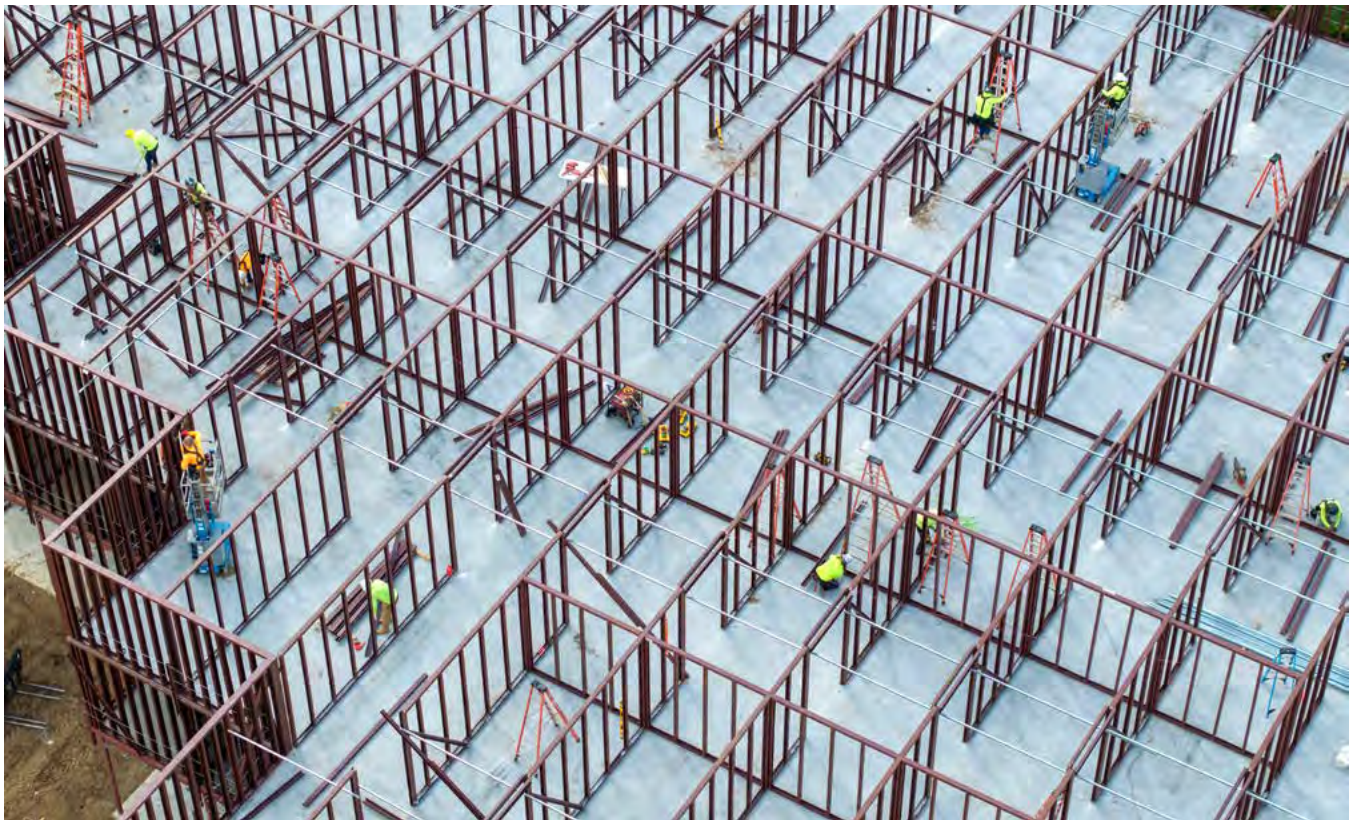

An overhead view of a building construction site.

Deconstructing and Reconstructing Strategic Counterintelligence

Toward a New Model

Roald Moyers

Roald Moyers is a counterintelligence professional who served in the Department of Defense and Department of Homeland Security and in the US Army as a HUMINT collector.

