EXPECTATIONS OF INTELLIGENCE IN THE INFORMATION AGE

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

REBALANCE TASK FORCE

OCTOBER 2012

ACKNOWLEDGEMENTS

INSA REBALANCE TASK FORCE

Dr. Stephen Cambone, *Task Force Chair*

Randall Fort, *Raytheon*

General (ret.) Michael Hayden, *The Chertoff Group*

John Jolly, *General Dynamics Advanced Information Systems*

Carmen Medina, *Deloitte*

Philip Mudd, *New America Foundation*

Craig Parisot, *Invertix*

EDITORIAL REVIEW

Joe Mazzafro, *CSC*

COPY EDITOR

Elizabeth Finan

The Task Force wishes to acknowledge the advice it received from a number of current and former intelligence and national security officials as well as members of INSA who enriched the paper through their contributions during Task Force meetings and interviews.

Participation on the Task Force does not imply personal or official endorsement of the views in the paper by any participating member or his/her respective parent organization(s).

INSA CHAIRWOMAN

Frances Fragos Townsend

INSA SENIOR INTELLIGENCE ADVISOR

Charlie Allen

INSA STAFF

Chuck Alsup, *INSA Acting President and Vice President of Policy*

Jeff Lavine, *INSA Director of Administration & Management*

Ted Brisbin, *INSA Fellow*

Jay Fox, *INSA Fellow*

Philip Walker, *INSA Intern*

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.

As we consider the relatively narrow question of the Asia pivot, a broader knowledge revolution is underway, challenging security services to redefine the role of intelligence in the 21st century. Is it secrets, or is it knowledge? Today, the United States Intelligence Community (IC) still lives largely in the world of secrets defining intelligence; tomorrow, it will either embrace a new understanding of intelligence and knowledge or risk marginalizing analysts from this century's knowledge revolution and hence fail to serve policy makers as well as possible.

LEAD OBSERVATIONS

1. The heightened expectations of decision makers for timely strategic warning and current intelligence can be addressed in significant ways by the IC through "open sourcing" of information.
2. "Open sourcing" will not replace traditional intelligence; decision makers will continue to expect the IC to extract those secrets others are determined to keep from the United States.
3. However, because decision makers will access open sources as readily as the IC, they will expect the IC to rapidly validate open source information and quickly meld it with that derived from espionage and traditional sources of collection to provide them with the knowledge desired to confidently address national security issues and events.

I. INTRODUCTION: A PERSPECTIVE ON THE STRATEGIC PIVOT

In January 2012, President Obama went to the Pentagon to announce a change in U.S. military strategy and, by implication, the nation's broader national security strategy:

"…As we end today's wars, we will focus on a broader range of challenges and opportunities, including the security and prosperity of the Asia Pacific."

What has come to be called a "strategic pivot" marks a significant adjustment in U.S. military and national security strategy. When the last U.S. combat forces are withdrawn from Afghanistan, nearly 14 years will have passed since September 11, 2001. During this time, the weight of U.S. national security efforts has been focused on combat operations in Iraq and Afghanistan, counterinsurgency operations in those and other theaters, and a worldwide campaign against terrorists who threaten the United States. These efforts not only draw very heavily on the nation's military forces, but on its diplomatic and intelligence resources as well.

> The call for a pivot is not an occasion to substitute one highly specific and geographically constrained theater for another. Rather, it presents an opportunity for the national security community to broaden its perspectives and approaches regarding U.S. national security in the coming decades.

With the death of Osama bin Laden and the anticipated end of conventional combat operations in Iraq and Afghanistan, the President signaled that it was not only possible, but essential, for the United States to broaden its national security strategy to take account of the remarkable changes in the international system that have become apparent since the turn of the century. Most commentary has focused on the "rise of China" as the motivating force behind the "pivot."

That said, the members of this task force are of the view that the call for a pivot is not an occasion to substitute one highly specific and geographically constrained theater (Middle East/Southwest Asia) for another (East Asia). Rather, it presents an opportunity for the national security community to step back from its intense focus on combating terrorism and conducting combat operations in Southwest Asia and the Middle East and to broaden its perspectives and approaches regarding U.S. national security in the coming decades.

The President's statement supports this conclusion. He and Cabinet officials have been careful to say that the United States would focus on a "broader range" of issues "including, but not limited to," those related to the Asia-Pacific region.

