DLT
A TECH DATA COMPANY

Reference Guide

Intelligence Community Reference Guide – Part One

A Roadmap to the Classified Universe

Mark S. Harris
Senior Director, Strategic Markets
U.S. Intelligence Community

ABOUT THE AUTHOR

Mark Harris serves as senior director, market intelligence for DLT Solutions, a Tech Data company. In his role, Mark is responsible for conducting U.S. intelligence community (IC) market intelligence activities for DLT and its technology vendors and channel partners. He also conducts “Introduction to the U.S. IC” and “Key Technologies for the U.S. IC” workshops on a quarterly basis to educate internal DLTers and partners on the IC.

Mark started his career with the U.S. Air Force where he was a computer/communications officer with tours at the Pentagon, Offutt AFB, NE, Keesler AFB, MS and Bolling AFB, DC. His last five years in the Air Force were in support of the Air Force Intelligence Agency working on classified intelligence systems. Additionally, as a major, Mark served as the Air Force representative to the Department of Defense Intelligence Information Systems (DoDIIS) Management Board (DMB) at the Defense Intelligence Agency (DIA) In this role he worked on the technical architectural framework allowing for interoperability between key IC systems.

After leaving the Air Force, Mark worked for Sun Microsystems, Cisco Systems, IBM, Oracle and Dun & Bradstreet. Mark’s exclusive experience within the IC conducting business development and sales management gives him the unique experience of understanding all the challenges of selling into the IC. It is from this experience and perspective that he is created IC Reference Guide which helps salespeople in the public sector maneuver the IC maze.

Mark holds a B.S. in Theoretical Mathematics from San Diego State University and a M.S. in Computer Science from George Washington University.

INTRODUCTION

The Intelligence Community Reference Guide series provides a framework for understanding the complex nature of the U.S. Intelligence Community (IC), as well as a quick reference for sales professionals to look up information and refresh basic concepts. While the IC has a very large information technology (IT) budget, doing business with the IC can be quite complex and even discouraging at times. Any company looking to do business with the IC must understand that there are unique requirements and investments necessary to be successful. We have worked with many companies that thought they had some "secret sauce" that was going to make them rich via a large IC procurement, only to finally give up after a lot of time and expense. The IC is large, complex, widely dispersed geographically, operates in a very secure environment and generally likes to do business with companies and/ or people they trust. So be prepared, do your homework and learn how to "speak IC," so you can be successful working with and selling into the IC. It is definitely a marathon journey, requiring patience, not a quick race. But once you get into the IC, it is well worth it.

When you look and the table of contents of each part of this series, you may wonder why the breath and depth of topics which at first glance don't seem necessary for a salesperson. But I assure you that if you try to call into a particular agency and you do not understand their mission and the unique lingo surrounding that agency, the person you are speaking with will quickly dismiss you. For example, if you are working with the National Geospatial-Intelligence Agency (NGA) and you know nothing about imagery or geospatial concepts, you simply will not be successful.

Once again, this reference guide series is meant to provide both a relatively quick introduction into key topics necessary for selling into the IC as well as more pragmatic sections such as how to get an account on the unclassified acquisition resource center (ARC), so you can review request for information (RFI) and requests for request for proposals (RFP). I also try to provide as many additional references as possible so those wanting to dive deeper can do so as needed.

Mark S. Harris
Senior Director, Strategic Markets
U.S. Intelligence Community
mark.harris@dlt.com
571-335-3977

Intelligence Community Reference Guide: Part One

This section of the reference guide contains IC background information that is necessary for anyone looking to business with the IC to understand before diving into a particular agency.

