



Photo courtesy of flickr

Beyond Find, Fix, Finish: Establishing a Counter-Network Interagency Organization to Combat the Convergence of Globally Connected Threat Networks

Hermann G. Hasken III
Department of Defense

T*ransnational illicit networks have grown tentacles that stretch around the world...all elements of our national power must work together in order to address this growing threat.*

Admiral (Ret) James Stavridis

Introduction

The globalization of the world's economies, advancing technologies, increasingly expanding trade routes, and porous borders have, unfortunately, brought with them the murkiness of an interconnected and enterprising underworld. Organized crime, violent extremists, drug traffickers, smugglers, and other non-state actors are moving a wide variety of contraband commodities along near-invisible logistical arteries to serve markets flush with growing clientele. These actors are making governance, safety, and security nearly impossible, particularly in countries with little resources to fight. They are now creating sanctuaries in multiple and dispersed ungoverned and under-governed spaces where law enforcement is outgunned or non-existent.¹ Today, illicit networks are creeping into stable government structures, as cartel leaders, organized crime, and other non-state actors invest millions into

The opinions, conclusions, and recommendations expressed or implied within /luce.nt/ are those of the contributors and do not necessarily reflect the views of the Naval War College, the Department of the Navy, the Department of Defense or any other branch or agency of the U.S. Government.

unwitting legitimate companies and worldwide financial institutions² or steal, hide, and move funds via a labyrinth of money laundering schemes, hawalas, or by cyber theft.³ Financial, logistical, and communications support networks have long been the most critical nodes to the health and vitality of criminal and violent extremist networks.⁴

Money is the oxygen that keeps the brain trust of illicit organizations functioning and alert. Smuggling routes are the arteries, and secure communications its lifeblood. In order to keep resilient and strong, the best financed organizations have recruited technical mercenaries—hired guns with expertise in cyber, intelligence, security, law and finance. Most act as independent contractors, selling their services to the highest bidder to facilitate illicit activities and in return, reap massive profits as well as protection from underground overlords. Governments and international organizations are witnessing the alarming spread of a loosely knit confederation of illicit, criminal, and violent extremist groups, or “dark networks,” giving rise to the threat concept called “convergence.”⁵ The dark network is now spilling over national boundaries, connecting the most unlikely criminal, gang, and terrorist elements across continents as opportunistic partners in an emerging web that the intelligence, law enforcement, and diplomatic communities are just beginning to understand.

“Convergence” is a new twist to drug cartels, terrorists, traffickers, and other criminal enterprises operating inside struggling nations, particularly those weakened by decades of civil war, insurgency, poverty, and corruption. As the Al Qaeda network and its affiliates have become more diffuse, the dark network has equally spread and deepened its presence throughout the international security environment. It has also crept through our own back door. While much of the concern in the United States focuses on the violence in Mexico and along our shared border, national decision makers have been informed of a growing body of evidence indicating that terrorist groups have been operating effectively (albeit quietly) in Canada, taking advantage of liberal immigration and political asylum policies and a porous Canadian-American border.⁶ In 2011, U.S. Border Patrol authorities discovered Tunisian radical cleric Said Jaziri in the trunk of a BMW trying to sneak into the United States with the help of Mexican contract smugglers after previously being deported from Canada back to Tunisia.⁷ The Royal Mounted Canadian Police (RCMP) and Canadian Revenue Agency recently shut down the International Relief Fund for the Needy and Afflicted (IRFAN-Canada) after being implicated in sending over \$15 million to Hamas.⁸ Law Enforcement and Immigration studies have shown the Iranian Qods Force, Lebanese Hezbollah, and other terrorist organizations have found opportunities to slip in and set up equal presence with support groups in the United States.⁹ In one of the most brazen attempts to conduct terror attacks in the United States, an Iranian-backed terrorist attempted to assassinate the Saudi Ambassador to the United States while dining in Washington DC.¹⁰ The FBI Joint Terrorism Task Force website is replete with vignettes that demonstrate how expansive this network has become and how easy it is to conduct human trafficking from our northern and southern borders, as well as our ports.¹¹ In 2014, human trafficking surged to become the highest value commodity smuggled across the southern Californian border, bigger in profit potential than drugs, according to the FBI.¹² The Center for Immigration Studies sees new concerns in the human trafficking phenomena, as many are not Mexican illegal immigrants or kidnapped sex slaves, but actually an increasing percentage of people from the Middle East.¹³

