Strategy Research Project

# DARK NETWORKS

BY

LIEUTENANT COLONEL JOHN D. MANNING
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2010

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From - To)* |
|---|---|---|
| 23-02-2010 | Strategy Research Project | |

**4. TITLE AND SUBTITLE**

Dark Networks

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

Lieutenant Colonel John D. Manning

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Dr. Paul R. Kan
Department of National Security and Strategy

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Distribution A: Unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The world today operates in a state of persistent conflict on a sliding scale. The conflicts in question are not traditionally military in nature and often involve non-state actors. This provides problems for the nation-state due to the historical methods for dealing with conflicts. In order to manage these conflicts, nation-states and global organization will have to develop mechanisms to deal with "dark networks." These are networks made up of illicit traffickers, organized crime, urban gangs, terrorist, and other nefarious characters. The purpose of this paper is to examine the environment that feeds the dark networks, the characters making up the networks, the networks themselves, and the policy and strategy issues related to defeating dark networks.

**15. SUBJECT TERMS**

Crime, Terrorism, Persistent Conflict, Combatant Command

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | **19b. TELEPHONE NUMBER** *(include area code)* |
| UNCLASSIFED | UNCLASSIFED | UNCLASSIFED | UNLIMITED | 28 | |

USAWC STRATEGY RESEARCH PROJECT

# DARK NETWORKS

by

Lieutenant Colonel John D. Manning
United States Army

Dr. Paul R. Kan
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## ABSTRACT

AUTHOR: Lieutenant Colonel John D. Manning

TITLE: Dark Networks

FORMAT: Strategy Research Project

DATE: 23 February 2010 WORD COUNT: 5,048 PAGES: 28

KEY TERMS: Crime, Terrorism, Persistent Conflict, Combatant Command

CLASSIFICATION: Unclassified

The world today operates in a state of persistent conflict on a sliding scale. The conflicts in question are not traditionally military in nature and often involve non-state actors. This provides problems for the nation-state due to the historical methods for dealing with conflicts. In order to manage these conflicts, nation-states and global organization will have to develop mechanisms to deal with "dark networks." These are networks made up of illicit traffickers, organized crime, urban gangs, terrorist, and other nefarious characters. The purpose of this paper is to examine the environment that feeds the dark networks, the characters making up the networks, the networks themselves, and the policy and strategy issues related to defeating dark networks.

# DARK NETWORKS

> We're locked in the generational struggle against the global extremist network that is out to destroy our way of life. And as a result, I believe that the next decades that we face will be ones of what I call persistent conflict.
>
> —General George W. Casey Jr.[1]

"Dark Networks" are part of persistent conflict that the U.S. is facing today and will likely face in the foreseeable future. Unlike traditional wars fought between uniformed militaries over clearly understood goals, dark networks are comprised of a variety of nefarious individuals and organizations and contribute to persistent conflict by working against the common good and impacting man's ability to pursue a meaningful and fulfilling life. While the dark networks do not cause persistent conflict, the networks enhance the ability of the nefarious characters to act within the points along the scale of persistent conflict.

The conflicts of today and tomorrow occur in five strategic environment categories: demographic, health, and social; economic and financial; environment, infrastructure, and resources; governance; and science, technology, and information.[2] It is within these categories that the persistent conflicts exist. It is within these categories that nation-states, organizations, and people will fight to survive. Whether the conflict involves religion, migration, uneven prosperity, corporate greed, insufficient energy, increasing virtual communities, access to private information, crime, or biological weapons; people representing themselves, organizations, or nation-states will have to manage these conflicts in order to reduce the negative impact on society.

Clausewitz said that the first rule in war is to understand the type of war you are fighting; in this case, persistent conflict.[3] It is Sun Tzu who provides us the next

imperative; understanding the enemy who you intend to fight.[4] The enemies within persistent conflict are not in uniform and not driving Boyevaya Mashina Pekhoty (BMP-3) infantry fighting vehicles or Sukhoi Su-30 fighter aircraft; and they are not manning Shang-class 93 attack submarines as led by a nation-state structure of governance. Belligerents of today, operating in a state of persistent conflict, are involved in actions that are not traditionally military in nature. What makes these enemy elements dangerous and hard to defeat is that they work in a network form, a dark network. These are networks operating illegally, in the shadows of society, valuing secrecy, and conducting activities contrary to the good order of the general society. This provides problems for nation-states which are hierarchically structured and comfortable with conventional methods for dealing with conflict. These dark networks are made up of modern day enemies including insurgents, terrorist groups and individuals, gangs, drug trafficking organizations, pirates, organized crime, and network infiltrators. In order to manage these conflicts, nation-states and global organizations need to develop mechanisms to deal with dark networks.

The purpose of this essay is to examine the environment that feeds the dark networks, the characters that comprise the networks, the networks themselves, and the policy and strategy issues related to defeating dark networks. One specific recommendation that will be addressed is to modify the modern day geographic Combatant Command into a light, hub type network, and renamed “Regional Interagency Security Command” with the intent of fighting a network with a network.