U.S. Intelligence Community Background

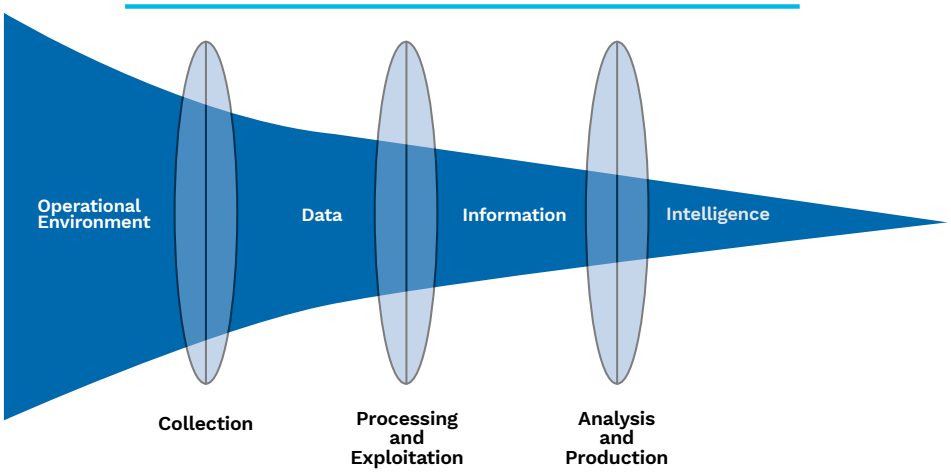
This section of the reference guide contains IC background information that is necessary for anyone looking to business with the IC to understand before diving into a particular agency.

WHAT IS INTELLIGENCE?

Intelligence is the product of a variety of collection methods funneling and converting raw data into detailed analysis using a variety of intelligence analytic methodologies similar to the scientific method. The process is done independently of any external considerations, political motivations or other outside forces. The purpose is to provide the end user, whether it be a military unit leader or the National Security Council, with critical information to make informed decisions.

Intelligence is information gathered within or outside the U.S. that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security. Intelligence can provide insights not available elsewhere that warn of potential threats and opportunities, assess probable outcomes of proposed policy options, provide leadership profiles on foreign officials and inform official travelers of counterintelligence and security threats. By its very nature, mostly because of the sources and methods for the collection of intelligence, it tends to be classified. This world of classified infor-

Relationship of Data, Information and Intelligence



mation is what generally separates much of what the U.S. Intelligence community does from other government agencies and thus often draws the ire and concern of both citizens and the U.S. Congress.

Intelligence is nothing new and has been the instrumental core of virtually every civilization's military in terms of using various techniques to gain more knowledge about advisories. Long-range observations and spying have always been a critical part of knowing an enemy's size, location, intent and thus allows for proper planning. Sun-Tzu is an ancient Chinese military strategist, writer and philosopher who wrote a famous piece called "The Art of War," which is required reading for all U.S. military officers because of its keen insights that have remained at the core of military and intelligence activities.

There are several key reasons why intelligence and the IC are so critical. First and probably foremost is to prevent a strategic surprise on the country, such as the attack on Pearl Harbor. It is one thing to have evidence of various troop movements, it is quite another thing to have insights into the intent of a foreign nation and respond prior to an attack. Second is to provide policy support to the U.S. President and Congress. The IC has a very large cadre of seasoned professionals that spend their entire career's becoming experts either on various technologies, terrorist organizations or nation states and they can offer tremendous insights on what the U.S. may or may not want to do in dealing with various national security concerns and policies.

Thus, intelligence can be thought of as a community of professionals that employ rigorous methodologies to collect, analyze and bring meaning to mountains of information with the result being a product delivered to the right customer at the right time to be able to impact their mission.