Most developing nations do not place counter-drug programs as a priority effort; their lack of strength against them is a clear demonstration of the national security challenges these networks present. The recent Malaysian Airlines Flight M370 mystery brought new attention to reporting that indicates nearly 40 million passengers have travelled on counterfeit documents (including U.S. passports) with nearly 2.4 million passports having been stolen, reported missing, or copied.¹⁴ Perhaps a dark portent of the future is the FBI’s recent report of American citizens returning to the U.S. after being



radicalized in Somalia and more than 50 believed to have fought in Syria.¹⁵ For those that are identified, they can be added to the No Fly List and denied reentry; otherwise, the fear is they will find ways to slip back into the United States. Since 2001, the dark network of cooperative and enterprising criminals have kidnapped and/or smuggled an estimated two million people via underground trafficking routes and their facilitators.¹⁶ The risks are high, but the financial rewards are staggering. The risks and consequences to the United States may be even higher.

Smuggling illicit commodities (drugs, blood diamonds, weapons, hazardous materials, toxic waste, exotic wildlife, ivory, human beings, and more) is filled with a host of complexities; however, all begin with a product and typically end with delivering payment, trade, or a service. The return cycle now includes wide-ranging types of payments used to acquire the commodities, from cash to weapons and other goods the seller may need or barter, or services rendered by other means.¹⁷ The United Nations Office of Drugs and Crime (UNODC) conservatively estimates the total amount of bulk cash smuggling, illicit finance, and associated money laundering alone to be approximately \$800 billion and perhaps well over one trillion dollars.¹⁸ The U.S. Justice Department and UNODC have competing estimates on the total value of drugs, but conservatively place the cartels' U.S. drug trade at \$39 billion¹⁹ and the total global drug trade at nearly \$400 billion.²⁰ If the combined worth of global illicit activity (excluding cyber crime) were calculated in the same manner as legitimate trade economies, the dark network's value would be in excess of \$1.8 trillion, placing it in the top 10 economies in the world.²¹ However, the UNODC's *2012 World Drug Report* concludes accurate profit amounts are elusive and perhaps higher than current estimates.²² The combined relative wealth of some groups is rising so fast, it rivals or even has underpinned the legitimate economies of the poorest countries in which they occupy.²³ Their ability to entice corrupt government officials (or eliminate them) makes targeting, capture, conviction, and disruption complicated but not impossible. It will require a bold and fresh look at existing capabilities, authorities, organizations and methods to make discovery, intelligence sharing, and evidence based apprehension an effective weapon against this network.

The U.S. has separate national level strategies to combat transnational organized crime, narcotics, human trafficking, and cybercrime. A national counter-threat strategy must be considered and tied to specific national security objectives. The convergence of these threats demands a national reassessment before such partnerships undermine the stability and security not only in ungoverned nations but also threaten the vital national interests of the United States and its allies. This growing activity cuts across legal, economic, political, military, humanitarian, tactical, and strategic lines. U.S. counter-network strategy must be tied to national policy, and national policy to empowered and enabled inter-agency action to achieve national objectives. A counter-network strategy is supported by U.S. National Security Strategy principles of ensuring the safety and security of its citizens and its U.S. allies; fostering a strong, innovative, and growing U.S. economy; promoting respect for the universal value and dignity of human rights; and advancing the ideals of an international community of nations that extends the offer of peace, security, and opportunity through stronger cooperation to resolve global challenges. Counter-threat network efforts cannot be done by separate organizations on independent vectors. National decision makers must consider nesting relevant and mutually supporting laws, activities, and appropriations into a National Counter-Threat Network coordinating body, fully vesting integrated military and law enforcement teams to conduct global counter-network operations abroad.

It is a great feat to steer a policy to a successful conclusion or to overcome one's enemies in a campaign, but it requires a great deal more skill and caution to make good use of such triumphs. Thus we find that those who have won victories are far more numerous than those who have used them well.

~ Polybius of Arcadia, 200-118 BC



What is the U.S. National Strategy to Combat the Dark Network?

Does the United States possess an overarching strategy to combat the dark network? The simple answer is no. Current authorities, resources, and organizations are separated between national counter-transnational organized crime, counter-narcotics, human trafficking prevention, and counter-terrorism strategies—each crossing several federal departments. The President's 2011 *Strategy to Combat Transnational Organized Crime (TOC)*, however, does at least provide a framework from which to build. The TOC strategy calls for enhanced intelligence sharing, protecting the U.S. financial system, strengthening interdiction, investigation and tougher prosecutions, disrupting the flow of drugs, and building international capacity.²⁴ The elements of this strategy, while specific to transnational organized crime, could be expanded to encompass other threats with relevant editing and modification. Additionally, the *National Security Strategy (NSS)* and *National Military Strategy (NMS)*, along with the State Department's *QDDR* and other Department-level strategy and policy documents that relate to illicit organizations must be knitted together, with clarifying language to demonstrate commitment, resources, and a feedback loop to ensure measures of effectiveness are being assessed and reported to national decision makers. Without a coherent strategy, the tentacles of these converging networks will not only continue to pose a foreign policy and national security problem for Washington, it will also increasingly exacerbate several domestic issues facing the United States, including immigration reform, surveillance laws and privacy, defense spending, and a growing prison population.²⁵ A deeper look into the successes of Joint Interagency frameworks may provide clear insight for establishing the right organization to hinder the advancing spread of converging networks and enhance the security posture of the United States. It will, however, also require a new targeting methodology.

