The New Great Game: Military, Police and Strategic Intelligence for Global Security

John P. Sullivan

Los Angeles Sheriff's Department, Emergency Operations Bureau

Published online: 03 Aug 2011.

To cite this article: John P. Sullivan (2007) The New Great Game: Military, Police and Strategic Intelligence for Global Security, Journal of Policing, Intelligence and Counter Terrorism, 2:2, 15-29, DOI: 10.1080/18335300.2007.9686895

To link to this article: http://dx.doi.org/10.1080/18335300.2007.9686895

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at http://www.tandfonline.com/page/terms-and-conditions
The New Great Game: Military, Police and Strategic Intelligence for Global Security

JOHN P. SULLIVAN
Emergency Operations Bureau
Los Angeles Sheriff’s Department

ABSTRACT

Intelligence and counter terrorism are key elements of the contemporary global security environment. Profound changes in the nature of states fuelled by globalization, information technology, and the influence of non-state actors are changing the structure and dynamics of intelligence. A range of global threats and conditions influence the contemporary global security and intelligence stage. These include global insurgency and terrorism (as seen in the Salafist jihadi struggle with the West), the rise of global business and civil society, global political movements, transnational organized crime, the rise of global cities, networked diasporas, global disease, and the prospect of planet-wide climate change. Yet, while all players in this new ‘Great Game’ recognize that intelligence is essential to situational understanding, few have the institutional structure, experience, and understanding of the various types of intelligence necessary to negotiate the current and emerging security environment. This article will review the threats and conditions influencing global security environment, and discuss the roles of military, police, and strategic intelligence in understanding this environment.

Introduction

During the nineteenth century Great Britain and Russia engaged in a shadow competition focused along the Raj’s North-West Frontier. Dominance of trade and lines of communication, along with geopolitical advantage were the goal. This first ‘Cold War’ was the pivotal conflict of the first wave of globalization. This ‘Great Game’ was primarily an intelligence war punctuated by small wars and police actions, espionage, diplomacy, and influence, intelligence – including ‘The Great Survey of India’ a forerunner of today’s geospatial intelligence (Ferguson, 2002).
Today’s security environment has triggered a ‘New Great Game’ where military, police, and strategic intelligence are essential elements of ensuring global security.

The changing nature of states is altering the nature of threats and the intelligence needs of both states and non-state actors. Globalization and new global security threats (both military and non-military) present novel challenges to individual and collective human security. Within this framework, non-state actors (both benign: civil society; and malign: criminals, third generation gangs, terrorists, pirates) are becoming more important than nation-states. Examples of this include ‘global cities’, lawless zones, and the growing importance of networked diasporas. This article discusses security threats, non-state actors, and the need to develop a global intelligence framework to address planet-wide security issues. Within this discussion, the differences, interplay and relationships among military, police, and strategic intelligence will be analyzed. Meta-analysis and the co-production of intelligence will be described as new ways of developing the intelligence needed to ensure global security. In conclusion, the article assesses global security networks and the need to balance collaboration and competition between traditional state-centred and global approaches.

**Changing nature of states and intelligence needs**

To start with the obvious: states are changing (Bobbit, 2002; Van Creveld, 1999). Technology and globalization are key drivers in this shift. Since states have been the primary instrument of international security since the Peace of Westphalia in 1648, a shift in state form and arrangement necessitates new security structures and new intelligence approaches to serve them (Treverton, 2003). As Robert Delahunty and John Yoo (2007, p. 28) observe,

as the nation-state declines, transnational terrorist networks rise; as nationalism recedes, tribalism and violent religious extremism take its place. Failed or dysfunctional states often become breeding grounds for civil wars, genocide and other atrocities, terrorism, famine and the spread of lethal diseases.

These challenges are likely to drive intelligence structures and processes into the future. Among the factors challenging law enforcement and intelligence agencies, and government at large, is the emergence of transnational networked actors on both the domestic and world stage. This situation is a result of the shift from the ‘nation-state’ as the dominant state form to what Philip Bobitt calls the ‘market-state.’ Bobbit (2002) postulates that this change is the latest of a series of changes in
state form. He posits that the result of the Long War (WWI, WWII, and the Cold War) set the stage for the transition to the market-state, which appears, at least for now, to be dominated by a new long war formerly known as the Global War on Terrorism (GWOT). Thus, a shift in international order, constitutional foundation(s), war-making, and security structures is under way. National security is morphing into global security. Market actors will play a bigger role in this era.