Secretary of State Clinton, in an article published in *Foreign Policy* magazine, defined the Asia-Pacific region as stretching from "… the Indian subcontinent to the western shores of the Americas, [a] region [that] spans two oceans…" This definition encompasses more than China and includes a broad swath of issues critical to the national security interests of the United States.

Secretary of Defense Panetta reinforced the notion that the security agenda of the United States is expanding to include increased focus on the Asia-Pacific, not narrowing to concentrate primarily on that region. In commenting on the defense guidance to support the strategy adjustment, he said:

"…[The joint force] will have a global presence emphasizing the Asia-Pacific and the Middle East while ensuring our ability to maintain our defense commitments to Europe, and strengthening alliances and partnerships across all regions. It will preserve our ability to conduct the missions we judge most important to protecting core national interests: defeating al Qa'ida and its affiliates and succeeding in current conflicts; deterring and defeating aggression by adversaries, including those seeking to deny our power projection; countering weapons of mass destruction; effectively operating in cyberspace, space and across all domains; maintaining a safe and effective nuclear deterrent; and protecting the homeland. The Joint Force will be prepared to confront and defeat aggression anywhere in the world."

This adjustment or rebalancing of the nation's security and defense strategies give rise to a seminal question of interest to users and providers of the nation's intelligence: in a "post-pivot" environment, what will the policy-making community expect of the IC in support of national security decision making? That, in turn, raises the question: how will the IC go about meeting, and managing, those expectations?

In a "post-pivot" environment, what will the policy making community expect of the IC in support of national security decision making? That, in turn, raises the question: how will the IC go about meeting, and managing, those expectations?

EXPECTATIONS

The policy-making community will continue to expect timely, relevant IC assessments related to the capabilities and intentions of entities of interest around the world. IC assessments will continue to address known or anticipated threats and challenges by state or non-state actors, related principally to their development, deployment, or employment of force to achieve objectives inimical to U.S. interests; these may be realized through military action or asymmetrical threats, but also through diplomatic, economic, or political initiatives. These assessments are essential to inform U.S. decision making on what some might call the "hard" elements of power—e.g., military forces, international diplomatic initiatives, or economic policies pursued primarily in state-to-state relations or in recognized international forums.

Increasingly, however, policy makers are likely to demand more timely reports with knowledgeable insight into the trends that drive groups of individuals to form ad hoc or organized networks attempting to undertake activities that may be outside the immediate control of governments and that may pursue objectives at odds with, or in opposition to, official government policy. This phenomenon has manifested itself repeatedly in recent years to include the "color" revolutions in post-Soviet countries, the Arab Spring, the civil war in Syria, and most recently in the attacks on U.S. diplomatic facilities in Libya, Egypt, and elsewhere. These social- or people-generated events have had, and will continue to have, direct effects on U.S. national security interests.

To fully serve policy makers, the IC will need to continue to expand—to a much greater degree than has been assumed or accomplished to date—its reliance on open sources of information that contain or reflect the sentiments, intentions, and actions of non-governmental actors; what might be called "social intelligence."

Policy makers will demand that these less traditional assessments provide "indications and warning (I&W)" or strategic warning of impending events. This warning is essential to provide policy makers time to develop, deploy, and employ what some call "whole of government" or "smart power" initiatives—e.g., public diplomacy, economic development, global trade, and alliance and institution building—to address the underlying issues and the resulting national security events that have become increasingly frequent drivers of U.S. security decision making.

The range of underlying issues is broad. Among others, they include, often in combination:

- The advent of political movements, fueled by modern telecommunications and social media, in opposition to weak, corrupt, or authoritarian government;
- The destabilizing effects of emigration, immigration, and massive demographic shifts;
- The corrupting influence of interlocking or overlapping networks engaged in illicit activities related to financial fraud and money laundering;
- The smuggling or marketing of weapons, drugs, commodities, and people;
- The exploitation of vulnerabilities within the global communications network to undermine the security of governments, private sector entities, and individuals who are increasingly dependent on that network;
- Localized but widespread shortages of food, water, and preventative medicines;
- The effects of disruptive secular, ethnic, and sectarian strife;
- Unrest leading to conflicts fueled by political repression, economic depression, or the failure of governments to meet the essential needs of the population.

In the face of these underlying issues, the preference of policy makers is to avoid having to react to events and manage crises once they emerge through the employment of "hard power," thereby running the risk that a local crisis might escalate. Rather, by employing "smart power," the policy maker can attempt to shape events in such a way that avoids crises and creates more stable conditions at local, state, regional, and international levels.