The Department of Defense's (DoD) wartime successes in developing and operating Joint Inter-Agency Task Force (JIATF) organizations are unmatched in the history of modern warfare, particularly in counter-terror (CT) and counter-insurgency (COIN) operations conducted by Special Operations Forces (SOF). SOF's Find, Fix, Finish, Exploit, Analyze, Disseminate (F3EAD) targeting cycle was forged, sharpened, and perfected in combat operations in Iraq and Afghanistan. However, the post-OEF/OIF global security environment will be much less conducive to future Direct Action (DA) "find, fix, finish" operations. According to a recent White House press release, the President may only authorize future lethal action against terrorist targets and only as a last resort.²⁶ Authorized use of military force (AUMF) may soon become the least preferred tactic of choice for operations outside designated theaters of armed conflict (OODTAC). It most certainly will be restricted to terrorist targets, eliminating potential to expand these authorities to other actors in threat networks with interests equally harmful to the United States. While offering a fresh start on the legitimacy of global counter-terror operations, this restriction may significantly impede counter-network operations designed to prevent another catastrophic domestic attack in the United States. Concerns of AUMF aside, the United States must move beyond F3EAD and find a complementary detection, analysis, targeting and decision-making cycle that will fit the future global operating environment.

DoD's intelligence and special operations forces (SOF) capabilities, resources, and authorities could provide a baseline from which a new "counter-network" organization and functional defeat approach can emerge. Borne out of the Joint Inter-Agency Task Force (JIATF) concept and based on a mix of Counter-Narcotics, counter-insurgency (COIN) and counter-terror (CT) lessons learned, a newly formed U.S. Counter-Threat Network (CTN) effort would provide a whole of government network vs. illicit network approach to combat the convergence of the dark network in the United States and abroad. Single-agency approaches and disparate national strategies can no longer address convergent threats. It requires the combined resources, authorities, political will, and cooperation among law enforcement, justice, intelligence, as well as our diplomatic corps and military organizations in the United States and



abroad. Much of our successes, some of them quite large, may appear as mere pin pricks in a much broader effort by the convergence of these global illicit and violent organizations. While transnational organized crime is addressed, “convergence” does not receive clear mention in the most recent Defense Planning Guidance. Without the recognition, there will be no strategy, policy, or coordinated action.

Borrowing Stanley McChrystal’s phrase, “it takes a network to defeat a network,”²⁷ the U.S. must team with empowered and enabled international and non-government organizations to understand, discover, and ultimately dismantle or destroy these illicit nodes where their strengths, weaknesses, and dependencies are critical and vulnerable.

The role of grand strategy...is to coordinate and direct all the resources of a nation, or band of nations, toward the attainment of the political object of war – the goal defined by a fundamental policy.

Sir Basil Liddell Hart, 1937, Green Pamphlet

Authorize, Organize, and Act!

Successful government strategy is optimally achieved when three components—authorities, resources, and organization—are effectively combined.²⁸ Above all, a strategy requires national level leadership with mission focus and Presidential directive. National decision makers must consider streamlining relevant and mutually supporting counter-network laws under one organization, empowering and enabling a national counter-network coordinating body, and fully funding a national counter-threat network organization.

The President’s TOC strategy, along with the national strategies for counter-terrorism, counter-proliferation, and prevention of human trafficking can lay a foundation for a more prescriptive Presidential Policy Directive (PPD) for countering the convergence of global illicit and violent extremist networks. A Counter-Threat Network PPD, accompanied by a National Strategy for Countering Illicit and Violent Threat Network, does not have to supersede previous PPD’s or national level strategies for narcotics, trafficking, counter-terrorism or counter-proliferation. The PPD for Countering Global Threat Networks (PPD-CGTN) should set the stage for all supporting documents assigned to each relevant government department. Organizationally, a National CTN organization can be welded to or modeled after several organizations to include the DHS Global MOTR Coordination Center,²⁹ or the National Counter-Terrorism Center.³⁰ It must be mindful of the 1981 GAO report³¹ on the systemic issues of organizing task forces (e.g., DEA and FBI) and avoid repeating those same conflicts regarding the sharing of information that the current FBI-DEA Organized Crime and Drug Enforcement Task Force has experienced.³² An overarching decision making body, like those designed in Joint Inter-Agency Coordinating Groups (JIACG), is most likely the best option.