Failures of governance in the face of this epochal shift lead to state failure and the emergence of lawless zones. This in turn fuels conflict and a reordering of the state system. This shift creates new spaces for the privatization of security and violence: private military firms or corporations as well as gangsters, insurgents or warlords. Bobbitt (2002, pp. 820-821) observes that Osama bin Laden’s Al Qaeda is a malignant and mutated version of the market-state. As such, Al Qaeda and its kin are more than stateless gangs. These new networked adversaries possess standing armies, treasury and revenue sources (even if derived from criminal enterprises), a bureaucracy or ‘civil’ service, intelligence collection and analysis organs, welfare systems, and the ability to make alliances (with state and non-state entities). They also promulgate law and policy, and declare war. As such, the Al Qaeda network and others like it are virtual states – although they sometimes hold and control territory through insurgency and terrorism.

Intelligence to understand and anticipate threats in a global networked environment requires new types of information among a larger variety of players. Intelligence for this setting must inform not only policy makers and states, but also police and public safety organizations at all levels of government, private sector actors, such as corporations, as well as international organizations. Intelligence is more about early warning, strategic foresight, and real-time decision support for cooperative risk management than about gaining a secret advantage over a single state adversary.

**Impact of globalization and global security threats**

Globalization links the world and its political and economic structures. It also links people and provides an opportunity for local threats to spread and gain global reach. This is true for political activity and violence in all of its forms (terrorism, insurgency). This is also true for diseases, such as pandemics, and criminal threats, such as organized crime and complex transnational or third generation street gangs. Third generation street gangs are mercenary or terrorist in orientation. They are criminal gangs that operate with a high degree of sophistication, have political aspirations, and influence or operate in broader geographic or

Health situations and climate change can also serve as drivers for conflict. Disease itself can be a significant security threat. Consider the impact of a global pandemic, perhaps triggered when a highly pathogenic avian flu of the H5N1, or any range of other strains, mutates and spreads from city to city via global lines of commerce and travel (Davis, 2005). Famine, biological warfare and terrorism, and disease outbreaks can fuel inter-group conflict, stimulate violence and humanitarian crisis or disaster. Global connectivity through travel can spread the impact of disease planet-wide.

This leads to a new arena for security and warfare. According to Michael Vlahos (2006),

New war is simply one of the three sub-sets of war that all states have faced since, say, the Romans. There is war with states, there is war with unrecognized armed communities, and there is war against lawless elements, which the Romans called bagaudae (bandits) and which we call terrorists. The first is usually well-established and rule based, while the third is not usually even given the courtesy of being called a ‘war’. It is sort of a background tasking, an ongoing gendarmerie.

One component of this threat stream is the global Islamist jihad – essentially a global insurgency. According to David Kilcullen, Islamist movements operate in a cooperative manner among ‘theatres of operation’, where local groups gather intelligence and target data and share them across theatres within the global jihadi network, which is a loose confederation of independent movements and networks with varying local, regional, and global roles and reach. Killcullen observes that this movement is best viewed as an insurgency. Countering it “demands extremely close coordination and integration between and within police, intelligence, military, development, aid, information and administrative agencies”, a problematic task when applied at the global level (Kilcullen, 2005, p. 607).

Developing the intelligence needed for local police and public safety, health care organizations, global corporations, as well as traditional states and supranational organizations requires new structures. Intelligence is no longer only secret information provided to a military commander or head of state; it is timely and pertinent information about threats, communities, and interactions among various interests with disparate roles in order to make decisions at various levels by a range of actors. Increasingly, this information is derived from open source intelligence (OSINT) and requires situational awareness and strategic understanding.
of all geo-social factors that culminate in a threat, crisis, or activity. Threats include diseases, environmental factors, and threat actors. Threat actors still include the traditional state competitors (nations and armies), but increasingly include non-state actors. Intelligence for this emerging era requires knowledge of all of these dimensions and their interactions.

Benign and Malign non-state actors

Non-state actors have always played a role in global and subnational politics. Prior to the Westphalian Peace “the international system witnessed a broader diversity of forms of sovereignty, including city-states, empires and loose regional confederations – and overlapping religious or ethnic authorities, such as the Catholic Church” (Delahunty & Yoo, 2007, p. 10). Contemporary non-state actors include benign forces such as non-governmental organizations, humanitarian groups or civil society actors, as well as groups that privatize violence and challenge the state’s monopoly on force. Criminals, third generation gangs, terrorists, and pirates are examples of malign non-state actors. The nexus or potential for linkages among these actors is particularly worrisome. Examples can include: transnational organized crime groups that facilitate terrorists; third generation gangs such as maras that operate throughout the western hemisphere through the good offices of prison gangs; or pirates in the Straights of Malacca or in the waters off Africa joining with terrorists or insurgents. The confluence of these diverse threat actors leads to a situation much like classic irregular warfare where “an elusive enemy could control the strategic pace of the war, withdraw deep into the country and nullify the technological and firepower advantage [of conventional forces]” (Porch, 2006, p. 131).

