Operationalizing Intelligence Collection in a Complex World: Bridging the Domestic & Foreign Intelligence Divide

James Burch, DM
Colorado Technical University

Abstract

Intelligence collection is a powerful US intelligence capability, which has demonstrated its effectiveness in categorizing complex threats. Intelligence collection, however, is not "operationalized" in the sense that it can quickly shift collection capabilities to focus on adaptive threats. Additionally, it is not bridged to effectively function across the domestic and foreign elements of the intelligence community. Modern-day threats are adaptive, complex, and span national boundaries, while intelligence collection remains largely within its domestic and foreign confines. While there are high-level bodies that coordinate collection, a key gap in the intelligence community's approach is an organizational element that operationalizes and bridges domestic and foreign intelligence collection to ensure the community can meet the highest priority threats. This represents a significant seam in the community's capacity to meet modern-day threats in a complex environment. This conceptual paper uses Hesselbeim's seven-faceted transformation framework to develop an approach to operationalizing and bridging intelligence collection across the domestic and foreign divide. It concludes that such an organizational bridging function is valid and necessary in order to meet modern-day and emergent threats.

Keywords: intelligence collection, organizational design, change management, transformation

Recopilación de inteligencia operativa en un mundo complejo: superando la brecha de inteligencia nacional y extranjera

Resumen

La recopilación de inteligencia es una poderosa capacidad de inteligencia de EE. UU., Que ha demostrado su eficacia para categorizar

doi: 10.18278/gsis.5.2.7

amenazas complejas. Intelligence Collection, sin embargo, no está "operacionalizado" en el sentido de que puede cambiar rápidamente las capacidades de recopilación para centrarse en las amenazas adaptativas. Además, no tiene un puente para funcionar eficazmente a través de los elementos nacionales y extranjeros de la comunidad de inteligencia. Las amenazas de hoy en día son adaptables, complejas y traspasan las fronteras nacionales, mientras que la recopilación de inteligencia permanece en gran medida dentro de sus límites nacionales y extranjeros. Si bien hay organismos de alto nivel que coordinan la recopilación, una brecha clave en el enfoque de la comunidad de inteligencia es un elemento organizativo que operacionaliza y une la recopilación de inteligencia nacional y extranjera para garantizar que la comunidad esté preparada para enfrentar las amenazas de mayor prioridad. Esto representa una veta importante en la capacidad de la comunidad para enfrentar las amenazas modernas en un entorno complejo. Este documento conceptual utiliza el marco de transformación de siete facetas de Hesselbeim para desarrollar un enfoque para poner en funcionamiento y unir la recopilación de inteligencia a través de la división nacional y extranjera. Concluye que dicha función de puente organizativo es válida y necesaria para hacer frente a las amenazas actuales y emergentes.

Palabras clave: Colección de inteligencia, diseño organizacional, gestión del cambio, transformación

在复杂世界中对情报收集进行操作化：在国内和国外情报鸿沟之间搭建桥梁

摘要

情报收集是美国强有力的情报能力，其已通过对复杂威胁进行分类从而证明了有效性。然而，情报收集还未实现“操作化”，即能迅速转变收集能力，聚焦于适应性威胁（adaptive threats）。此外，情报收集还无法在国内和国外情报界之间进行有效运作。现代威胁具有适应性和复杂性，并且跨越国家边界，然而情报收集在很大程度上还局限于国内和国外范围。尽管存在能协调情报收集的高级别机关，但情报界方法的关键不足在于没有一个能对国内和国外情报收集进行操作化并在二者间搭建桥梁的组织要素，以确保情报界能准备好面对最需优先处理的威胁。这代表情报界在应对复杂环

境中的现代威胁的能力方面存在显著缺陷。本篇概念性文章使用学者Hesselbeim的转型框架（包含七个方面），以期提出一项能在国内和国外情报鸿沟之间对情报收集进行操作化并搭建桥梁的方法。本文结论认为，这样一个跨越障碍的组织功能是有效且必要的，以期应对现代新兴威胁。

关键词：情报收集，组织设计，变革管理，转型

> We need to deal with the realities of globalization—the blurring these days of foreign and domestic matters. Because when threats like terrorism and international organized crime transcend borders, it's critical that we think holistically about intelligence. But we're also a people who—Constitutionally and culturally—attach a high premium to our personal freedoms and our personal privacy.
>
> —James Clapper, former Director of National Intelligence (DNI 2013)

Introduction

The 9/11 attacks ushered in a new era and challenge for the US national security and intelligence communities. Within the span of several hours, two major US cities and a downed civilian airliner suffered significant loss of life that resulted in a tremendous psychological impact. The 9/11 attacks highlighted the intelligence and security challenges of living within an integrated and globalized environment. While global threats have always had domestic implications, the economies of scale associated with the attacks were significantly egregious. A relatively small group of motivated terrorists planned and executed an extremely lethal attack at the expense of approximately $400,000 to $500,000 with nineteen suicide operatives, inflicting over 3,000 deaths and billions of dollars in damage (National Commission on Terrorist Attacks Upon the United States 2004). This attack triggered trillions of dollars in expenditures and the largest reorganization of the US government since the *National Security Act of 1947* created the Department of Defense (DoD) and the modern-day US Intelligence Community. The impact and the scale of the attacks illustrated the need to significantly re-evaluate the foreign-domestic divide of national security.

Within the national security context, the 9/11 attacks also marked a stark departure from the Cold War approach to addressing and categorizing intelligence issues. The US Intelligence Community, traditionally focused on threats posed by nation-states, was suddenly faced with an unconventional, adaptable, asymmetric, complex, and non-state threat. Intelligence estimates, traditionally based on analysis of weapon systems, procurement, and movement of major military units, were challenged with having to assess an individual's intent, strategies, and motivations. Because these attacks occurred on US soil, the convenient organizational demarcation between foreign and domestic intelligence was forever blurred and altered.

The organizational response to dealing with this contrived demarcation, however, was not novel or forward leaning, nor did it span the domestic and foreign intelligence communities' resources and capabilities. In the aftermath of the attacks, intelligence reformists called for dismantling the barriers to information sharing. Slogans and buzzwords that highlighted the ineffectiveness of integrating intelligence, sharing information and failure to act upon promising intelligence led to the promises of a "culture of continuous improvement" in response to the key findings in the Congressional Joint Inquiry (US Senate 2002), which stated:

> Serious problems in information sharing also persisted prior to September 11, between the Intelligence Community and relevant non-Intelligence Community agencies. This included other federal agencies as well as state and local authorities. This lack of communication and collaboration deprived those other entities, as well as the Intelligence Community, of access to potentially valuable information in the "war" against Bin Laden.

Another slogan, "failure to connect the dots," was popularized by the National Commission on Terrorist Attacks Upon the United States (2004) to highlight these shortfalls.

While the sharing of information within and among organizations is arguably a fundamental premise for success, it is also singularly narrow in its perspective. Merely sharing information or even achieving the ultimate end state of "information sharing" does not guarantee a secured homeland. It glosses over the other intelligence functions and tasks necessary to work together to better posture intelligence capabilities. Additionally, while the post-9/11 changes to the national security and intelligence communities were significant, they were also narrowly focused on international terrorism with linkages to and within the United States. The creation of the Department of Homeland Security (2002), the establishment of the National Counterterrorism Center (2004), and the proliferation of state and local fusion centers with the original mandate to focus on terrorism are tangible manifestations of this narrow focus. Sharing information and fusion centers alone do not support the broader integration of functional intelligence activities—planning, analysis, collection, targeting, to name a few—necessary to bridge the various organizations engaged with making a safer homeland.

This concept paper focuses on one functional activity—intelligence collection. The 9/11 attacks realigned the US Intelligence Community to focus largely on combatting Islamic terrorism from both domestic and foreign perspectives, given the contiguous nature of the threat. Over time, however, the rise of near-peer competitors, proliferation, transnational organized crime, espionage, cyber threats, and even consequence management responses to natural disasters have highlighted the need to operationalize and bridge intelligence collection across domestic and foreign communities. The term *operationalizing* suggests that intelligence collection must be aligned to support the highest priority strategic intelligence objectives in an integrated and timely manner according to an established strategy. Additionally, the term suggests that collection assets and resources should ideally be shifted quickly to meet emergent and trending threats. The term *bridging* highlights the organizational, process, and technological gaps that currently exist and that inhibit the operationalization of intelligence collection at the strategic level.