It is a fair assumption that many of the crises driven by the issues sketched above develop outside the control of governments. In cases where governments remain strong, crises can lead to repression and escalation, as demonstrated by the Syrian civil war. In cases where governments are weak or non-existent, such as in the post-Arab Spring Maghreb region, containing emergent and expanding threats to U.S. interests is exceedingly difficult.

In either case, the lack of government control over the development of crises highlights one of the critical "lessons learned" over the last decade and can be applied in the post-pivot environment. To fully serve policy makers, the IC will need to continue to expand—to a much greater degree than has been assumed or accomplished to date—its reliance on open sources of information that contain or reflect the sentiments, intentions, and actions of non-governmental actors—what might be called "social intelligence."

However, the reality is that the requirement for the IC to continue to perform its traditional intelligence functions—espionage and other actions directed by the President against state actors—will not diminish. Hence, given the likelihood that its resources will be limited going forward, the IC has an incentive to find ways to maximize the value it can extract from "social intelligence" even as it strains to meet demands for its traditional products born of espionage and other sophisticated collection methods.

While technology has transformed the world of knowledge, it is imperative that U.S. laws and practices keep pace in a manner that respects privacy and civil liberties.

Given what is already an increased reliance on these new sources of knowledge and the likelihood that their use will expand dramatically in the years ahead, the government (and IC specifically) must be ever mindful that the rights of individuals are the very foundation of U.S. national security. While technology has transformed the world of knowledge, it has also introduced new challenges and threats to the security of the United States. Going forward, it is imperative that U.S. laws and practices keep pace with this information revolution in a manner that respects privacy and civil liberties. This core value must be woven into the fabric of what one might call "open sourcing" of intelligence.

II. DEMAND PULL FROM POLICY MAKERS

Whether addressing issues of hard or smart power, or likely a combination of the two, policy makers will likely demand that the IC compile, assess, and present the myriad threads of information promptly and in a manner that would permit them to take timely decisions to head off or influence events that might adversely affect U.S. interests. Because policy makers want to avoid surprises, or at least have ample time to prepare for impending events, they are likely to demand these assessments in the form of "actionable strategic warning." Once an event or crisis begins to unfold, it is reasonable to suppose that, in an age of instant information generated by individuals with smartphones from the streets of urban centers (as well as distant battlefields), policy makers will want their "current, actionable" intelligence not in days or hours, but in real time.

The stress on "actionable" intelligence by policy makers is a reflection of the speed at which events can move in an era when mobile communications are the norm even in the most remote locations.

The stress on "actionable" intelligence by policy makers is a reflection of the speed at which events can move in an era when mobile communications are the norm even in the most remote locations. Moreover, those local communications are part of a larger, global network of communications. Ironically, that network was first created to enable communications among a limited number of users, but is now accessible by anyone, anywhere, with a relatively inexpensive device. Within that network reside innumerable sub-networks (public and private) that can form and reform nearly instantaneously in response to events. There also resides, within that global network, a vast repository of information that is accessed, used, added to, managed, distorted, and often purposely manipulated by those sub-networks.

That network is a rich "ecosystem" containing an enormous amount of data and information, which if accessed, managed, and efficiently assembled, can yield actionable knowledge for decision makers. Whereas in the past the analog of these digital networks was the sole (or nearly so) province of governments or large organizations (e.g., financial institutions or news organizations), today they are accessible by a wide array of non-government entities and individuals. Those same entities and individuals are as capable (and sometimes more so) of managing, assembling, and yielding actionable knowledge for their own purposes as are governments.

STRATEGIC WARNING

Given the ubiquity, speed, and penetration of communications and the velocity at which events can escalate to crises, one of the great challenges to the broader security and defense strategy of the United States is surprise. The myriad vulnerabilities of political societies and economies that are globally oriented and interconnected; the availability and deadly nature of modern, ever-proliferating weapons technology; and the stealth with which it can be delivered by those intent on imposing damage with no regard to the collateral effects of their actions, magnifies the risk posed by surprise.

Managing national security affairs in a way that avoids the worst of surprises requires a broad knowledge of evolving circumstances, an acute situational awareness of those developments that bear the hallmarks of risk and strategic warning, and an understanding of the potential effects of possible events. Policy makers will turn to the IC for this knowledge, awareness, and understanding.

Given the ubiquity, speed, and penetration of communications and the velocity at which events can escalate to crises, one of the great challenges to the broader security and defense strategy of the United States is surprise.