Joint Inter-Agency Coordination Groups (JIACGs) have proven very successful in previous U.S. government efforts, especially when international collaboration is encouraged, invited, and anticipated. A CTN JIACG, headed by an interagency steering group of senior level decision makers—officially endorsed by the President and given specific authorities by Congress for USG counter-network efforts—would provide the leadership, direction, and mission goals for the U.S. portion of an international counter-network organization. A Counter-Threat Network JIACG consisting of a Defense-Justice-Intelligence triad would be the most effective organization, tying capacity, authority, evidence, and judicial processes to an empowered and enabled counter-network organization. It must be led by senior executives with substantial experience working within the Interagency, particularly with State, Treasury, Justice, and the Department of Defense. As proven in Iraq, Afghanistan, Yemen, Colombia and beyond,



the Special Operations Forces, the Intelligence Community, and the Inter-Agency present a most formidable opponent to any illicit organization, and a willing partner to the international community.

The best ideas in the world are of no benefit unless they are carried out.

~ President Harry S. Truman

A Conceptual Plan for a DoD Counter-Network Operations Coordinating Body

At the DoD level, a Joint Inter-Agency Task Force (JIATF-CTN or a Defense Counter-Network Operations Coordination Center), co-chaired by special operations, law enforcement and defense intelligence senior executives/officers, conceptually would provide the core senior executive team that provides the focus, goals, and objectives for the military's contribution to an overarching national counter-network strategy. This type of organization would enable the interagency to pair their authorities with DoD resources and synchronize global Special Operations activities with legally sufficient intelligence and information to conduct warrant based counter-network operations. As the challenge of the legitimacy to conduct U.S. unilateral actions against terrorist networks increase, USSOCOM, DIA, and law enforcement agencies have the resources, authorities, and global reach to provide presence and expertise to work with partner nations to train, advise, and assist.

USSOCOM's ability to network across the globe by, with, and through partner nation Special Operations Forces (SOF) and other specialized U.S. and foreign capabilities, leveraging Theater Special Operations Command (TSOC) capabilities in each region is unmatched in the DoD. Further, SOCOM serves as the DoD proponent for combating terrorism, illicit finance, and for combating trafficking of weapons of mass destruction.³³

SOCOM is also a partner with the Deputy Assistant Secretary of Defense for Counter-Narcotics (DASD/CN) and transnational organized crime and is a recognized expert in the field of biometrics and document exploitation. SOCOM has the experience and ability to leverage a wide variety of funding streams to build partner nation capacity to join in the fight against the dark nodes, deny sanctuary, and prevent the spread of extremist ideology or public support for illicit groups. With a globally dispersed command totaling nearly 55,000 personnel, SOCOM is America's best positioned resource capable of achieving success against illicit networks. Most of the anticipated counter-network activities are directly related to SOF's core activities and competencies. This CTN concept envisages SOCOM leading planning and coordination, to include leading the Defense Counter-Threat Network Operations (DCTNO) Coordination Center. However, this concept also suggests significant leadership, direction, and authority be vested in the law enforcement community, supported by the Intelligence Community.

Conceptually, the DCTNOC Director would be a flag level military officer from U.S. SOCOM, the Deputy Director, a flag level civilian executive from DHS, and the Executive Director, a flag level executive from the FBI. These three key leaders form the Defense Counter-Network Senior Steering Group and report to the National Advisory Group, which would be chaired by a senior member of the Office of the Attorney General. In order to facilitate key leader engagement across the Interagency, the Defense Counter-Network Coordination Center would be headquartered in the Washington DC area, with exceptions given to already established operations and logistical support locations. The DCTNOC Senior Steering Group would also be supported by senior personnel from DIA, Treasury, State, DEA, and U.S. Marshals.

The Defense Counter-Threat Network Operations Coordination Center (DCTNOCC) creates the hub from which all DoD counter-network activity is coordinated, executed, tracked, and reported. The Director, DCTN Center coordinates and executes operations in accordance with a SECDEF approved CTN



EXORD as part of the Secretary's CTN Campaign Plan, in support of the President's Counter-Network strategy. Under guidance set forth by the SECDEF, the Director, DCTNOCC, would be responsible for publishing an annual Counter-Threat Network Strategic Plan, collect requirements from the GCCs to address the threats, and adjudicate GCC issues and their input to the Counter-Network Campaign Plan. These requirements and responsibilities would be reflected in new language in the Unified Command Plan. The DCTNO Center's activities would ideally be monitored by the USD/P, and managed by ASD/SOLIC. The USD/P or ASD/SOLIC would be a sitting member and deputy chair of the CTN-National Advisory Group.