## Defining “Persistent Conflict”

The Chief of Staff, U.S. Army, introduced this term in his address to the Association of the United States Army in 2007. This concept then made its way into

both the 2008 and 2009 Army Posture Statements.[5] The 2009 Statement defines persistent conflict as “protracted confrontation among state, non-state, and individual actors that are increasingly willing to use violence to achieve their political and ideological ends.”[6] This term is used 11 times in the 32 page statement in order to reinforce this term for continued usage. The statement goes further to explain that these persistent conflicts are fueled by a number of global situations to include failed states, globalization, competition for natural resources, and demographic changes.

The definition of persistent exists on a sliding scale. While the conflicts are constant, unrelenting, and continuing, they change in time with varying degrees. Each conflict falls in different areas, or points, on a sliding scale. Managing the scale of conflict depends upon the assessment of national, organizational, or individual interests viewed in conjunction with the best ways to achieve the desired goal. Some of these actions are occurring on the end of the scale which depicts the conflict in almost non-conflict terms or simple, matter of fact, disagreements between one actor’s methods and another’s. The opposite end of the scale includes actors engaged in armed conflict with one another using various methods of lethal force to achieve a goal. A key point is that the “sliding scale” includes non-violent as well as violent activities. Furthermore, the concept of winning is not part of the sliding scale. Attempting to “win” will simply cause confusion and frustration on the part of leaders, policy makers, and citizens. The goal is to manage the conflicts to acceptable or reasonable levels. It is this concept that is somewhat confusing in modern day military doctrine which points out “persistent conflict” and “winning” in the same context.[7]

Understanding the Enemy

The most dangerous enemy in the realm of persistent conflict falls within the general term "unconventional" or "irregular."[8] Elements within these realms include insurgents, terrorist groups and individuals, gangs, drug trafficking organizations, pirates, organized crime, and network infiltrators. These groups and individuals are often non-state actors who operate in the seams of society. The concept of "non-state actors" often leads to the confusion over how to deal with the affects of their actions. Many states, governments, leaders, and policy-makers believe that the entities listed above are criminals and should be dealt with in the civilian sector rather than military. Dr. Mark Clark recently conducted a study to determine whether or not the theories of the famous military strategist Karl von Clausewitz apply to what he terms "modern day warfare" or what we term persistent conflict. "What may be at stake is whether – and how – we may be compelled to fight such entities."[9] It is through a thorough understanding of the enemy that a state can begin to match elements of power against the effects of enemy activity. For the purpose of this paper, I will briefly highlight seven enemies within the dark network which cause the most danger in a time of persistent conflict.

*Insurgents* "Insurgents may attempt to seize power and replace the existing government or they may have more limited aims such as separation, autonomy, or alteration of a particular policy."[10] Insurgents often have efficient leadership and are quick to learn from their mistakes and adapt to the weaknesses of their adversaries. Their intelligence gathering ability is a key component of their work along with their logistical and communication capabilities.[11] One example is the Taliban.

*Terrorist Groups and Individuals* Regardless of the type of terror, people and groups labeled as terrorists use violence, have political motives, act against innocent people, and desire a reaction of fear.[12] This is also known as the process of terror; a process of seizing attention through shock and horror, getting out the message, and continuing the fight.[13] Terrorists operate in every domain of the globe. They seek sanctuary "…wherever possible: in state-controlled territory, under-governed areas, urban terrain, and increasingly, in cyberspace."[14] One example is al Qaeda.

*Gangs* While gangs exist in most areas of the world, the gangs in Central and South America have made a particularly notorious name for themselves. U.S. Southern Command estimates that the last decade has seen 1.2 million deaths linked to crime in Latin America. Many of these deaths have come from the hand of gang members, a membership total that reaches over 100,000.[15]

> Typically, gangs have some degree of permanence and organization and are generally involved in delinquent or criminal activity. Gangs may be involved in criminal activities ranging from graffiti, vandalism, petty theft, robbery, and assaults to more serious criminal activities, such as drug trafficking, drug smuggling, money laundering, alien smuggling, extortion, home invasion, murder, and other violent felonies.[16]

One example is Mara Salvatrucha (MS-13).

*Drug Trafficking Organizations* Their trade negatively impacts citizens throughout the world and their methods of trafficking and distribution often requires the use of extreme violence. The illicit drug trade of narco-groups threatens the social, economic and political fabric of all societies. Ultimately, the illegal production and trafficking in drugs undermines the security, stability, and prosperity of all nations and people involved and affected. One example is the Revolutionary Armed Forces of Colombia (FARC).

*Pirates* Contemporary pirates have captured our attention in the last few years almost as much as terrorists. It is hard not to pay attention to U.S. military snipers taking lethal action against pirates off the coast of Somalia on Easter Sunday. While sensational news, modern day pirates pose a significant danger to the lives of the citizens in the affected shipping lanes. Piracy also has a negative impact on global economic growth due to stolen cargo and costly insurance. Weakened nation-states suffer under piracy due to the undermining aspects of pirate activity.[17] One example is the pirates from the region of Puntland in Somalia.