The emerging cadre of policy makers come to the IC with considerable prior experience with the power of modern communications and associated computational capabilities. They are accustomed to having unrestricted access to globally sourced and indexed information and will be adept at analyzing that data. Those policy makers have come to expect instant knowledge delivered on their smartphones and tablets and are therefore very likely to expect their intelligence apparatus to emulate—if not outperform—the "open source" world of information, which many of them will have used extensively throughout their personal lives and careers.

To meet this expectation, the IC will need to accelerate its evolution in the sourcing and reporting of information. Historically, the IC has been the gatherer of the secrets of other governments and the keeper of its own. For much of its history, those secrets (and associated analysis) formed the core of the presentations policy makers sought from the IC. That was in large measure because that which was most threatening to the United States was controlled by governments with known or knowable behavior engaged in practices that could (with enough effort and ingenuity) be monitored, observed, overheard, and measured, despite the efforts of those governments to keep them secret.

In this emergent era, governments are rarely the sole source of the principal threat(s) to U.S. interests—sometimes, governments might not even be a source at all. To be able to accurately inform the policy maker, the IC will need to monitor, observe, overhear, and measure what is taking place within the vast and evolving Internet and the social networks that make use of it. Social media analysts call it "trending" and "sentiment analysis." The process identifies what a population of interest is focused on at a particular moment; the web sites, blogs, feeds, etc., that are gaining or losing visitors; what stories are capturing attention; whose attitudes are being promulgated to whom and how are those in receipt of messages reacting, etc. That information is used for a wide variety of purposes, such as shaping and targeting ad campaigns that appear on personal monitors or to tweak the content of products to avoid consumer complaints, or to call potential interest groups to action.

In this emergent era, governments are rarely the sole source of the principal threat(s) to U.S. interests—sometimes, governments might not even be a source at all.

That the Internet and its associated social networks are a place where information critical to U.S. security can be found is not news to the IC. What may be new is that the policy makers they serve will expect that the information and knowledge resident on the web and within the networks it enables will be woven into the fabric of the IC's reporting in advance of, during, and following events of national security interest. This expectation is likely to arise if for no other reason than the likelihood that those same policy makers not only have their televisions tuned to CNN, but have RSS feeds, Twitter feeds, Facebook accounts, blogs, and other open source information available to them independently of the IC.

This observation suggests that the IC may need to reflect on the sourcing and content of its products and the relative weight to give its components in response to a demand pull from policy makers.

The task force framed the issue by reflecting on the availability and value of information obtained through traditional sources and methods—broadly put, espionage and other sensitive collection, by whatever means—and analysis, on the one hand, and the other information that is readily available to and created by non-government sectors.

Much of the information needed to provide strategic warning is increasingly available to attentive observers and analysts from the publicly accessible global information environment. That information (sifted, indexed, analyzed, and presented through technical means) provides users with a wealth of knowledge on events of interest. The private sector is heavily invested in "business intelligence," which is derived from such capabilities. To appreciate power and utility of private sector intelligence, one need only visit the trading floor of a financial firm or one charged with providing weather and other environmental and market alerts for the agricultural sector. The sources, methods, tools, and products available in the private sector rival and, in many instances, surpass those of the IC.

That said, there is information the private sector, by law or due to the care exercised by private and public entities, cannot access. Here lies the comparative advantage of the IC. It is indisputably better situated to gather information that others, especially state and non-state actors, wish and work hard to keep private or secret. The IC also has the capacity (and unenviable task) of validating the many strands of intelligence, traditional or otherwise, to which it has access. But validation that arrives as history or forensic evidence is more useful for gleaning "lessons learned" and will be of little value in translating knowledge into effective action. Finding a way to close the validation cycle on social intelligence and melding it with traditional intelligence will be a demand the IC can expect from policy makers.

In the estimation of the task force, the diversity and depth of information available in the "clear" should shape policy makers' demands of the IC. Policy makers need to acquaint themselves with the breadth and depth of the IC's capacity to discover secrets, distinguishing that which is unique or singularly enlightening from that which is additive to a known (or knowable) body of information. Distinguishing the former from the latter can free the IC to focus its scarce resources on those priority tasks for which it has a comparative advantage, the accomplishment of which is most likely to satisfy the demand pull of the policy makers.

