

## Chapter 2

# Information Fusion: Intelligence Centers and Intelligence Analysis

Victor Catano and Jeffery Gauger

**Abstract** September 11, 2001, marked a major turning point for domestic and international information sharing among militaries and civilian security services. The U.S. Department of Defense, for one, transformed itself from a Cold War fighting force to one tailored to fighting global terrorism and terror-sponsoring regimes. The international character of terrorism required new information technology and new sources of information. The variety and volume of information also required an organizational structure to overcome the compartmentalization of intelligence. Fusion centers became the solution. This chapter summarizes the existing literature on information and intelligence fusion in both civilian and military fusion centers. It recounts the development of civilian fusion centers intended to deal with domestic terrorist threats and examines how the concept has been applied in military organizations. The paper reviews different models that have been used to develop fusion centers.

**Keywords** Information fusion • Fusion centres • Military intelligence

## Introduction

Militaries have always recognized the need for superior intelligence. Operational success depends on the ability to integrate information about the battlespace and enemy forces. Until the late twentieth century, intelligence came primarily from human sources, with the strength of the information being based on the credibility

---

V. Catano (✉)  
Department of Psychology, Saint Mary's University,  
923 Robie St., Halifax, NS B3H 3C3, Canada  
e-mail: Vic.Catano@smu.ca

J. Gauger  
Director Research Personnel Generation (DRPG 3-4),  
Department of National Defence, Ottawa, ON K1A 0K2, Canada  
e-mail: Jeffery.Gauger@forces.gc.ca

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence 2017

I. Goldenberg, J. Soeters and W.H. Dean (eds.), *Information Sharing in Military Operations*, Advanced Sciences and Technologies for Security Applications, DOI 10.1007/978-3-319-42819-2\_2

of the source. Aerial reconnaissance and satellite technology were big Cold War advances in intelligence gathering. By today's standards, the information and sources of information were limited, but they did draw a picture of the adversary's social, political, and economic strengths and weaknesses (Whitfield 2012). A good illustration is the Cuban Missile Crisis where aerial reconnaissance identified what appeared to be Russian missile silos on Cuban territory. The only analysis involved correctly identifying the images and then assessing the threat.

Over the last few decades, however, both the sources and quantity of information have expanded exponentially. Information now comes from radio, television, media, the internet, electronic signals, cell phones, satellites, and unmanned aerial vehicles. The sheer quantity of information can undermine accurate interpretation of the data or cause crucial intelligence to go unobserved (Chizek 2003).

In response to the information glut, militaries have increasingly used technology to collect and integrate mapping, reconnaissance and surveillance, and aerial photography. In addition, massive databanks now exist where data mining reveals crucial information hidden among the noise. These advancements have increased the amount and the rate at which information is gathered. Nonetheless, commanders must still rely on their human personnel to quickly and accurately gather and synthesize raw data (from numerous intelligence, surveillance, and reconnaissance [ISR] platforms) into a format that will provide the commander with a detailed yet succinct overview of the environment. This process of synthesizing complex information has become known as intelligence or information fusion.

One factor complicating information fusion is that much of the information relevant to a synthesis is developed in "silos," meaning within discrete agencies or among different units within or across agencies (Chizek 2003). Not only is there a large number of organizations involved in information gathering (both at the micro and macro levels), but these agencies tend to be possessive of "their" information and can be slow to share it. Clark (2013) argues that collectors, analysts, and intelligence organizations see few benefits of sharing information and have more incentives for concealment, in spite of the consequences. One reason for the success of the 9/11 terrorist attacks was the failure of law enforcement and the intelligence community to share information with one another (National Commission on Terrorist Attacks Upon the United States 2004; Whitfield 2012). Similarly, the report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005) found that collectors and analysts of intelligence failed to act as a team and did not share information effectively. Clark (2013) reviews other significant intelligence failures attributable to a failure to share information. In addition to 9/11 and the pursuit of weapons of mass destruction in Iraq, he cites the intelligence failures that occurred in Great Britain's invasion of the Falkland Islands in 1982 and Israel's Yom Kippur War in 1973.

At any rate, the events of 9/11 served as a turning point for information gathering and sharing, dividing traditional from contemporary approaches. The U.S. Department of Defense (DoD) undertook a major alteration in its capabilities, from a force designed to fight the Cold War to one tailored to fight twenty-first century adversaries and terrorism and to adapt to the use of improved technology, especially

information technology (Chizek 2003). One major initiative has been to overcome compartmentalizing information into silos through fusion centers. In this paper we review the concept of information fusion and the fusion center as a process for synthesizing technical and human information resources into a form that allows commanders to make informed decisions.

## Defining Information Fusion<sup>1</sup>

Information fusion generally denotes an applied field concerned with combining data from multiple sources in support of decision making. Traditionally, fusion focused on electronically combining online sensor data. More recently, information fusion has evolved to include other sources, such as databases, simulations, the internet, text documents, and human intelligence. Intelligence fusion technologies can now provide information for decision making without human intervention. There is no single method of information fusion that applies to all situations, so there is no single definition of it. U.S. military doctrine defines intelligence fusion as the process of collecting and examining information from all available sources and intelligence disciplines to derive a complete assessment of detected activity. It relies on an all-source approach to intelligence collection and analysis (Connable 2012). Boström et al. (2007) provide reviews of several definitions of intelligence fusion. We developed the following operational definition of intelligence fusion based on human-user involvement, as opposed to machine or computational fusion, which does not involve a human operator:

Information fusion is the transformation by a human operator of information from different sources and from different times into a representation that provides effective support for human decision making. The overall goal is to combine the multiple sources of data into information that has greater benefit to the decision maker than would have been derived from each source separately.