*Organized Crime* Vadim Volkov refers to the term Violent Entrepreneurs as "…the economic dimension of the activities of wielders of force."[18] Whether we are discussing the Sicilian Mafia, Chinese Triads, Japanese Yakuza, or the Russian Mafia, "violent entrepreneurs" is a good general term of description. It is through enabling organized force that members of groups conducting illicit activity convert that activity into money or valuables. One example is the Solntsevskaya Brotherhood of Russia.

*Network Infiltrators* Hackers, Cyber-Terrorists, Information Warriors, and Cyber Criminals are all terms included in the definition of Network Infiltrator. These people attack the control system of countries and the heart of the financing aspect of the world.[19] While their crime may not be violent in nature, the effects of the outcome can not only destroy nations but lead to violent or lethal actions in trying to recover from a catastrophic net failure. One example is the Chinese Cyber-Militia.

What we gain by examining these groups is the ability to look for commonality of action, philosophy, reason, goals, makeup, culture, and behavior as examples of areas to focus on in order to manage the issues or affect caused by these groups. The terms

often become mixed such as narco-insurgency, cyber-terrorist, narco-terrorist, drug gangs, etc. This linking of topics is critical to understanding the enemy and developing laws, policy, strategies, and tactics to attack and manage the enemy situation in a more effective manner.

"Dark Networks"

When most people think of "networks" they tend to focus on computer networks, systems of lines, interconnection, group of people with similar interests, and a method of sharing information. Networks are often characterized by interdependence between organizations. These organizations are continually interacting with one another as network members allowing for the exchange of resources and ideas for common purposes.[20]

> Defined in simplest form, as any interconnected nodes, networks are ubiquitous. The nodes can be individuals, groups, organizations, or states (as well as cells or Internet users); the connections or links can consist of personal friendships, trade flows, or valued resources.[21]

The individuals or groups make up the nodes and the linkages are what binds or brings them together. Understanding what brings the individuals or groups together, or the nature of the linkages helps to understand the overall purpose of the network.

The definitions above highlight exchange between people, nodes, connections, in a relationship of actors, and a need for trusting relationships that are not hierarchical. Regardless of the exact vision or definition of a network, people tend to think of networks as helpful rather than hurtful, or good rather than evil. As Rabb and Milward point out, "most of the literature on networks and collaboration is quite positive."[22] The globalization of the world today has allowed the concept of networks to become the intellectual centerpiece for organizational development, leadership, and management.[23]

Networks are also a popular form of social organization as witnessed with the growth of social media activities and systems such as Facebook, LinkedIn, and Twitter.

> Networks vary in size, shape, membership, cohesion, and purpose. Networks can be large or small, local or global, domestic or transnational, cohesive or diffuse, centrally directed or highly decentralized, purposeful or directionless. Networks facilitate flows of information, knowledge, and communication as well as more-tangible commodities.[24]

What is important to realize is that, while networks can be benign, they can also be malicious. It is logical to assume that nefarious characters would also accept the network concept as a best practice for their own endeavors and form dark networks. These are groups of individuals and organizations that build networks striving to achieve goals that create problems for governments, organizations, and people all over the world.[25] A wide variety of illegally operating organizations to include insurgents, terrorist groups and individuals, gangs, drug trafficking organizations, pirates, organized crime, and network infiltrators make up the dark networks. These illicit entrepreneurs exploit network forms of organization because they help to conceal illegal activity through a dispersion of resources and operations. These illegal entities have found networks "useful for coordinating behavior, sharing information, and building relationships among conspirators" just as network elements of their lawful counterparts.[26] The graph below depicts an example of complex network structures of the ties between nodes of terrorist elements.