At the same time, the IC will need to engage the policy community to learn how to meet its demand for both highly specific information and broad contextual understanding of a development, event, or trend of interest. Conversely, that unique community of thoughtful current and former policy makers will need to give requisite thought to what they believe the United States needs from the IC, with equal urgency to the "introspection" being asked of the IC. Toward that end, policy makers might encourage the IC to organize a segment of its collection and analysis capability to act as curators of data, capable of assembling, reassembling, ordering, reordering, validating data—and gathering more as necessary—with an eye to presenting both timely and contextual information. Within their area of responsibility, curators are able to help the observer or user understand what the pieces of information mean independently, what relationships each piece has to one another, and to the whole.

> The sources, methods, tools, and products available in the private sector rival and, in many instances, surpass those of the IC.

CURRENT INTELLIGENCE

The value added by the IC as curator—providing a product that translates secret and open information into useful knowledge for strategic warning—might increase as the focus of policy makers becomes more operational and tactical as a national security event unfolds. There is an inevitable and irresistible urge to narrow one's focus as events escalate toward crisis. It is at precisely such moments, however, that leaders in the policy community are likely to turn to the IC and ask for context and help in understanding the implications of what has been done, is occurring, and what might be contemplated.

The longer a crisis lasts, the more time the involved parties have to learn and understand. However, in an environment where there is often a premium on bringing a crisis to an early end, policy makers can be expected to look to the IC to bring to it a depth of understanding well in excess of that possessed by the policy makers alone.

This is an occasion when the role of curator may come to the fore. Having knowledge and being able to convey understanding of the personalities, agendas, relationships, networks, local circumstances—cultural, ethnic, sectarian, governance, etc.—as well as the higher order effects of the relationships and factors in play would be of immense value to the decision maker.

III. INTELLIGENCE IN THE GLOBAL INFORMATION ERA

Given the importance and relevance of knowledge and understanding that can be gained from the diverse and large repositories of publicly available information, policy makers should review the role they might envision for "stolen secrets" in satisfying their knowledge needs with IC partners. There are some information needs that only traditional intelligence can provide, most notably in areas related to science and technology, as well as diplomatic and military activities. The policy maker needs to grasp the difference and relationships among sources (where or from whom information is obtained) and methods (how it is obtained and used). By doing so, the policy maker can better appreciate the value of a secret relative to whether or not it contributes to his knowledge of a national security issue and/or the secret's relation to an intelligence activity or operation.

If policy makers come to the conclusion that the intelligence delivered to them is a mix of history and undistinguished judgement, they will raise the question of who will be best-qualified to present the President and policy makers with the best knowledge.

In anticipation of such a review, the IC itself might consider evaluating the value of its non-operational secrets to its knowledge creation. That way the IC can be persuasive about the relative value added by the stolen secret to its ability to "get it right" and will be in a position to preserve its pre-eminent role in conveying knowledge to policy makers. If policy makers come to the conclusion that the intelligence delivered to them on a daily basis is a mix of history and undistinguished judgment (or worse, little more than informed speculation), they will look elsewhere for incisive analysis of national security affairs, raising the inevitable question of who will be best-qualified to present the President and associated policy makers with the best knowledge.

This is as likely to be true of strategic intelligence, the President's Daily Brief, and briefs that are presented to senior officials as it is with respect to current intelligence and the support given to operational units in the DOD, DHS, DOJ, and Treasury Department, among others. At the senior levels there are extensive suppliers of information easily available from sources other than the Intelligence Community, often as reliable as those used by the IC. At the tactical levels, operational units—military, diplomatic, domestic—will have their own capacity and capability for generating reliable current intelligence (and perhaps strategic as well) relevant to their activity.

The challenge for the IC is to sustain its relevance beyond the stolen secret in the era of global access to diverse and rich sources of data and information. The task force employed the following diagram *(Figure 1)* to examine this proposition.

