Inter Agency Paper

No. 14W
November 2014

Strategic Approach to Combat Transnational Organized Crime

Derrick Iwanenko, Simon McKenzie, Nishawn Smagh, Natalie Vanatta and Jason Shinn

Arthur D. Simons Center
for Interagency Cooperation

Fort Leavenworth, Kansas

An Interagency Occasional Paper published by the CGSC Foundation Press

Strategic Approach to Combat Transnational Organized Crime

Derrick Iwanenko, Simon McKenzie, Nishawn Smagh, Natalie Vanatta and Jason Shinn

Arthur D. Simons Center
for Interagency Cooperation

Fort Leavenworth, Kansas

InterAgency Paper No. 14W, November 2014

Strategic Approach to Combat Transnational Organized Crime

by Derrick Iwanenko, Simon McKenzie, Nishawn Smagh, Natalie Vanatta and Jason Shinn

---

U.S. Air Force Major Derrick Iwanenko is an assistant director of operations and E-3 AWACS mission crew commander in the 965th Airborne Air Control Squadron, Tinker Air Force Base. In his prior job, he served as the senior Air Force analyst, Commanders Initiative Group, Headquarters United States Forces Korea where he was responsible to the commander, U.S. Forces Korea/Combined Forces Command/United Nations Command for focused studies and joint/combined staff initiatives.

U.S. Army Major Simon McKenzie is the battalion executive officer for the Army's only Airborne Signal Battalion, the 112th Signal Battalion (Special Operations) (Airborne). He was recently transitioned from being the battalion operations officer this past summer and is a graduate of the Army's Resident Command and General Staff Officer Course at Fort Leavenworth, Kan.

U.S. Air Force Major Nishawn Smagh serves as a branch chief within the Strategic Relocatable Targets Division for the Joint Intelligence Operations Center, United States Strategic Command. In prior operational assignments he served as the director of operations for both the 324th Intelligence Squadron and the 495th Expeditionary Intelligence Squadron.

U.S. Army Major Natalie Vanatta is a signal officer currently serving as the 509th Signal Battalion executive officer. She has worked from tactical to operational levels in the signal arena while also teaching/researching in the cyber field. She earned her doctorate degree in Applied Mathematics from the Naval Postgraduate School.

U.S. Army Major Jason Shinn is an intelligence officer with more than 20 years experience. He has worked from tactical to strategic levels in intelligence and has served in several joint and interagency assignments.

Questions about this paper and the InterAgency Paper series should be directed to the Arthur D. Simons Center, 655 Biddle Blvd., PO Box 3429, Fort Leavenworth KS 66027; email: office@TheSimonsCenter.org, or by phone at 913-682-7244.

Contents

Introduction

Conservative estimates state that transnational organized crime (TOC) generates at least $6 trillion dollars in illicit funds annually.[1] These funds disrupt free markets by detracting from the global gross domestic product (GDP), finance criminal activities that undermine both democracy and global stability, and victimize unstable governments via bribery, violence, and terror. Organized crime consists of sophisticated groups and networks that aim to obtain power, influence, and monetary and/or commercial gains by operating illegal, international enterprises that are capable of moving people, drugs, money, and weapons across borders.[2] These transnational criminal networks are growing and diversifying their illicit operations resulting in the dangerous convergence of threats that has evolved to become more complex, volatile, and destabilizing.[3]

In July 2011, President Obama designated transnational organized crime as a national security threat.

In July 2011, President Obama designated TOC as a national security threat.[4] Despite this emphasis, the U.S. government still lacks a comprehensive, whole-of-government approach to combat the influences, activities, and threats posed by TOC toward U.S. national security in the homeland and strategic regions around the world. The President's "National Strategy to Combat Transnational Organized Crime" identifies this threat as a multifaceted and complex network that presents a serious threat to the lives of U.S. citizens and the American way of life. The following excerpts represent, arguably, the most threatening aspects of TOC toward U.S. national security.