This rise in violent non-state entities leads to diminished local capabilities for security. Police organized to address limited local crime issues are now faced with a range of criminal threats, including terrorism, transnational gangs and organized crime. These non-state entities operate across borders and local jurisdictions. They interact in a variety of ways cooperating with other criminal or terrorist enterprises to further their goals. These criminal enterprises use higher levels of violence, more sophisticated weapons, and exploit emerging information technology quicker than traditional security bureaucracies.

When combined with the global impact of many terrorist or transnational criminal acts, the challenge to the public monopoly on war and security – both internal and external – to individual states is enhanced. At the least this renders the distinction between foreign and domestic security (and intelligence) increasingly anachronistic. More likely, however, this will require a re-engineering of security and
intelligence structures and relationships to embrace networked forms and capabilities to navigate this global shift.

Michael Hardt and Antonio Negri (2004) describe this situation as a state of global war requiring global governance – an ‘empire’ ruled by the ‘multitude’. Within this broader analysis, where they see the current security situation as “a state of war in which network forces of imperial order face network enemies on all sides” (Hardt & Negri, 2004, p. 62), they emphasize the need for networked approaches to counter global insurgency. They note that the “networked form of power is the only one today able to create and maintain order” (Hardt & Negri, 2004, p. 59). Essentially, Hardt and Negri assert that networks are more agile than traditional hierarchies because they adapt to changing circumstances and disperse sensing and decision-making across the network’s nodes.

These dynamics were examined in the paper ‘Multilateral Counter-Insurgency Networks’, which noted:

Existing security structures (domestically the police, and internationally the military and foreign intelligence services) designed to counter state-on-state threats find this new operational environment challenging at best. Preserving global and national security requires traditional organs of national security (the diplomatic, military and intelligence services) to forge new partnerships with police and public safety organizations at the state and local (sub-national) level to effectively counter these threats. Significant operational, policy and cultural challenges must be overcome to forge an effective global network of public safety, law enforcement and traditional intelligence organizations to understand and anticipate current and evolving terrorist threats. (Sullivan & Bunker, 2002, p. 353-4)

Global cities, lawless zones and networked diasporas

New forms of social, political, and criminal opportunity are emerging from the influence of networks and technology on economic processes. Saskia Sassen describes the rise of ‘global cities’ in this context (Sassen, 2005). Sassen, a sociologist, observes that the flow of capital, labour, goods, and people – all cross-border economic transactions – have traditionally occurred within the context of an inter-state structure of nation-states. This has changed as the result of privatization, deregulation, transnational firms, and technology enabling the participation of national economic actors in the global market. The
redistribution of strategic economic territories, where national units are no longer the primary geospatial focus of transnational economic transactions, is the result. Non-state actors are the principal beneficiaries of this economic restructuring (Sassen, 2004). Cities, sub-national regions, cross-border hubs, trade blocs and supranational markets are among those impacted.

This geographic dispersal of economic activity that relies on activities geographically distributed among local, regional, and global nodes fuels the need for complex centralized corporate functions. These in turn stimulate the need for outsourcing to specialized firms that derive their personnel pool from the deep mix of talent, capability and expertise available in metropolitan areas that provide “an extremely intense and dense information loop” (Sassen, 2004, pp. 28-29). Individual firms develop a network of affiliates and partners to leverage these capabilities. Such global links strengthen transnational node-to-node interaction. As a result, cities become nodes in cross-border networks – in Sassen’s words, “a series of transnational networks of cities” (Sassen, 2004, p. 29).

As can be expected, the transnational network dynamics among ‘global cities’ and regions embrace a range of transactions and influence a broad range of activities: political, economic, cultural, social, and criminal. Interaction among immigrant and diaspora communities provides richness and context to communities, but when expectations to benefit from inclusion in the global community are thwarted or not realized, discontent can resonate globally (as in the case of Muslim youth attracted to the global Salafist jihad). The connectedness that results from cross-border networks increases social and political exchanges, including non-formal issue-specific transnational political networks focused on environmental and human rights issues among others. Sassen notes that these new ‘agoras’ or political spaces are “largely city-to-city cross-border networks”, since it is currently easier to capture “the existence and modalities of these networks at the city level. The same can be said for the new cross border criminal networks” (Sassen, 2004, p. 32).

