Small Wars Journal

www.smallwarsjournal.com

The Frontiers of Global Security Intelligence: Analytical Tradecraft and Education as Drivers for Intelligence Reform

John P. Sullivan

Global security intelligence is an emerging need. Changes in technology, societal organization, and the security challenges and arrangements within and among states demand novel approaches and structures to ensure human security. Terrorism, insurgency, and transnational crime challenge traditional security and intelligence structures. In this 'not crime-not war' operational environment, non-state actors, transnational criminal enterprises, gangs, warlords, terrorist and insurgent networks, and private armies intersect with traditional state organs and emerging elements of civil society. New security structures and legal regimes are potentially evolving, yet traditional structures are slow to adapt. This paper will explore the emergence of networked security structures, and new ways to approach intelligence (including the open source intelligence movement, terrorism early warning, and the co-production of intelligence), together with the role of research, analytical tradecraft, and education as potential drivers of intelligence reform.

Globalization, technology, transnational threats, and shifts in societal organization demand new approaches and structures for achieving security and developing intelligence to support operational and policy requirements. As such, global security intelligence is an emerging need. Terrorism, insurgency, and transnational crime are threats that are driving the current and future conflict environment.[i] These individual—and increasingly linked—threats result in a diffuse security environment that is neither crime nor war. Non-state actors: transnational criminal organizations, gangs, warlords, private armies, terrorist and insurgent networks on the dark side and private military or security corporations, global corporations, civil society, NGOs, and evolving state, sub-state, and supra-state institutions on the bright side demand the development of new security and intelligence structures to ensure global stability and human security.[ii] Networks are an important element of this environment as is the flow of information in real-time through modern digital technology to empower all of the aforementioned actors. This paper discusses the role and evolution of networked intelligence approaches—including open source intelligence (OSINT), terrorism early warning, and the need for co-production of intelligence. In addition, this paper briefly discusses the role of research, analytical tradecraft, and education as drivers of intelligence reform.

Understanding the Need for Intelligence Reform

Intelligence is essential to formulating sound policy and responses (strategic, operational, and tactical). In short, "the first task of any intelligence organization is to establish where danger lies."[iii] The intelligence 'organizations' needed to address the global

threats of terrorism and strategic crime must embrace new approaches and support a wider range of decision-makers than traditional intelligence entities. After all, strategic crime is characterized by "the combined lawlessness of organized crime, drug trafficking, and terrorism of a quantity and quality that threatens a range of security interests of a state."[iv] Combating these threats is the focus of what Thomas calls America's 'new intelligence war.'[v] In reality, this is not solely America's war, it more than a war or conflict, and it involves all of the world's governmental and corporate security services. Nevertheless, the demands of intelligence in war apply. As John Keegan points out, for intelligence to be useful it must involve five fundamental stages: 1) acquisition; 2) delivery; 3) acceptance; 4) interpretation; and 5) implementation.[vi]

The public and professional understanding of intelligence and its role is frequently defined by failures of intelligence. Intelligence failures—such as the failure of the US Army or Naval intelligence structures to provide adequate warning and prevent the attack on Pearl Harbor by the Japanese and the failure of the contemporary US intelligence and law enforcement communities to predict al-Qaeda's synchronized 9-11 attacks on the World Trade Center and Pentagon—justifiably lead to questions about the definition and role of intelligence in a democratic society. They also provide the backdrop for public and parliamentary discussions about the proper organizational architecture for intelligence services in war and peace.

The Central Intelligence Agency (CIA) and its constellation of supporting—and sometimes competing—agencies in the US intelligence community were formed to correct the situation that led to Pearl Harbor. The Department of Homeland Security and Director of National Intelligence (DNI) were established to correct the intelligence failures that are believed to have led to 9/11.[vii] We can expect new structures to continue to evolve to address the threat and lack of understanding of our current terrorist and criminal adversaries. Despite an understanding that intelligence must evolve, a lack of a basic understanding of the definition, nature and need for intelligence pervades the halls of government, and is endemic among police and public safety personnel and, ultimately, among the public for whom intelligence serves as a protection. What, in fact, is intelligence? Is it merely the province of secret agents, conducting espionage against foreign governments? Is it information to support decision-making? Or is it some combination of those elements and much more?