- **Convergence of terrorism and TOC**: The line between terrorism and TOC has become increasingly blurred as these organizations discover common interests and learn from one another. Indeed, some suggest that terrorism and TOC comprise a new, hybrid threat rather than two separate problems. Terrorists have discovered the advantage in using existing TOC logistical networks, while TOC organizations are increasingly relying on violent tactics learned from their terrorist counterparts. Additionally, TOC provides significant funding and resource support to terrorist activities. In 2010, the Department of Justice (DOJ) indicated that 29 of the 63 top drug trafficking organizations possessed links to terrorist organizations.[5] TOC networks are highly adaptive and able to transport and distribute a variety of illegal products that ultimately cross U.S. borders undetected thousands of times each day.[6]

- **Potential to transfer weapons of mass destruction (WMD)**: Terrorist acquisition of chemical, biological, and radiological or nuclear capabilities is the highest national security threat facing the U.S. today and for the near future. Existing TOC networks can easily facilitate the stealthy movement of WMD across borders, as they already possess the capability to transport and distribute other illicit materials. The financial capabilities and affiliations of TOC also provide an opportunity to successfully acquire and sell WMD materials to enemies of the U.S.

Transnational Organized Crime threatens the economic interests of the U.S. and causes irreparable damage to the world financial system by undermining legitimate markets.

- **Potential to threaten interconnected global trading and financial systems**: TOC threatens the economic interests of the U.S. and causes irreparable damage to the world financial system by undermining legitimate markets. The World Bank estimates that about $1 trillion are spent each year to bribe public officials.[7] Additionally, United Nations estimates suggest that drug trade revenues may surpass $400 billion annually, placing drugs between the auto and oil industries as the planet's top earners.[8] Illegal activities conducted by organized crime weaken the global economy and result in lost tax revenue for local, state, and federal governments. While this may seem to be a victimless crime, the loss of income to governments impacts the provision of essential services to their populations.

- **Successful use of human smuggling channels**: The United Nations Office on Drugs and Crime estimates that the smuggling of persons from Latin America to the U.S. generates approximately $6.6 billion annually in illicit proceeds.[9] International human smuggling networks are also linked to drug trafficking, government corruption, and numerous TOC organizations and may serve as a covert means for terrorists to enter the U.S. However, terrorist groups may also be involved in human smuggling and other travel-related criminal activities—not only as a source of terrorist financing but also for logistics purposes. As the "9/11 Commission Report" explains, terrorists use evasive methods to travel without detection, including the use of altered and counterfeit passports and visas, human smuggling networks, and immigration and identity fraud.[10] For terrorists, it further states, "travel documents are as important as weapons."[11] Terrorists must travel clandestinely to meet, train, plan, survey targets, and gain access to attack.[12] In other cases, criminal organizations may pay terrorist groups for security support, armed protection, and safe passage of contraband through terrorist-controlled territories.

- **Potential to impede the development of weak states**: Weak or failed states provide the permissive environments necessary

for TOC to conduct illicit activities. TOC organizations not only migrate into weak states, but also actively seek to prevent strong governance by providing resources to opposition elements and fostering state corruption.

- **Access to virtually unlimited resources**: TOC organizations maintain threat capabilities through their successful resourcing ability and the sheer scale of their enterprise. The two most profitable activities that fund these organizations are drug trafficking and cybercrime. Drug trafficking provides the added bonus of directly killing Americans and increasing local crime and corruption within the U.S. Cybercrime has the added bonus of cheaply disrupting essential services to create panic and uncertainty in the public. The "National Strategy to Combat Transnational Organized Crime" estimates $6 trillion as the global criminal proceeds—this is 10 percent of the world's GDP.[13]

Combating Transnational Organized Crime

Disjointed efforts, a lack of understanding, and limited motivation to participate characterize the current state of affairs on combating TOC. Multitudes of agencies and organizations within the U.S. have roles in collection, analysis, enforcement, or prosecution; however, a culture of collaboration and trust on how to combat TOC does not exist. Individual agencies are focused on specific individuals or countries looking for the quick, easy victories. However, as the U.S. has learned from attempting to dismantle Al Qaeda, when one cuts off a cell or a leader, another steps in to take his place. The support network needs to be dismantled in order to have lasting effects on the organization. This is not a quick or easy task to perform.