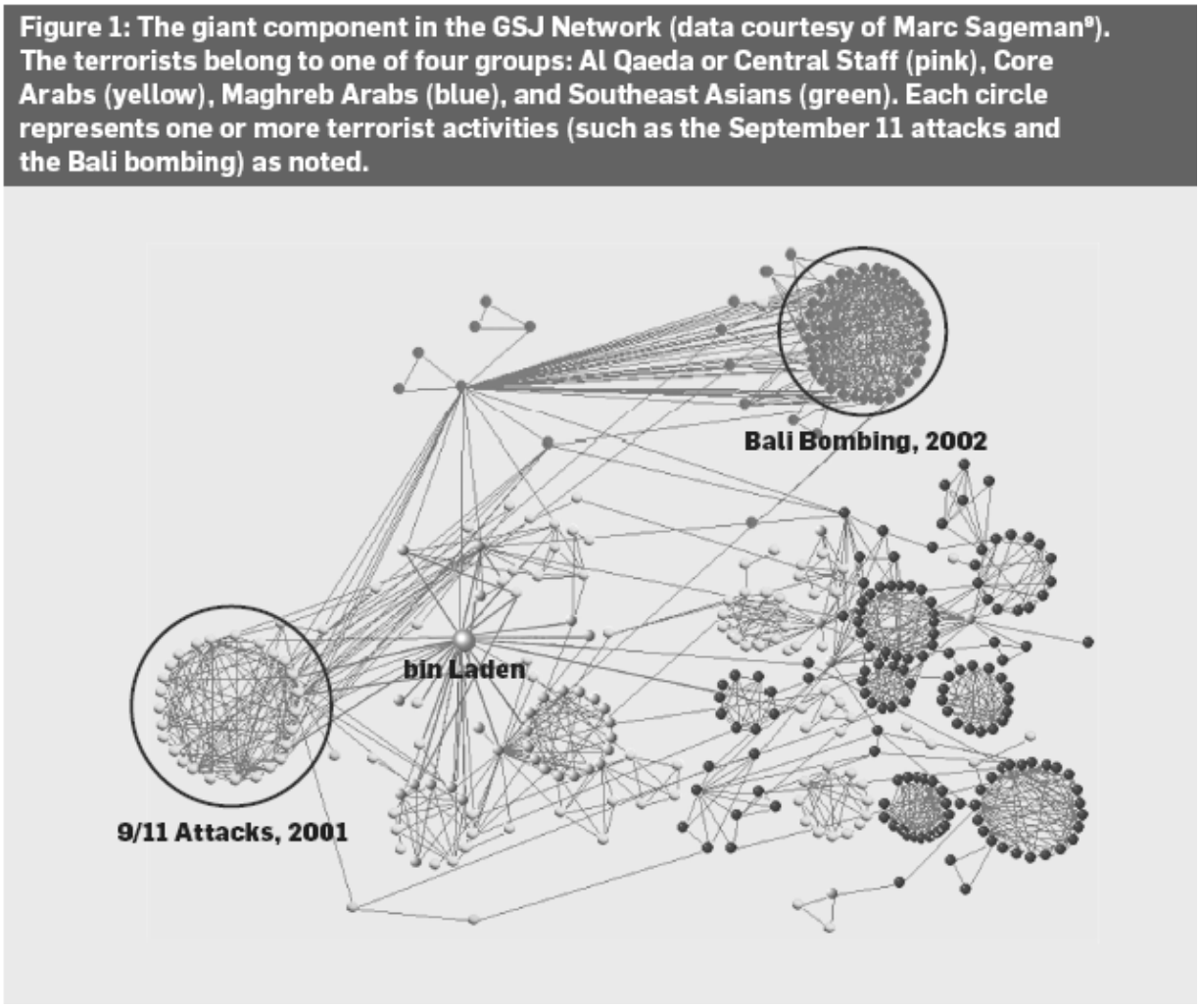


Figure 1.[27]

The U.S. National Intelligence Council describes a transformed world in 2025 which includes a power shift regarding nation-states and non-state actors "…including businesses, tribes, religious organizations, and even criminal networks."[28] The emphasis on networks of criminally related people and activities reflect a continued acknowledgment that there is no dominant hierarchical or organizational structure used by nefarious characters to commit their acts of conflict.[29] "Contemporary processes of political, cultural and economic globalization have generated a new world of security risks resulting from the illicit activities of 'nodes' and networks whose methods of

organization defy sovereign boundaries."[30] These networks, dark networks, require stealth or covert and clandestine behavior along with incredibly flexible node and link structures to achieve resiliency. One problem causing a lack of "literature" or study of the dark network problem is the issue itself – the dark networks are not only illegal but also covert and "…the dynamism of contemporary transnational crime makes it difficult to develop any single, elegant theory of dark networks."[31]

> The redundancy and hence resilience, of dark networks achieved through ebbs and flows of people in and out of particular functions is something that Gross Stein highlights in her analysis of terror networks. She too used the language of 'nodes' and 'networks' in an attempt to shift thinking away from the assumption that security threats can be eliminated through traditional command and control governance exercised in the wielding of military might.[32]

Networks allow actors to rapidly change organizational structure in order to adapt to a new environment. Colombian drug trafficking networks and the al Qaeda terrorist network are two good examples of networks that have changed their structure to meet their needs. Both have modified their existing centralized networks to more decentralized networks in order to flatten their organizations thereby leaving more autonomy for all members and reducing the possibility of law enforcement countermeasures.[33]

> As law enforcement succeeded in breaking down drug cartels and organized criminal syndicates, drug trafficking evolved from hierarchical organizations based on kinship, ethnicity, common experience, and tradition to networked enterprises with flattened lateral structure based on ad hoc arrangements with other groups.[34]

Similar to al Qaeda, the Taliban are part of a network which includes groups such as the Jalaluddin Haqqani network and al Qaeda associated movements. The Taliban connection in the network provides them political, military, and logistical support to oppose those they consider to be occupiers of Afghanistan."[35] Comparable to the

Taliban, Saddam Hussein established a clandestine transnational network based on trust relationships and mutual profitability which helped him remain in power while fighting the U.S. containment strategy.[36]

Operational Connections

> Terrorism and drugs go together like rats and the bubonic plague - they thrive in the same conditions, support each other, and feed off each other. Drug traffickers benefit from the paramilitary skills, access to weapons and links to other clandestine groups that terrorists can provide. Terrorists, for their part, gain a source of revenue and expertise in money laundering from drug traffickers. Sometimes terrorists and drug traffickers facilitate each other's operations by providing protection or transportation services. Other times, terrorists and drug traffickers are one-in-the- same, with drug revenues providing the financing for terror campaigns. Today, almost half of the international terrorist organizations identified by the State Department are linked to illicit drug activities.[37]

Or more simply stated, "terrorists use drug profits to fund their cells to commit acts of murder."[38] Narco-terrorism is one of the earlier elements of a nexus in two major elements of the dark network. While originally considered distinct, the common ground links became obvious.[39] The U.S. Drug Enforcement Agency has conservatively linked 19 of 42 officially designated Foreign Terrorist Organizations to drug trafficking activities of varying levels.[40] These linkages are far more than marriages of convenience. Terror groups and drug trafficking organizations work together for their own survival and gains, whether for simple financial gain or financial gain to support future operations.