The most pressing challenge is likely to involve global crime and terrorism. Generally, transnational organized crime groups benefited from the existence of a stable state order. While they exploited the seams between states, they did not seek to challenge the state; rather they exploited corruption and political influence to further their enterprises. This appears to be changing, as a new range of global gangsters creates parallel states to exploit the absence of effective states, endemic corruption, and grey or shadow economies (Shelley, 2005).

According to Louise Shelley, Director of American University’s Transnational Crime and Corruption Center, “the newer crime groups most often linked to terrorism have no interest in a secure state” (Shelley, 2005, p. 102). They promote and exploit grievances at local levels and
through the globalization of conflict to secure the maneuver room to capture profit. The embedded nature of network crime structures in local communities and the inability of both domestic and international militaries, as well as law enforcement agencies, to control their activities make these new criminal soldiers a growing danger. These terrorist-criminal interactions are particularly virulent in ‘global cities’ and sub-national or cross-border enclaves or ‘lawless zones’ (Sullivan & Bunker, 2003). The interactions of technology, networks, ‘global cities’ and non-state actors and enclaves set the stage for a discussion of state transition.

Criminal soldiers have altered the nature of crime and war, thereby altering the operational space within which police and security services function. As stated in the essay ‘Terrorism, Crime and Private Armies’,

Terrorists, criminal actors, and private armies of many stripes have altered the ecology of both crime and armed conflict. In many cases, the two are intertwined. Several factors reinforce these links. Global organized crime, which increasingly links local actors with their transnational counterparts, coupled with chronic warfare and insurgency (which yields economic benefits to some of its participants) can propel local or regional conflicts into genocidal humanitarian disasters. These regions, which are essentially criminal free-states, provide refuge and safe haven to terrorists, warlords, and criminal enterprises. (Sullivan, 2002, p. 241)

Lawless zones and criminal enclaves are areas (ranging from neighbourhoods, to regions, to states, and cross-border zones), where gangs, criminal enterprises, insurgents, or warlords dominate social life and erode the bonds of effective security and the rule of law (Sullivan & Bunker, 1998, 2003).

**Difference, interplay and relationships among military, police and strategic intelligence**

Intelligence is essential to framing decisions at all levels of government. Traditionally, intelligence has been viewed as a tool for understanding and shaping battle-space. Military intelligence is traditionally devoted to understanding weather, enemy and terrain to allow the commanding general to develop a concept of operations. This includes warning of potential attack by an adversary, and knowledge of the enemies’ order of battle and intentions. Police and law enforcement also utilize intelligence to further their efforts to investigate and prosecute crime. Law enforcement intelligence tends to be largely reactive and case-focused looking to identity criminal actors and their relationships
within one case or conspiracy. Strategic intelligence looks to the future to anticipate emerging threats and trends that influence grand policy. Usually, these individual streams of intelligence operate separately within bureaucratic stovepipes. Understanding the scope and disposition of networked adversaries of different types across global space while masked within the noise of society’s many legitimate transactions requires interaction and new relationships among these traditional intelligence silos.

Bringing together these different approaches to intelligence is essential to addressing the current and emerging threat environment. Modern threats impact military, police, and strategic ‘policy’ activities. Intelligence about a terrorist group or drug-trafficking organization operating abroad can inform law enforcement investigative and crime control activities locally. Both inform policy decisions at national levels. Tactical operations by local police can inform broader strategic warning and so on. As a result, formerly independent intelligence activities must be integrated to allow a range of users to make decisions at tactical, operational, and strategic levels for their own activities, as well as for activities within and across disciplines and organizational boundaries. Intelligence is potentially an enabler not only of cooperative decision-making, but also of effective interdisciplinary and inter-organizational cooperation and operations.