Despite the contiguous, changing, and dynamic nature of intelligence threats, the way intelligence collection is managed has not evolved. In other words, intelligence collection is not postured to meet modern day threats in a holistic and integrated manner. The requisite authorities, functions, and management tools to leverage these capabilities in an agile and timely manner remain divided and stove-piped across various domestic and foreign intelligence organizations and communities of interest. This represents a key seam in the US Intelligence Community and limits its ability to align and leverage intelligence collection against the highest priority threats. The purpose of this paper is to establish a conceptual framework to explore the issue of operationalizing and bridging intelligence collection across the domestic and foreign elements of the intelligence community. It is meant to serve as a foundational concept that drives follow-on research and scholarship into an intelligence capability that is not fully realized.

Literature Review

The following review focuses on the misalignment of intelligence collection from a three-fold perspective. It delves first into the nature of the intelligence collection function in the modern day to gain a sense of the challenges and gaps that exist. Secondly, the review focuses on existing organizational designs within the US Intelligence Community that serve to operationalize intelligence collection. The review also focuses on current research to identify trends and issues framing intelligence collection. The majority of the literature reviewed is derived from peer reviewed journals and sources, but also includes relevant US government documents and doctrine.

Intelligence Collection

The issue of intelligence and its role in the post-9/11 world has been extensively debated. That said, much of the public debate deals largely with topical issues such as terrorism, regional crises, cyber, or other functional issues such as intelligence analysis, information sharing, or knowledge management. The topic of intelligence collection, and more importantly, how it is managed, integrated, and leveraged to drive other intelligence functions has not been as extensively evaluated. Moreover, examining the issue of intelligence collection management from the perspective of bridging the foreign and domestic elements within the US Intelligence Community is largely absent.

Much of the recent literature and doctrine of intelligence collection stems from the US military and its involvement in major overseas engagements in Southwest Asia since the 2001 terrorist attacks. At the strategic level, the most recent *National Intelligence Strategy* (US Government 2019) effectively outlines several key attributes to enable effective intelligence collection. The strategy highlights the importance of Integrated Mission Management, which is to "Prioritize, coordinate, align, and deconflict IC mission capabilities, activities, and resources to achieve unity of effort and the best effect in executing the IC's mission objectives" (Office of the Director of National Intelligence [ODNI] 2019). The key enabler is the importance of integration of capability, mission, knowledge, and intelligence collection to meet the highest priority threats across the intelligence community's enterprise. The intelligence strategy also highlights the need for integration to bring the power of persistence in intelligence collection to meet complex threat challenges. A recent RAND study concluded, "Taken together, these challenges present the IC with a daunting task and underscore the need for **persistence** [author's emphasis] in collection, global analytic coverage, and more-agile intelligence organizations that can seamlessly and rapidly surge to crises" (Weinbaum et al. 2018, 44). The strategy acknowledges up-front that the strategic operating environment is "complex and uncertain world in which threats are becoming ever more diverse and interconnected" (National Commission on Terrorist Attacks Upon the United States 2004, 4). To operate within this environment, the national strategy outlines five necessary attributes critical to enabling enterprise objectives; namely, *intelligence integration*, *IC workforce*, *IC partnership*s, *transparenc*y, and *technological innovation* (National Commission on Terrorist Attacks Upon the United States 2004, 26). These attributes broadly capture the key initiatives to enable vertical and horizontal integration across the enterprise. They are also meant to operate across both the foreign and domestic components of the US Intelligence Community.

The intelligence collection capabilities employed to support the Integrated Mission Management function are divided into five disciplines: Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), Signals Intelligence (SIGINT), Measurement and Signatures Intelligence (MASINT), and Open Source Intelligence (OSINT). Fundamental to the management of these five "INTs" are two key functions. First, *Collection Requirements Management (CRM)*, which involves the development and tasking of collection, processing, exploration, or reporting requirements of assets under a collection manager or where tasking requests are sent to the asset owner, and secondly, *Collection Operations Management (COM)*, which deals with the direct scheduling and control of collection operations, processing, exploitation, and reporting. Viewed another way, CRM is "what" the intelligence community does to satisfy its requirements while COM is "how" the community collects its intelligence (ODNI 2011, 46–47).

Much of the literature that frames the topic of intelligence collection is organized along the examination of how these individual collection functions operate. Robert Clark's (2014) seminal work, *Intelligence Collection*, provides a detailed insight into the various forms of collection and techniques and challenges of the tasking, collection, processing, exploitation, and dissemination (TCPED) process. He also distinguishes the challenges of managing "front-end" expectations with the customer and the establishment of collection priorities versus the innards of "back-end" individual collection challenges in terms of data management and production (Clark 2014). The challenges of managing the "back-end" TCPED architecture on a broader level is also identified as a key issue in a RAND Policy Paper, *Perspectives and Opportunity in Intelligence for US Leaders* (2018), which highlights the stove-piped nature and lack of transparency of the processing and exploitation of individual collection programs and the inability to make data discoverable across the enterprise (Weinbaum et al. 2018). As the policy paper further points out, the promises of technology and integration has the possibility to serve as a key enabler for agnostic data discovery across the enterprise. Interestingly, the brief conceptualizes this approach to tackle the challenges associated with the US counterintelligence mission and challenges, which clearly contains both foreign and domestic elements.

The *5 Disciplines of Intelligence Collection* (2016) by Mark Lowenthal and Robert Clark further examines the five intelligence collection disciplines individually and concludes with a strategic-level overview of managing collection. While they acknowledge that each of the intelligence collection disciplines is examined individually, they also emphasize the importance of developing cross-INT strategies to leverage intelligence collection across the spectrum of capabilities. While *Intelligence Collection*, the *5 Disciplines*, and the RAND study focus largely on the technical aspects of the individual INTs and establish a clear description of collection capabilities while addressing some of the integration issues, there is little discussion on bridging the gap between the domestic and foreign intelligence communities.

Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments (2012) by Wayne Michael Hall and Gary Citrenbaum examines the issue of intelligence collection within a foreign-military perspective, but introduces several key and conceptual frameworks to illustrate the challenges of collection in the modern age. First, while focusing largely on the ability of the US military and foreign intelligence to operate overseas, they recognize the growing complexity of the operating environment and the nonlinearity of the challenges. In other words, the global environment is increasingly complex, where intelligence activities are faced with complex adaptive systems operating in the expanse of the information age (Hall and Citrenbaum 2012). Faced with such challenges, they propose a forward-leaning definition of *Advanced Collection,* which is framed as "the creative design and use of technical, cyber, human, and open-source collectors in all domains—air, ground, sea, space, information, and cyber—in pursuit of discrete, subtle, nuanced, and often fleeting observables, indicators, and signatures" (Hall and Citrenbaum 2012, 3). More importantly, they posit that advanced collection approaches oriented on increasingly complex operating environments are necessary to mitigate an adaptive and agile adversary. While their research is oriented toward a foreign context, it is clear that these concepts equally apply and bridge foreign and domestic intelligence communities.

Most notably, *The US Domestic Intelligence Enterprise: History, Development, and Operations* (2015) by Darren Tromblay provides an extremely insightful, expansive, and in-depth examination of the domestic Intelligence Community. He describes the militarization of intelligence during the aftermath of the Cold War at the expense of not only domestic intelligence, but on other elements of national power (ENPs), such as diplomacy and economics. In terms of intelligence collection, he articulates how collection requirements should be framed to support the decision-makers' views on maintaining ENPs. He further identifies shortfalls to the current structure of establishing national priorities and how the current domestic intelligence structure is not optimally aligned to support them. He emphasizes, "Requirements-oriented collection, covering the scope of an issue, will inevitably produce coverage on which action can be taken" (Tromblay 2015, 9). In other words, there is inherent power in leveraging intelligence collection to focus on key requirements that span across the domestic and foreign elements of the US Intelligence Community. The challenge is conducting intelligence-driven operations within an integrated and enterprise approach that span these domestic and foreign elements.