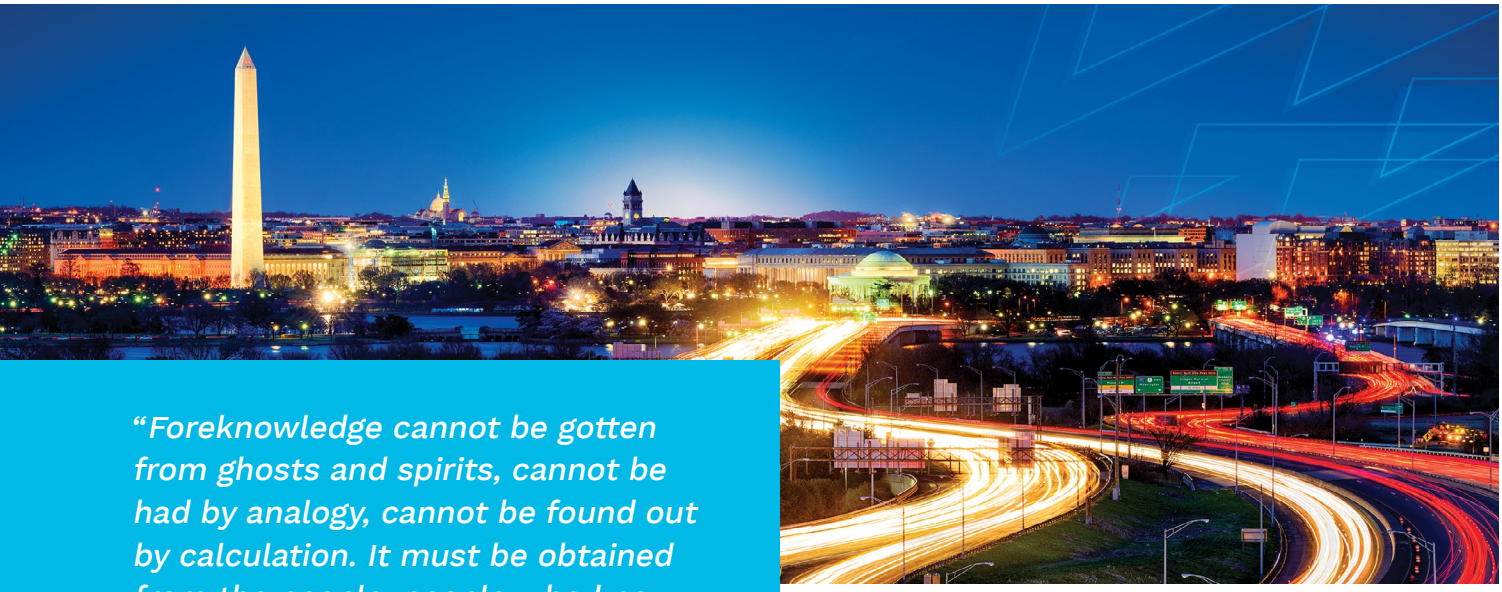
CUSTOMERS OF INTELLIGENCE

At the highest, simplest level, the National Security Act of 1947 defines the IC's customers as the:

- U.S. President
- U.S. National Security Council
- U.S. Heads of Departments and Agencies of the Executive Branch
- U.S. Chairman of the Joint Chiefs of Staff and Senior Military Commanders
- U.S. Congress

The above customers are generally at the more policy level and/ or concerned with implications of world events which impact the security of the nation. At the other end of the spectrum would be tactical military intelligence which are more focused on information around an Area of Responsibility (AOR) impacting current military operations.

Intelligence Community Reference Guide: Part One



"Foreknowledge cannot be gotten from ghosts and spirits, cannot be had by analogy, cannot be found out by calculation. It must be obtained from the people, people who know the conditions of the enemy."
- Sun-Tzu, The Art of War

BRIEF HISTORY OF THE CREATION OF THE U.S. INTELLIGENCE COMMUNITY

Understanding history allows for a fuller understanding of the present and often provides insights on how the future will unfold. Thus, it is of interest to provide the reader with a very brief general history of intelligence. The first real use of the intelligence tradecraft was well documented during the American Revolution by General George Washington. The use of spying by Washington was considered critical for the success of the American victory. In 1775, when the Second Continental Congress chose Washington as commander in chief of the Continental armies, Washington appointed a soldier named Thomas Knowlton to organize the war's first spy unit. The roughly 130-man group, known as Knowlton's Rangers, played a key role in the 1776 battle of Harlem Heights in New York, scouting out the British advance guard. In the blazing musket fire of the skirmish that followed, Knowlton was killed, and his place in history cemented. Even today, the seal of the U.S. Army intelligence service bears a 1776 stamp, in honor of his unit. In November 1778, General Washington appointed Benjamin Tallmadge to director of military intelligence and ordered him to construct a spy ring inside New York City, which was occupied by the British. They were dubbed the "Culper Ring" at Washington's suggestion.

I would highly recommend to the interested reader to check out "How George Washington Used Spies to Win the American Revolution" by A.J. Baime on History.com. It is an incredible tale of bravery and the importance of spying during this critical period in American history.

For the most part, from the American Revolution up until World War II, there was not much of a true centralized non-military intelligence organization within the U.S. While the U.S. Army and U.S. Navy both continued with the needs to spy and collect

information on the military forces of foreign advisories, the U.S. to a large extent felt somewhat isolated from the world from an invasion threat perspective and had virtually no concerns with border protection in the Northern Hemisphere. The surprise attack on the U.S. by the Japanese at Pearl Harbor change that somewhat naive perspective. The Office of the Coordinator of Information (OCI) was an intelligence and propaganda agency of the U.S. Government and was founded in 1941 by President Franklin D. Roosevelt. It was intended to overcome the lack of coordination between existing agencies. The OCI was headed by William J. Donovan.