The Director, DCTN Center, underpinned by Presidential directive, Congressional appropriation, and authorities delegated to him through the SECDEF would conceptually be granted authority to conduct warrant-based operations through a DoD published, Interagency coordinated *Counter-Threat Network Campaign Plan (CONPLAN 7XXX-series)*, and a SECDEF approved CTN EXORD. The National Agency Group (NAG), chaired by a senior representative from the Department of Justice (National Security Division), would serve as the chair for a senior authoritative body that would approve counter-network operations abroad. The NAG would be composed of representatives from Justice, Law Enforcement, State, Defense, Office of National Drug Control and Policy (ONDCP) and Homeland Security. The NAG would provide Executive Summary Operational and Intelligence reports (prepared by the Director, DCTN Center and through USD/Policy) on a quarterly basis to the National Security Staff, much like the Department of Homeland Security's Maritime Global Operations Threat Response Center (MOTR) does today.³⁴ The MOTR serves as a model for efficiency and results-oriented action against maritime threats. The concept behind the DCTN Operations Coordination Center is to expand operations beyond the maritime domain and provide full spectrum defense to the homeland, and to international partners in this effort.

The DCTN Center would also coordinate with U.S. law enforcement entities to ensure they do not compromise active judicial cases in either U.S. or international courts of law unless the node or threat poses a significant and imminent threat to the United States or its allies. The DCTN Operations and Coordination Center will also coordinate with and work through the DOJ/Asset Forfeiture Program in the event significant assets are seized from major illicit networks. The Director's special staff (primarily comprised of senior executives from the law enforcement and justice communities) coordinate with international agencies and offices for the repatriation of foreign seized assets. Those assets that remain would be utilized to purchase equipment for Counter-Network entities or used for training opportunities with partner nations for capacity building and security assistance programs. This incentivizes action and repatriation to regional partners and additional funding otherwise not available through 1200-series funding programs. Remaining funding would otherwise be utilized to support and fund the directorates of the DCTN Center.

The Defense Counter-Threat Network Center would consist of three major directorates – Intelligence, Operations, and Global Support. DIA would provide the bulk of the intelligence support, conceivably from DIA's Defense Counter-Terrorism Center (DCTC). DCTC (and its predecessor Joint Intelligence Task Force – CT) has maintained a high level of cooperation, success, and history with the SOF Community, contributing the highest number of deployed personnel in the CENTCOM AOR since 9-11 to Joint Special Operation Task Forces (JSOTFs). DCTC would be a natural extension for the creation of a counter-network intelligence operations and analysis directorate with DIA's mastery of media exploitation, all source analysis, and HUMINT. The creation of the Intelligence Directorate under the DCTN Center would form a superstructure for a Joint Intelligence Operations Center (JIOC).



SOCOM has already established the Global Mission Support Center (GMSC) in Tampa, Florida. It could serve as a global support facilitator for the Defense Counter-Threat Network Center, much as it envisions doing the same for the TSOCs. The GMSC would provide 24/7 global logistics, communications, and crisis management support not only for SOCOM headquarters, as it does for the TSOCs. It would maintain awareness of all ongoing or planned counter-network operations worldwide. The TSOCs already form the bulk of the forces U.S. available in well over 80 countries annually. This forward presence would assist in providing that “finger tip feel” in forward locations, train host nation forces in countering these networks, and a platform for other interagency train, assist, and build activities. The GMSC would also host and coordinate weekly Operations and Intelligence (O&I) briefings for the Commander, USSOCOM and the Senior Steering Group.

Probably one of the most important interagency capabilities inside SOCOM is its network of highly trained senior liaison officers networked throughout the government as part of the Inter-Agency Partnership Program or IAPP. Special Operations Support Teams, or SOST officers provide the baseline SOF liaison network in the National Capital Region (NCR). SOCOM also maintains an extensive and distinguished list of Interagency LNOs, one of the legacies of the wars in Iraq and Afghanistan that must be sustained. The SOF LNO network now also extends out to partner nation special operations units and includes exchange officers at the headquarters.

SOCOM recently stood up the Special Operations International Collaboration and Coordination Center in MacDill AFB, FL. The center, known as the ISCC, for the first time provides foreign special operations liaisons space in SOCOM headquarters to coordinate on special operations activities around the world.³⁵ This new organization provides promise to inclusivity in Counter-Network activities at the international level.