As Nilsson et al. (2012) note, information fusion has traditionally conceived the human user as a passive recipient of information fused by computers. Because our definition emphasizes the fusion of information by human analysts, however, the definition intentionally excludes automatic or semi-automatic integration of information by machines or computers. The human operator still integrates computer data as part of the fusion process, and computer inputs are a valuable part of the process, but our intent is to explore what the human analyst does with the information.<sup>2</sup>

---

<sup>1</sup>*Information fusion* and *intelligence fusion* are used interchangeably in both the military and civilian literature. In this chapter we will use *information fusion* to include *intelligence fusion*. Intelligence is defined in the U.S. military as information and knowledge obtained through observation, investigation, analysis, or understanding. Surveillance is systematic observation and reconnaissance in a mission designed to obtain specific information (Chizek 2003).

<sup>2</sup>Note, however, that there is a paucity of research on the active role of humans in processing fused information (Nilsson et al. 2012).

## Origins of the Concept

Information fusion predates 9/11. It began with local and regional initiatives to combat crime, drug trafficking, and terrorism (Carter and Carter 2009), where the intent was to cross-reference information from several agencies that had jurisdiction over the specified problem in a geographic area. Carter and Carter (2009) trace the origins of these initiatives back to the development of regional High Intensity Drug Trafficking Area (HIDTA) intelligence centers, products of counterdrug initiatives. The HIDTA centers involved federal, state, and local partnerships to develop analytical expertise that could be provided to the operational commands. The HIDTAs were successful in fighting the war on drugs because their multiagency organizational structure concentrated on the mission and not higher policy goals. The concept was not conducive to fighting local crime that involved only one jurisdiction. Nonetheless, the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives did use the concept to identify gun trafficking, often co-locating with HIDTA centers. Although the intent was to integrate information from various sources to understand and prevent multijurisdictional crime, there was little incentive to expand the centers until the events of 9/11 (Carter and Carter (2009).

The following sections review the development of civil fusion centers within police forces and other security agencies. This is followed by a review of military fusion centers in NATO and in the U.S. military.

## Civilian Policing and Security

The HIDTA intelligence centers showed promise in fighting crime that cut across several jurisdictions and agencies. HIDTAs were used as a model to defend against terrorism. The U.S. Department of Homeland Security funded the establishment of such centers at the state and local levels with the purpose of overcoming the effects of “stovepiping,” where different agencies collected intelligence information but did not share or cross-reference their data with other agencies (Carter 2007). These regional centers have proliferated to the extent that the Department of Homeland Security and the Department of Justice now coordinate the centers to identify the resources needed to support and integrate information across the centers (General Accountability Office 2007).

There are several formats for information sharing, but many U.S. agencies have adopted the format used by the Los Angeles Terrorist Early Warning Group (TEW; Carter and Carter 2009), which has the following functions:

The Los Angeles TEW includes analysts from local, state and federal agencies to produce a range of intelligence products at all phases of response (pre-, trans-, and post-attack) specifically tailored to the user’s operational role and requirements. The TEW bridges criminal and operational intelligence to support strategic and tactical users. As part of this process, the TEW seeks to identify emerging threats and provide early warning by

integrating inputs and analysis from a multidisciplinary, interagency team. Toward this end, the TEW has developed a local network of Terrorism Liaison Officers at law enforcement, fire, and health agencies, formed partnerships with the private sector to understand threats to critical infrastructure, and has developed and refined processes to analyze and synthesize threat data to support its client agencies (Sullivan 2005, p. 1)

A TEW is usually organized into six cells: command, analysis–synthesis, consequence management, investigative liaison, epidemiological intelligence, and forensic intelligence support. The analysis–synthesis cell is responsible for coordinating activities and providing actionable intelligence to the command cell. The lower level cells, below command, are responsible for actively acquiring information from citizen reports, local police, and the internet. Raw data from many different inputs are shared among members of the TEW, and then analyzed and synthesized into an output that is presented to the command and shared with other potential users of that information.

In Canada, police and security agencies developed models similar to the TEW and fusion centers in response to terrorism threats directed at major international events, such as the Vancouver Olympics and the Toronto G8/G20 summits. In 2003, police and security agencies created integrated security units (ISU) to centralize intelligence functions. The ISUs were composed of representatives from municipal, regional, and provincial police departments, the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), and the Canadian Armed Forces (CAF; Monaghan and Walby 2012). The ISUs were also tasked with coordinating security with international allies and with issuing “threat assessments” of major events taking place in Canada. The initial intelligence functions were carried out by joint intelligence groups (JIGs) but later the ISU tasked the Integrated Threat Assessment Centre (ITAC) with centralizing all national security-related intelligence distribution and coordination. ITAC is an anti-terror intelligence hub within CSIS, which includes representatives of the RCMP, the CAF, and various federal departments (Monaghan and Walby 2012).