Disjointed efforts, a lack of understanding, and limited motivation to participate characterize the current state of affairs on combating TOC.

Disjointed efforts occur because government agencies and organizations are familiar and comfortable working within their stovepipes of excellence (fiefdoms). Extending trust to outsiders in order to coordinate efforts is difficult. This lack of collaboration causes groups to reinvent the wheel. In a time of constrained fiscal policy, this is not an efficient use of resources.

Additionally, a general lack of understanding of TOC and its environment hampers U.S. government efforts. Ask twenty people what TOC is, and each will provide a different answer. More importantly, only limited TOC network analysis exists, and it is not shared effectively. Therefore, there is no analytic study of the emergent behavior of the groups and/or the effects of U.S. government actions on various portions of the network. Having an

incomplete understanding of the environment and its issues makes it difficult, if not impossible, to achieve long-term goals.

Finally, over the last decade, the intelligence community has focused its efforts toward the War on Terrorism and the two ensuing wars in Iraq and Afghanistan. Globalization and adversary access to resources and technology have added to the complexity of its task, and few resources remain available to monitor or combat TOC. More importantly, there is limited motivation to commit these scarce resources or re-task resources to focus on transnational criminal organizations.

Integrated Transnational Organized Crime-Strategic Center

...the U.S. government should "build, balance, and integrate the tools of American power" against TOC...

In order to succeed, the U.S. government should "build, balance, and integrate the tools of American power" against TOC,[14] which necessitates a whole-of-government approach with partner-nation contribution. First, a TOC-focused analytic capability is required to identify organizations, networks, and activities that pose a national security threat. Elements from across the government should be integrated into this capability to function as both producers and consumers of this analysis.

Second, a TOC leadership integration board must be established and capable of prioritizing targets, deconflicting requirements, and committing organizational resources to support and conduct counter-TOC activities. This board will serve as a balance across the various agencies and communities to ensure that efforts meet U.S. policymakers' priorities.

Third, the U.S. government must build mechanisms to channel the outputs of these capabilities to the action arms of the government (both U.S. and partner nations). Conduits of information flow already exist within the intelligence community, but an additional capability must be built to optimize information sharing and bolster the capabilities within the U.S. to/from our partner nations. The implementation of a Transnational Organized Crime-Strategic Center (TOC-SC) will enable a whole-of-government and partner-nation collaborative strategy to limit the influence of transnational criminal activities threatening U.S. national security.

TOC-SC Mission

The TOC-SC will focus U.S. government strategic efforts to accomplish two missions: (1) identify areas where TOC poses a credible threat to U.S. national security, and (2) enable whole-of government and partner-nation collaboration to limit the influence of transnational criminal organization activities threatening U.S. national security. The central goal of these missions is to reduce

TOC from a U.S. national security threat to a manageable public safety problem in the U.S. and strategic regions around the world.[15] The TOC-SC will accomplish this mission by:

- Maintaining a robust analytical hub to identify threats and their resource networks.
- Prioritizing threats (networks, groups, activities, and actors).
- Developing counter-threat network approaches.
- Managing and enabling information sharing among organizations across the globe.
- Coordinating intelligence to enable law enforcement actions.
- Fostering transnational and cross-organizational strategic security partnerships.
- Building international capacity, cooperation, and partnerships.

TOC-SC should operate as a partnership of organizations and serve as the primary organization to analyze and integrate all intelligence pertaining to TOC possessed or acquired by the U.S. government. The TOC-SC director will serve as the principal advisor to the Director of National Intelligence (DNI) on intelligence operations and analysis to counter TOC while advising the DNI on how well U.S. intelligence activities, programs, and budget proposals for counter-TOC conform to priorities established by the President. Given the gravity of this topic and to facilitate interagency cooperation and collaboration, the TOC-SC director should be appointed as the National Intelligence Manager (NIM) for TOC. NIMs are senior government enterprise leaders with experience coordinating activities and managing issues across diverse organizations so that requirements are met on a daily, short-term, and long-term basis.