There is also a significant link between terrorists and organized crime. "It was bin Laden who had managed the drug profits for the Taliban and arranged money laundering operations with the Russian Mafia…"[41] According to the United Nations Office of Drug Control, "it has become more and more difficult to distinguish clearly between terrorist groups and organized crime units, since their tactics increasingly overlap."[42] Therefore, the effects caused by their actions are similar if not the same. The

significant difference between organized crime and terrorists is that the terrorist are usually motivated by religious or political concepts and organized criminal's desire financial gain, similar to the commonalities between terrorists and drug trafficking organizations.

The link of organized crime and drug trafficking organizations is even stronger. The United Nations states that one of the most serious issues from the 2009 World Drug Report concerns organized crime. United Nations analysis shows that the drug markets have generated an economic system based on violence and corruption which falls within the realm of what is calls international drug mafias.[43] Money laundering is a good example of a tactic required by both of these groups. While money laundering is a crime in and of itself, the customers of the laundering include drug trafficking organizations, terrorists, and organized crime elements. The source of income for legitimate business organizations is transparent but the source of income for illegal organizations must remain concealed.[44] Whether an organized crime element is conducting advanced money laundering operations such as using offshore financial centers or a drug runner is simply converting illegally acquired cash into money orders, money laundering is occurring for the advancement of future illegal activity.[45]

> With the exception of crimes of passion, most criminal behavior is motivated by greed and thus begets illegally gotten money that must be introduced into legitimate financial channels via seemingly legitimate sources.[46]

Another linkage of two similar organizations is that of insurgents and gangs, especially transnational gangs. Comparing gangs to insurgents, Dr. Manwaring highlights that "the common denominator that can link gangs to insurgency is that some gangs' and insurgents' ultimate objective is to depose or control the government of

targets countries."[47] Whether you look at gangs as the primary evolutionary beginning to insurgent organizations or accept the traditional street gang model, their actions do not fall within a single law enforcement code and impact citizens across various levels of state borders. The primary thread enabling these two types of illegal organizations to succeed is freedom of movement.[48] Whether you are part of the Taliban living in the relatively safe area of Pakistan and conducting operations in Afghanistan or a member of the Mara Salvatrucha (MS-13) moving and operating between California and Central American nations such as Honduras and El Salvador, freedom of movement is critical to your life and operations. This freedom of movement is enhanced because of un-governed or under-governed areas of sovereign territories. These two terms represent the failure of a sovereign entity to exercise power within its boundaries. An extreme level of un-governed areas is found within failed states, such as Somalia where pirates, gangs, and terrorists roam freely throughout the territorial lands and waters.

As all of these groups, operating on the scale of persistent conflict, expand their operations and continuously improve though innovation. Many latch on to the technical capacity and capability of the cyber domain. The U.S. Strategy to Secure Cyberspace highlights that the "primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security."[49] While this concern is at the violent end of the spectrum, another concern that could cause equal problems in order of magnitude is the basic usage of the internet as a tool for terrorist communication. In between these two concerns are terrorists using the cyber domain for recruitment, funding, or launching terror attacks.

“The FBI predicts that terrorist groups will either develop or hire hackers, particularly for the purpose of complimenting large physical attacks with cyber attacks.”[50]

While the motives may differ, the operational and tactical commonalities of insurgents, terrorists, gangs, drug trafficking organizations, pirates, organized crime elements, and network infiltrators cross the spectrum of operational activities. Their tactics are often similar and their baseline affects are virtually identical, especially by the casual observer or someone directly impacted by the tactic used. Their need to recruit, train, house, and equip specific types of people and acquire funds, sanctuary, and false documentation to develop and conduct operations allows these groups to understand and capitalize on their own commonalities.[51]

One Possible Solution – The New Light Network

A common theory is that it takes a network to fight a network. While there are numerous types of networks, the dark networks appear to prefer the all-channel type which is diverse, dispersed, and made up of small nodes with no or limited central leadership. These nodes are linked together with the mission of coordinating and acting jointly (not hierarchical).[52] While this type of non-hierarchical, limited central leadership may not appeal to nation-state leaders, there are network forms that retain leadership but capitalize upon the strengths of dispersed and diverse nodes.