The Office of Strategic Services (OSS) was a wartime intelligence agency created in 1942 and was a predecessor to the State Department's Bureau of Intelligence and Research (INR) and the Central Intelligence Agency (CIA). The OSS was formed as an agency of the Joint Chiefs of Staff (JCS) to coordinate espionage activities behind enemy lines for all branches of the U.S. Armed Forces. Prior the formation of the OSS, various departments including State, Treasury, U.S. Navy and U.S. Army all conducted American intelligence activities on an ad hoc basis with no overall coordination. It is very important to understand the relationship with the United Kingdom and its impact on the establishment of America's intelligence agencies during World War II and moving forward. The British intelligence organizations and practices were much more organized and experienced than that of the U.S. and as such, America very much emulated much of the British practices. In fact, the British were instrumental in helping the U.S. establish a more robust and centrally coordinated intelligence program.

Despite the rich history of critical work done by the OSS during World War II, there was a desire by many to dissolve it after the war. This stemmed from the general distrust by Americans of any government intelligence organizations and fears of invasion of privacy versus the benefits of protecting the security of the nation. However, having the OSS clearly showed the value of having a centralized organization that could coordinate activities across various agencies. Thus, the CIA was formed in 1947 under the National Security Act of 1947 that also created the National Security Council. The CIA is an independent agency with responsibility for foreign intelligence. The CIA by law cannot conduct surveillance on U.S. citizens and does not have any law enforcement capabilities. However, the CIA is the only agency authorized by law to carry out and oversee covert action at the behest of the U.S. President. It should be noted that the FBI, State Department and military intelligence groups all opposed the creation of the CIA as an independent non-military intel-

Intelligence Community Reference Guide: Part One

Intelligence analysis is the process by which the information collected about a target or an enemy and is used to answer strategic and/ or tactical questions about current operations or to predict future behavior.

ligence agency. That opposition and some of those prejudices against the CIA still exist today.

While Human Intelligence (HUMINT) or spying was the mainstay of military intelligence as well as the CIA, as America moved toward the Cold War with the Soviet Union as well as chilled relationships with China, there became the need for more and more technical collection capabilities because of the difficulties of spying in closed societies such as the Soviet Union and especially China. This technical specialization directly led to the creation of specialty agencies such as the National Security Agency (NSA) in 1952 for cryptology and Signals Intelligence (SIGINT), the National Reconnaissance Office (NRO) in 1961 for launching spy satellites and most recently the National Geospatial-Intelligence Agency (NGA) in 1996, which specializes in imagery and geospatial intelligence (GEOINT).

Check out **The Creation of the Intelligence Community: Founding Documents** for more information.

WHAT IS INTELLIGENCE ANALYSIS?

According to the CIA, "intelligence analysis is the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context". As a key founder of CIA analytic practices phrased it, "the mission of intelligence analysts is to apply in-dept substantive expertise, all-source information, and tough-minded tradecraft to produce assessments that provide distinctive value-added to policy clients' efforts to protect and advance U.S. security interests."

The depth and breadth of intelligence analysis varies greatly depending on what is being analyzed and the environment that intelligence analysts are working. For example, at the tactical military level in a forward war zone, military analysts may be looking at recent

Want to delve deeper on understanding the world of intelligence analysis? Below are a few great books on the subject:

Scientific Methods of Inquiry for Intelligence Analysis

Henry W. Prunckun

Cases in Intelligence Analysis: Structured Analytic Techniques in Action

Randolph H. Pherson and Sarah Miller Beebe

Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present

Timothy Walton

A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis

Center for the Study of Intelligence

Intelligence Analysis: A Target-Centric Approach

Book by Robert M. Clark

imagery and other sources to determine the location of enemy troops with an overlay to civilian facilities which need to be taken into consideration for targeting and engagement strategies. This kind of analysis is very localized and often occurs constantly over a 24-hour period to keep the analysis up to date with battlefield conditions. On the other hand, counter-terrorism analysts tracking a particular terrorist group may work for many months to gather information on who the members are, where they are and what is their intent. This can be even more complex if weapons of mass destruction are involved (e.g., chemical, biological, nuclear) because the analysts also need to be an expert on those weapons in terms of understanding how they are constructed, where the materials come from, how they might be delivered as a weapon system, etc. These types of intelligence analysts are generally civilians with advanced degrees working at the Defense Intelligence Agency (DIA), CIA or the National Counter Terrorism Center (NCTC).