## Civilian Fusion Centers

The TEW is a model for current U.S. civilian fusion centers, which are defined as follows:

A collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity. The intelligence component of a fusion center focuses on the intelligence process, where information is collected, integrated, evaluated, analyzed, and disseminated. Non-traditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information that can be “fused” with law enforcement data to provide meaningful information and intelligence about threats and criminal activity (Global Intelligence Working Group 2005, p. 8)

Fusion centers were designed to manage the flow of information and intelligence across different levels and sectors of government and, at times, the private sector, and to integrate that information for analysis (Carter and Carter 2009). They are designed to promote information sharing among various federal, state, and local police and security agencies. Their purpose is to identify threats and stop them before they occur (Monahan 2009).

Fusion centers are staffed by representatives from the different supporting agencies that compose the center, with each liaison responsible for the input of raw data from their agency and the transmission of synthesized information back to the liaison's home agency. Fusion centers are normally located in an office supplied by one of the member agencies. The analysts working at the center are normally drawn from the Department of Homeland Security, local police, and the private sector. A number of fusion centers operate tip hotlines and also invite relevant information from public employees, such as sanitation workers and firefighters (Monahan and Palmer 2009).

O\*NET (2015) states that civilian intelligence analysts gather, analyze, and evaluate information from a variety of sources, such as law enforcement databases, surveillance, intelligence networks, and geographic information systems, and then use these data to anticipate and prevent organized crime activities and terrorism. They engage in a number of tasks directly related to these activities. Most prominent among these are the following:

- Validate known intelligence with data from other sources.
- Gather, analyze, correlate, and evaluate information from a variety of resources, such as law enforcement databases.
- Prepare comprehensive written reports, presentations, maps, and charts based on research, collection, and analysis of intelligence data.
- Study activities related to narcotics, money laundering, gangs, auto-theft rings, terrorism, or other national security threats.
- Collaborate with representatives from other government and intelligence organizations to share information and coordinate intelligence activities (O\*NET 2015).

## Criticisms of Civilian Fusion Centers

Civilian fusion centers have received a lot of scrutiny and some criticism. Monahan and Palmer (2009), for example, argue that they are relatively ineffective at identifying terrorist threats, that the information they collect can be used for secondary purposes, and that they are a risk to civil liberties. These criticisms reflect findings made public in various reports, and they were echoed by Newkirk (2010), who also argued that the fusion centers' data mining and murky lines of authority rendered them unaccountable to the public and, hence, a threat to democracy. Taylor and Russell (2012) attributed the failure of fusion centers to the structure and mission of

law enforcement agencies and to their characteristic traits, such as autonomy and “interagency ego.” Taylor and Russell also argued that local police agencies were ill-equipped to take on the roles, strategies, and techniques inherent in military and federal law enforcement. The following sections elaborate on these criticisms.

In the United States, the Senate Homeland Security Permanent Subcommittee on Investigations came to the conclusion that fusion centers were ineffective (Smith 2012). The Senate report stated that fusion centers frequently produced shoddy reports that were rarely timely and that in some cases violated civil liberties or privacy and often had little to do with terrorism. The subcommittee reviewed data from over 70 fusion centers between April 1, 2009 and April 30, 2010 and did not find one instance where a center had uncovered a terrorist plot or terrorist threat. Rittgers (2011) reports instances where members of the public who had voiced contrarian views or who belonged to certain groups were identified as threats to national security:

The North Texas Fusion System labeled Muslim lobbyists as a potential threat; a DHS analyst in Wisconsin thought both pro- and anti-abortion activists were worrisome; a Pennsylvania homeland security contractor watched environmental activists, Tea Party groups, and a Second Amendment rally; the Maryland State Police put anti-death penalty and anti-war activists in a federal terrorism database; a fusion center in Missouri thought that all third-party voters and Ron Paul supporters were a threat; and the Department of Homeland Security described half of the American political spectrum as “right wing extremists.”

The American Civil Liberties Union (ACLU) issued a report in 2007 that argued fusion centers presented a threat to the privacy and civil liberties of Americans. The ACLU argued that the participation of agencies from multiple jurisdictions in fusion centers created ambiguous lines of authority and allowed authorities to manipulate differences in federal, state, and local laws to maximize information collection while evading accountability and oversight—a practice called policy shopping. Furthermore, the secrecy under which fusion centers operated limited public oversight, impaired centers’ ability to acquire essential information, and impeded their ability to fulfill their stated mission, all of which brought the value of fusion centers into doubt. The ACLU also raised questions over privacy, arguing that the inclusion of private corporations into the intelligence process destroyed the arm’s length relationship between the corporation and government that protected the privacy of the corporation’s employees and customers. The ACLU was also concerned that the civilian fusion centers involved military personnel in law enforcement activities, leading to the militarization of policing (ACLU 2007).

Suffice it to say that government and other officials have taken issue with these criticisms. They argue that the various reports have failed to consider relevant data, misunderstood the role of the federal government in the process of supporting information fusion, and overlooked the significant benefits of fusion centers for local, state, and federal law enforcement agencies. Carter and Carter (2009) note that fusion centers have evolved over time and that there is now more concern with civil rights. They point out that privacy and civil rights issues are the same for any other aspect of information gathering related to intelligence. Fusion centers, as a consequence of the criticism leveled at them, now have components related to civil

right policy, training, supervision, and public information. Carter and Carter (2009) argue that fusion centers hold great promise for effective intelligence gathering across jurisdictional boundaries. To do so, fusion centers must stay on message as an analytic center to support efficient, effective, and lawful intelligence operations. They further noted that, as part of its evolution, the fusion center personnel are learning and developing best practices to protect citizens from foreign and domestic threats while observing the rights of those citizens they are protecting.