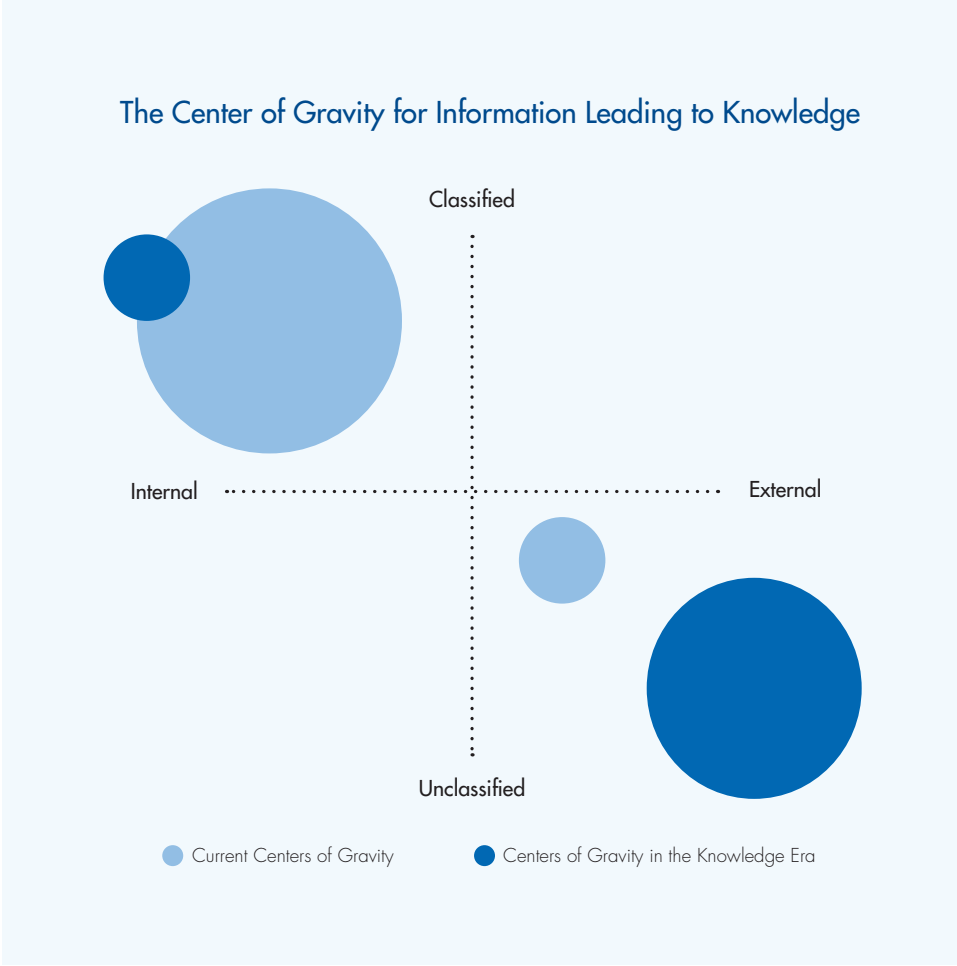

Figure 1

The horizontal axis addresses information gathered from espionage or created internally versus information gathered from external sources by ordinary means. The vertical axis represents information that is classified from its creation due to the sensitivity of the information as a result of the sources and methods used to develop and/or acquire it (or both), as opposed to that which is available in the public domain.

The light blue circles are meant to represent the "center of gravity" for intelligence collection, analysis, and distribution. Situated in the upper left hand quadrant, and fairly filling it, the light blue circle implies that historically, information—irrespective of source, method

The challenge for the IC is to sustain its relevance beyond the stolen secret in the era of global access to diverse and rich sources of data and information.

or sensitivity—was viewed and treated within the IC and accepted by policy makers as secret. The light blue circle in the lower right quadrant acknowledges that historically neither the IC nor policy makers ignored information gathered from open sources—recall the Foreign Broadcast Information Service—but that such information was rarely delivered in an unclassified format to policy makers. Hence, that smaller circle resides closer to the crossover point between classified and unclassified information.

Conversely, the darker circles are suggestive of the shift the task force believes is taking place in the center of gravity for intelligence. The first is the relative difference in both the location and size of the two sets of circles. The movement of the dark circle to the outer edge of the upper left hand quadrant conveys the task force's belief that traditional intelligence activities will become increasingly sensitive—and by implication more essential—to the policy maker. As noted earlier, there are still real secrets being kept (which are harder to access by means that are increasingly more sensitive) and the validation of which remain critical to policy makers. Gaining that information and assuring for as long as possible that the original owner of the information does not know its security has been compromised will remain the comparative advantage of the IC.

The larger dark circle in the lower right hand quadrant represents that vast and growing repository of information, and potential knowledge, which is increasingly available in the open and unclassified space. The task force acknowledges that for a variety of reasons, information gleaned in this space could be classified by reason of its association with U.S. government intentions, ongoing activities, etc. That does not diminish the inherent value of that information for either strategic or current intelligence purposes, especially given the relative decline in the control of governments to manage socially motivated events.