As noted in the paper, ‘Networked Force Structure and C4I’,

The rise of networks (and hence networked adversaries) results from the migration of power to non-state actors that are able to organize into multiorganizational networks (particularly ‘all-channel’ networks where every node is connected to every other node) more readily than hierarchical, state actors. As a result of this trend, network-based conflict and crime are a growing threat. As Ronfeldt, Arquilla and others [2001] have often noted, hierarchies have a difficult time fighting networks. Thus, to combat networks, that is to master counternetwar, the police, military and security services must first understand the nature of the networked threat, and then as described later forge the proper balance between networks and hierarchies to combat these emerging threats. (Sullivan, 2003, p. 145-6)

**Meta-analysis and co-production of intelligence**

One way to bridge the gaps in current practice is to foster the development of intelligence fusion and meta-analysis of potential intelligence of many types. Meta-analysis would bring together current
intelligence, warning intelligence, epidemiological intelligence, open source information, geospatial information, and cultural intelligence. It would then place the various feeds into context to anticipate future threats and form an understanding of the social networks and forces within and surrounding potential threats. Co-production of intelligence would allow individual nodes engaged in intelligence fusion and analysis to link in a distributed manner to address global scale threats.

The concept of intelligence ‘co-production’ emerged from the work of the Los Angeles Terrorism Early Warning Group (LA TEW). The LA TEW was established in 1996 bringing together 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. Several TEWs based on the LA model have been formed throughout the United States. The TEW concept integrates criminal and operational intelligence to support strategic, operational, and tactical users. As part of this process, TEWs seek to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team. Intelligence developed in this effort is derived from all potential sources (classified, sensitive but unclassified, and open sources) to provide information and decision support at all phases of a threat/response. Information needed to understand an event is available from local through global sources (Sullivan, 2005).

The immediate precursor for an attack may be in the local area, across the nation, in a foreign nation, in cyberspace, or in a combination of all. Identifying global distributed threats and achieving an understanding of their impact requires more than simple information sharing. It demands collaborative information fusion and the production of intelligence among cooperative nodes that are distributed among locations, where terrorists operate, plan, or seek to attack. For example, terrorists may plan their attack in the tribal frontiers of Afghanistan or Pakistan, while obtaining logistical and financial support in East Africa, South America and the Asia-Pacific. They may simultaneously conduct reconnaissance in their target city in North America or Europe, recruit and train operatives in Iraq, all the while receiving direction from another location all together.

Developing the intelligence needed to anticipate, prevent, disrupt, or mitigate the effects of an attack requires the production of intelligence in a collaborative and integrated endeavour by a number of agencies across this dispersed area. This is known as ‘co-production’ of intelligence. In essence, TEWs are designed to serve as a node in a counter-terrorist intelligence network. To achieve this local through global fusion, or co-production, the LA TEW developed an organizational structure and processes, including the Transaction Analysis Cycle (Sullivan, 2005), and embraces a networked framework for node-to-node collaboration.
The 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 (shown in Figure 1) is a non-linear analytical approach for discerning terrorist activity within noise-laden, dynamic and diffuse data sets masked by a fog of uncertainty. It emerged as a way to teach analysts how to interpret activity in order to assess leads and other inputs while developing iterative collection plans to identify patterns and define hypotheses about a potential terrorist ‘kill chain’ (i.e., a hypothesis about a projected terrorist attack plan and observable efforts required to execute a specific attack) or sequence of activities required to envision, prepare for and execute a terrorist attack. It is a pattern generator centred on the analysis/synthesis (A/S) function.

Figure 1: Transaction Analysis Cycle

![Figure 1: Transaction Analysis Cycle](source: Sullivan, 2005)

Utilizing this framework, analysts can observe activities or transactions conducted by a range of actors looking for indicators or precursors of terrorist or criminal activity of many types. Individual transactions (such as acquiring finances, material, weapons, munitions, expertise or capability, recruiting members, conducting reconnaissance, mission rehearsal, and an attack, etc.) have signatures that identify them...
as terrorist or criminal acts, or are 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). Ultimately, they can 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 transactions and signatures that confirm or disprove its hypothesis.

Analysis can start at any point to support the illumination of specific terrorist trends, potentials, capabilities or intentions. Individual transactions and signatures (such as tactics, techniques and procedures [TTPs] or terrorist statements) can be assessed through a tailored collection plan to assemble a notional terrorist ‘kill chain’ that can be disrupted, or an objective that can be protected by selection of appropriate friendly courses of action. Thus, the transaction analysis cycle becomes 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.

While the TEW model has demonstrated that networked fusion is possible, a number of challenges remain. First among these is organizational and bureaucratic competition. Networked forms compete with their hierarchical predecessors. Bureaucratic inertia slows down steps toward collaboration both within and especially across disciplines, jurisdictions, and nodes. Fiscal competition and struggles for intergovernmental primacy are additional complicating factors.