While these criticisms may have validity with respect to civilian policing and security forces, they are not relevant to information fusion within a military organization because the intent of military information fusion is along the lines presented by Connable (2012). Connable notes that the primary purpose of information fusion in the military is to support the decision-making process of military commanders, who shape the intelligence-collection process as much as, or perhaps more than, the military intelligence leadership. Persson (2013) provides a more positive view of fusion centers. She reviewed the lessons learned from the experiences of 11 counties that had established civilian fusion centers at the national level. Those lessons are equally applicable to military fusion centers. In her report to the Swedish National Defence College, she identified a number of common issues that should be considered in establishing or operating a fusion center: To be successful and to obtain community support, fusion centers had to have an accepted and established purpose. They had to have the trust of the community along with that of stakeholders and government agencies, particularly the agencies involved in the center. The right personnel are crucial to the center's success. Staff should be co-located at the center and have significant experience and expertise to make critical assessments of information. Centers have to have access to information from the different agencies participating in the center. Increasingly, these national fusion centers are involved in multilateral international cooperation and coordinating their work on the basis of national needs in dealing with serious terrorist attacks and threats. They had to be flexible with respect to the different types of intelligence and security structures needed to deal with emerging needs. Persson sees fusion centers as a key element in addressing global threats to a nation's security through establishing multilateral cooperation among both large and small nations. She notes the need for cooperation between intelligence and security forces, both domestic and foreign, to accurately assess threats based on domestic and foreign information.

## Models of Information Fusion

Over the years, more than 30 different models have been proposed for information fusion. The vast majority of these models are computational algorithms or human-computer models with little research devoted to the human operator. They have focused, primarily, on fusing data from physical sensors that address physical targets (Hall and Jordan 2010). Fewer models have been developed to explain the role of the fusion analyst within a fusion center. Only two of these models appear to



be very influential in informing military decision making: the Joint Directors of Laboratories (JDL) process model and the observe, orient, decide, and act (OODA) loop model. These models have a significant role for the human operator and have originated in research conducted by military organizations as a means of providing better information fusion for decision-making purposes.

## **The Joint Directors of Laboratories (JDL) Process Model**

The JDL was an administrative group that coordinated research across a number of U.S. DoD laboratories. The JDL created a technical subgroup to oversee multi-sensor research. The Office of Naval Intelligence first published the JDL model in 1991, with modifications being made over the years. The JDL model has been the most influential in forming research on information fusion (Hall and Jordan 2010). The modified model involves six stages of data collection and analysis, but human information analysts play a significant role only in the last two stages. Level 1 combines data from multiple sources to obtain the best estimate of an object's location, characteristics, and identity. Level 2 seeks to provide context for Level 1 processing by an assessment of the situation and its relation to objects and entities. Level 3 is an impact assessment and uses the results from the previous levels to project future threats based on the current state of intelligence. Level 4 is refinement of data acquisition and processing to support sensing objectives. At Level 5 the analyst fields requests for information and manages the data retrieved to support cognitive decision-making functions. At Level 6, the analyst determines spatiotemporal control of assets (e.g., airspace operations) and route planning and goal determination to support team decision making and actions (e.g., theatre operations) over social, economic, and political constraints. That is, Level 6 involves command execution based on analysis of information obtained at the lower stages. It is not only making a decision about the best way to proceed, but also how to implement an action based on those decisions. Hall and Jordan (2010) summarized the limitations of the JDL model. The most glaring is the limited involvement of the human operator, from the lack of human observers at the first level, to difficulty in linking human information needs to sensor control at Level 4, to failure to consider how human analysts make decisions at Level 5. Criticism of the original model led to greater incorporation of human decision making into the modified model; however, the role of the human operator in the modified JDL model is still minimal although greater than in the original conception.

## **Observe, Orient, Decide, Act (OODA) Loop**

The OODA model was developed in the mid-1950s by Boyd (1987). It was based on observing effective decision making among military commanders. Specifically, it was proposed as an explanation of why U.S. Air Force pilots in F-86 Sabre jets

were successful against technologically superior MIG-15 aircraft (Bryant 2006). The model was an intuitive exercise that was never intended to explain decision making in complex situations. Nonetheless, the OODA loop has had immense influence on NATO militaries. The OODA loop distinguishes between information gathering (observe, orient) and implementation (decide, act). The model also highlights the roles that time constraints and uncertainty play in decision making (Bryant 2006). Observations are expected to lead to an orientation that allows faster decision making and then action on the decision. The OODA loop is a framework of command decision making with a goal of affirming the decision cycle and impairing that of the enemy. It is a framework for human decision making and embedded in the doctrine of several military forces (Bryant 2006). It is a structured analytic technique that forces analysts to externalize their thought processes and divides the analysis into logical steps. The analytical team “sees” each step and the connections between steps (e.g., data and inference) and comes to more logical conclusions.

Bryant (2006) notes several flaws in this model. He criticizes it for being a reactive rather than proactive model that waits for facts to emerge from observations, which the OODA model suggests is an unbiased process. Breton and Rousseau (2005) argue that the model has led to a conception that understanding of the battlespace solely develops from gathered data and that decision making becomes a function of acquiring more data. A number of revisions have been proposed to the OODA model, but they have failed to gain traction among the fusion community, and the original model is still commonly used (Nilsson et al. 2012).

