction are spelled out in documents such as the 2 February 2007 USD (I) memorandum "Deconfliction of DoD Counterintelligence (CI) Cyber Operations with the Intelligence Community (IC)," the May 2007 "Trilateral Memorandum of Agreement among DoD, DoJ, and the IC regarding CNA and CNE activities," and the DNI- and AG-approved "The United States Government-Wide Cyber Counterintelligence Plan" (2008).

Tactics Techniques and Procedures (TTP) across the DoD. This standardization will allow the community to communicate in the same operational language and more easily integrate joint operations.

CI in Cyberspace TTP development is a collaborative project among the members of the DoD CI community. At the operational level there will be differences in the specifics of TTP driven by the differing missions and functions of the individual services, defense agencies, and combatant commands—consistent with the need for creativity and innovation. Nevertheless, standardization based on lessons learned and best practices will facilitate a more effective DoD CI in Cyberspace Program.

Enterprise Objective 2: Develop, increase, and improve force readiness.

CI in cyberspace force development is already underway within DoD. The process of optimizing the recruiting, training, deploying, and retaining a CI in cyberspace force is a collaborative effort across DoD.

To sustain and continuously improve CI in cyberspace force readiness, the DoD CI community will focus on the following:

- Enhance recruitment and mentoring of the CI in cyberspace force.
- Develop CI in cyberspace professional standards.

Enhance recruitment, mentoring, and retention of the CI in cyberspace force.

Recruiting, mentoring, and retaining CI in cyberspace skills and resources is both crucial and challenging. To expand the professional workforce, the DoD CI in Cyberspace Program will establish relationships with institutions of higher learning and the national laboratories, and expand training courses offered by the Joint Counterintelligence Training Academy (JCITA) and the DoD Cyber Investigations Training Academy (DCITA).

Develop CI in Cyberspace professional standards.

The DoD CI in Cyberspace Program recognizes that the CI workforce must master many disciplines to accomplish its mission. Accordingly, the CI in Cyberspace Program will introduce professional and educational standards for CI collectors, analysts, investigators, and operators across the Department.

The DoD CI community will reach across the U.S. government to coordinate with centers of cyber and CI training excellence, to address deficiencies, and to upgrade the availability and uniformity of CI in cyberspace training. The workforce will be trained to safeguard the civil liberties of U.S. persons and to operate in accordance with all applicable laws and presidential directives. Where appropriate training is lacking, training programs and standards will be developed.

Enterprise Objective 3: Continue to Mold and Shape the DoD CI in Cyberspace Enterprise.

The process of establishing the CI in Cyberspace Program includes developing this strategy and a follow-on implementation plan for it, along with the development of TTP, readiness plans, and training requirements and standards.

Developing the professional CI force who can operate effectively in cyberspace requires recruiting, training, and retaining CI professionals. In addition, DoD must establish research and development requirements to create CI tools that support operational cyber needs.

To accomplish these objectives the CI in Cyberspace Program will:

- Prioritize resources to combat FISS and international terrorists and their intelligence elements, as well as insider threats.
- Exploit emerging scientific and research advances.

Prioritize resources to combat threats.

The process of obtaining the funding and resources necessary to deploy an effective CI in cyberspace force has already begun. Training requirements are being established and resources are being allocated across DoD.

Allocation of the initial resources will be based on needs analysis that has been conducted in collaboration with stakeholders of the CI and Intelligence Communities. In the early stages of implementation, resources will be directed at the most serious FISS, international terrorist, and insider threats.

Exploit emerging scientific and research advances.

The National Intelligence Strategy states "globalization and accelerating scientific and technological progress threaten to erode the Intelligence Community's technical collection means."[17]

In order to avoid such erosion, the DoD CI in Cyberspace Program will collaborate with the scientific research and technology communities along with commercial vendors to stay at the leading edge of technology and well ahead of our adversaries.

The CI in Cyberspace Program will address pressing technology requirements by using commercial off-the-shelf tools. The CI in Cyberspace Program will also draw from the resources of the U.S. government and industry including emerging capabilities from among the military services, the defense agencies, the national laboratories, and the Defense Advanced Research Projects Agency (DARPA).

[17] Ibid., 17.

CONCLUSION

The NMS-CO directs DoD to develop a "cyberspace force." The objective of this force is "to ensure U.S. military strategic superiority in cyberspace."[18]

To address the CI functions and missions in cyberspace the NMS-CO requires the DoD CI community to "form a DoD Counterintelligence Cyber Program."[19]

To meet this requirement, the DoD CI community is working to establish formalized policy, planning, and guidance, to increase resources, to provide training and tools, and to standardize tradecraft and professional standards that will support the CI force operating in cyberspace.

The first step in this management planning process is to establish this strategy for CI in Cyberspace in collaboration with the entire DoD CI enterprise to set the major themes that will guide future planning.

A DoD CI in Cyberspace Implementation Plan will expand on these themes and establish roles and responsibilities, task assignments, milestones, and performance measures to implement the objectives of this strategy. The Defense Intelligence Agency, Defense Counterintelligence and HUMINT Center CI in Cyberspace Program Management Team will oversee the implementation of the strategy across DoD.

Further guidance documents will be issued to expand on the doctrine, tactics, techniques, and procedures to be implemented in the field that address the individual operational needs and requirements of the military services, defense agencies, and combatant commands.

The DoD CI mission in cyberspace is to deter, detect, identify, assess, and neutralize or exploit, and ultimately defeat adversary activities in cyberspace. This is accomplished through CI investigations, operations, collection, analysis and production, and functional services in cyberspace.

Fulfilling this mission is a significant challenge considering the breadth and scope of adversary activities in cyberspace, and the speed with which technology in cyberspace advances.

The DoD CI components in the military services, defense agencies, and combatant commands, will take action to fully implement a CI in Cyberspace Program and develop a professional DoD CI force that will accomplish the mission and enterprise objectives set-forth in this strategy.

[18] Joint Chiefs of Staff, *Memorandum for Distribution: Guidance for National Military Strategy for Cyberspace Operations Implementation Planning* (Washington, D.C., 15 February 2007), Attachment – Terms of Reference for the National Military Strategy for Cyberspace Operations, 1.

[19] Department of Defense, *The National Military Strategy for Cyberspace Operations Implementation Plan* (Washington, D.C., dated 24 September 2007, signed October 1, 2007), A-26.

APPENDIX

Definitions

- **Counterintelligence:** Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.[20]

- **CI Functions:** Investigations, operations, collection, analysis and production, and functional services.[21]

- **CI Mission Areas:** CI support to Research and Technology Protection (RTP), Critical Infrastructure Protection (CIP), Force Protection and Combating Terrorism, and support to Information and Capabilities Protection.[22]

- **Cyberspace:** A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (NSPD-54).[23]

- **Counterintelligence in Cyberspace:** Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.[24]

[20] The White House, *Executive Order 12333: United States Intelligence Activities* (Washington, D.C., 4 December 1981 (as amended by Executive Order 13470, 2008)), 36.

[21] Department of Defense Directive O-5240.02, "Counterintelligence," December 20, 2007.

[22] Department of Defense, *The Department of Defense Counterintelligence Strategy - Fiscal Years 2008 – 2013* (Washington, D.C., 2008).

[23] Department of Defense, *Joint Publication 1-02: Dictionary of Military and Associated Terms* (Washington, D.C., 12 April 2001 (as amended through 30 May 2008)), 141.

[24] Ibid.