IV. CONCLUSION

Globalization and the Internet are spreading knowledge and enabling public access to information that security services and governments once viewed as secret intelligence. From social media feeds' descriptions of unfolding events in Tehran to Google Earth images of suspected nuclear facilities, evolving sources of information provide analysts with insights into questions that only classified methods—diplomatic reporting, clandestine sources, and satellites—could answer as recently as two decades ago.

These new means may reduce the need for the range of expensive collection tools that U.S. agencies once had as their specialty and comparative advantage.

The last generation of analysts worked with data feeds that were much more circumscribed; information collected from various U.S. government sources flowed into paper, and then to electronic inboxes, mixed with open-source media culled from foreign news reports. Broader access to open source typically meant subscriptions to news services, or occasional interaction with academics or private sector companies with unique access overseas. The digital inbox, even in the 1990s, included embassy cables, satellite imagery, intercepts, and clandestine reporting from human sources. Knowledge outside these areas was helpful, but it was neither critical nor readily accessible.

With many intelligence problems today, the slice of the knowledge puzzle represented by these traditional secret sources, as opposed to the growing slice represented by new media, is declining. Unrest in Tehran, activity at a North Korean nuclear site, demonstrations in Tahrir Square, and opposition activity in China are all collection targets that are easily accessible by newly available means. These new means may reduce the need for the range of expensive collection tools that U.S. agencies once had as their specialty and comparative advantage. This will increase the requirement for security agencies to evolve into knowledge agencies, with training, policies, and procedures that guide analysts on how to live in an open world with its attendant opportunities, responsibilities, and potential vulnerabilities to counterintelligence activities.

As noted, these developments are nowhere close to eliminating the need for secret intelligence acquired by methods unique to governments and security services, nor will they ever be. As long as there are governments, non-state groups, and rogue individuals who violate international norms and seek to keep their aims and activities secret, there will be a need for the human spies and novel methods of accessing data, which tend to dominate the budgetary commitments of the IC. However, these areas of truly secret information are decreasing in comparison to the relative explosion in public access to previously private, or even secret, knowledge.

Policy makers will increasingly demand knowledge at the frenetic pace of the world news cycle. As suggested earlier, the formation of a coalition composed of thoughtful current and former policy makers and associated policy organizations that will contemplate how policy makers' requirements will evolve in this environment would provide a valuable service in catalyzing and guiding the evolution of the IC in the tradecraft associated with "open sourcing."

Standards are evolving, and we have a pervasive sense that the future of privacy and civil liberties may be so different in future decades that we struggle to imagine how the digital world of the next generation will appear.

We do not yet have a clear understanding across society of how we should set boundaries for these new knowledge sources. Many of these sources of knowledge, such as social media sites or mini-drones that might operate in American cities to report on everything from traffic snarls to high-crime areas, are less than a decade old, and we do not have culturally agreed-upon norms. The contrast to intrusions in our physical space is striking: we readily accept highly intrusive searches at airports, for example, but we would not accept the same invasion of personal space when entering a supermarket. By contrast, we know that Facebook pages are visible to a user audience of nearly a billion people, but we are uncomfortable with the government viewing this readily accessible information. Standards are evolving, and we have a pervasive sense that the future of privacy and civil liberties may be so different in future decades that we struggle to imagine how the digital world of the next generation will appear.

Both the executive and legislative branches of government have an interest in conducting a discussion of relevant issues in a structured manner in which the views of the public are given voice. For the executive branch, this need might be addressed by a commission sponsored by the Attorney General; for the legislative branch, it might be met by a congressional commission. Either or both would be charged with examining the issues associated with privacy and civil liberties to enable the nation to best posture itself in this rapidly evolving world of knowledge.

Intelligence experts rightly point out the challenges of analysts operating in this environment. More analysts operating in an increasingly open world will give hostile security services more access to potential recruitment targets. Additionally, analysts working in this world will need training and guidelines to ensure that they understand the differences between asking questions as a private citizen and asking identical questions as a representative of a government office. For example, asking an aid worker in Somalia about

conditions in refugee camps might seem benign unless those questions come from an intelligence analyst and a hostile intelligence service misinterprets this interaction as indication that the aid worker has a clandestine role. As the 10th anniversary of the Intelligence Reform and Terrorism Prevention Act of 2004 approaches, Congress should review whether the nation's premier analytic capabilities are optimally organized, trained, and equipped to sustain their world-class leadership in this increasingly complex age of information and knowledge.