The United States is actively engaged in combating what is being termed systems-destruction warfare, in a manner that Chinese military scholars refer to as unrestricted warfare. Within systems confrontation, conflict is waged in the traditional physical domains of air, land, sea, and space, but also the non-physical cyberspace, electromagnetic, and information domains. Systems-destruction warfare applies predominantly to the application of military resources and systems to wage war and dominate within these domains. China's vision of unrestricted warfare, however, relates to more overarching principles for new warfare that is omnidirectional, asymmetric, and unlimited in its application.

Full-Spectrum Contest

Unrestricted warfare is executed across and through all the instruments of national power.[1] As a Defense Department report noted in 2023, international rivalry today is "far more complex than the 19th century's Great Game, the 20th century's Cold War, or the beginning of the 21st century's War on Terror. It transcends traditional diplomatic and military solutions to yield a full-spectrum contest of powers vying for strategic advantage through diplomacy, military strength, and economic and technological superiority."[2]

In particular, China views and applies its instruments of national power (diplomatic, informational, military, and economic) as operational systems to achieve its national interests. Beijing's intent is to degrade, deny, and disrupt the United States first and foremost, but also Western-dominated international norms and systems by applying all facets of China's instruments of national power in a directed effort. Today's battlefield is not confined to traditional force-on-force conflict; it comprises the breadth of instruments and systems that the United States depends on for everyday life, including the military systems and instruments that underpin military capability and the interstitial spaces that bridge them together.

The complex blending and interrelation of national power dimensions and the strategic battleground has proven to be a very difficult concept for the counterintelligence (CI) community to adapt to. For decades, our broader CI community has suffered in both identity and responsibility in its mission. Underlying CI's "fractured, myopic, and marginally effective" report card is CI's continued lack of operationally minded philosophy, and established theory, which lead to misfocused practices and priorities.[3,4] Counterintelligence professionals such as Michelle Van Cleave, Paul Redmond, John Ehrman, and James Olson, among others, have called to revitalize and refocus CI toward strategic counterintelligence and to operationalize CI. Some 40 years ago, George Kalaris and Leonard McCoy called to redefine CI considering the growing technical threats across the intelligence disciplines, where CI must learn to adapt, understand, apply, and professionalize in.[5]

Despite encountering and struggling to combat systematic unrestricted warfare, the CI community remains locked in a mental model where CI serves as a security function, as opposed to a strategic intelligence discipline. To be sure, there have been CI successes and the CI community appreciates the daunting challenge of its mission. On balance, however, the CI community fails to break down, analyze, and rebuild new models to succeed in today's complex operating environment. Using a grounded theory of CI, this paper deconstructs the current CI model and reconstructs it to propose a more effective and operationally relevant model of CI for the current and future operating environment.

Literature Review

There is much in the current body of CI literature on practitioners writing about their experiences. Although these provide breadth and depth on CI's application and challenges, they generally focus on the more traditional roles associated with CI functions such as counterespionage, insider threat, and the nexus of security, analysis, and classic offensive operations. Academics have also greatly contributed to the discipline of CI by heeding the calls of practitioners to develop a theory to better define, understand, and apply CI. What remains to be written and established for strategic CI, however, is grounding the theories with practice.[a] This paper leaves ample space to continue grounding practice and theory through the application of strategic CI theory and policy.

This paper builds on Prunckun's (2011) theory of

a. See, inter alia, Executive Order (EO) 12333, CI Enhancement Act of 2002, and Intelligence Community Directives (ICDs) 750 and 700. See also Department of Defense Manual (DODM) 5240.01, DOD Directive (DODD) 5240.02, DOD Instruction (DODI) 5240.10, among other Defense policies.