Not surprisingly, many views about the nature and utility of intelligence color this debate. We know, at least collectively, that deception and surprise are closely related to intelligence matters. We also know that uncertainty complicates our understanding of conflict in general and terrorism in specific. Fog (unclear circumstances), friction (obstacles to action) and noise (too much information) are familiar to all decision-makers and commanders who seek to make good decisions in war and crisis. The 'smog' of terrorism complicates action against terrorists due to its ambiguous and diffuse political nature.

"Know the enemy, know your self; your victory will never be endangered. " *Sun Tzu*[viii]

Knowing an enemy's (or opposing force's) capabilities and intentions is the foundation of intelligence. To gain this knowledge, a variety of intelligence disciplines are involved.

All seek to discern several essential elements of information for a commander, decision-maker or end user. These typically involve weather, enemy, tactics and threat. It is not enough to know the adversary alone; knowledge of our own capabilities and needs helps define information requirements and place potential threats into an operational context.

"By 'intelligence' we mean every sort of information about the enemy and his country– the basis in short, of our own plans and operations." *Clausewitz*[ix]

Much like the observation that there are several English 'languages' and, as the rest of this collection demonstrates, there are different 'terrorisms,' there are also different forms of intelligence—'intelligences.' Understanding and properly utilizing these intelligences will help address the information requirements for combating global terrorism. The first distinction is between foreign and domestic intelligence. This is particularly important as it limits or bounds the activity of intelligence agencies or practitioners.

This distinction is based in the experience of conflict among states and is designed to preserve liberties of citizens within a state and limit the abuse of secret information as a form a state coercion of its own residents. In the US this is seen in the separation of the CIA's intelligence operations from the internal security and law enforcement functions of the Federal Bureau of Investigation (FBI) and state and local police agencies concerned with criminal intelligence. The same distinctions are seen in the UK's Secret Intelligence Service (SIS) and Security Service and police special branches.

As terrorists frequently operate transnationally and globally as non-state actors, the need to coordinate foreign and domestic operations becomes important to prevent terrorist acts. The distinction between law enforcement and intelligence is derived from these crucial liberty considerations. As a result, police, who often have contact with potential terrorists, are blind to threats on their own 'beat.' Consequently, much criminal intelligence is tactically-based investigative support lacking strategic context. A balanced approach that also preserves liberties is also essential for long-term legitimacy.

Classical human intelligence (either overt or covert) known as HUMINT is another important variety of intelligence. In the recent past, however, forms of technical intelligence (*techint*) known by a number of acronyms (*imint* for imagery intelligence, *sigint* for signals intelligence, etc.) have taken front stage in western intelligence services. Sophisticated tools, super computers, intelligent software for processing information, sensors, and high-resolution satellite imagery (now commercially available along with a plethora of data-mining tools and geo-spatial information systems for terrain and data fusion) have predominated. Intelligence in its classic form—that of actionable secret information derived from human sources—became scarce.

"Secret operations are essential in war; upon them the army relies to make its every move…An army without secret intelligence is exactly like a man without eyes or ears." *Sun Tzu*[x]

HUMINT is especially important in discerning terrorist threats, since technical means are a poor indicator of terrorist capabilities and an especially poor indicator of terrorist intentions. Understanding why, when and how a group may choose to attack requires

knowledge of the human and cultural dimension, an understanding of ideas. This understanding can only be gained effectively by information obtained from people in the streets, homes and social circles of terrorist actors and their supporters—classic espionage and liaison, conducted in partnership and through alliances with police and intelligence services worldwide.

Classical human intelligence gathering is not, however, the only element needed to understand terrorism and emerging threats. All of the technical means, plus others such as open source intelligence (OSINT), *e.g.*, media reportage and public documents, and *cyberint* (novel means of exploiting the Internet, information grid and cyber means such as data-mining and fusion) are equally important. As is incorporating disease surveillance (epidemiological intelligence: *epi-intel*) and consequence management intelligence to understand the interaction between threat, vulnerability and risk and develop appropriate response plans for civil protection. Together these disciplines can provide indications and warning, an understanding of trends and potentials, and an assessment of capabilities and intentions to provide viable net assessment for leaders.