Although the model is an analytical tool, it has a heavily data-driven orientation that ignores top-down, or executive, cognitive processes that are used in making sense of perceptions. An overarching criticism of fusion models is that they do not place enough emphasis on cognitive processes, such as goal-directed cognition, constructive theories of perception and understanding, mental models, and critical thinking. The model does not take sufficient account of the necessary dependence of perception on preexisting knowledge and concepts. This failure has led to the OODA model being seen as a “bottom-up” process that creates understanding in the battlespace solely from gathered data (Bryant 2006). There have been a few attempts, with modest success, to address this problem (Hall and Jordan 2010). Breton and Rousseau (2005), among others, sought to include aspects of the user’s cognitive processes into the OODA loop; these models are generally termed C-OODA, with the C-signaling that the model contains an explication of cognition.

## C-OODA

Breton and Rousseau (2005) examined the four modules of the OODA model in a military command and control environment. They modified the OODA loop so that each module was represented as a generic module structured around three components: process, state, and control. Their modification also allowed for bi-directional

data flow between modules and a feedback loop within each module, which provided a basic architecture for modeling a variety of team decision making with the OODA loop. Essentially, the C-OODA model divides up the decision-making cycle. Control is based on the time available for decision making as well as the level of uncertainty in the situation. If uncertainty is high and time short, the cognitive processing is stopped. Blasch, Breton, Valin, and Bosse (2011) argued that C-OODA offered a “high level of cognitive granularity” and detailed criteria-based control modules that include both time and uncertainty factors as part of cognitive processing. Although these C-OODA models recognize the important contribution of cognition, these models do not explicate the role played by cognitive functions, such as selective attention, perception, memory, and comprehension in intelligence fusion.

## Military Information Fusion Centers

Decision makers, including operational commanders, need to be informed by all-source, fused intelligence. The end is to provide decision makers with “the best possible holistic expression of an inherently complex environment based on all available, collectable, and relevant information” (Connable 2012, p. 3). To provide the best possible information to decision makers, including commanders, both the NATO alliance and the U.S. military have established fusion centers to share information, such as the U.S. European Command Joint Analysis Center (JAC) and Joint Information Centers (JIC). Other militaries rely on intelligence analysts; however, the Mexican military recently announced that it would develop both regional and national fusion centers (Guevara 2014, September). Several different models of fusion center operations have been used by different militaries; however, we look at fusion centers that NATO, the U.S. Army, and the U.S. Air Force currently use to collect and share vital information about possible security threats.

Military fusion centers integrate military specialists and civilians as intelligence analysts. Military intelligence analysts are typically trained in several areas, including imagery analysis, signals intelligence, and operational intelligence. An intelligence analyst collects, analyzes, and disseminates intelligence, which is collected from multiple sources, including aerial and satellite imagery and foreign communications. They collect, collate, and evaluate the vast amount of information used in useable and actionable intelligence reports and threat assessments. They assist with the production of current operational intelligence reports and briefings. The intelligence analyst is often the person at the front, assisting the senior commander in making key decisions on aspects of a military operation. Intelligence analysts work with data obtained from reconnaissance and surveillance systems from all sources that produce imagery using electro-optical, radar, and infrared sensors, including satellite and unmanned aerial vehicles. The reports produced by intelligence analysts are distributed to domestic national agencies, allies, and NATO. Analysts also carry out extensive background research to ensure the accuracy of reports.

## **The NATO Intelligence Fusion Centre**

The NATO Intelligence Fusion Centre (NIFC) is located in the United Kingdom and became fully operational in 2007. Its mission is to facilitate the sharing of information and the fusion of intelligence gaps to enable the planning and execution of NATO operations. Its vision is to have a professional, adaptable, technologically competent, and operationally focused intelligence organization that delivers timely, relevant products that enhance NATO's situational awareness and operational effectiveness. The NIFC comprises over 200 multinational military and civilian intelligence and support professionals from 26 of 28 NATO nations and one North Atlantic Council approved non-NATO nation. This workforce is experienced and culturally diverse and is able to support decision making for senior leaders through well-informed, insightful analysis. The NIFC provides a unique environment where participating nations join forces to fuse intelligence for the common good of the alliance and in direct support of NATO operations. The NIFC strives to encourage analysis collaboration. It works with national analysis centers, academia, think tanks, and relevant international and private organizations to develop a deep understanding of key intelligence issues (NATO Information Fusion Centre 2015, June). The center provides around-the-clock (four shifts) all-source strategic and tactical theater intelligence (ASAS) that incorporates geospatial, air defense, and targeting data. The fusion center is staffed by both military and civilian personnel whose general duties follow those of a military intelligence analyst. It responds to requests for information from all U.S. and NATO commands and points to gaps in intelligence and recommends improved intelligence processing. It also supports electronic battle plans, cyber-defense and cyberattack planning at the tactical and technological levels. It is particularly focused on the Middle East, South Asia, and Northern Africa (Korkisch 2010).

## **The U.S. Joint Analysis Center (JAC)**

The U.S. European Command Joint Analysis Center is co-located with the NIFC at RAF Molesworth in the UK. It is a joint intelligence center (JIC) that processes, analyzes, and consolidates data to produce fused intelligence information focusing on an area of responsibility covering 77 countries across Europe, Africa, and the Middle East. The JAC supports mission planning and operations by U.S., allied, and NATO commanders during peace, crises, and war. Although it provides information analysis to NATO allies and coalition forces, the JAC is staffed solely by U.S. personnel. Military commanders and decision makers at all levels rely on data produced at the JAC. The JAC is the principal element for ensuring effective intelligence support for combatant commanders in chief and theater forces. Support is provided by all-source, fused, timely, and predictive intelligence (Mackrell 1997).