Evolution of Counterintelligence

The current CI model has been shaped through continual reforms over the past 25 years, beginning in earnest with Presidential Decision Directive *75*, *US Counterintelligence Effectiveness – Counterintelligence for the 21st Century* promulgated in December 2000. PDD-*75* called for a predictive and integrated CI system. Over the next 25 years, the IC took steps to continue strengthening US capabilities and effectiveness by integrating CI into and across the national security enterprise and into US industry. These steps also include the establishment of functional and mission managers within the Office of the Director of National Intelligence (ODNI). Functional managers were charged with the authorities for developing and implementing strategic guidance, policies, procedures for activities related to a specific intelligence discipline, or set of intelligence activities; set training and tradecraft standards; ensure coordination within and across intelligence disciplines and intelligence community elements and with related non-intelligence activities.[20] In 2010, DNI James Clapper merged the CI and security offices into the Office of the National Counterintelligence Executive (later the National Counterintelligence and Security Center). Intelligence Community Directive (ICD) *750* on counterintelligence programs was implemented in 2021.

counterintelligence, which leans on Johnson's (1987 and 2009) and Ehrman's (2009) earlier efforts to develop a CI theory.[6] Although Wettering (2000) addresses organizational, behavioral, and institutional challenges, his focus remains on CI as a security, and counter-espionage function of intelligence which perpetuates the mental models this paper calls to break down and reconstruct.[7] This paper also leans on John Boyd's work on deconstructing and reconstructing mental models.[8] As outlined by EO 12333, CI means 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.[9]

Bedrock Of Intelligence

CI is the bedrock of intelligence and operational functions. Sound CI processes and activities applied to the collection and analysis of information (including its own counterintelligence information) for intelligence purposes lends credibility to intelligence which supports the development and execution of policy, strategy and operations. Prunckun (2011) lists four principles of CI: deter, detect, deceive, and neutralize. In addition, Prunckun lists three axioms, or conditions of CI: surprise, data collection, and targeting.[10]

This paper modifies this to five CI principles based on CI as defined through EO 12333: *identify, deceive, exploit, disrupt,* and *protect*. The five CI principles have both an *offensive* and *defensive* focus. As Prunckun argues, for intelligence, military, or even strategic business operations to be successful, they must achieve an intended degree of surprise. CI enables surprise at all operational levels by establishing and maintaining secrecy.

Data Collection

In order for CI to establish and maintain secrecy for its supported organization and missions, CI must collect data. An adversary, or competitor's intelligence functions will use all available means (legal, illegal, technical, non-technical) to collect information on its competitor. Simply put, an adversary will conduct reconnaissance on its target to collect intelligence. That reconnaissance can occur through a myriad of means purpose built or assembled to specifically target the information needed to develop operational and strategic intelligence

and to enable the adversary's own surprise.

To establish and maintain secrecy, CI must understand the range of means and methods available to collect information, what can be targeted, how, and why, and what information, through what means can be collected against its supported element. In other words, CI must conduct counterreconnaissance. To be effective, CI must collect information across the breadth of its operating environment. CI must be where adversarial foreign intelligence entities (FIE) operate and are attempting to collect on, penetrate, and exploit.

Third, adversary intelligence activities and national and military strategies focus on targeting information that enables it to disrupt, deny, degrade, or exploit its target, and its target's vulnerabilities, sphere of influence, operations, capabilities, and intentions—present and future. This means CI must continuously collect and analyze data across the scope of its operating environment on both friendly and the adversary to develop an understanding of CI vulnerabilities, threats, and opportunities to provide effective mitigation measures.[11] In other words, to enable security and secrecy.

Deterrence

CI's axiom of secrecy is where CI and security converge. CI supports security through the defensive counterintelligence principle of deterrence.[12] There are three premises to deterrence.

Unacceptable Damage

The premise of unacceptable damage holds that there must be some form of retaliation against the adversary or their intelligence organization. Retaliation may also extend into the domain of international relations. For example, political demarches, public expulsion of intelligence officers and or political officers, arrests, or conversely, dismissal from national security positions for security infractions.