After the erroneous 2002 National Intelligence Estimate of Iraq's weapons of mass destruction, there was the introduction of stronger structured analytic techniques for analysis which includes the following:

- Scenarios and indicators
- Hypothesis generation and testing (analysis of competing hypotheses)
- Assessment of cause and effect
- Challenge analysis
- Decision support

It is critically important to understand that intelligence analysis must be done independent of politics. You cannot have a situation where a political leader publicly states their uninformed opinion about a particular event or situation, then requires the IC to agree with him or her and have the analysts come up with proof for their incorrect assessment. This can lead to disastrous consequences.

INTELLIGENCE ANALYSTS

From a sales perspective, it is important to remember that most IT program dollars spent are either directly or indirectly spent on systems to support the collection of data and the transformation of that data into intelligence by analysts. Understanding what intelligence analysts do for a living and what their challenges and needs are will help you better target technology in a way that makes sense to these customers. Intelligence analysts are very smart and demanding of vendors and systems integrators, so it pays to be prepared.

Intelligence Community Reference Guide: Part One

An intelligence analyst is a professional who spends an entire career becoming an expert in the scientific method that we all learned in high school and college. They apply it to the field by examining the clues gained by intelligence collection. Without prior assumptions, they look at all the facts, develop hypothesis, test them, put them out for comment to fellow analysts for review and finally come up with a conclusion as to what it all means.

In the military intelligence community, many of the services have complete career fields for intelligence analysts that allow them to come in with little to no training and then spend their career enhancing their skills. On the civilian side, intelligence analysts are recruited out of college and graduate school where agencies pick the best in various fields of study. In the case of very scientific analysis, agencies work with key universities in the U.S. to select graduate students and PhDs. Even then all government intelligence analysts go to specialty university or programs where they learn the fine science and art of their trade craft.

Intelligence Community Schoolhouses

- National Intelligence University –Managed by DIA
- Sherman Kent School for Intelligence Analysis – is the analytic component of the CIA
- Defense Intelligence College – Managed by DIA
- National Cryptologic School – Managed by NSA
- FBI Academy – Offers new analysts a 16 week Intelligence Basic Course
- Geospatial-Intelligence College –NGA's core training and professional development school

To recap:

- Intelligence analysts are the heart and soul of producing usable Intelligence
- They specialize in various disciplines and tradecrafts
- Range from tactical military analysts to more strategic analysts at CIA and DIA
- Most are highly educated and often recruited after graduating with a master or doctoral degree from a top university
- They go through intense training methodologies for deductive reasoning and reporting the ground truth
- Often deliver complex reports and brief senior

military/political leaders
- Products range from local military daily enemy assessments to highly complex National Intelligence Assessments for foreign nations and the Presidential Daily Brief

KEY INTELLIGENCE PRODUCTS

There are a wide variety of intelligence products produced by intelligence analysts. They can range from very simple field reports to military field commanders informing them of Battle Damage Assessments (BDA), to very formal documents produced for the President and National Security Council.

President's Daily Brief

While there are obviously a wide variety of products that intelligence analysts produce, perhaps the most famous is the President's Daily Brief (PDB). The PDB is a daily summary of high-level, all-source information and analysis on national security issues produced for the president and key cabinet members and advisers. The PDB is coordinated and delivered by the Office of the National Director of National Intelligence (ODNI) with contributions from the CIA as well as other IC elements.

The PDB has been presented in some form to the president since 1946, when President Harry S. Truman received the Daily Summary. Over the years, the PDB has evolved to meet the needs and preferences of each president and has expanded to include more information. The original Daily Summary was not an all-source publication and reported only on foreign intelligence matters. In 2014, the PDB transitioned from a print product to electronic delivery at the request of President Barack Obama so he could view them on an iPad.

World Intelligence Review

The CIA's Directorate of Analysis (DA) flagship product is an electronic daily publication called the CIA World Intelligence Review (WIRe), which is a highly classified document provided only for a restricted readership of senior policy and security officials. WIRe articles vary in length and allow the reader to drill down for more depth information, if the topic is of greater interest to that reader.

World Factbook

The CIA DA also publishes the annual World Factbook which provides information on the history, people and society, government, economy, energy, geography, communications, transportation, military and transnational issues for 267 world entities. This is an incredible document that everyone ought to check out.