## Joint Intelligence Centers (JICs)

Joint intelligence centers (JICs) are fusion centers that act as the primary intelligence organization during joint warfighting at all levels. The Joint Analysis Center described above is one example of a JIC. The JIC concept fuses the main support capabilities of service, combat support agency, and combat units in one support center. The JIC is designed to be scalable and can expand to meet the needs of the joint force commander. During non-crisis periods, JICs operate at the minimum manning level required to perform their essential functions, such as intelligence and warning, current intelligence, collection management, delegated general military intelligence production, and support to the commander. As crises develop, the JIC brings together the personnel and equipment needed to manage intelligence support requirements. A JIC is a focal point for military intelligence gathered by different intelligence agencies and administered by the Defense Intelligence Agency.

JICs are responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. JICs exist at the national, regional, and local levels. The focus of each is the fusion of intelligence information in support of military commanders. For example, the Joint Intelligence Center Pacific (JICPAC) provides direct intelligence support for all forces assigned to the Commander in Chief, U.S. Pacific (CINCUSPAC). The JICPAC operates a fusion center, which conducts current situation analysis, collection management, and long-range assessments and threat estimates. JICPAC is responsible for a variety of intelligence products and processes. Some are immediate while others require many months or even years to produce. Fusion of all-source intelligence and defining analytical approaches allow JICPAC to provide seamless, timely intelligence to U.S. Pacific Command decision makers. JICPAC personnel disseminate their products, briefings, annotated situation maps, installation descriptions, pictures, and threat projections to command customers at all levels from the headquarters to deployed units and ships at sea. JICs have performed this fusion function historically and are well-structured to do so in the future, incorporating traditional and non-traditional intelligence sources and analytical expertise (Marchio [2008](#)).

## Air Force Joint Battlespace Info-Sphere

Apart from its own JICs, the U.S. Air Force operates the Air Force Office of Scientific Research (AFOSR), located at Wright-Patterson Air Force Base. The AFOSR program in information fusion addresses fundamental issues in the ways that information can be best combined and used to support decision making and the evaluation of decision outcome (Tangney [2002](#)). These programs are based on information technology that is in line with building the joint battlespace info-sphere (JBI) and do not examine the role of the human operator within the system (Linderman et al. [2006](#)).

The JBI defines a future combat information management system that creates and maintains a common operating picture for decision support at multiple echelons. Much of the technical infrastructure of the JBI is built around the collection, organization, and aggregation of information. The JBI concept allows “customers” to interact with JBI meta-databases through a publish-or-subscribe system. It is a technological interface between the data and the user of that data, who accesses the data on a need-to-know basis. As such, the JBI manages information and is not a true information-fusion center as defined in this report.

## **Criticism of U.S. Military’s Fusion Centers**

U.S. Major General Flynn, in his role as the Deputy Chief of Staff Intelligence created Stability Operations Information Centers (SOIC) outside of regional command fusion centers. The SOICs were created in response to his and others’ criticisms of existing military intelligence integration (Flynn et al. 2010). Flynn et al. (2010) quoted General Stanley McChrystal as saying, “Our senior leaders—the Chairman of the Joint Chiefs of Staff, the Secretary of Defense, Congress, the President of the United States—are not getting the right information to make decisions....The media is driving the issues. We need to build a process from the sensor all the way to the political decision makers.” Flynn et al. (2010) argued that the U.S. intelligence apparatus was unable to answer fundamental questions about the environment in which the military operates and the people it is trying to protect and save. They believed that while personnel in the field were well informed, they were not able to share information and that no one was looking at reports by civil affairs officers, Afghan soldiers, UN officials, and NGOs; that all attention was focused on information regarding insurgencies while intelligence regarding the local political, economic, and cultural climate was often ignored. They also held that information obtained at the grassroots level was not reaching high-level analysts in the U.S. Information was not being shared between NGOs, allies, civilians and military, despite willingness to share unclassified information.

The SOICs were established to rectify the criticisms leveled at the regional intelligence centers. Each SOIC focused on analyzing the local population, economic and development issues, and, to a lesser extent, the host-nation government. Flynn et al. (2010) developed a blueprint for commanders, intelligence professionals in Afghanistan, and the U.S. and Europe to make information more effective. While that blueprint is drawn from a counterinsurgency operation on the ground in Afghanistan, it does have wider applicability with respect to information fusion.

Flynn et al. (2010) proposed that SOICs should empower select teams of analysts to move between field elements, much like journalists, to visit collectors of information at the grassroots level and to carry that information back to the regional command level. These teams would then integrate the grassroots information with that collected by civil affairs officers, provincial reconstruction teams, atmospherics

teams, Afghan liaison officers, female engagement teams, willing non-governmental organizations and development organizations, United Nations officials, psychological operations teams, human terrain teams, and infantry battalions, to name a few. These analysts would divide their work along geographical lines, instead of along functional lines, and write comprehensive district assessments covering governance, development, and stability, instead of having all analysts study an entire province or region through the lens of a narrow, functional line. The analysts would then provide their data to teams of “information brokers” at the regional command level who would organize and disseminate the reports and data gathered at the grassroots level. In some cases, the SOIC would replace the regional centers, in other cases cooperate with them. The role of leadership was to staff the SOICs with the best analysts.