In order for one network to combat another network, there must be a focus on finding the network links that connect the nodes. Current governmental, crime fighting, drug enforcement, and military networked like entities are not known for their ability to decentralize decision making and reduce information flow to the level of their counterparts in the dark networks. Additionally, the light networks have the added responsibility of operating within the law.[53] “Our challenges require effective whole of

government integration – but we remain in outmoded, bureaucratic, inward-looking, competitive departmental stovepipes."[54] Freedom to communicate up, down, and across organizational spectrums based on a leaders vision is the key to converting hierarchical organization into flexible and agile networked organization.[55] Translating good ideas into action requires collaboration among all those involved in development and implementation of the ideas.[56]

Whether working to overcome challenges or striving for goals, there is no single focal point for the conduct of planning and operational activities to accomplish the desires of the U.S. and manage the dark networks conducting persistent conflict below the National Security Council level. There are only disparate stove pipes or cylinders of excellence to work particular aspects of these challenges and goals in a vacuum or at best with some consultation between entities. The current organization that is best structured, at the right level of government, most appropriately staffed, and given the mission to deal with meeting some of these challenges and achieving the national objectives is the Geographic Combatant Command.

While these organizations exist today, they operate as military organizations within the laws and policies as understood by the U.S. citizens. The Geographic Combatant Commands today are focused on detecting, deterring, and preventing attacks and planning for and executing military operations.[57] The Combatant Commands of today are led by military personnel and focused on military issues. While some have ventured into non-traditional military activities and claim to have an interagency focus their interagency partners have not completely embraced the collaborative, resource and information sharing concepts. "At the regional level, the only

entities who are trying to create interagency mechanisms are the Combatant Commands but they are only a shadow of what is really required."[58] They are not quite suited to deal with the majority of the conflicts caused by the dark networks on the sliding persistent scale. If the U.S. wants to continue to excel on the world stage, the U.S. should modify the Geographic Combatant Commands to take on a true whole of government approach and become Regional Interagency Security Commands (RISC) based on a hub type of network format.

The National Security Act of 1947 and Title 10 of the United States Code provide the basis for the establishment of the combatant commands with the Unified Command Plan providing the missions.[59] Combatant Command missions include activities such as: deterring and preventing attacks against the U.S., conducting security cooperation activities, and providing advice and assistance to chiefs of U.S. diplomatic missions.[60] While the Combatant Commands operate within the current law and continue to focus on the conduct of military planning and operations, some are moving toward an interagency approach to work in more of a whole of government, or whole of society, fashion within their respective areas of responsibility. Properly structured to include integrated and mutually supportive interagency representation and capabilities along with a Combatant Commander's headquarters and associated staff could provide the nucleus, or hub, for interagency reorganization and activities and become a whole of government focused RISC which would be better suited to take on the dark networks.[61] Hub type networks  allow super nodes may act like a hierarchical structure while allowing information and resources to be dispersed throughout the network. Focused on a hub style of network, the RISCs headquarters would be the convergence of activity

specifically in terms of information transfer, resource management, and idea sharing. They would be views as the first level of decentralize decision making at the national level if staffed and integrated by agencies forming all elements of national power. The U.S. could start this initiative by capitalizing on the transformational successes of U.S. Southern Command and U.S. Africa Command.

U.S. Southern Command and U.S. Africa Command are two geographic Combatant Commands which have recently undergone significant changes to become more focused on interagency activities. They have created slight modifications to their personnel staffing allowing for non-Department of Defense personnel from various U.S. governmental organizations to join their ranks with the minimum goal of infusing various interagency cultures within on headquarters element. A higher level goal is to provide the direct reach back of information gathering from both the national and sub-regional levels from the various agencies throughout the governmental enterprise.

The U.S. needs to continue taking steps to view the world through an interagency or whole of government lens rather than a military lens and a Regional Interagency Security Command is a mechanism well suited for the mission. In addition to the internal modification of the Combatant Command, there must be an adjustment to the upper, lower, and lateral functions of the command and the organizations making up the network of the command. Light networks must be outward looking, evolutionary, and flexible.[62] The required adjustments include the development of a network of people, organizations, and agencies with the missions dealing with the effects of the nefarious characters discussed in this paper. The modification of the current Geographic

Combatant Commands into Regional Interagency Security Commands based on becoming a “light network” is a good starting point.

There are many avenues of approach to continue Combatant Command level transformation. Future steps should include assessments from various governmental organizations to seek further areas within the Combatant Command for modification, specifically in the areas of communication and process management. Additionally, a thorough analysis of the existing policies along with U.S. Code must be conducted to determine current policy and legal hindrances to further merging of governmental organizations within one organizational element. A true Regional Interagency Security Command must have all of the elements or instruments of national power networked within the communication and decision making nodes to provide rapid and focused response to challenges, issues, and goal attainment activities. By co-locating the many whole of government elements, a super hub is created providing the ability to link with authority the various mission leadership and concepts to attack the dark networks and deal with the effects of the nefarious characters.