Additional insights into intelligence collection stem from operating within a complex operating environment and the challenges of automating the collection management process. Within the domestic environment, the topic of intelligence collection is naturally framed within the debate of US government overreach, concerns with privacy, and data retention. Faced with operating in complex environments during combat operations, several articles of military literature highlight the need for automation to integrate various CRM/COM functions, the importance of collection persistence to categorize complex environments, and the importance of planning to employ a complex array of collection assets with their own associated TCPED architecture and varying levels of control (Castagna 2004, 67–71; Schwerzler 2008, 25–27; Sterioti 2015, 46–48). The undercurrent themes in these articles highlight the challenge of intelligence collection within a complex operating environment. Additionally, the challenge lies not just in the complexity of the operating environment, but rather with the exponential growth of managing data given the digital revolution. As emphasized by Young (2013, 24–27), this "information overload" leads to cognitive overload, the potential for circular reporting, and inefficiencies in organizational management.

Although the US House of Representatives staff study, *IC21: The Intelligence Community in the 21st Century* (1996), predates 9/11 by several years, the scope of the study was expansive in nature and it was specifically enacted to examine the issues of intelligence collection within the community. The study recognized the changing global operating environment and the continued need for intelligence to support a growing number of disparate threats. In terms of collection, the study identified the challenge of integrating various intelligence stovepipes to leverage capabilities. It also identified the tasking and coordination shortfalls, along with the differences in culture between the intelligence and law enforcement communities. Of note, the study found:

> Much of this information [intelligence] is disseminated to law enforcement and other agencies as strategic intelligence. It has followed that in seeing these capabilities, law enforcement would at times like to task the intelligence community to collect on specific subjects. Of all the issues before the Interagency Task Force, this one has been the most difficult to resolve. (House of Representatives 1996, 312)

Interestingly, while the report identified the linkage between law enforcement and intelligence as one of the most difficult tasks, the key witnesses summoned to testify before the house committee and staff panels did not delve further into this topic—a key gap that remained unresolved.

While the focus of this paper lies solely on the issue of optimizing intelligence collection, there are naturally concerns with the topic as it applies to domestic intelligence. The passage of several key pieces of legislation introduced the use of mass surveillance systems capable of collecting prodigious amounts of data. With the disclosures of Edward Snowden and PFC Bradley Channing and an acrimonious bipartisan political environment accusing the opposing party of politicization, the issue of retaining information and data within a domestic environment is a highly charged issue. As outlined by Pulver and Medina, "80 percent of adults 'agree' or 'strongly agree' that Americans should be concerned with government surveillance of phone and internet communication" (Pulver and Medina 2018, 241–56). Similarly, there have been growing concerns that Bush-era warrantless wiretapping to pursue the "war on terror" has developed into broader intelligence objectives (Edgar

2017). Additionally, given the broader implications of domestic surveillance, there are growing concerns with not only data surveillance and data mining, but also the use of CCTVs and other tools and how these surveillance techniques are changing underlying culture (Bellaby 2012, 93–117). Given the disclosures and the inability of the current political climate to effectively address public concerns, the need to establish effective intelligence oversight mechanisms is clear (Galliott and Warren Reed 2016).

Clearly, intelligence collection in the modern era operates within an increasing complex environment. The need for agility, persistence, and bridging the foreign and domestic divide is critical to better posturing the US Intelligence Community to provide strategic warning and inform decision-makers. Additionally, there is a need for intelligence collection to support a broader set of customers, ranging from traditional national security and military customers to new ones within the homeland security enterprise and the public health and private sectors. This requires a highly adaptive, scalable, and forward-leaning approach to intelligence collection.

Organizational Design

Aligning US Intelligence Community collection capabilities to meet increasingly complex operating environments is a challenging task. It requires an examination into the development and design of organizational structures, policies, and mechanisms that are necessary to lead and manage a modern-day intelligence enterprise. Much of the literature has tangentially addressed this topic—more from the perspective of justifying the existence of an organization rather than questioning the narrative of how the enterprise should be aligned. In terms of intelligence collection, few if any studies have focused on leveraging this key enabler across the domestic-foreign divide in an era of contiguous threats.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD) Commission (WMD Commission 2005), which examined the US Intelligence Community's prewar assessment of WMD in Iraq addressed some of these design issues. Specifically, the commission identified the need for adopting an *Integrated Collection Enterprise* defined by the function and synergies created by target development, collection management, data management, strategic planning, and investment and for developing new collection techniques (WMD Commission 2005). It further states, "The goal of our recommendation is to create an integrated collection process that performs each of these functions from the perspective of the entire Intelligence Community, rather than individual agencies" (WMD Commission 2005, 357). In short, this would involve a collection enterprise bridging the domestic and foreign elements of the intelligence community.

The National Intelligence Collection Board (NICB), established in the early 1990s, had the mission of managing the US Intelligence Community's overall intelligence collection process while ensuring coordination among the various intelligence agencies. It was envisioned that the board would evaluate the performance of collection methods and ensure the integration of the various INTs (Director of Central Intelligence Directive [DCID] 1993). Intelligence Community Directive (ICD) 300, the *Management, Integration, and Oversight of Intelligence Collection and Covert Action* (2006), established under the newly formed DNI, created the Deputy Director of National Intelligence for Collection (DDNI/C) to oversee the NICB and various other community collection boards aligned to the various intelligence collection disciplines (ODNI 2006). These functions now fall under the Deputy Director of National Intelligence for Mission Integration (DDNI/MI).

The integrated community collection enterprise envisioned by the WMD Commission (2005) was critical of NICB and how individual collection agencies worked within their specific areas with little crosstalk of requirements to develop integrated collection strategies. In this case, the commission recommended the establishment of Target Development Boards to focus collection and develop strategies to address prioritized target sets. In terms of domestic intelligence, the commission also recognized the resistance to change within the Federal Bureau of Investigation (FBI) and the importance of integrating domestic intelligence into the overall efforts of the US Intelligence Community to meet modern-day challenges. During their investigation, they discovered little linkage between national-level and community intelligence collection requirements and intelligence activities being conducted in the field. As the report outlined, "at the working level, we found that national intelligence requirements were not uniformly understood" (WMD Commission 462). As such, one of the key commission recommendations, which was later adopted, called for the creation of the National Security Branch within the FBI with the authority to direct collection tasking to the FBI's domestic field offices and to serve as a conduit to coordinate on foreign intelligence collection. This new organization incorporated elements of the FBI's Counterterrorism and Counterintelligence Divisions along with elements of the Directorate of Intelligence.

With the post-9/11 debate concerning the reform of the US Intelligence Community and with the creation of the Department of Homeland Security (DHS) and the FBI's National Security Branch, there was also an extensive debate on whether the United States should adopt a solely dedicated domestic intelligence agency modeled along similar lines to many Allied countries. The purpose of such an agency was twofold: first, to solidify domestic intelligence processes and relationships with law enforcement and second, to serve as a conduit to leverage collection with foreign intelligence organizations. The Markle Foundation's (2002) *Protecting America's Freedom in the Information Age* narrowly focused on the domestic intelligence issues from the need to ensure the balance of protecting civil liberties while gaining efficiencies with intelligence collection through improved use of technology and management.[1] The Markle study recommended that DHS assume the lead in domestic intelligence activities, but without a law enforcement responsibility. This finding is consistent with the original vision of DHS, as outlined in the *Homeland Security Act of 2002*. While the study emphasized the role of technology to enable intelligence collection, it also outlined the serious blowback should these efforts suffer mismanagement and lack of oversight.