With its global reach and light presence through the Theater Special Operations Commands, SOCOM is best paired in the Intelligence Community with the Defense Intelligence Agency (DIA), which can provide specialized HUMINT support, national level document and media exploitation, regional threat analysis (country, narco, terrorist, etc.), and functional analysis of geographically specific nodes that are critical to trafficking routes and organizational sustainment.

The Defense Intelligence Agency (DIA) is already configured into analytic centers as well as DCTC. As stated previously, DCTC could form the basis for Counter-Network Intelligence Operations and Analysis Directorate. Tied directly with the DIA's National Media Exploitation Center (NMEC), DIA, in coordination with FBI and the Department of Treasury, could develop information and intelligence that would form the basis of warrant-based operations and U.S. Treasury Department designations against illicit nodes. SOCOM currently serves as the DoD proponent for illicit finance,³⁶ and the DCNOCC's counter-network activities would go far in operationalizing the work already done by SOCOM's Counter-Threat Finance (CTF) office and other interagency efforts. This concept may streamline very well with DoD Directive 5205.14 *DoD Counter-Threat Finance Policy*, which also directs the Defense Intelligence Agency to conduct intelligence support to threat finance. The Defense Counter-Threat Network concept would establish a Center for Seized Assets under the DCTN Center's Assistant Deputy Director for Partner Engagement (ADDO/PE), which would coordinate all claims and adjudication of seized property to 1) ensure proper repatriation of assets to foreign entities, 2) coordinate sales of remaining property on the open market, 3) return claims to the countries of origin, or 4) destroy residual material (primarily all seized drugs and HAZMAT). A portion of the proceeds captured would be used to fund equipment and other costs associated with conducting counter-network operations. This would require changes to the Asset Forfeiture laws currently managed by the U.S. Marshals.³⁷

The Defense Intelligence Agency (DIA) serves as America's strategic warning system with analysts and collectors across the world, experts in their field of socio-cultural analysis, HUMINT, biometrics, foreign weapons, counter-terrorism and counter-narcotics analysis. Gil Kerlikowski, the President's former director for the Office of National Drug Control Policy (ONDCP), and recent appointee as Customs and Border Protection (CBP) at Department of Homeland Security, visited DIA in December 2013 to discuss the close working relationship between DIA and other U.S. government organizations committed to the counter-narcotics mission. It is partnerships like this that portend positive trends towards gaining efficiencies as budgets are squeezed in tight economic times. With an endorsement from national offices like ONDCP and DHS, the White House has an opportunity to take this momentum forward and begin a series of confidence building measures to develop a comprehensive Counter-Network strategy. Through the historical ties between DIA and SOCOM, a Defense Counter-Threat Network Collaboration Center or Cell may prove to be the start of a much more comprehensive and effective "one-stop" organization.

Conclusion

In order to build momentum for a proof of concept, a series of senior level orientation meetings at the national advisory level on the topic of "Illicit Networks - Combatting Convergence," might be in order, modeled after the Proliferation Security Initiative, or "PSI" table top exercise recently hosted by U.S. Southern Command.³⁸ The Miami exercise was the first presentation of this framework and an associated toolkit that provides specific measures to enhance a nation's capability to interdict -- from legal tools and rapid decision making best practices to operational training, in concert with other U.S. government programs like the U.S. State Department's Export Control and Related Border Security Program.³⁹ After three years of negotiation, USSOCOM and NORTHCOM will host a Transnational Organized Crime conference in May 2014, with the intent of bringing this subject to the interagency level. As the proof of concept for Counter-Threat Network Operations grows, a follow on "Countering Illicit Networks" Table Top exercise, with cooperation from representatives of the Organization of American States (OAS), Association of South East Asian Nations (ASEAN), and NATO may be the next step.

A final proof of concept tied to a real world operation could be presented to the White House (through State, Defense, and Justice) for approval based on cooperating nations that request support from the provisional Counter-Threat Network Task Force. Measures of effectiveness must be identified to ensure the U.S. and its partner nations have a list of realistic and achievable goals and objectives. There is much to be done. Up to the present day, there have been multiple conferences and seminars across the globe discussing this growing threat. Several governments, associations, and international NGOs have all recognized the need to bring an end to this human scourge. The question is always resources and authorities. The United States possesses unparalleled capability and reach. SOCOM, tied with DIA has the personnel, subject matter expertise, and historical ties throughout the globe to be an effective partner in this effort. It takes a network to defeat a network. It is time to make that interagency network a reality.