Connable (2012) expressed similar views in that the people involved in information fusion were more concerned with interpreting information from their own disciplinary viewpoint than with integrating that information into a holistic analysis. He argues that the “system of systems” approach used to identify physical and material factors as part of an institutional analysis development framework simplifies people and groups to ease the system-mapping process and that the simplicity undermines information fidelity. The analysts’ training causes them to separate political, military, geographic, and economic systems and to analyze each in isolation. As well, fusion center staffs were simply more comfortable working from traditional information analysis perspectives. Connable makes this criticism of military fusion centers:

The absence of a holistic vision or approach throughout the early and middle stages of the analytic process tends to harden thinking, arguably creating another type of path dependency in which analysts are driven to offer a narrow and incompletely informed set of options to commanders. Sometimes, a fusion officer can compensate, at least to a degree, for the lack of a holistic approach across the intelligence fusion center. The job of the fusion officer is somewhat self-explanatory (to fuse analyses), but in practice, he or she often serves as the senior analyst and the arbiter of analytic debates on the intelligence floor. Because they have the last say on analytic findings before analytic reports are sent up the chain of command, talented and willful intelligence fusion officers can do much to integrate analyses before they reach the commander. But reliance on a single individual, or even a small team, to integrate what may be a widely diffused analytic picture is an uncertain and haphazard solution—and less desirable than a comprehensive solution to the problem of red, white, and green integration (Connable 2012, p. 17).

Connable (2012) further argued that anyone working in a fusion center who is contributing to analysis—for the purposes of targeting, collection, or obtaining a holistic analytic picture—should be trained to view people and groups as intrinsically complex, nuanced, and predominantly as “targets” for a spectrum of kinetic and non-kinetic command options. The fusion analysts would use common tools such as social network analysis and advanced human factors analysis, but targeting would become an all-analyst, all-source, fused process.

## Conclusion

Intelligence or information fusion centers were created by law enforcement and militaries to facilitate and foster information sharing within and between organizations—that is, to break down communication silos to allow commanding officers to make the best decision possible based on all the relevant information. Although civilian versions are somewhat controversial, military fusion centers have been less so. There are several different models of fusion center operations that have been used by different military agencies. We have briefly illustrated the fusion centers used by NATO and the U.S. Army and Air Force to gather and share information. Basically, all fusion centers work in some way with issues regarding terrorism. Some centers makes strategic threat assessments while others work with operational assessments. Fusion centers have staff from various agencies co-located at particular locations. All rely on both technology and human personnel for integration of information (Persson 2013). In a world where countries are globally dependent on politics, economics, trade, and crisis management, international cooperation with respect to intelligence and security structures is ever more vital. Fusion centers are a valid mechanism for insuring that information does not simply stay in the hands of one agency. While they may not be the perfect way of ensuring information sharing, they are preferable to the alternative, which is dealing with information in isolation and not seeing the overall landscape.

## References

- American Civil Liberties Union. (2007). What's wrong with fusion centers? Retrieved from <https://www.aclu.org/technology-and-liberty/whats-wrong-fusion-centers-executive-summary>
- Blasch, E., Breton, R., Valin, P., & Bosse, E. (2011). *User information decision-making analysis in the C-OODA model*. Paper presented at the 14th International Conference on Information Fusion, Chicago, IL.
- Boström, H., Andler, S. F., Brohede, M., Johansson, R., Karlsson, A., van Laere, J., et al. (2007). *On the definition of information fusion as a field of research (Research report HS-IKI-TR-07-006)*. Skovde, Sweden: University of Skovde.
- Boyd, J. R. (1987). *A discourse on winning and losing* [Briefing slides] (Document No. M-U 43947). Maxwell Air Force Base, AL: Air University Library.
- Breton, R., & Rousseau, R. (2005). *The C-OODA: A cognitive version of the OODA loop to represent C<sup>2</sup> activities*. Paper presented at the 10th International Command and Control Research and Technology Symposium: The Future of C<sup>2</sup>, McLean, VA.
- Bryant, D. J. (2006). Rethinking OODA: Toward a modern cognitive framework of command decision making. *Military Psychology*, 18(3), 183–206. doi:10.1207/s15327876mp1803\_1.
- Carter, D. (2007). *The intelligence fusion process for state, local and tribal law enforcement*. Intelligence Program School of Criminal Justice Michigan State University [White paper]. Retrieved from <http://www.cops.usdoj.gov/files/ric/CDROMs/LEIntelGuide/pubs/IntelligenceFusionProcessWhitePaperv3.5.pdf>
- Carter, D. L., & Carter, J. G. (2009). The intelligence fusion process for state, local and tribal law enforcement. *Criminal Justice and Behavior*, 36(12), 1323–1339. doi:10.1177/0093854809345674.