There were also two early Congressional Research Service (CRS) studies focusing on the creation of a domestic intelligence organization. The first study in 2003 was enacted to evaluate the issue as a result of pending US Senate legislation on establishing a Homeland Intelligence Agency within DHS (Masse 2003). The study specifically examined the United Kingdom's domestic intelligence organization, MI-5, and compared it to traditional US approaches. The study concluded that the differences in culture between the US and the United Kingdom, governance structures, and differences within their respective intelligence communities would limit the feasibility of creating such an organization in the United States. The second study enacted in 2005 evaluated the creation of an independent domestic intelligence organization while comparing the recommendations offered by the WMD Commission (2005) and its recommendation to establish the National Security Branch within the FBI (Cumming and Masse 2005). This study concluded that there were greater benefits to keeping the functions within one organization, where both mission areas could mutually support one another to create synergies between intelligence and law enforcement. In terms of recommendations, the CRS studies left the issue of integrating domestic and foreign intelligence collection undecided.

A series of RAND Corporation studies examined the issue of domestic intelligence. Like the CRS studies, the first, *Confronting the Enemy Within* (2004), examined the feasibility of a US domestic intelligence agency by evaluating the organizational approach of four countries: the United Kingdom, Australia, Canada, and France (Chalk and Rosenau 2004). The study was expansive in that it looked into the overall approach, institutions, history, and cultural differences between the United States and each of these countries. The study determined that domestic intelligence organizations without arrest powers tended to focus more narrowly on intelligence issues and that these organizations had a clearer interface with local communities. As the study further pointed out, these organizations had a longer history of recruiting and vetting sources and tailoring their approach to intelligence geared more toward human

[1] In addition to the foundation, the Task Force consisted of members from the Miller Center of Public Affairs, the Brookings Institution, and the Center for Strategic and International Studies.

networks, while aligning their intelligence activities more precisely to support law enforcement operations. There was an absence of discussion, however, on leveraging intelligence collection that bridged the domestic and foreign elements of these networks.

Another study in the series, The *State and Local Intelligence in the War on Terrorism* (2005), more narrowly focused on the topic of domestic intelligence within the framework of state and local efforts to meet the threat posed by terrorism after the 9/11 attacks (Riley 2005). This RAND study identified some of the shortfalls within state and local efforts in terms of training, capacity, and sustainability. It also identified the lack of a standardized approach across the state and local efforts in terms of dissemination, reporting, and use of technology to facilitate integration. The report did not, however, address broader intelligence collection concerns to bridge efforts across the foreign-domestic communities.

Another RAND study, *Reorganizing US Domestic Intelligence: Assessing the Options* (2008), was sponsored by DHS and was tasked to examine the issue of creating an independent domestic intelligence agency (Treverton 2008). This study did not recommend a specific course of action but evaluated the issue more within the challenges of conducting domestic intelligence activities within a US setting. It highlighted the importance of clarifying mission, roles, and responsibilities—particularly when facing a duality of mission sets such as found in the FBI with having to conduct both domestic intelligence and law enforcement. This finding is consistent with challenges identified by the WMD Commission. The study also found domestic intelligence fractures, where it was difficult to apply collection activities across the enterprise. This study also recognized the potential for recruiting from a more diverse skill set than individuals opting to enter more of a law enforcement-centric organization. There was no mention of bridging the concept of intelligence collection across the foreign-domestic divide.

The Challenge of Domestic Intelligence in a Free Society (2009) was another RAND study, which examined the evolution of domestic intelligence within a US historical context and the balance between ensuring national/homeland security and civil liberties (Jackson 2009). It also examined some of the costs associated with creating an independent agency. Similar to the other RAND studies, this volume did not recommend a specific course of action as to whether to create an independent agency. The final RAND study, *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom* (2009) was similar to the 2004 *Confronting the Enemy Within* study in that it focused on the benefits of an organizational design implementing a clarity of mission within a domestic intelligence agency (Jackson 2009). It also identified shortfalls in collaboration between the intelligence elements of these Allied organizations and their respective law enforcement organizations and outlined some of the challenges of these domestic intelligence organizations with having to coordinate with their foreign intelligence counterparts. The study did not go into detail, however, on the nuances of coordinating intelligence collection requirements across the foreign-domestic divide.

The literature reviewed outlines several key issues with the organizational designs of the US Intelligence Community. While the WMD Commission (2005) outlined the need to adopt a more integrated approach to collection that spans across the foreign and domestic communities of the enterprise, there has been little discussion on precisely how to bridge and optimize that gap. Several studies have examined the issue of domestic intelligence, but there is very limited insight into how to bridge intelligence collection across the community. The Markle Report (Markle Foundation 2002) identifies a key challenge; when addressing challenges facing the newly formed Department of Homeland Security, it stated:

> there is enormous resistance to giving the new department [DHS] the authority to receive intelligence in its "raw" form from other entities. But without these authorities the new directorate will be hampered significantly. An intelligence directorate with no collection powers of its own will not be able to set its own priorities or pursue avenues it considers important if it cannot influence directly the intelligence it receives. One of the Administration's first priorities once the Department of Homeland Security is established must be to coordinate a set of understandings among the relevant entities that will give the Department of Homeland Security real authority—without bureaucratic hurdles—to receive the information and analysis that it needs. (72)

This challenge of operationalizing and bridging intelligence collection across agencies and organizations remains a key bureaucratic challenge within the US Intelligence Community. It denies the ability to effectively employ a key and powerful intelligence activity to meet the nation's threats. As such, it makes the community ill postured to meet the complexities of the global operating environment and the dynamic spectrum of threats that it faces.

Research

An examination of current research on intelligence collection and its underlying processes yields a broad perspective on current trends. Many of these trends examine the complexity of applying intelligence collection techniques against dynamic and enterprising adversaries operating in complex operational environments. The focus of this research primarily stems from the US military's involvement in major combat zones, particularly in Afghanistan and Iraq. Much of the research deals with overcoming the planning process to enable intelligence and effectively orient it to modern-day issues. One study addressed the inherent rigidity in how the current intelligence collection management approach, while well suited for static environments, fails to adequately address focusing on agile adversary operations and dealing with what Hall and Citrenbaum call complex adaptive systems (Brown 2013). Another study accounts for how collection managers operating at local levels use gaming techniques to skew the intelligence collection requirements process to advocate for more collection assets as part of a zero-sum environment (Lamb 2014). Additional research examines the issue of planning by implementing automated decision support systems to optimize the development of intelligence collection requirements to ensure they are appropriately aligned to key intelligence issues (Tong 2010), while another study focuses on the need to reevaluate the concept of strategic warning (Kimmelman 2017). While much of this research is focused on developing collection strategies oriented toward tackling foreign intelligence issues, the need to ensure a suitable collection management process capable of dealing with complex operating environments is also appropriate for dealing with issues in the domestic environment.

Another line of research deals with the need for reevaluating collection more from a “bottom-up” versus a “top-down” process. Traditional intelligence collection systems, methodologies, and approaches are driven from the strategic level downwards. With the challenges of operating in hostile overseas environments, the US Army has recognized the need to establish organic collection assets and capabilities at the front-end of their ground units in order to operate in complex environments. The development of front-end tactical analysis and collection efforts within Brigade Combat Teams (BCTs) to categorize the complex operating environments is viewed as an essential element to support ongoing operations (McGarry 2011; Murrill 2003). Reconciling the need for developing local intelligence collection capacity and integrating it with national efforts is also a challenge within the domestic setting. The focus of another study recognized the challenges facing state and local fusion centers with integrating national-level and federal sources of intelligence (Gomez 2013). Additional research has also focused on reevaluating some of the technologies that are used to process and exploit intelligence collection. Due to the digitization of data and the subsequent information overload that has taxed intelligence collection systems, there is a significant amount of effort to optimize the front-end of collection to enable the classification and sifting of data to occur at a much quicker rate (Ellis 2013).

In summary, numerous studies have examined trends in intelligence collection issues. While much of the current research is focused on supporting US military operations overseas in combat zones, the ability of the US military to operate in these complex environments has been challenged. The collection management processes that have been employed to direct collection, pushing sophisticated intelligence collection capabilities to the lowest-level possible, and tailoring these capabilities to support local US military commanders are but a few of the many lines of research. It should be noted that effectively mapping complex networks at the local level, enabling intelligence collection, and managing collection are also relevant issues to the domestic intelligence environment. This is not to suggest that simply applying intelligence collection methods used overseas can be applied quickly in the domestic environment. It does, however, highlight many of the similar challenges that exist within the domestic intelligence enterprise.