Co-Production of Intelligence & The 'TEW' Model

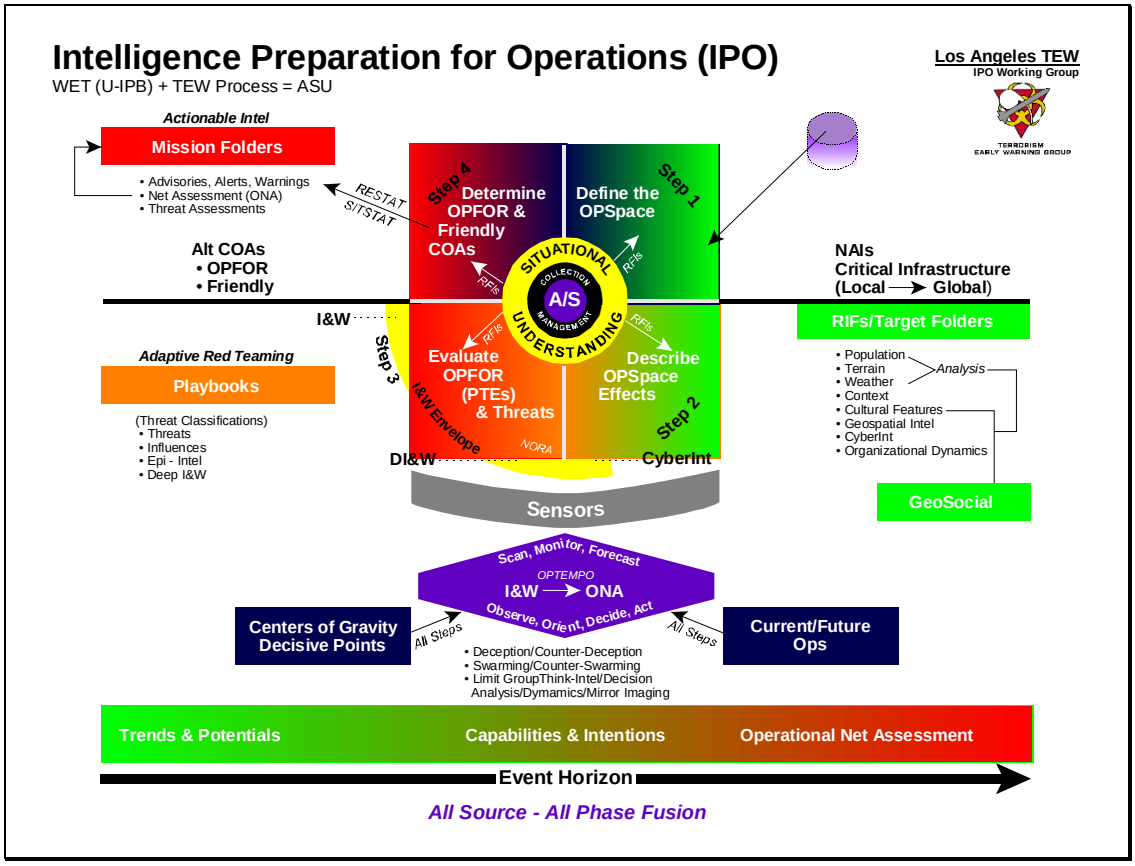
Essentially all intelligence seeks to inform policy or decision. Strategic intelligence is as discussed above in light of Sun Tzu knowledge of the enemy. Keegan shares this view.[xi] Achieving the understanding necessary to decide requires analysis and synthesis of data, ideas, concepts, actions, and intentions and then placing them in context. When facing a range of diverse and diffuse adversaries this is a problematic task requiring the collection and analysis of accurate, timely, and pertinent information. Since terrorists and criminals operate globally within interlocking networks, a networked approach to both intelligence collection (acquisition of data) and analysis/synthesis (interpretation of data) is essential for both current and emerging threats.