¹ Angel Boraza, Steven Borel, eds., *Ungoverned Territories: Understanding and Reducing Terrorism Risks*, 2007 (Santa Monica, CA: 200&), see: www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG561.sum.pdf, accessed: January 12, 2014.

² Alex Knapp, *Did Organized Crime Save the Banking Business?*, OutsideTheBeltway.com, December 14, 2009, see: http://www.outsidethebeltway.com/did_organized_crime_save_the_banking_system/, accessed January 12, 2014.



³ William Becker, *Hawala Underground Banking*, (Source: Mr. John Cassara, US Department of Treasury), DecodeTransmission, December 27, 2010, see: <http://decode.transmission.blogspot.com/2010/12/hawala-underground-banking.html>, accessed: December 11, 2013.

⁴ Christopher Sims, *Fighting the Insurgents War in Afghanistan*, SmallWarsJournal.com, January 12, 2012, see: <http://smallwarsjournal.com/jrnl/art/fighting-the-insurgents%E2%80%99-war-in-afghanistan>, accessed February 3, 2014.

⁵ Thom Shanker, *Globalization Creates a New Worry – Enemy Convergence*, WashingtonPost.com, May 30, 2013, accessed January 31, 2014, see: http://atwar.blogs.nytimes.com/2013/05/30/globalization-creates-a-new-worry-enemy-convergence/?_php=true&_type=blogs&r=0.

⁶ Canada and Terrorism, ADL.org, January 2004, accessed January 2014, see: http://archive.adl.org/terror/tu/tu_0401_canada.html#.Utros-ko6M8.

⁷ Richard Marosi, *Controversial Cleric Arrested by Border Agents*, TheStar.Com, January 26, 2011, accessed January 7, 2014, see: http://www.thestar.com/news/world/2011/01/26/controversial_cleric_arrested_by_border_patrol_agents.html.

⁸ Robert Spencer, *Canada: Islamic Charity Group Classified as Terrorist Group, Aided Hamas for Years*, JihadWatch.com, April 29, 2014, accessed: April 29, 2014, see: <http://www.jihadwatch.org/2014/04/canada-islamic-charity-classified-as-terrorist-group-aided-hamas-for-years>.

⁹ Source Figure: Source: <http://urbansurvivalplan.com/wp-content/uploads/2009/06/terrormap.png>.

¹⁰ Andrea Stone, *Iran Plot to Assassinate Saudi Ambassador Foiled by DOJ Sting*, HuffingtonPost.com, November 12, 2011, accessed: February 4, 2014, see: http://www.huffingtonpost.com/2011/10/11/iran-terror-plot-saudi-arabia-ambassador-us-assassination_n_1005861.html.

¹¹ See: <http://www.fbi.gov/news/stories/story-index/>.

¹² Omari Fleming, *San Diego Gangs Cash in on Sex Trafficking*, NBC News San Diego, January 29, 2014, see: <http://www.nbcsandiego.com/news/local/San-Diego-Gangs-Cash-in-On-Sex-Trafficking-242683571.html>. accessed: February 4, 2014.

¹³ Steven Camarota, *Immigrants from the Middle East: A Profile of the Foreign Born Population from Pakistan to Morocco*, Center for Immigration Studies, August 2002, see: <http://www.cis.org/articles/2002/back902.html>, accessed: February 4, 2014.

¹⁴ Ong Sor Fin, *Six Facts About Fake Passports*, The Nation, March 12, 2014, see: <http://www.nationmultimedia.com/opinion/Six-facts-about-fake-passports-30228944.html>, accessed: March 25, 2014.

¹⁵ National Journal, *FBI Monitors Fighters Trained in Syria, Now Back in US*, February 5, 2014, NTI.org, accessed February 7, 2014, see: <http://www.nti.org/gsn/article/fbi-monitors-fighters-trained-syria-back-us/>.

¹⁶ United Nations News Center, *UN-backed Container Exhibit Spotlights Plight of Sex Trafficking Victims*, United Nations Office of Drugs and Crime, February 6, 2008, see: <http://www.un.org/apps/news/story.asp?NewsID=25524&Cr=trafficking&Cr1>, accessed: March 14, 2014.

¹⁷ Douglas Farah, *Fixers, Super Fixers and Shadow Facilitators: How Networks Connect*, ed., in *Convergence: Illicit Networks and National Security in the Age of Globalization*, Center for Complex Operations, Institute for National Strategic Studies, (Washington, DC: National Defense University Press), 2013, p. 75.