DIA/J2 Executive Highlights

DIA produces the Executive Highlights product primarily for Department of Defense (DoD) policymakers, but it is also available to the executive branch. This product is equivalent to the CIA's WIRe, but has a military perspective. In many ways having two similar products, one from CIA and one from DIA, is viewed as a positive in terms of getting different and more enriched perspective on the same or similar topics.

National Intelligence Estimates

While the PDB, WIRe and J2 Executive Highlights are current intelligence reports focusing on very near-term issues, the National Intelligence Estimates (NIE) is a long-range product which represents the consolidated opinion of the entire IC. It is developed by national intelligence officers (NIO) working within the Director of National Intelligence (DNI) organization and is designed for national policy makers to have the information necessary to develop U.S. policy to counteract nation states and terrorist organizations planning negative actions toward the U.S. Special NIEs (SNIE) are written for more urgent time sensitive focus areas that require near term actions by senior policy makers.

Intelligence Community Reference Guide: Part One

Worldwide Threat Assessment

The IC as a whole, under the leadership of the DNI also produces an unclassified product annually call the Worldwide Threat Assessment which is briefed to the U.S. Congress and is well worth reading by all Americans. It provides a high-level overview of the major threats to the U.S. by both nation states such as Russia, China, Iran and North Korea as well as terrorist organizations. It also discusses items such as cyber threats, weapons of mass destruction, counterintelligence, economics, space and counterspace.

STRATEGIC VS TACTICAL INTELLIGENCE

It is important to understand and distinguish the differences along the spectrum of intelligence from strategic through tactical. The scope, resources involved, timelines and analytic expertise required varies vastly depending on what is being analyzed.

Strategic intelligence is concerned with broad issues such as economics, political assessments, military capabilities and intentions of foreign nations and increasingly, non-state actors. Such intelligence may be scientific, technical, tactical diplomatic or sociological but these changes are analyzed in combination with known facts about the area in question, such as geography, demographics and industrial capacities.

	Strategic Intel	Tactical Intel
Mission Objectives	Formulating National Policy by looking for trends by other nations indicating a threat to the U.S. homeland	Very focused information for small, specific geographic area aiding near term military operations planning
Audience	U.S. President, National Security Council, Congress	Battlefield commanders
Collection Sources	National Technical means (satellites, special aircraft)	Drones and tactical collection assets
GEOINT Collection	Broad collection looking for trends or threats over a large geographic area	Broad collection looking for trends or threats over a large geographic area
SIGINT Collection	Focused on code breaking and other activities that would give the U.S. a key advantage	Might focus on radio transmissions to triangulate for the targeting of weapons

Strategic intelligence is formally defined as "intelligence required for the formation of policy and military plans at national and international levels." It corresponds to the Strategic Level of Warfare that is formally defined as "the level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives."

An example of strategic intelligence could involve the utilization of extensive overhead satellite coverage of North Korea combined with other sources for several months. The goal being to track missile sites to determine the intent of that nation to build and use nuclear weapons. This is a very complex process requiring many specialized intelligence disciplines resulting in assessments and reports that can often go all the way up to the U.S. President.

Tactical intelligence is focused on support to operations at the tactical level and would be attached to the battlegroup. At the tactical level, briefings are delivered to patrols on current threats and collection priorities. These patrols are then debriefed to elicit information for analysis and communication through the reporting chain

Tactical intelligence could be as simple as tasking a drone to take pictures of an enemy's current location and using that information to brief a military unit commander. It is very local in nature to the Area of Operations (AO) and tends to be time sensitive due to the speed of war.

DIFFERENCES BETWEEN NATIONAL AND MILITARY INTELLIGENCE

There are a wide variety of differences between the concepts and missions of national intelligence and military intelligence. As noted in an earlier section, the U.S. really did not have any national intelligence as in a centralized intelligence organization concerned with intelligence for the overall national benefit until during World War II via the OSS. In 1947 the Director of Central Intelligence (DCI) and the NSC were created from what was the OSS. Up until that time the U.S. Navy and U.S. Army had their own intelligence capabilities focused on what was important to their mission but nothing for the overall U.S. The DCI was dual hatted by both the director of CIA as well as other elements of the IC. The president issued executive orders to guide intelligence activities including covert operations and sensitive collection methods. As a result of the terrorist acts of September 11, 2001, the National Commission on Terrorist Attacks recommended a new form of centralized coordination of the IC's organization. This recommendation led to the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA) which created the DNI and moved the community authorities to the DNI from the DCI and dissolved the DCI as the community manager. As you might imagine, this led to much concern and consternation from both the CIA who was effectively losing some power as well as the military intelligence agencies worrying about additional oversight.