One novel approach to developing a networked predictive intelligence analysis capacity is the Terrorism Early Warning group (TEW) concept that emerged in Los Angeles in 1996. The Los Angeles TEW brought together local, sate, and federal law enforcement, fire, and health analysts together with their private sector counterparts to develop counterterrorism intelligence products for the Los Angeles region. In doing so, the TEW embraced open source intelligence (OSINT)[xii] and collaborative analysis and assessment. As the LA TEW's model and approaches to analysis were replicated at other jurisdictions, the various TEW nodes started to participate in distributed analysis and production of intelligence leading to recognition of the potential value for intelligence co-production.[xiii] Two analytical approaches utilized within TEWs are Intelligence Preparation for Operations (IPO) and the Transaction Analysis Cycle.

Intelligence Preparation for Operations (IPO)

Intelligence preparation for operations (IPO) is a civil analog to the military's intelligence preparation of the battlefield (IPB). IPO is designed to serve response information needs and can form the foundation for public-private interaction to develop the intelligence products needed to address complex networked threats.[xiv] IPO provides a standard tool set for situational recognition, course-of-action development, and

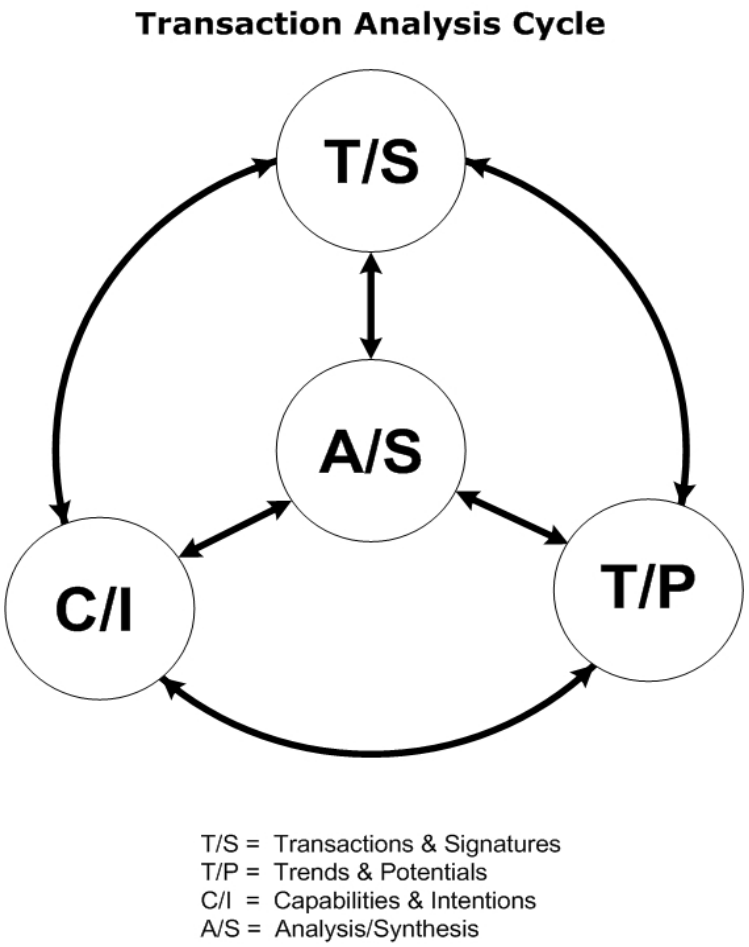
response rehearsal. This process bridges the gap between deliberate planning and crisis action planning for all facets of a unified multi-organizational response organization. The IPO framework is depicted in the diagram below.



Transaction Analysis Cycle

Terrorist activity plays itself out over time, which can be expressed in a linear fashion as an event horizon, or in a non-linear fashion. The 'Transaction Analysis Cycle' developed by Sullivan is a non-linear analytical approach for discerning terrorist activity within dynamic and diffuse data sets laden with noise and masked by a fog of uncertainty. Individual transactions (such as acquiring finances, expertise, acquiring materiel, munitions or capability, recruiting members, conducting reconnaissance, mission rehearsal, conducting an attack, etc.) have signatures that identify them as terrorist or criminal acts, or consistent with the operations of a specific cell or group. These transactions and signatures (T/S) can then be observed and matched with patterns of activity that can be expressed as trends and potentials (T/P), which can ultimately be assessed in terms of a specific actor's capabilities and intentions (C/I). At any point, the analytical team can posit a hypothesis on the pattern of activity and then develop a collection plan to seek specific transaction and signatures that confirm or disprove its hypothesis. The transaction analysis cycle provides a common framework for assessing patterns, hypotheses and social network links among a range of actors within a broad spatial and temporal context, making co-production of intelligence and situational understanding viable.