TOC-SC should operate as a partnership of organizations and serve as the primary organization to analyze and integrate all intelligence pertaining to TOC possessed or acquired by the U.S. government.

TOC-SC will establish a robust intelligence and analytic capability in order to identify areas where TOC poses a credible threat to U.S. national security. The strength of this analytic cell comes from its (1) interagency work force, (2) access to information, (3) focused expertise, and (4) integrated and rigorous analysis. Therefore, this cell must include multiple U.S. government agencies, each of which brings unique capabilities to the table. The TOC-SC should be composed of, but not limited to, elements from each of the following organizations: DNI, Central Intelligence Agency (CIA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Department of Defense (DoD), Department of State, DOJ, Department of Energy, Department of Transportation, Department of Homeland Security

(DHS), Treasury, National Reconnaissance Office (NRO), National Geospatial-Intelligence Agency (NGIA), U.S. Immigration and Customs Enforcement (ICE), combatant commands, U.S. Agency for International Development (USAID), and the "Five Eyes" partner nations (Australia, Canada, New Zealand, the United Kingdom, and the U.S.). This mixture of expertise will integrate the communities of intelligence, law enforcement, cabinet departments, and allies. It will also enable each group to tie in its organic networks of information to the TOC problem set. To reinforce interagency cooperation and collaboration, the TOC-SC analytic cell must be centrally located with each agency representative possessing access to both a TOC-SC common information technology network and his/her parent organization's command, control, communications, and intelligence networks.

The TOC-SC analytic cell must also be tied into the other national fusion centers. TOC is such a diverse network that several other centers already maintain analytic capabilities and information on their portions of associated national security challenges. For example, the National Counterproliferation Center and the National Counterterrorism Center (NCTC) maintain critical information that should be shared with the TOC-SC and vice versa.

In its mission to combat TOC, the TOC-SC analytic cell will be in direct support to its operational counterparts—intelligence, law enforcement, military, diplomatic, and regulatory.

In its mission to combat TOC, the TOC-SC analytic cell will be in direct support to its operational counterparts—intelligence, law enforcement, military, diplomatic, and regulatory. This analytic cell will conduct network analysis and establish a common visualization of the operational environment. The intent is not to reinvent the wheel but to leverage all departments' and agencies' current frameworks, tools, programs, and expertise. Some suggested frameworks are discussed in a recent National Security Affairs report, "The 'New' Face of Transnational Crime Organizations: A Geopolitical Perspective and Implications to U.S. National Security." Additionally, the analytic cell will create and maintain viable approaches to countering the identified TOC threats. These methodologies should allow rigorous assessments of the credibility of threats and the relevance of incidents. Finally, the analytic cell must capture and utilize lessons learned from regional TOC efforts, as well as similar efforts throughout the U.S. government.

Visualize and Understand the Environment

A method to visualize and understand the environment is to define it in terms similar to the military's operational variables: political, military, economic, social, infrastructure, information, physical environment, and time (PMESII-PT).[16] However, slight alterations to address TOC provide a more complete method to visualize and understand the TOC environment. TOC analysis in terms of visualizing and understanding politics should include state governance strengths, weaknesses, and sources of corruption. Additionally, the rule of law analysis should include law enforcement, the judiciary, and the correctional systems. The economic variable must include an understanding of legitimate financial markets and the black market along with a focus on key goods. The social variable must monitor the key elements that describe or influence social dynamics within the organization and the state. The infrastructure variable includes the status of basic services, education, health, and transportation within the area that a TOC network operates. Finally, the information variable has the key elements of state and TOC information capabilities that facilitate information sharing and distribution with the local population. Analysis of these focus areas will support efforts to understand the environment and identify areas where the U.S. government and partner nations can address shortfalls and capitalize on strengths in order to diminish the influence of TOC. Key to this effort is performing an equivalent level of analysis focused on how TOC interacts, influences, and undermines each of these elements. This focus area will reinforce efforts to map TOC networks at the local, state, regional, and global levels and provide opportunities to identify threats presented by transnational criminal organizations.