Perception

The second premise is perception by an adversary. The adversary must perceive that a threat has been communicated to it.

Credibility

The third premise, credibility, requires both capability and intent. An adversary must perceive the threat of retaliation to be credible and that it would jeopardize the success of their capability, operations, and or strategy.[13] Another aspect of this is the capability and intent to identify an adversary's penetration (e.g. the CI insider threat) and exploit it to the adversary's disadvantage, which ultimately leads to deterrence.

Current Application

So how does theory shape the practice of strategic CI? Today's model is fragmented, with an over-emphasis on security-focused policies and processes. It lacks a coordinated whole of government effort enabled by baseline professional expertise and acuity. It severely limits effective responsiveness to adapt preemptively and recursively to adversarial threats. As a result, CI struggles to achieve the desired objectives and results of the national counterintelligence strategies.

Currently, CI is outlined in DODD 5240.02, which breaks CI into distinct mission areas: 1) countering espionage, international terrorism, and the CI insider threat; 2) support to force protection; 3) support to the defense critical infrastructure program; and 4) support to research, development, and acquisition. CI activities—analysis, collection, investigation, operations, production, and functional services—are applied toward a distinct mission area. Functional services are the combined application of CI activities.[14]

DODM 5240.02 also directs CI to be integrated into all operations, programs, systems, exercises, planning, doctrine, strategies, policies, and information architectures. This is also consistent with ICD 750. In keeping with its security centric mental model, CI approaches this directive through

the lens of support to security whereby CI, as a second tier system seeks to integrate its resources into existing operational security, information security, personnel security and physical security processes and technologies in an effort to passively bolster security as a deterrent, thereby enabling its principle of deny (focused inwardly) across the security architecture.[15] However, its protection measures are hollow and without real authority, as they are inherently the protection measures afforded by and through the security architecture when and where they are integrated. As outlined in ICD 750, Defense Department policies, and DHS policies, CI is also responsible for CI training as defensive measures and in some cases perceive training as a proactive CI measure.

Organizational CI efforts are focused on one or more functions. Additionally, the application of the functions are siloed, resulting in a stunted understanding and awareness of the full breadth of CI. Moreover, most CI organizations are not imbued with full authorities under EO 12333, and even when CI organizations have full authorities under EO 12333, they choose to further constrict themselves to functional services consistent with the prevailing model, which further reduces the overall application of CI functions. These factors exacerbate a constrained mental model where CI only operates and applies to narrowly defined mission areas that are easily conceivable. Additionally, with ICD 750 and the merger of CI and security, countering insider threats and espionage have blurred into CI as security. This approach focuses resources and policies inward and subordinates them to the security mission.

In short, security enables secrecy and CI assesses whether secrecy remains feasible. Secrecy is enabled through security-oriented policies and procedures such as security classification guidance, information security, and operational security. CI supports security by deterring potential security violators through the subjection of punishment under espionage-related statutes.[16] Deterrence is also achieved through its defense measures of training.

Despite policies explicitly directing the incorporation and support of CI activities into the security framework, the implementation of CI for deterrence remains a secondary security priority, as it creates a redundancy of security processes at an increased cost to security. The prevailing CI model also presents significant gaps in CI collection across the larger national security framework due to increased costs for the required intelligence architecture required for limited perceived benefits. These gaps are the results of the fragmented approaches and integration of CI with security and redundant security measures since security and cyber security incidents are generally reported through respective reporting channels.

Well-established CI programs incorporate a CI review process in the security and information technology architectures, but the degree of incorporation is not equal across the executive agencies. The organizational integration of CI and security divorced from the intelligence architecture limits CI's ability to collect relevant information. The fragmentation of CI and mental models of integrated CI/SEC functions exaggerate these issues, where IT systems are distinct, and CI takes on more of an educational and consultative role as presupposed through ICD 750 and patchwork of fragmented CI policies throughout the national security enterprise.