Co-production of intelligence to counter the evolving terrorist threat requires the development of multilateral structures. Much of the information necessary to understand the dynamics of a threat – indeed, even to recognize that a threat exists – is developed from bottom-up, as well as through horizontal (as opposed to top-down) structures. Multilateral exchanges of information, including indicators of potential attacks and alliances among networked criminal actors are needed to counter networked adversaries. This requires the development of new analytical tradecraft, processes, and policy. Intergovernmental instruments are needed to fully exploit lateral information sharing, along with the development of distributed intelligence processing across organizational and political seams. This includes the development of mechanisms for sharing information among both intra-national and international nodes.
Conclusion: Global security networks - collaboration and competition between national and global security

Managing the profound changes in the nature of states, the increased influence of non-state actors and global security threats requires the development of disaggregated structures for global security and governance. Within these structures, security and response will necessarily adapt to address global threats. The resulting structures will link law enforcement, criminal intelligence, national security intelligence, operational intelligence (including epidemiological intelligence) from public and private sectors within and among states and non-state organs to develop a networked approach to global security.

As John Arquilla and David Ronfeldt are frequently quoted, “it takes networks to fight networks” (Arquilla & Ronfeldt, 2001, p. 15). But networks are more than just a way of organizing criminal and terrorist conspiracies. Al Qaeda is a classic network, or network of networks, but as Anne-Marie Slaughter observes, we live in a “world of networks: of corporations, of nongovernmental organizations, of criminals, of government officials” (Slaughter, 2005, p. M2). Slaughter argues that networks are decentralized, informal, and flexible, relying upon regular interchange among participants. Like Ronfeldt, Arquilla, Bunker and Sullivan, she posits that nations can address networked threats by establishing networks of their own: global or regional networks of financial regulators, prosecutors, criminal investigators, immigration officials, transport officials and customs agents.

Slaughter notes that the emerging state form is likely to be a disaggregated state dominated by a new global landscape of government networks (Slaughter, 2004). The state has not disappeared but has morphed – or is morphing. This network will include horizontal government networks (characterized by peer-to-peer links with professional counterparts across borders) and less frequently vertical government networks between national government officials and their supranational counterparts (as seen in the International Criminal Court and the European Court of Human Rights) (Cooper, 2004; Slaughter, 2004).

Slaughter offers a typology of three types of networks: information, enforcement, and harmonization that can be arranged as horizontal, vertical, or disaggregated international organizations (Slaughter, 2004). Information networks are cooperative and frequently informal. Enforcement networks result from the inability of individual agencies to enforce the law. Harmonization networks are typically authorized by treaty or by executive agreement. All can be formal or informal. These
emerging forms of governance are fuelling the development of new forms of regional and global organization (within the rise of a system of ‘market-states’). Slaughter notes that judges are leading the networked quest for global jurisprudence; legislators are building a global parliamentary profession. Law enforcement is adopting inter-linking networks such as the Financial Action Task Force on money laundering (FATF) (Slaughter, 2004, p. 54) along with established groups such as Interpol and the TREVI group as enforcement networks (Slaughter, 2004, pp. 39-41).

These are examples of selective multilateral action. The FATF, which seeks to detect and prevent misuse of world financial systems by terrorists, is a noteworthy case. Europol and Eurojust are further examples. Europol links national police for broad analysis and threat assessments of terrorist and transnational criminals. Eurojust seeks to increase judicial cooperation and information exchange through direct contact among judges, an implicit recognition of the need for cross-border judicial relations to address transnational threats (Bensahel, 2003).

Bringing together the police, military, and national security agencies required to combat a global insurgency or global organized crime is a Herculean task in a single nation. Adding public health and public safety agencies, and private interest engaged in providing critical infrastructure functions and NGOs engaged in civil society and humanitarian relief adds further complexity. Linking these individual domains across national boundaries and political and ideological divides is complex and problematic at best. Yet, in order to effectively negotiate the continuing conflict horizon it must be done. National security interests compete with global security interests. Intelligence – as much as it prefers an advantage in the quest for power – will remain a competitive game. Despite this potential for competition and bureaucratic battles, common interest and the need for stability of global structures and networks require development of a networked intelligence capability to address global security threats. The rules of the ‘New Great Game’ make collaboration and co-production essential approaches within a distributed intelligence network for global security.

REFERENCES


Slaughter, A. (2005, April 25). We can beat terror at its own game: Networks are both the problem and solution. *Los Angeles Times*, p. M2.