Insights and Discussion

> The most difficult problem I have found with my clients, whether they are profit or nonprofit, is to change their mindset. It's not technology; it's not economic conditions. It is to change their mindset.
>
> —Peter Drucker (2010)

Integrated Collection Management seeks to leverage the power of intelligence collection to align a suitable array of capabilities against a prioritized set of targets. Just as important, the concept seeks to deconflict, match the "right" resources and capabilities at the "right" time, to achieve the unity of effort necessary to secure the homeland and protect US and Allied interests. In a dynamic operating environment categorized by complex adaptive systems, networks, and threats, the US Intelligence Community needs the capacity to quickly shift intelligence collection resources and capabilities to mitigate these threats. This requires not only a well-integrated set of collection strategies, but also the authorities and mechanisms capable of being implemented across an enterprise to realize these strategies. As evidenced by the literature, there is no clearly established mechanism or process within the community that leverages and aligns intelligence collection across the domestic and foreign components of intelligence. There is no operationalized intelligence collection function that serves to bridge the domestic-foreign gap.

There are clear sets of challenges that continue to face the US Intelligence Community despite the post-9/11 attempts at intelligence reform and reorganization. This article does not seek to enumerate them, but rather makes a case for operationalizing intelligence collection across the domestic and foreign elements of the community to achieve the integration necessary to operate within a complex operating environment. Intelligence collection, and more importantly the synergies and persistence that collection can bring to illuminate a target, is one of the more powerful US intelligence capabilities. For the US Intelligence Community to fully leverage collection capabilities, this means having to also operate across the domestic and foreign components of the community. Peter Drucker, noted management consultant and "change advocate," emphasized the need to change the mindset or approach when faced with difficult challenges (Drucker 2010). In other words, the US national security and intelligence communities—both their domestic and foreign components—need to reconceptualize and revamp from scratch the function of intelligence collection to ensure that it is optimized to meet the challenges of the complex operating environment while operating within a framework that protects civil liberties.

This leads to the question of "how?" How can the US Intelligence Community reconceptualize and revamp intelligence collection that bridges the domestic and foreign components of the community? Another noted leader and management consultant, Frances Hesselbein, offers an excellent framework for reevaluating and transforming organizational culture. As she states, "Culture does not change because we desire to change it. Culture changes when the organization is transformed; the culture reflects the realities of people working together every day" (Hesselbein 2012, 26). To transform an organization and reconceptualize its approach, she proposes a seven-faceted framework, which consists of:

- Environmental Scanning
- Determining Implications
- Revisiting Mission
- Banning the Old Hierarchy
- Challenging the Gospel
- Communicating to Mobilize and
- Dispersing Leadership. (Hesselbein 2012, 27–28)

In terms of *environmental scanning*, Hesselbein proposes the identification of two to three trends that will have the greatest future impact to the organization. Any organizational design should be suited and aligned to operate in its environment, and it is important to orient transformation initiatives to the identified trends that have the most significant impact. One of the key points emphasized by Professor Zegart in many of her works is that the US national security and intelligence "systems" are ill suited to meeting modern-day challenges (Zegart 1999). In this sense, Hesselbein's insight to revisit and reassess current and emergent environmental trends before creating the organizational solution is a valid one. Her second point, *determining implications,* emphasizes the environmental context up front as the first measure of analysis as opposed to going with a "what we know approach." In other words, it is necessary to frame and conceptualize the nature of a future approach free from its antecedents and on its own merits. A clear evaluation of current processes, an understanding of the trending issues, and their implications orient the nature of transformation.

Revisiting mission involves reevaluating the purpose of the endeavor. In this case, intelligence collection is recognized as a powerful capability—perhaps the ultimate high ground in the US Intelligence Community. Intelligence collection and the information and data that it generates are significant capabilities that can be leveraged to focus on the highest priority threats. Revisiting the underlying mission and purpose, however, of a new approach that bridges the domestic and foreign elements of the intelligence community is a fundamental and valid exercise, as intelligence collection introduces several contentious issues across the community and the public at large.

Hesselbein's concept of *banning the old hierarchy* is probably one of the more controversial aspects of her framework. People and organizations are vested in their processes and approaches. In other words, change is hard. One of the criticisms of the US Intelligence Community is its resistance to change. Hesselbein's framework of creating or transforming a new organization based on its merits is a novel approach and one that can represent a radical departure of the prevailing organizational norm. For example, the very nature of creating an element within the US Intelligence Community that manages and operationalizes intelligence collection across the domestic and foreign components of the community is a stark departure from the prevailing norm. From the perspective of the *ancien régime*, such an approach could infringe upon the accepted bureaucratic norms of how the community conducts its "business."

Challenging the gospel is by its definition a difficult proposition. It is a challenge to orthodoxy. In terms of intelligence collection, it challenges the very notion of distinct intelligence collection disciplines: HUMINT to OSINT operating within its own distinctive stovepipe. It also crosses the several organizational boundaries that closely guard the sources and methods of intelligence collection. Integrating intelligence collection vertically and horizontally across the enterprise and developing mechanisms to operationalize CRM and COM functions is a daunting task. The scale and scope of the endeavor is not sufficient cause, however, for not pursuing a key functional gap in the community.

Communicating to mobilize is fundamental to any transformation effort. Change causes disruption to prevailing norms and the intent and necessity for change can be lost during a reform effort if not communicated effectively. Mobilizing the workforce and disseminating a compelling narrative for why change is necessary is a complex task that seeks to change perspective and behaviors. Hesselbein emphasizes selectively focusing and sustaining messaging efforts on *mission*, *goals*, and *values,* while actively engaging internal and external stakeholders to create dialogue and collaboration as opposed to merely disseminating communications in a piecemeal and one-way fashion.

Dispersing Leadership across the enterprise is the last attribute in Hesselbein's framework, which involves the devolution of leadership to the appropriate level. In other words, while there is still a need for strategic-level leadership at the apex of intelligence collection efforts, the devolution of leadership and developing leaders with the appropriate skills and authorities to manage collection is necessary. Overly centralized and rigid organizational structures face significant challenges when attempting to operate in a dynamic operating environment. Creating a shared leadership concept across an enterprise allows for greater agility to meet present-day challenges.

Operationalizing Intelligence Collection: A Conceptual Way Forward

Aligning an *Integrated Collection Management* system to meet modern and dynamic threats will require a novel approach. The conceptual framework for this article posits that intelligence collection—a key intelligence enabler and US capability—should be operationalized across the domestic and foreign elements of the US Intelligence Community. While intelligence collection requirements are coordinated and evaluated within the community through the NICB and other community bodies, a strategic-level coordination process that supports high-level CRM efforts is not postured to meet the complexities of the modern-day environment. This was one of the key findings from the IC21 study, which states, "it is not yet the body to compel the needed integration of the collection process within the community" (US House of Representatives 1996,70). The current literature shows little evidence to suggest that integrating collection across the community and in a dynamic fashion has been realized.

Key Assumptions

Hesselbein's transformation and change framework is a useful tool to conceptualize a way forward to tackle the issue of bridging the domestic and foreign elements of the US Intelligence Community in terms of intelligence collection. Additionally, the term "operationalizing" intelligence collection is based on several assumptions that frame the need for moving forward. These key assumptions are:

- The global security environment will continue to evolve in an adaptive, complex, and transnational fashion, categorized by a spectrum of threats ranging from near-peer competitor nation-states to non-state and topical threats, such as terrorism, crime, and cyber.

- The implications of time and distance will continue to diminish as a result of increased globalization, integration of world markets, and enhanced communications.

- Intelligence collection efforts are not effectively bridging the domestic and foreign elements of the US Intelligence Community where it can align collection capabilities in a dynamic and transparent fashion.

- Synchronization of intelligence collection across the domestic and foreign elements of the community and within individual collection stovepipes are not being optimized where they can be applied to the highest priority targets in an agile manner.

- The processing and exploitation of the "collection-take" is neither aligned nor transparent in how these processes are supporting higher-level requirements and intelligence problem sets.