- Chizek, J. G. (2003). *Military transformation: Intelligence, surveillance and reconnaissance: Report for congress*. Washington, DC: Congressional Research Service Library of Congress.
- Clark, R. M. (2013). *Intelligence analysis* (4th ed.). Los Angeles: Sage.
- Connable, B. (2012). *Military intelligence fusion for complex operations: A new paradigm*. Arlington, VA: Rand Corporation.
- Flynn, M. T., Pottinger, M. F., & Batchelor, P. D. (2010). *Fixing intel: A blueprint for making intelligence relevant in Afghanistan*. Washington DC: Center for a New American Security. Retrieved from [http://www.cnas.org/files/documents/publications/AfghanIntel\\_Flynn\\_Jan2010\\_code507\\_voices.pdf](http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf)
- General Accountability Office. (2007). *Homeland security: Federal efforts are helping alleviate some challenges encountered by state and local fusion centers* (No. GAO-08-35). Washington, DC: Author.
- Global Intelligence Working Group. (2005). *Guidelines for establishing and operating fusion centers at the local, state, tribal and federal level*. Washington, DC: U.S. Department of Homeland Security.
- Guavara, I. (2014, September 3). Mexican military details intelligence capabilities, new fusion centres. *Jane's Defence Weekly*. Retrieved from <http://www.janes.com/article/42787/mexican-military-details-intelligence-capabilities-new-fusion-centres>
- Hall, D. L., & Jordan, J. M. (2010). *Human-centered information fusion*. Norwood, MA: Artech House.
- Korkisch, F. W. (2010). *NATO gets better intelligence (strategy paper 1-2010)*. Vienna: Institut fur Aussen-und Sicherheitspolitik.
- Linderman, M., Combs, V. T., Hillman, R. G., Muccio, M. T., & McKeel, R. W. (2006). *Joint battlespace infosphere (jbi): Information management in a netcentric environment (Report Number AFRL-IF-RS-TR-2006-178)*. Rome, NY: Air Force Research Laboratory/IFSE.
- Mackrell, E. (1997). Combined forces support: The evolution in military (intelligence) affairs. *NATO Review*, 45, 20–25. Retrieved from <http://www.nato.int/docu/review/1997/9706-06.htm>
- Marchio, J. D. (2008). *The evolution and relevance of joint intelligence centers: Support to military operations*. Retrieved from [https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html\\_files/the\\_evolution\\_6.html](https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/the_evolution_6.html)
- Monaghan, J., & Walby, K. (2012). Making up “terror identities”: Security intelligence, Canada’s integrated threat assessment centre and social movement suppression. *Policing and Society: An International Journal of Research and Policy*, 22(2), 133–151. doi:10.1080/10439463.2011.605131.
- Monahan, T. (2009). The murky world of fusion centers. *Criminal Justice Matters*, 75(1), 20–21. Retrieved from <http://torinmonahan.com/papers/FC-CJM.pdf>
- Monahan, T., & Palmer, N. A. (2009). The emerging politics of DHS fusion centers. *Security Dialogue*, 40(6), 617–636.
- National Commission on Terrorist Attacks Upon the United States. (2004). *9/11 Commission Report*. Retrieved from <http://govinfo.library.unt.edu/911/report/index.htm>
- NATO Information Fusion Center (2015) [Website]. Retrieved from <http://web.ifc.bices.org/index.htm>
- Newkirk, A. (2010). The rise of the fusion-intelligence complex: A critique of political surveillance after 9/11. *Surveillance & Society*, 8(1), 43–60.
- Nilsson, M., van Laere, J., Susi, T., & Ziemke, T. (2012). Information fusion in practice: A distributed cognition perspective on the active role of users. *Information Fusion*, 13(1), 60–78. doi:10.1016/j.inffus.2011.01.005.
- O\*NET (2015, June). *Intelligence analyst*. Retrieved from <http://www.onetonline.org/link/summary/33-3021.06>
- Persson, G. (2013). *Fusion centres—Lessons learned: A study of coordination functions for intelligence and security services*. Stockholm: Swedish National Defence College.
- Rittgers, D. (2011). *We’re all terrorists now*. Cato Institute. Retrieved from <http://web.archive.org/web/20110415064139/http://www.cato-at-liberty.org/we’re-all-terrorists-now/>

- Smith, R. J. (2012). Senate report says national intelligence fusion centers have been useless. *Foreign Policy*. Retrieved from [www.foreignpolicy.com/articles/2012/10/03/senate\\_report\\_says\\_national\\_intelligence\\_fusion\\_centers\\_have\\_been\\_useless](http://www.foreignpolicy.com/articles/2012/10/03/senate_report_says_national_intelligence_fusion_centers_have_been_useless)
- Sullivan, J. P. (2005). *Terrorism early warning and co-production of counterterrorism intelligence*. Paper presented at the Canadian Association of Security and Intelligence Studies, Montreal, Quebec, Canada.
- Tangney, J. F. (2002). *AFOSR programs in higher levels of information fusion*. Arlington, VA: Directorate of Mathematics and Space Sciences Air Force Office of Scientific Research.
- Taylor, R. W., & Russell, A. L. (2012). The failure of police “fusion” centers and the concept of a national intelligence sharing plan. *Police Practice and Research*, 13, 184–200. doi:[10.1080/15614263.2011.581448](https://doi.org/10.1080/15614263.2011.581448)
- The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. (2005). *Report to the President*. Retrieved from [http://fas.org/irp/offdocs/wmd\\_report.pdf](http://fas.org/irp/offdocs/wmd_report.pdf)
- Whitfield, C. L. (2012). *Intelligence fusion paradigm: Understanding complex operational environments implementing the institutional analysis and development framework* (Unpublished master’s thesis, U.S. Army Command and General Staff College).

Information Sharing in Military Operations

Goldenberg, I.; Soeters, J.; Dean, W.H. (Eds.)

2017, XIV, 274 p. 11 illus., 4 illus. in color., Hardcover

ISBN: 978-3-319-42817-8