## Conclusion

> Power is migrating to small, mostly nonstate adversaries who can organize into sprawling networks more readily than can traditionally hierarchical nation-state actors. Not only civil society bus also uncivil society is benefiting from the rise of network forms of organization. Some uncivil actors, such as terrorists and criminals, are having little difficulty forming highly networked, nonhierarchical organizations. Thus, networked adversaries may be expected to pose increasing threats to the United States and its interests around the world. Conflicts will more often be fought by networks than by hierarchies.[63]

While it remains important for civil societies to continue working toward the elimination of the underlying causes of crime, terror, drugs, gangs, and piracy, there must be a concentrated, coordinated, and collaborative effort put forth to deal with the actors

within and the effects of the persistent conflicts. It is important to realize that "the conflicts we are engaged in are bigger than DoD, and they will require a global effort."[64] The gap continues to widen within nation-state governmental capabilities and capacity to address the actors within persistent conflict. The enemy functioning on the sliding conflict scale are innovating faster than the legal elements of society creating a fissure that appears to be growing at an accelerated pace and causing the citizens to question their government's ability to perform the number one function – secure the people. The U.S. must begin to reform and reorganize as a network to defeat a network. "National security reform is not something that would be nice to do it is something that must occur for the benefit of the entire nation and world stage."[65]

Endnotes

[1] General George W. Casey. Speech Delivered on October, 9, 2007 at the Association of the United States Army

[2] USSOUTHCOM J5, CJCS Offsite Prep, "Strategic Environment, Assumptions, Vital National Interests, Grand Strategy Information Paper," for ADM Stavridis, Miami, FL, September 4, 2008.

[3] Clausewitz, Carl von, *On War*. Edited and translated by Michael Howard and Peter Paret (New York: Everyman's Library, 1993), 100.

[4] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1971), 84.

[5] Peter Geren and George W. Casey. "A Statement on the Posture of the United States Army 2008 and 2009" (February 2008 and May 2009), III and V.

[6] Ibid., V.

[7] U.S. Department of the Army, *Operations, Field Manual 3.0* (Washington, DC: U.S. Department of the Army, February, 2008), Forward.

[8] Nathan Freier, *Known Unknowns: Unconventional "Strategic Shocks" In Defense Strategy Development*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, November 2008), vii, 13.

[9] Mark T. Clark, "Does Clausewitz Apply to Criminal-States and Gangs?" in *Criminal-States and Criminal-Soldiers*, ed. Robert J. Bunker (London: Routledge Taylor & Francis Group, 2008), 80.

[10] Steven Metz and Raymond Millen, *Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, November 2004), 2.

[11] Gilles Dorronsoro, *The Taliban's Winning Strategy in Afghanistan*, (Washington: Carnegie Endowment, 2009), 8.

[12] Cindy Combs, *Terrorism in the Twenty-First Century*, (Upper Saddle River, New Jersey: Prentice Hall, 2003), 17.

[13] Charles Townshend, *Terrorism*, (Oxford: Oxford University Press, 2002), 8.

[14] Andrew Krepinevich, Robert Martinage and Robert Work, *The Challenges to US National Security*, (Washington, Center for Strategic and Budgetary Assessments, 2008), 20.

[15] James Stavridis, *U.S. Southern Command 2009 Posture Statement to the House and Senate Armed Services Committees before the 111th Congress*, (Miami, U.S. Southern Command, 2009), 20.

[16] Clare M. Ribando, *CRS Report for Congress – Gangs in Central America*, (Washington, DC: Congressional Research Service, Updated October 17, 2008), 2.

[17] Peter Chalk, *The Maritime Dimension of International Security*, (Santa Monica, CA: Rand Corporation, 2008), xii.

[18] Vadim Volkov, *Violent Entrepreneurs*, (New York: Cornell University, 2002), 27

[19] U.S. *The National Strategy to Secure Cyberspace*, (Washington DC: U.S. Government, February, 2003), 1.

[20] Jenny Fleming and Jennifer Wood, "Introduction: New Ways of Doing Business: Networks of Policing and Security" *Fighting Crime Together* (Sydney, Australia: UNSW Press, 2006), 3.

[21] Miles Kahler, "Networked Politics" in *Networked Politics,* (Ithaca, NY: Cornell University Press, 2009), 3.

[22] Jorg Raab and H. Brinton Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory*, Vol 13, No 4 (2003): 413.

[23] Kahler, "Networked Politics" in *Networked Politics,* 2.

[24] Phil Williams, "Transnational Criminal Networks" in *Networks and Netwars*, ed. John Arguilla and David Ronfeldt (Santa Monica, CA: RAND, 2001), 65.

[25] Raab, “Dark Networks as Problems,” *Journal of Public Administration Research and Theory*, 415.

[26] Michael Kenney, “Turning to the Dark Side” in *Networked Politics,* (Ithaca, NY: Cornell University Press, 2009), 78.

[27] Jennifer Xu and Hsinchun Chen, “The Topology of Dark Networks,” *Communications of the ACM*, Vol 51, No 10, (October, 2008), 60.

[28] C. Thomas Fingar, *Global Trends 2025: A Transformed World*, (Washington, DC: U.S. Government Printing Office, November, 2008), 1.

[29] Phil Williams, “Transnational Criminal Networks” in *Networks and Netwars*, ed. John Arguilla and David Ronfeldt (Santa Monica, CA: RAND, 2001), 63.

[30] Fleming “Introduction: New Ways of Doing Business: Networks of Policing and Security” *Fighting Crime Together*, 1.

[31] Jennifer Wood, “Dark Networks, Bright Networks and the Place of the Police,” *Fighting Crime Together* (Sydney, Australia: UNSW Press, 2006), 252.

[32] Ibid., 254.