- The dissemination and follow-on evaluation as the result of intelligence collection and analysis is not clearly understood by the broad set of customers that rely on the US Intelligence Community to support their needs.

- A holistic and *Integrated Collection Management* approach that spans both the domestic and foreign intelligence environment will fully leverage a core US intelligence capability and better posture the community to provide strategic warning on the full continuum of conflict to include measures falling short of conflict lying in the "gray zone." (Hoffman 2018, 34–36)

The first two assumptions deal with the complexities of the global operating environment and the diversification and implications of the threat. Threats in the modern age are contiguous and have implications that span national borders. Additionally, despite anti-globalization efforts, the overall trend in human advancement will continue to lie in the integration of systems, markets, and issues. The next two assumptions deal with Clark's "front-end" categorization of collection. There is no organizational element within the community that focuses purposefully on operationalizing intelligence collection across the domestic and foreign elements of the US Intelligence Community from a holistic perspective. Additionally, the synchronization of intelligence collection across its domestic and foreign elements while horizontally integrating across the individual intelligence collection stovepipes is not part of a well concerted intelligence collection strategy. The following two assumptions address "back-end" collection issues in terms of aligning the TCPED architecture to maximize and leverage resources while aligning efforts to meet customer needs. Additionally, the dissemination architecture is not conducive to the customer to provide contextual and tailored feedback to the intelligence collector. The last assumption describes the complexity and challenge of intelligence in having to operate in an uncertain and changing environment, where many issues fall short of classic force-on-force confrontations. The US Intelligence Community will remain challenged with providing the key and critical insights to support warning analysis. Intelligence collection is the *sine qua non* of warning analysis. Maximizing the ability of intelligence collection efforts across the full expenses of the community and with all its capabilities will fulfill a critical role in better dealing with uncertainty and provide warning to existing and emergent threats.

A Way Forward

Environmental Scanning and Determining Implications

Utilizing Hesselbien's transformational network and applying it to develop a conceptual way forward can offer some insights into the issues that a proposed operationalization of intelligence collection will have to consider. There are many issues that frame modern-day intelligence collection; it is recognized in the literature that intelligence collection functions within a complex environment. For fully leveraging intelligence collection that spans across the domestic and foreign intelligence components of the comment, Hall and Citrenbaum (2012, 1) state: "We find ourselves in a knowledge war. This notion of knowledge war finds us wandering in a dense forest and coming to a precipice. The precipice allows us to peer into the dark abyss, which is the future." They continue to state that we have three options: *purposeful stasis*, which acknowledges the issue, but accepts risk and avoids measures to resolve it; the appearance of action, which feigns reform; and lastly, to *fly* above the forest by taking a fresh approach, where all issues are subject for consideration. As Hall and Citrenbaum (2012, 2) suggest, "It is nonlinearity that defines the character of many of our challenges." It is precisely this complex and nonlinear environment that compels a reevaluation of how the community manages intelligence collection to align it against the greatest and highest priority threats. A key issue in this case is the need for transforming intelligence collection.

The need for transforming intelligence collection to operate within a complex operating environment compels the US Intelligence Community to acknowledge a significant issue that has plagued the community for many decades, but which remains unresolved. The issue of information overload was foreseen in the late 1960s and early 1970s. This was a key finding of the Schlesinger Report (Review of the Intelligence Community 1971), which examined the significant rise in collection coupled with the minimal improvement in intelligence products and assessments. With the advent of digitization and the World Wide Web, this issue has grown exponentially and beyond the ability of the community to effectively manage. As Young (2013, 24) points out, "The US intelligence community is currently inundated with information. This poses a serious challenge to effective intelligence work. Overwhelmed by data, analysts lose the ability to pick out what is important and fail to make good judgments." In terms of intelligence collection, the ability of the "system" to process and exploit the information and data to form a coherent understanding of the "collection-take" is equally daunting. Information overload, coupled with a poor organizational design that focuses collection within individual stovepipes, makes it difficult, if not impossible, to make sense of the intake of collection when facing complex and nonlinear threats. Managing and addressing information overload will continue to impact the community for many decades to come.

Lastly, as alluded to above and emphasized by Clark (2014), the US Intelligence Community needs to address the intelligence collection function in terms of the barriers that prevent the integration of collection along vertical and horizontal organizational lines. As Clark (2014, 468) states, "We would like to achieve synergy in collection, which means real-time cross-INT collaboration among all collection groups. But the boundaries, or stovepipes, make it harder to allocate requirements to the assets and to collaborate in collection to achieve synergy." Without first addressing the barriers, stovepipes, and sharing processes that can enable collection managers to effectively fulfill their CRM/COM functions, any future intelligence collection transformation efforts will result in negligible improvement. In this case, vertical and horizontal integration must be the community's end state.

To summarize, we need to ask the question "Is there a need to transform the intelligence collection function?" While the answer may be self-evident, it will require an approach that takes a radically new approach to the issue. Creating a capacity that operationalizes and leverages intelligence collection across the domestic and foreign elements of the community is that new approach. Any future efforts aimed at fully leveraging intelligence collection, however, will have to deal with the realities and challenges faced by information overload and the need to effectively address the barriers to horizontal and vertical integration of intelligence functions within the US Intelligence Community.

Revisiting Mission

While the US Intelligence Community receives much of the blame when things go wrong and little credit when supporting a successful policy outcome, it is worth remembering a key and fundamental purpose for the community. As Cynthia Garbo (2004, 34), noted theorist on warning analysis, stated, "the Intelligence Community is expected to make daily judgments about the current situation, such as the state of military preparedness or combat readiness, in a variety of countries which habitually conceal or attempt to conceal nearly all the strategic information." In the present, the US Intelligence Community is charged with assessing issues beyond the narrow confines of politico-military analysis and intentions. Global threats have evolved within an increasingly complex operating environment. These threats also have domestic and foreign components that relate to each other in nonlinear ways and that exist in gray zones and emergent environments. As Hall and Citrenbaum (2012, 3) postulate in coining their term for *Advanced Collection*, it is "the creative design and use of technical, cyber, human, and open-source collectors in all domains—air, ground, sea, space, information, and cyber—in pursuit of discrete, subtle, nuanced, and often fleeting observables, indicators, and signatures." They further assert that the notion of advanced collection seeks to address the *why* for intelligence collection, *where* the collection is occurring, *when* the community is collecting, *what* is being sought, the *contextual basis* for the collection in terms of its background and justification, the *criteria for success*, and defining the *relationship* or linkage to decision-making and policy objectives. In terms of ***revisiting mission***, this paper offers an added requirement—the need to bridge the domestic and foreign elements of the community to operationalize intelligence collection.

Banning the Old Hierarchy & Challenging the Gospel

As stated earlier, operationalizing intelligence collection across the domestic and foreign elements of the community is a stark departure from the prevailing norm. In many respects, it is a threat to how the community conducts its business. That said, however, national and homeland security, law enforcement, and intelligence and military communities have and continue to evolve in the post-9/11 environment—a term that is increasingly anachronistic itself. After 9/11, the proliferation of state and local fusion centers, for example, was viewed with suspicion by the Intelligence Community. These centers have evolved beyond the narrow confines of focusing on terrorism to support a broader range of issues. Additionally, as the result of combat experience in Iraq, Afghanistan, and other areas across the globe, the integration of intelligence capabilities directly supporting the warfighter has enabled the ability of precision strike and tailored intelligence to quickly attain combat objectives. US involvement in these post-9/11 conflicts has resulted in the employment of intelligence capabilities never before envisioned. In other words, these evolutionary developments did not result in *banning the old hierarchy*, but rather orienting the community to meet the present-day complexities of the operating environment.

Challenging the Gospel follows closely with reassessing established hierarchies. This is where developing novel approaches to dealing with the two key implications, information overload and vertical and horizontal integration, will challenge the established norms. Adopting integrative technological architectures that span organizational boundaries, linking underlying processing and exploitation architectures to enable cross-INT fusion and management of intelligence collection or establishing integrated CRM/COM processes that also span organizations and stovepipes will fall within the "too hard to do" or *purposeful stasis* approach as described by Hall and Citrenbaum. While outside the scope of this conceptual paper, it will also require a reevaluation of the legal frameworks to enable operationalized sharing across the domestic and foreign elements of the community.