- ¹⁸ UNODC World Drug Report. June 2013, accessed January 14, 2014, see: <http://www.unodc.org/wdr/>. Note: \$800B is author's estimate based on the cumulative totals from charts available in UNDOC Annual Reports.
- ¹⁹ Evelyn Morris, "Think Again: Mexican Drug Cartels," Foreign Policy.Com, 14 DEC 2013, see http://www.foreignpolicy.com/articles/2013/12/03/think_again_mexican_drug_cartels.
- ²⁰ David Malone, A Word About Banks and the Laundering of Drug Money, Golemiv.co.uk, August 18, 2012, accessed January 18, 2014 see: <http://www.golemiv.co.uk/2012/08/a-word-about-banks-and-the-laundering-of-drug-money/>.
- ²¹ Andrew Bergman, CNN Money, *Worlds Largest Economies*, CNN.com, accessed January 11, 2014, see: http://money.cnn.com/news/economy/world_economies_gdp/.
- ²² UNODC World Drug Report. June 2013, accessed: January 14, 2014, see: <http://www.unodc.org/wdr/>.
- ²³ United Nations Office of Drugs and Crime, *Transnational Organized Crime in East Asia and the Pacific – A Threat Assessment*, April 25, 2013, see: <http://www.unodc.org/southeastasiaandpacific/en/2013/04/toc-env-crime/ story.html>, accessed: March 19, 2014.
- ²⁴ Office of the President of the United States, *Strategy to Combat Transnational Organized Crime – 2011* (Washington DC: Government Printing Office, 2011).
- ²⁵ Evelyn Morris, Think Again: Mexican Drug Cartels, in ForeignPolicy.com, December 4, 2013, accessed January 11, 2014, see: http://www.foreignpolicy.com/articles/2013/12/03/think_again_mexican_drug_cartels
- ²⁶ See: <http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism>.
- ²⁷ Stanley A. McChrystal, *It Takes a Network: The New Front Line of Modern Warfare*, ForeignPolicy.Com, February 22, 2011, accessed: January 29, 2014, see: http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network.
- ²⁸ Center for Government Interoperability, *Blueprint for Better Government*, Gov-Ideas.com, See: <http://www.gov-ideas.com/cfgio.htm> accessed: March 29, 2014.
- ²⁹ See: <http://www.dhs.gov/global-motr-coordination-center-gmcc>.
- ³⁰ See: www.nctc.gov
- ³¹ United States Government Accounting Office (GAO), *FBI-DEA Task Forces: An Unsuccessful Attempt at Joint Operations*, March 26, 1982, (Washington, DC: GAO).
- ³² Kelly Riddel, *Anti-Drug Task Force Withholds Data, Blocks Probes*, Washington Post, March 26, 2014, see: [http://www.washingtontimes.com/news/2014/mar/26/anti-drug-task-force-withholds-data-blocks-probes-/,](http://www.washingtontimes.com/news/2014/mar/26/anti-drug-task-force-withholds-data-blocks-probes-/) accessed: March 29, 2014.
- ³³ US Special Operations Command, *About USSOCOM*, see: <http://www.socom.mil/Pages/AboutUSSOCOM.aspx>, accessed: March 29, 2014.
- ³⁴ See: <http://www.dhs.gov/global-motr-coordination-center-gmcc>, accessed: March 29, 2014.
- ³⁵ Howard Altmann, *Tampa to Become Epi-Center of International Special Operations Coordination*, Tampa Bay Tribune, October 18, 2013, see: <http://tbo.com/list/military-news/tampa-to-become-epicenter-of-international-special-operations-coordination-20131018/>, accessed: March 18, 2014.
- ³⁶ Office of the Secretary of Defense, *DoD Directive 5205.14: DoD Counter Threat Finance Policy*, August 19, 2010, incorporated with changes on November 16, 2012, (Washington, DC, 2010), see: www.dtic.mil/whs/directives/corres/pdf.520514p.pdf, accessed: March 29, 2014.
- ³⁷ See: <http://www.usmarshals.gov/assets/assets.html>, accessed: March 29, 2014.
- ³⁸ Michael Wimbish, *SOUTHCOM hosts Caribbean security leaders to discuss illicit trafficking*, US SOUTHCOM Public Affairs release, December 12, 2012, see:



<http://www.southcom.mil/newsroom/Pages/SOUTHCOM-hosts-Caribbean-security-leaders-to-discuss-illicit-trafficking.aspx>, accessed: March 29, 2014.

³⁹ Jim Garamone, US Combats Nexus of Illicit Networks, WMD Proliferation, Defense.gov, January 30, 2014, accessed January 31, 2014, see: <http://www.defense.gov/news/newsarticle.aspx?id=121574>.