Security is derived from CI. In this model the execution of CI leads to the implementation of defensive security measures and postures. The defensive activities and postures are the security policies and measures implemented resulting from the execution of CI. In this model, CI executes what it perceives as its three primary principles of deny, through CI as a deterrent, proactively identify through the security architecture (and in the case of the larger CI model, through fragmented relationships and coordination measures), protect by bolstering the security architecture across operations, programs, systems, exercises,

planning, doctrine, strategies, policies, and information architectures. Protection is afforded through the collection of information, which enables the feedback to defensive measures. They are considered offensive, in that they are directed and engage directly with an adversarial FIE through controlled operations.

In this limited model, security supports CI as a mechanism to detect, in order for CI to carry out the classical principle of exploitation. The limited model of CI attributes deception through the principle of exploitation. In this context, deception enables controlled double- agent operations against an adversary. The prevailing Defense model of CI, however, has distanced itself from the general principle of deception and left it to develop into its own discipline of military deception. The divergence of deception from CI and the importance of its role in offensive and defensive CI was and remains a crippling blow to strategic counterintelligence. Deception is a fundamental principle of counterintelligence.

Toward A Strategic Model

China has taken on a system-of-systems worldview and has aligned its instruments of national power to pursue a system of systems approach to becoming the preeminent global power. The battlefield comprises all operational domains. Within this framework, China has developed a multidimensional and multifunctional operational system to be employed against all domains. Yet, it must also be flexible to incorporate new technologies and new functions over time. What this system of systems affords is a modular approach of applying any combination of elements, components, and systems in an integrated fashion to achieve dominance over an opposing system.[17]

For CI, this means the current fragmented and security-focused model of CI is ineffective at identifying and countering the CI threats across the instruments of national power. Moreover, the fractured nature of the CI discipline, where a limited application of CI functions are applied to one problem set at a time, will never effectively identify and counter the FIE threats across the modern warfare domains. To be effective, it must take on a strategic system-of-systems perspective toward CI authorities, institutions, and threat landscapes. Moreover, CI must take on an operational model freed from its self-imposed shackles of constraints and restraints.

Strategic CI is both offensive and defensive. Its state in support of a particular operation, activity, domain, or intelligence function comprises both offensive and defensive properties. Much like light is both an electromagnetic wave and a particle, CI depends on how it is approached. The current mental models associate offensive activities with clandestine activities and are distinct from defensive activities. It also associates intelligence activities in confrontation with FIE to require approaches and methods equal to those of clandestine intelligence activities.

However, as an intelligence discipline, CI leverages its fundamental authority and responsibility derived from EO 12333 to seek out and collect targeted information to identify adversarial reconnaissance and collection efforts. Strategic CI leverages this fundamental responsibility to proactively seek out across all possible threat domains (internal and external) information of intelligence value for CI to identify, deceive, exploit, disrupt, and protect. It is through the intelligence authorities imparted upon CI through EO 12333, the CI Enhancement Act of 2002, and the successive intelligence legislation that enables strategic CI to exert its intelligence authorities across all domains. The limiting factors are which organizations can apply clandestine intelligence activities, and the full scope of CI investigative activities to independently prosecute identified FIE threats.

Offensive Counterintelligence

Offensive CI comprises those activities that are executed proactively through counter-reconnaissance and counter-collection efforts across the operational

domains that actively seek out FIE reconnaissance and collection activities. Offensive activities can either use existing security functions, processes, and technologies to seek out and collect adversarial collection and reconnaissance efforts related to penetration (i.e., CI insider threats), or through targeted collections across the operating domains to identify adversarial collection and reconnaissance efforts.