[33] Kahler, “Networked Politics” in *Networked Politics*, 10.

[34] Paul R. Kan, *Drugs and Contemporary Warfare,* (Washington, DC: Potomac Books, Inc, 2009), 23.

[35] Dorronsoro, *The Taliban’s Winning Strategy in Afghanistan*, 1.

[36] Phil Williams, *Criminals, Militias, and Insurgents: Organized Crime in Iraq*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, June, 2009), 33.

[37] John Ashcroft, “Prepared Remarks for DEA/Drug Enforcement Rollout,” Washington, DC, March 19, 2002, linked from The Center for International Policy at “Colombia Program,” http://www.ciponline.org/colombia/02031903.htm (accessed December 3, 2009).

[38] George W. Bush, “Remarks on Signing Legislation To Reauthorize Drug-Free Communities Programs,” Washington, DC, December 14, 2001, linked from The American Presidency Project, http://www.presidency.ucsb.edu/ws/index.php?pid=62854 (accessed November 20, 2009).

[39] Frank Bovenkerk and Bashir Abou Chakra, “Terrorism and Organised Crime,” in *Terrorism, Organised Crime and Corruption,* ed. Leslie Holmes, (Cheltenham, UK: Edward Elgar Publishing, 2007), 29.

[40] Michael W. Jefferson, “Crime Terror Nexus Unit,” briefing slides, U.S. Southern Command, Miami, FL, December 16, 2008.

[41] Rachel Ehrenfeld, *Funding Evil*, (Chicago, IL: Bonus Books, 2003), 53..

[42] Antonio Maria Costa, "UN Warns About Nexus Between Drugs, Crime and Terrorism," Press Release SOC/CP/311, January 10, 2004, linked from the United Nations Home Page at http://www.un.org/News/Press/docs/2004/soccp311.doc.htm (accessed December 1, 2009).

[43] United Nations Office on Drugs and Crime, *World Drug Report, 2009*, (New York: United Nations Publications, 2009), 1.

[44] Paul R. Kan, *Drugs and Contemporary Warfare,* (Washington, DC: Potomac Books, Inc, 2009), 43.

[45] Rachel Ehrenfeld, *Funding Evil*, (Chicago, IL: Bonus Books, 2003), 13.

[46] John A. Cassara, *Hide & Seek*, (Washington, DC: Potomac Books, Inc, 2006), 62.

[47] Max G. Manwaring, *Street Gangs: The New Urban Insurgency*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, March, 2005), 2.

[48] Ibid., 17.

[49] U.S. *The National Strategy to Secure Cyberspace*, viii.

[50] Keith Lourdeau, "Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, February 24, 2004, linked from the Federal Burea of Investigation Home page at http://www.fbi.gov/congress/congress04/lourdeau022404.htm (accessed January 9, 2010).

[51] Rachel Ehrenfeld, *Funding Evil*, (Chicago, IL: Bonus Books, 2003), 1.

[52] John Arquilla and David Ronfeldt, "Looking Ahead: Preparing for Information Age Conflict," in *In Athena's Camp* (Santa Monica: CA, RAND, 1997), 455.

[53] Michael Kenney, *From Pablo to Osama*, (University Park, PA: The Pennsylvania State University Press, 2007), 216.

[54] James R. Locher, "Keynote Address: Leadership and the National Security Reform Agenda," *Colloquium Report, Leadership and National Security Reform: The Next President's Agenda*. Strategic Studies Institute, (October, 2008): 26.

[55] Thomas X. Hammes, *The Sling and the Stone*, (St. Paul, MN: Zenith Press, 2006), 275.

[56] Donald F. Kettl, "The Key to Networked Government," in *Unlocking the Power of Networks*, ed. Stephen Goldsmith and Donald F. Kettl (Washington, DC: Brookings Institution Press, 2009), 1.

[57] The White House, *Unified Command Plan* (Washington, DC: December 17, 2008), 8.

[58] James R. Locher III, "Keynote Address, Unrestricted Warfare Symposium Proceedings," Johns Hopkins University Applied Physics Laboratory, Laurel, MD, March 24, linked from http://www.jhuapl.edu/urw_symposium/Proceedings/2009/Authors/Locher.pdf (accesses November, 2009,), 20.

[59] The White House, *Unified Command Plan,* 1.

[60] Ibid., 5-9.

[61] Christopher Naler, “Are We Ready for an Interagency Combatant Command,” *Joint Forces Quarterly*, Issue 41, 2d Quarter, 2006, 26.

[62] Kettl, “The Key to Networked Government,” in *Unlocking the Power of Networks*, 10.

[63] Arquilla, “Looking Ahead: Preparing for Information Age Conflict,” in *In Athena’s Camp*, 456.

[64] Eric T. Olson, “U.S. Special Operations: Context and Capabilities in Irregular Warfare,” *Joint Forces Quarterly*, Issue 56, 1st Quarter, 2010, 70.

[65] James R. Locher III, “Seven Questions: James R. Locher III,” interview by Foreign Policy Magazine, December, 2008, linked from Foreign Policy, http://www.foreignpolicy.com/story/cms.php?story_id=4564&page= (accessed November 25, 2009).