THREATS THE IC PROTECTS THE U.S. FROM

The IC works diligently on a global basis to protect the U.S. homeland from a wide variety of threats, both conventional from nation states as well as from terrorist organizations. Key areas of concern intelligence analysts concentrate on are:

Terrorism is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents. This is usually intended to influence an audience via violence as evidenced in the U.S. on September 11, 2001. It is important to note that terrorism means all forms of terrorism, not just by foreign groups, but also domestic terrorism by anti-government groups as well as white nationalist and other

Intelligence Community Reference Guide: Part One

The threat to the United States that the Intelligence Community must mitigate takes several forms.

racially motivated acts of violence. Under law, the FBI is responsible for domestic terrorism while the CIA works in the international space. The two agencies work together at the National Counter Terrorism Center (NCTC) to coordinate activities due to the overlap as terrorists travel throughout the world.

Nuclear Proliferation is the provision of nuclear weapons and/ or technology by states that possess them to states that do not. There is deliberate proliferation in the sense of countries such as North Korea and Iran which possess nuclear material and could be providing such material to non-state terrorist actors. Furthermore, terrorists can steal this technology and/ or materials during transport or even small amounts from places such as hospitals where various medical machines have active nuclear material. This is one of the reasons the Department of Energy (DOE) is considered to be part of the IC.

The DOE has some of the world's foremost experts on nuclear weapons and intricate methods of protection for materials in transport.

Chemical Warfare (CW) can be considered the military use of toxic substances that cause incapacitation or death. It is the impact of chemical effects instead of physical effects that distinguishes chemical weapons from conventional weapons, even though both contain chemicals. A chemical weapon comprises two main parts: the agent and a means to deliver it. Optimally, the delivery system disseminates the agent as a cloud of fine droplets. This permits coverage of a broad amount of territory evenly and efficiently.

Biological Warfare (BW) is the use of pathogens or toxins for military purposes. BW agents are inherently more toxic than CW nerve agents on a weight-for-weight basis and can potentially provide broader coverage per-pound of payload than CW agents. BW are potentially more effective because most are naturally occurring pathogens – such as bacteria

and viruses – which are self-replicating and have specific physiologically targeted effects, whereas nerve agents are manufactured chemicals that disrupt physiological pathways in a general way.

Information Infrastructure Attack is defined as the use of cyber communication to distribute or coordinate plans for a terrorist attack, incite an attack, or otherwise assist in the facilitation of terrorism. Political activism on the internet has generated a wide range of activity, from using email and websites to organize web page defacements and denial-of-service attacks. These computer-based attacks

are usually referred to as hacktivism, a marriage of hacking and political activism.

Narcotics Trafficking is defined as any illicit activity to cultivate, produce, manufacture, distribute, sell, finance, or transport narcotic drugs, controlled substances, or listed chemicals, or otherwise endeavor or attempt to do so, or to assist, abet, conspire, or collude with others to do so. Drug dependence is a chronic, relapsing disorder that exacts an enormous cost on individuals, families, businesses, communities and nations. Addicted individuals frequently engage in self-destructive and criminal behavior. Along with prevention and treatment, law enforcement is essential for reducing drug use. Illegal drug trafficking inflicts violence and corruption on our communities. Law enforcement is the first line of defense against such unacceptable activity. The IC must support this defense to the extent feasible and allowable by law. Intercepted documents from Chinese military and intelligence agencies clearly show that as part of the overall Chinese plan to reduce the world power of America, they are assisting with drug trafficking into the U.S. as a way of subverting our society.

Information Warfare (IW) is different from a cyber-attack in that rather than trying to simply disrupt infrastructure components such as banking, electric grids, or manufacturing, IW seeks to create confusion and even chaos in the adversary's military, government, or general citizen population by inserting false information into the system. The clear effects of this can be seen over the past two years with the overall infusion of false news and stories by Russia into our social media and other sources. For very little money, IW can cause a lot damage.