These approaches provide an alternative to traditional military bureaucratic intelligence and can provide a foundation of praxis for a new theory of intelligence for global security.[xv] Intelligence analysis is a foundational element of intelligence writ large. Hauer describes the steps needed to improve analysis itself, as well as the requirements for creating an organizational environment where analytical excellence can flourish. These are research, training, exposure to alternative mind-sets, and guiding analytical products.[xvi] Utilizing OSINT as a core component of intelligence production will ensure the real-time access to information necessary for innovation and creativity in the analytical process. Reshaping the intelligence community and the decision-makers it serves requires new analytical approaches and tradecraft, and the development of theory and model to support intelligence for the current and emerging geosocial environment. Analytical tradecraft and education in its use can thus become important drivers of intelligence reform.



Conclusion

Virtually all agree that timely, accurate, reliable and actionable intelligence is essential. To achieve that charge is often extremely complicated. Essentially, intelligence provides understanding. Sherman Kent, the Yale-educated theoretician and practitioner of the early US intelligence community, would have termed this 'knowledge,' a knowledge

based on an effective relationship between intelligence and its users. As Kent (an OSS veteran who shaped the early CIA and Cold War intelligence practices) noted, there is a need to evolve an understanding of intelligence.[xvii] Kent viewed intelligence as an analytical discipline that resulted in 'all-source' analysis. As a consequence, collection and all source assessment led to a finished product that supports decision-makers. In his view, intelligence production was more than raw collection, but included the collection, evaluation, analysis, integration and interpretation of all available information to support planning and operations. His view serves as good guidance for negotiating current and future threats. We must also remember that classical human intelligence is a vital piece of this puzzle, one that can't be purged in favor of technical means, however attractive and risk neutral they may initially appear.

As we addressed the Cold War Threat, an understanding of the capabilities and intentions of our adversaries was pursued and, largely if sometimes imperfectly, gained. Yet during the Cold War, Soviet 'capabilities' not 'intentions' were decisive to Western understanding of the threat. As we enter into what appears to be the decisive conflict of the twenty-first century, a conflict against terrorists and networked global insurgents, we find a pressing need to understand *Jihadi* 'intentions'—a sharp contrast to the frequently predictable adversary of the past.

Combating terrorism and strategic crime is the decisive conflict of our time. To succeed we will need to recognize that this conflict is largely an intelligence war. Clandestine and covert services working together with other elements of government such as the military and police will likely be at the cutting edge of domestic and international efforts to contain terrorism and forge domestic and foreign policy and response. To do so, many factors must be balanced. These include balancing foreign and domestic, the 'push' and 'pull' of intelligence to users, the demand for an immediate 'scoop' vs. strategically relevant product, the tension between criminal and intelligence investigations, the balance between sharing and security and, finally, the most important element: the balance between intrusive protection and liberty.

We are at the frontier of this intelligence war. Like Sherman Kent at the formation of the US intelligence community, we must start the dialog to build the craft, discipline and knowledge necessary to evolve an understanding of intelligence for the conflict of our time. The sooner we resolve these issues and define intelligence for combating post-modern, networked adversaries, the sooner we can thwart the threat and preserve the liberties of Americans and other persons of good will worldwide.

John P. Sullivan is a lieutenant with the Los Angeles Sheriff's Department. He is also a researcher focusing on terrorism, conflict disaster, intelligence studies, and urban operations. He is co-founder of the Los Angeles Terrorism Early Warning (TEW) Group and co-editor of Countering Terrorism and WMD: Creating a global counter-terrorism network (Routledge, 2006).