Within the strategic model, offensive activities do not equate to clandestine activities, but rather proactive targeting of intelligence information within the breadth of the mission space to actively seek out to identify FIE collection and reconnaissance activities. In other words, preemptively and proactively conducting counter-reconnaissance and counter-collections to identify FIE collection and penetration attempts and, or activities. Additionally, defensive measures include vulnerability assessments, and the implementation of security procedures to mitigate vulnerabilities, and conducting CI overwatch, or countersurveillance of friendly forces, or of other intelligence activities. The prevailing fragmented CI model distinguishes these CI activities as distinct functional services (CI support to HUMINT, CI Support to Force Protection, etc).

Surprise

Surprise in strategic CI is more effectively achieved by its role as an intelligence discipline where it stands outside security, and not as a sub-function of security. Timely information is key to maintaining and generating surprise. Organizations create and architect intelligence assets in a manner that affords timely and efficient collection and reporting of information. For the sake of achieving operational surprise elements of security can be sacrificed. Moreover, at times, security must be deceived for the sake of exploiting opportunities to achieve or maintain surprise. Positioning CI within security (unless done for clandestine purposes), denies our own ability to enable surprise.

Surprise is also more effectively achieved when CI and security are distinct from one another, by allowing for the use of the breadth of intelligence authorities that are bestowed upon intelligence functions. Secrecy is achieved in strategic CI by employing the espionage statutory frameworks to compel and bind others to secrecy. This facet also creates effective deterrence by directly compelling and subjecting others to the espionage criminal statutes for the purpose of protecting intelligence sources, methods, and activities. CI merged with, or subordinated to security architectures loses this critical and effective facet of deterrence thereby hollowing out CI as a credible deterrent.

Deterrence

Deterrence is more effectively achieved by its role as an intelligence discipline. CI is inherently a unique intelligence discipline, in that it is afforded the option of pursuing its responsibilities and authorities under intelligence legal frameworks, or under federal criminal statutes. However, they are not strictly mutually exclusive. Strategic CI allows for the full breadth of intelligence partnerships and sharing of authorities to achieve the most effective use of resources, while ensuring and enabling surprise and secrecy. Leveraging whole government authorities and partnerships as intended allows the greatest opportunities for deterrence by uncovering a greater extent of FIE espionage and intelligence networks, activities, and methods.

Deterrence from a strategic perspective also does not simply equate to public charges or dismissal of intelligence or political figures, or of political responses. Deterrence can also be achieved by leveraging the exploited networks to exploit the opportunities they present and offensively attack and penetrate the FIE's intelligence systems at a time and place of our choosing. This positions strategic CI as a critical enabler of surprise, by enabling other operational attack systems (kinetic, and non-kinetic) to penetrate adversarial networks across the warfare domains.

Recommendations

All the of the necessary legislative requirements and authorities are already in existence to

reconstruct CI toward a strategic model. Additionally, the institutional systems and mechanisms for both overt and clandestine activities are already present, to include the sharing of resources and authorities, coordination and deconfliction, and referrals of intelligence activity opportunities. Strategic CI is also already doctrinally established and can be observed through joint warfare doctrines such as command and control warfare and irregular/unconventional warfare doctrines.[1819] Historically, strategic CI can also be observed in the obsolete US Army Counterintelligence Field Manual, where CI was applied through the full range of operational planning and intelligence activities.

A successful strategic CI model for the national security enterprise requires policies that reinforce CI as an intelligence discipline distinct from organizational positions subordinate to security architectures. It will require in policy that organizational CI functions incorporate the respective intelligence oversight required of intelligence activities and functions to ensure the appropriate protection of civil protections, while enabling protection of sources, methods, and activities.

While this may seem an unnecessary statement, many non-Title 50 executive branch departments that maintain small national security elements for intelligence and counterintelligence do not possess the basic oversight structures required of a functioning intelligence and counterintelligence activity. Strategic CI requires a more concerted national mission management role for CI within ODNI for the vast CI missions across the US government. This would entail stronger representation and coordination of intelligence priorities and missions from the disparate CI missions across the executive offices of the US government and among the IC.