The underlying justification and premise of this discussion, however, is that intelligence collection—a key US Intelligence Community capability and strength—is not fully leveraged and operationalized to meet the complexities of the modern-day operating environment and global threats. As such, it is necessary to elevate these critical issues, whether addressing information overload or integration efforts, to ensure that intelligence collection is fully leveraged. Instead of referring to the post-9/11 environment and using a current event, such as the COVID-19 pandemic, intelligence professionals and policymakers should ask: how could an *Integrated Collection Management* approach that spans the domestic and foreign elements of the community have better postured the United States to meet the COVID-19 threat? Could strategic warning and analysis have been enhanced? Would the US Intelligence Community be better aligned to support ongoing public health and recovery efforts? In the present age framed by complexity and non-linearity, the ability of the US Intelligence Community to operate and provide support to a wide variety of customers—including public health—will require extensive horizontal integration across communities and networks where communities of collection managers and intelligence analysts can collaborate to assess indicators in a seemingly nonlinear problem set. As envisioned by Dunn Cavelty and Mauer (2009, 139), "this means that horizontal knowledge networks need to be embraced, even at the expense of vertical integration."

Communicating to Mobilize

Transformational efforts are also contingent on mobilizing the workforce and engaging with key stakeholders. When viewed another way, sustainable transformation is also contingent upon change to organizational culture. In terms of its people, the *National Intelligence Strategy* (US Government 2019, 20) addresses the need for an inclusive culture that "connects each employee to the organization; encourages collaboration, flexibility, and fairness; and leverages diversity throughout the organization so that all individuals are able to participate and contribute to their full potential." While there is considerable professional debate among management theorists on the relationship between an inclusive organizational culture and organizational effectiveness, the need for partnering and working collaboratively outside traditional intelligence confines is extremely relevant to operating in a dynamic environment. Mobilizing support across a broad set of organizations and stakeholders will be contingent on the receptivity of such a message.

Perhaps more important than mobilizing is the need to sustain change initiatives over time. While many post-9/11 intelligence reformists decried the need for change by focusing on creating new organizations and systems, the focus of mobilization and sustaining change is truly on the intelligence professionals within the community. For example, the aftermath of the 9/11 attacks resulted in significant impetus to create the DHS and the DNI. While the efficacy of these organizations is beyond the scope of this paper and the creation of new organizational elements can serve to enact change, it is perhaps more important to recognize that transforming and professionalizing the workforce results in sustainable change. As one group of management theorists state,

> Most leaders get it wrong. They think that organizational productivity and performance are simply about policies, processes, structures, or systems .... So when their software product doesn't ship on time, they benchmark others' development *processes*. Or when productivity flags, they tweak their performance management *system*. When teams aren't cooperating they *restructure* ... these types of nonhuman changes fail more often than they succeed. That's because the real problem never was in the process, system, or structure—it was in employee *behavior*. (Patterson et al. 2012, 13)

Much of the literature focusing on the successful employment of special operations overseas engaged in complex operating environments affirms this focus. Schultz identifies six critical factors for transforming intelligence within an interagency environment. A clearly defined mission, single organizational leads, and leadership are three factors critical to success. Of equal importance, however, are the necessity to build collaborative partnerships through the establishment of trust, imbuing a cohesive and transparent culture, and creating an organization that learns and adapts (Schultz 2020). To operate in the modern-day environment, intelligence professionals will have to adopt such an approach to mobilize and sustain change over time.

Dispersing Leadership

Hesselbeim's concept of dispersing leadership calls for a leadership approach that can adapt and evolve to meet the change and challenges that typify the operating environment. It requires that leadership and the workforce are comfortable operating in a complex and nonlinear environment. Operationalizing intelligence collection across the domestic and foreign elements of the intelligence enterprise will require leadership at all levels. It will also require a counterintuitive approach that has been prevalent in the US Intelligence Community, which has focused on overly centralized and rigid management structures and processes. As Schultz (2020, 183) further emphasizes, leaders "are successful not because they are forceful, decisive, or charismatic. Rather it is because they build team systems that achieve successful outcomes by decentralizing authority and by empowering those closest to the fight." As intelligence collection activities and functions will reside at varying levels and organizations within the enterprise, a dispersed leadership framework that is supported by clear standard operating procedures, processes, and technology will enable the intelligence community to leverage collection across a broad set of stakeholders.

Conclusion

The issue of national and homeland security, intelligence, and law enforcement all function to mitigate threats against the homeland. The "threat" however has evolved significantly since the 9/11 attacks to where the US Intelligence Community is charged with assessing a spectrum of existing and emergent threats. Additionally, these threats are dynamic and shifting and can manifest themselves quickly. The community possesses significant intelligence collection capabilities that can be used to gain insight into the nature of these threats. As currently postured, however, intelligence collection is still largely confined to its stovepipes. More importantly, this paper postulates that a true *Integrated Collection Management* approach is not being optimized for because of the nature of these stovepipes and because a key gap exists between bridging the domestic and foreign elements of the intelligence community.

Operationalizing intelligence collection that bridges the domestic and foreign divide is necessary to meet an adaptive and complex operating and threat environment. In terms of environmental scanning, the key issues that will face a new intelligence collection enterprise are information overload and horizontal integration to create synergies between the various collection INT-stovepipes and organizations. While these two issues might be the most intractable facing intelligence collection, they are not the only ones. The paper has not explored the many other issues, such as intelligence oversight, legal reforms, technologies, and processes, that would be necessary to develop an integrated approach to intelligence collection. This paper has also not recommended the form of an organizational bridging function. These are areas for further research, with the priority being to address the key question: "In what form will this organizational element look like and precisely what authorities will be commensurate with such organization?" Without first addressing the conceptual approach, "reform" will just add another organization to an already bureaucratized community. The key take-away, however, is whether such a conceptual approach for operationally bridging intelligence collection across its domestic and foreign intelligence characteristics is a valid one. In an age of complexity where issues and threats manifest themselves quickly, this issue should be explored further.

References

Addicott, Jeffrey F., and Michael T. McCaul. 2008. "The Protect America Act of 2007: A Framework for Improving Intelligence Collection in the War on Terror." *Texas Review of Law & Politics; Austin* 13 (1): 43–71.

Bean, Hamilton. 2009. "Organizational Culture and US Intelligence Affairs." *Intelligence & National Security* 24 (4): 479–98.

Bellaby, Ross. 2012. "What's the Harm? The Ethics of Intelligence Collection." *Intelligence & National Security* 27 (1): 93–117.

Berman, Emily. 2014. "Regulating Domestic Intelligence Collection." *Washington and Lee Law Review; Lexington* 71 (1): 3–91.

Canaday, Johanna. 2017. "How the Democratization of Technology Enhances Intelligence-Led Policing and Serves the Community." Master's Thesis, Naval Postgraduate School.

Castagna, Michael J. 2004. "A Decision-Support Tool for Collection Management." *Marine Corps Gazette; Quantico* 88 (9): 67–71.

Chalk, Peter, and William Rosenau. 2004. *Confronting "the Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*. Santa Monica, CA: RAND Corporation.

Chalk, Peter, Richard Warnes, Lindsay Clutterbuck, and Aidan Kirby. 2009. *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*. Edited by Brian A. Jackson. Santa Monica, CA: RAND Corporation.

Clark, Robert M. 2014. *Intelligence Collection*. Thousand Oaks, CA: CQ Press.

Covey, Travis J. 2015. "Defense Support of Civil Authorities: A Primer on Intelligence Collection During Civil Disturbance and Disaster Relief Operations." *The Army Lawyer; Charlottesville*, 25–38.

Cumming, Alfred, and Todd Masse. 2005. *Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress*. Washington DC: Congressional Research Service.

Dillon, Robin L., Genevieve Lester, Richard S. John, and Catherine H. Tinsley. 2012. "Differentiating Conflicts in Beliefs versus Value Tradeoffs in the Domestic Intelligence Policy Debate." *Risk Analysis: An International Journal* 32 (4): 713–28.