References

[i] See John P. Sullivan. "Public-Private Intelligence Models for Responding to the Privatization of Violence," paper presented to Intelligence Studies Section of the International Studies Association (ISA*), 2007 ISA Annual Convention*, Chicago, Illinois, 28-Februray-3 March 2007 (isa07_proceeding_181284.pdf) as a complement to this paper. Also see Robert J. Bunker (Ed.) *Non-State Threats and Future Wars*, London: Frank Cass, 2003 and Robert J. Bunker (ed.) *Networks, Terrorism and Global Insurgency*, London: Routledge, 2005 for a detailed discussion of the global threat environment.

[ii] John P. Sullivan, "Fusing Terrorism Security and Response," in Peter Katona, Michael D. Intriligator, and John P. Sullivan (Eds.), *Countering Terrorism and WMD: Creating a global counter-terrorism network*, London: Routledge, 2006, pp. 272-288.

[iii] Thomas Powers, *Intelligence Wars: American Secret History from Hitler to Al-Qaeda*, New York: New York Review Books, 2002, p. 381.

[iv] Douglas Menarchik, "Organizing to Combat 21st Century Terrorism," in James M. Smith and William C. Thomas (Eds.), *The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors*, Colorado Springs, CO: USAF Academy, 2001, p. 259.

[v] See Powers, note 3, Chapter 24: "America's New Intelligence War," pp. 381-420.

[vi] John Keegan, *Intelligence in War*, New York: Alfred A. Knopf, 2003, pp. 5-6.

[vii] For a general discussion of strategic failure in general see Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War*, New York: Vintage Books, 1991. For a discussion of Pearl Harbor see Gordon W. Prange with Donald M. Goldstein and Katherine V. Dillon, *Pearl Harbor: The Verdict of History*, New York: McGraw Hill, 1986. The intelligence failure related to the 9/11 attacks is discussed in *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Authorized Edition), New York: W.W. Norton & Co. (no date).

[viii] Sun Tzu (trans. Samuel B. Griffith, *Sun Tzu, The Art of War*, New York: Oxford University Press, 1971, p. 129.

[ix] Carl von Clausewitz (ed. and trans. Sir Michael Howard and Peter Paret), *On War*, Princeton, NJ: Princeton University Press, 1984. p. 117.

[x] *Sun Tzu, The Art of War*, p. 149.

[xi] See Keegan, note 6, pp. 7-25.

[xii] For a discussion of the role and utility of open sources versus secret information see Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, London: Cambridge University Press, 2003, pp. 8-13. Treverton also discusses the role of intelligence in the emerging 'market-state' at pp. 54-56.

[xiii] See John P. Sullivan. "Public-Private Intelligence Models for Responding to the Privatization of Violence," note 1 and "Terrorism Early Warning and Co-production of Counterterrorism Intelligence," paper presented to Canadian Association for Intelligence and Security Studies, CASIS 20th Anniversary Conference, Montreal, Quebec, Canada, 21 October 2005.

[xiv] See John P. Sullivan, Hal Kempfer, and Jamison Jo Medby, "Understanding Consequences in Urban Operations: Intelligence Preparation for Operations, *INTSUM Magazine*, Marine Corps intelligence Association, Vol. XV, Issue 5, Summer 2005, pp. 11-19 for an in depth discussion of IPO.

[xv] For a discussion of the development of a contemporary theory of intelligence see Gregory F. Treverton, Seth G. Jones, Steven Boraz, and Phillip Lipscy *Toward a Theory of Intelligence: Workshop Report*, Santa Monica: RAND, 2006. Treverton himself provides an excellent overview of the transition of intelligence from the Cold War to the Information Age see Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, London: Cambridge University Press, 2003 in its entirety. The need for a global security network is articulated in Peter Katona, Michael D. Intriligator, and John P. Sullivan (Eds.), *Countering Terrorism and WMD: Creating a global counter-terrorism network*, London: Routledge, 2006.

[xvi] Richards J. Heuer, Jr., Chapter 14: "Improving Intelligence Analysis," in *Psychology of Intelligence Analysis*, Langley, VA: Center for the Study of Intelligence, Central Intelligence Agency, 1999, pdf version found on line at https://www.cia.gov/csi/books/19104/index.html.

[xvii] Sherman Kent is pivotal to the understanding of US national intelligence practices. See especially: Sherman Kent, "The Need for an Intelligence Literature," *Studies in Intelligence*, Vol. 1, No. 1 (September 1955), pp. 1-8.