The problems of absorbing this data are yet more problematic. How can one sort through billions of social media inputs and determine which add value? And if foreign security services, or private sector actors, want to shape our thinking by manipulating these media, how does one look for deception? Finally, and most importantly, can a balance be struck between the ready acceptance by citizens that they are exposing their private lives on these media—from webpages to drone images of a private residence—to their concerns that government access to this same publicly available information is an invasion of privacy?

Cases are already highlighting the importance of new sources of information for collection and analysis that also raise privacy questions. If a high school student posts hate speech on a Facebook page and then begins purchasing ammunition online, should his actions be subject to investigation? Is hate speech free, or do our definitions change if this behavioral flag is combined with other information? And when a U.S. Army major emails a radical cleric overseas (as in the case witnessed at Ft. Hood a few years ago), what is the government's appropriate role in collecting, analyzing, holding, and responding to this information? In the broadest sense of this rapidly and relentlessly expanding knowledge world, if an analyst can access a growing volume of information from his personal information devices, what limits should be set on his accessing the same information when he enters a government office?

We do not yet have answers, but we should accept that the knowledge world will fundamentally challenge and change intelligence and that the IC will become less effective if it fails to assimilate these new and dynamic information technologies, capabilities, processes, and means of conveying knowledge to policy makers. As we consider the relatively narrow question of the Asia pivot, a broader knowledge revolution is underway, challenging security services to redefine the role of intelligence in the 21st century. Is it secrets, or is it knowledge? If it is indeed knowledge, the IC must look at this juncture as a unique opportunity to contemplate a fundamental cultural pivot with regard to its potential role as the preeminent curator and purveyor of knowledge for the nation. Today, we still live largely in the world where intelligence is defined as "secrets;" tomorrow, we will either embrace a new understanding of intelligence and knowledge, or risk marginalizing analysts from this century's knowledge revolution and hence fail to serve policy makers as effectively as possible.

The IC will become ineffective if it fails to assimilate these new and dynamic information technologies, capabilities, processes, and means of conveying knowledge to policy makers.

PROPOSALS

- That the policy makers of the incoming administration engage the IC to better understand the relative roles of open source and traditional intelligence in meeting the policy makers' demand for timely, accurate, and relevant knowledge of national security issues and events.
- To ensure that the privacy and civil liberties issues raised by open sourcing are protected, the executive and legislative branches, as they have with the other intelligence disciplines, should propose and/or make policy, regulatory, and statutory changes, as appropriate and necessary, to guide policy makers and the IC in the creation of a new intelligence discipline.
- That a coalition of current and former decision makers and intelligence practitioners, as well as interested policy organizations, be formed to consider and recommend ways to resolve the practical issues associated with the collection, analysis, validation, integration, and dissemination of openly sourced intelligence.

ABOUT THE INSA REBALANCE TASK FORCE

INSA established the Rebalance Task Force to assess the implications for the Intelligence Community of the new defense strategy and the adjustments in the broader national security policy agenda which it implies. The Task Force is chaired by former Undersecretary of Defense for Intelligence, Dr. Steve Cambone. He is joined on the Task Force by former CIA and NSA Director General (ret.) Michael Hayden; INSA's Senior Intelligence Advisor and former Undersecretary for Intelligence/DHS, Charlie Allen; former Deputy Director of the CIA's Counterterrorist Center/Deputy Director of the FBI's National Security Branch, Phil Mudd; former Deputy Director of Intelligence/CIA, Carmen Medina; former Assistant Secretary of State for Intelligence and Research, Randall Fort; Executive Vice President and COO of Invertix, Craig Parisot; and Vice President and General Manager, Cyber Systems Division, of General Dynamics Advanced Information Systems, John Jolly. The purpose of the Task Force is to inquire whether, and in what ways, the national intelligence enterprise might need to adjust as an evolving national security strategy increases its focus in the coming decade toward Asia and other strategic interests and on threats to the national interest that include non-terror related issues.

This white paper is intended to help focus attention on the critical role of intelligence for planners and decision makers who will be anticipating, preparing for and protecting U.S. national interests in an era of dynamic change and identify the complex demands the IC may confront as a result. The intended audience of this paper includes agencies within the Executive Branch, the Legislative Branch, and the interested public.

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.

As a non-profit, non-partisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities.

INSA has over 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
SUPPORTING ADVANCES IN THE NATIONAL SECURITY AGENDA

901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org