WHAT CAN INTELLIGENCE DO AND NOT DO

It is important to understand what the limits of intelligence are in terms of the law. There are many factors at play which make this quite complicated, including the following: (1) the differences between Title 10 authority and Title 50 authority and (2) U.S. privacy laws which do not allow the government in general and the IC in particular to collect information on U.S. citizens. Title 10 generally refers to authorities and budget granted to the DoD. Title 50 generally refers to the CIA's authority to conduct its intelligence operations and covert actions, such as drone strikes. Over the past 10 years there has been more intermingling of military and CIA personnel in convert special operations activities, thus blurring the lines of authority even more.

With respect to U.S. citizen privacy, it is important to remember that the FBI is responsible for law enforcement, counter-intelligence and counter-terrorist activities related to U.S. citizens while the CIA is responsible for foreign targets.

Intelligence Community Reference Guide: Part One

Despite what you may hear on the news, agencies must follow very strict guidelines for collection activities, undergo constant training on data privacy laws and submit a wide variety of legal requests to judges for any collection on U.S. citizens.

What can intelligence do then? It can provide valuable services, such as:

- Providing decision advantage by improving the decision-making of consumers and partners while hindering that of our enemies
- Warning of potential threats from both nation states and rogue actors
- Insight into key current events, both political and military
- Situational awareness of advisories intents and capabilities
- Long-term strategic assessments on issues of ongoing interest such as global climate change and its impact on different parts of the world, refugee issues, genocides, military build-ups, etc.
- Assistance in preparation for senior-level meetings that include national security-related subjects
- Pre-travel security overviews and support to the Secret Service and other advance teams
- Reports on specific topics, either as part of ongoing reporting or upon request for short-term needs, including the all-important President's Daily Brief (PDB).
- Compiling U.S. government knowledge on persons of interest
- The Terrorist Identities DataMart Environment (TIDE) is a classified central U.S. repository of information on foreign terrorists
- The Terrorist Screening Database (TSDB), which is operated by the FBI's Terrorist Screening Center (TSC), is an unclassified database of all known or suspected terrorist names on which the U.S. government has information. The TSDB is available to law enforcement officials at all levels of government and also to federal government organizations (such as the State Department) that have name screening requirements.

What intelligence cannot do includes the following:

- Predict the future. Intelligence can provide assessments of likely scenarios or developments, but there is no way to predict what will happen with certainty
- Violate U.S. law or the U.S. Constitution. For example:
  - The activities of the IC must be conducted consistent with all applicable laws, to include the National Security Act of 1947, as amended, the Foreign Intelligence Surveillance Act (FISA), the Intelligence Reform and Terrorism Prevention Act (IRTPA), the Detainee Treatment Act, and the Military Commission Act.
  - The activities of the IC must also be carried out consistent with all Executive Branch policies, such as Executive Orders, Presidential Directives, and Intelligence Community Directives.
  - All activities of the IC are subject to extensive and rigorous oversight both within the Executive Branch and by the Legislative Branch, as required by the National Security Act of 1947, as amended.

FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

With all the recent misinformation promoted for political reasons and realizing how many American citizens really do not understand what FISA is. It makes sense to include a bit of background here to make sure the reader understands what the IC does and does not do relative to surveillance. The Foreign Intelligence Surveillance Act of 1978 is a U.S. federal law that establishes procedures for the physical and electronic surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers suspected of espionage, terrorism, or active counterintelligence operations. The law was enacted because of concerns that the NSA and other agencies were abusing their surveillance privileges. The law also created the Foreign Intelligence Surveillance Court (FISC) to oversee requests for surveillance warrants. Since the 9/11 attacks, many amendments have been made to broaden the scope of FISA to monitor terrorist organizations, especially those not associated with "foreign powers."

Now, it must be noted the FBI is the only IC agency that can conduct investigations of American citizens directly that are suspected of criminal or terrorist activities. During the 2016 American election campaigns, there were many foreign nationals being monitored by both U.S. intelligence agencies as well as by our allies such as Australia. This is standard operating procedure as these targets were suspected of being a part of Russian intelligence conducting operations in America and within our allies countries. During these surveillance activities there were many conversations picked up between the Russian targets and American citizens who happened to work for a particular campaign. The number of people involved, and the number of contacts, led to considerable concern for national security and ultimately the unmasking of the names of the American citizens as part of an FBI investigation. It is important to note that not a single American in this case was being spied on directly, rather because of their communication with a known Russian intelligence operative, they got caught up in the investigation.

2411 Dulles Corner Park, Suite 800, Herndon, VA 20171

Main: 800.262.4358 | eFax: 703.709.8450

dlt.com