Increased professional training and standardization of training and certifications will also be a requirement. Current training standards and baselines are already in existence; however, the IC should seek to improve standardizations amongst the broader CI community and elevate the baseline CI certifications to more advanced levels of CI to ensure equal integration and transferability amongst the broader CI community.

Our adversaries have been studying our systems and our methods and technologies of warfare over the course of the 21st century. In response to our strengths, they have advanced forms and domains of warfare that we have been slow to accept, adapt, and respond. If the United States is to succeed in this era of unrestricted warfare, the CI community must deconstruct and reconstruct CI as a singular, holistic, and adaptable intelligence discipline. An offensively postured mindset would continuously look across all domains, disciplines, and functions to proactively identify, deceive, exploit, disrupt, and protect. We must be adept at recognizing opportunities and knowledgeable in leveraging the whole of government to exploit opportunities. In this way, the CI community can adapt to the changing threat environment. ■

Endnotes

1. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (People's Liberation Army, 1999).
2. Defense Counterintelligence and Security Agency, *Targeting U.S. Technology: A Report of Threats to Cleared Industry* (2023), 3.
3. Michelle Van Cleave, "Strategic Counterintelligence: What Is It, and What Should We Do About It?" *Studies in Intelligence* 51, No. 2 (June 2007).
4. John Ehrman, "Toward a Theory of CI: What are We Talking About When We Talk About Counterintelligence?" *Studies in Intelligence* 53, No. 2 (June 2009).
5. George Kalaris and Leonard McCoy, "Counterintelligence for the 1990s," *Studies in Intelligence* 32, No. 1 (Spring 1988).
6. William Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer* (Stone Trail Press, (1987; Georgetown University Press, 2009).
7. Wettering, "Counterintelligence: The Broken Triad," *International Journal of Intelligence and CounterIntelligence* (2000):13, published online October 29, 2010.
8. John Boyd, "Destruction and Creation" (1976). https://www.coljohnboyd.com/static/documents/1976-09-03__Boyd_John_R__Destruction_and_Creation.pdf.
9. President, United States of America. "EO 12333, As Amended." Federal Register. Vol. Vol. 46. Washington D.C., 8 December 2008.
10. Hank Prunckun, "A Grounded Theory of Counterintelligence," *American Intelligence Journal* 29, No. 2 (2011), 8–10.
11. Ibid., 10.
12. Ibid.
13. Ibid.
14. Department of Defense, Department of Defense Directive 5240.02, Counterintelligence (Government Publishing Office, 2018).
15. Ibid., Section 3.d., 2.
16. 18 U.S. Code Chapter 37 Part I – Espionage and Censorship.
17. Engstrom, 2018.
18. Milan Vego, Joint Operational Warfare: Theory and Practice (Naval War College, 2009). Command and Control Warfare, (C2W) as defined by Joint Operational Warfare "is understood as integrated use of information operations, security, military deception, psychological operations, electronic warfare, and physical destruction all supported by intelligence to influence, degrade, deny information to or destroy an adversary C2 capabilities while protecting one's own or against similar actions applicable across the entire spectrum of conflict" (VIII-45). C2W is both offensive and defensive and is employed simultaneously across the operational spectrum (tactical to strategic).
19. For more on the application of CI in irregular warfare see Aden Magee, "Counterintelligence in Irregular Warfare: An Integrated Joint Force Operation," *American Intelligence Journal* 29, No. 2 (2011): 16–23.
20. 108th Congress. Intelligence Reform and Terrorism Prevention Act. Public Law 108-145. US Federal Register, 2004.
21. For a timeline of CI events see: ODNI. Time-Line of CI Milestones. n.d. 2024. https://www.dni.gov/index.php/ncsc-features/203-about/organization/national-counterintelligence-and-security-center?start=36.