Director of Central Intelligence Directive. 1993. *National Intelligence Collection Board*. Washington DC: Government Printing Office.

Drucker, Peter F. 2010. *The Drucker Lectures: Essential Lessons on Management, Society, and Economy*. New York, NY: McGraw-Hill.

Dunn Cavelty, Myriam, and Victor Mauer. 2009. "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence." *Security Dialogue* 40 (2): 123–44.

Edgar, Timothy H. 2017. *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, DC: Brookings Institution Press.

Ellis, Duncan R. 2013. "Algorithms for Efficient Intelligence." Master's Thesis, Naval Postgraduate School.

Galliott, Jai, and Warren Reed. 2016. *Ethics and the Future of Spying: Technology, National Security and Intelligence Collection*. London, UK: Taylor & Francis Group.

Gomez, David C. 2013. "Should Cops be Spies? Evaluating the Collection and

Sharing of National Security Intelligence by State, Local, and Tribal Law Enforcement." Master's Thesis, Naval Postgraduate School.

Grabo, Cynthia M. 2004. *Anticipating Surprise: Analysis for Strategic Warning*. Lantham, MD: University Press of America.

Hall, Wayne Michael, and Gary Citrenbaum. 2012. *Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments*. Santa Barbara, CA: Praeger.

Hesselbein, Frances, and James M. Kouzes. 2012. *More Hesselbein on Leadership*. New York: John Wiley & Sons, Incorporated.

Hoffman, Frank G. 2018. "Examining Complex Forms of Conflict." *PRISM* 7 (4): 30–47.

Jackson, Brian A. 2014. *How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts*. Santa Monica, CA: RAND Corporation.

Jackson, Brian A., Agnes Gereben Schaefer, Darcy Noricks, Benjamin W. Goldsmith, Genevieve Lester, Jeremiah Goulka, Michael A. Wermuth, Martin C. Libicki, and David R. Howell. 2009. *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a US Domestic Counterterrorism Intelligence Agency*. Santa Monica, CA: RAND Corporation.

Jenkins, Brian Michael, Andrew Liepman, and Henry H. Willis. 2014. *Identifying Enemies Among Us: Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing*. Santa Monica, CA: RAND Corporation.

Johnson, Loch K. 2006. *Handbook of Intelligence Studies*. London, UK: Taylor & Francis Group.

Kimmelman, Susann. 2017. "Indications and Warning Methodology for Strategic Intelligence." Master's Thesis, Naval Postgraduate School.

Lamb, Jason B. 2014. "Gaming the System: A Game Theory Analysis of Theater Airborne ISR." Research Report, Air War College.

Litt, Robert S. 2013. *Privacy, Technology and National Security: An Overview of Intelligence Collection*. Brookings Institution.

Lowenthal, Mark M., and Robert M. Clark. 2015. *The Five Disciplines of Intelligence Collection*. Thousand Oaks, CA: CQ Press.

Markle Foundation. 2002. *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*. New York.

McGarry, Christopher C.E. 2011. "Inverting the Army Intelligence Pyramid." Monograph, School of Advanced Military Studies.

Masse, Todd. 2003. *Domestic Intelligence in the United Kingdom: Applicability Of The MI-5 Model To The United States*. Washington DC: Congressional Research Service.

Moses, Bruce D. 2004. "Intelligence Collection: Supporting Full Spectrum Dominance and Network Centric Warfare?" Monograph, School of Advanced Military Studies.

Murrill, Terrence L. 2003. "Projecting Organic Intelligence, Surveillance, and Reconnaissance: A Critical Requirement of the Stryker Brigade Combat Team." Monograph, Command Staff College.

National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York, NY: W.W. Norton & Company.

Office of the Director of National Intelligence. 2011. *Intelligence Community (IC) Consumers Guide*. Washington DC: Government Printing Office.

———. 2013. *Domestic Approach to National Intelligence*. Washington DC: Government Printing Office.

Patterson, Kerry, Joseph Grenny, Ron McMillan, and Al Switzler. 2012. *Crucial Conversations: Tools for Talking When Stakes are High*. 2nd Edition. New York: McGraw Hill.

Posner, Richard A. 2010. *Remaking Domestic Intelligence*. Stanford, CA: Hoover Institution Press.

Pulver, Aaron and Richard M. Medina. 2018. "A Review of Security and Privacy Concerns in Digital Intelligence Collection." *Intelligence and National Security* 33 92): 241–56.

Regens, James L., Nick Mould, Carl J. Jensen, David N. Edger, David Cid, and Melissa Graves. 2017. "Effect of Intelligence Collection Training on Suspicious Activity Recognition by Front Line Police Officers." *Security Journal; London* 30 (3): 951–62.

Richelson, Jeffrey T. 2015. *The US Intelligence Community*. New York: Taylor & Francis Group.

Riley, Kevin Jack. 2005. *State and Local Intelligence in the War on Terrorism*. Santa Monica, CA: RAND Corporation.

Schultz, Richard. 2020. *Transforming US Intelligence for Irregular War: Task Force 714 in Iraq*. Washington, DC: Georgetown University Press.

Schwerzler, Martin. 2008. "Collection Management in the COIN: A 3rd Infantry Division Perspective." *Military Intelligence Professional Bulletin; Ft. Huachuca* 34 (3): 25–27.

Sterioti, Anthony J. 2015. "Information Collection Management in the BCT." *Military Intelligence Professional Bulletin* 41 (4): 46–48.

Tangeman, Darrin K. 2014. "Intelligence Collection, Targeting and Interdiction of Dark Networks." Master's Thesis, Naval Postgraduate School.

Tekin, Muhammet. 2016. "New Perspectives on Intelligence Collection and Processing." Master's Thesis, Naval Postgraduate School.

Tong, Khiem Duy. 2011. "Framework for Optimizing Intelligence Collection Requirements." Master's Thesis, Rochester Institute of Technology.

Treverton, Gregory F. 2008. *Reorganizing US Domestic Intelligence: Assessing the Options*. Santa Monica, CA: RAND Corporation.

Tromblay, Darren E. 2018. "Intelligence Collection versus Investigation: How the Ethos of Law Enforcement Impedes Development of a US Informational Advantage." *Intelligence and National Security* 33 (7): 1070–83.

———. 2015. *The US Domestic Intelligence Enterprise: History, Development, and Operations*. Boca Raton, FL: CRC Press.

US Government. 2004. *National Commission on Terrorist Attacks Upon the United States* (the 9/11 Commission). Washington DC: Government Printing Office, 2004.

———. 2005. *The Commission on the Intelligence Capabilities of the United States*

Regarding Weapons of Mass Destruction (The WMD Commission Report). Washington DC: Government Printing Office.

———. 2019. *National Intelligence Strategy of the United States of America*. Washington DC: Government Printing Office, 2019.

US House of Representatives. 1996. *IC21: The Intelligence Community in the 21st Century*. 104th Cong., 2d sess., H. Rep 23-708.

US Senate. 2002. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*. 107th Cong., 2d sess., S. Rep. 107- 351.

Walsh, Patrick F., and Seumas Miller. 2016. "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden." *Intelligence & National Security* 31 (3): 345–68.

Weinbaum, Cortney, John Parachini, Richard Girven, Michael Decker, and Richard Baffa. 2018. *Perspectives and Opportunities in Intelligence for US Leaders*. Santa Monica, CA: RAND Corporation.

Whaley, Kevin J. 2005. "A Knowledge Matrix Modeling of the Intelligence Cycle." Master's Thesis, Air Force Institute of Technology.

Wippl, Joseph W., and Donna D'Andrea. 2014. "The Qualities That Make a Great Collection Management Officer." *International Journal of Intelligence and Counter-Intelligence* 27 (4): 806–14.

Young, Alex. 2013. "Too Much Information Ineffective Intelligence Collection." *Harvard International Review; Cambridge* 35 (1): 24–27.

Zegart, Amy B. 1999. *Flawed by Design: The Evolution of the CIA, JCS, and NSC*. Stanford, CA: Stanford University Press.