TOC analysis in terms of visualizing and understanding politics should include state governance strengths, weaknesses, and sources of corruption.

Mapping the TOC network provides the opportunity to understand the network as a whole and not as disparate entities that perform specific functions. Central to this effort is identifying key TOC leaders, facilitators, capabilities, resources, strengths, and weaknesses. In short, mapping the network enables center of gravity (CoG) analysis to include analysis of the network's critical capabilities, critical requirements, and critical vulnerabilities. U.S. Army Colonel Dale C. Eikmeier defined CoG as "a system or network's source of power that creates a critical capability that allows an entity to act or accomplish a task or purpose."[17] In the case of TOC, the supporting network is arguably the CoG.

Critical capabilities are the key abilities that a CoG possesses

that help produce conditions for achieving an identified end state. For example, an organization establishes a goal; in terms of TOC, a plausible goal includes gaining increased profits. The critical capability is the means to achieve that goal, i.e., trafficking and smuggling of drugs, money, people, or weapons. Critical requirements are the essential means for a critical capability to be fully operative. For example, critical requirements of a TOC organization may include transportation and logistics, money, protection, weapons, weak governments, and corruption. Without critical requirements, a CoG (the network) cannot function successfully and will cease being a source of power that generates the critical capability (trafficking and smuggling). Although a network might require many things, few requirements are critical. The task is to identify those that are and then identify if those requirements are vulnerable to action. Critical vulnerabilities are those critical requirements that are vulnerable. All networks possess deficiencies that are vulnerable to attack, disruption, or exploitation. Critical vulnerabilities make great targets and objectives for action. The discovery of these critical vulnerabilities should drive and bolster law enforcement and intelligence operations to identify persons, organizations, activities, threats, and/or capabilities for collection, exploitation, and/or action. In the case of TOC, money is a prime critical vulnerability that, if attacked, will impact the ability of the network to operate successfully.[18]

National-Level Integration Board

When the TOC-SC analytic capability identifies threats to national security, a national-level integration board should prioritize the resources and efforts.

When the TOC-SC analytic capability identifies threats to national security, a national-level integration board should prioritize the resources and efforts. This board would handle issues ranging from collection and analysis to interdiction. To achieve this mission, the TOC Integration Board should consist of senior representatives, empowered to commit resources from their respective agencies. This board should meet twice a year or as needed. Voting members would include DoJ, FBI, CIA, DoD, Chairman of the Joint Chiefs of Staff, NSA, NGIA, DIA, DEA, DHS, Department of State, Treasury, and DNI. Voting members are established due to their inherent capability to limit the influence of TOC activities; all other participating agencies will serve as valued advisors. Ultimately, the DNI should serve as the tiebreaker for the prioritization of resources and associated efforts.

TOC-SC Activities

On a day-to-day basis, the TOC-SC will enhance intelligence operations, analysis, and information sharing among U.S. government agencies and partner nations and help build international capability,

cooperation, and partnerships to counter TOC. The synergistic effects of these activities will enable a whole-of-government and partner-nation strategy to perform law enforcement activities; protect global and U.S. financial systems and strategic markets; help partner countries strengthen governance and transparency; sever state-crime alliances; strengthen interdiction, investigations, and persecutions; disrupt drug trafficking and its facilitation of other transnational threats; and, inevitably, defeat TOC networks that pose the greatest threat to U.S. national security.

Key to the execution of TOC-SC activities is the ability to share information among its members as well as fuse foreign intelligence with a wide spectrum of domestic information. This locally-gathered information comes from a broad array of law enforcement, public health and safety, and private sector sources.[19] Therefore, the TOC-SC should establish information systems and architecture that enable access to, as well as integration, dissemination, and use of TOC information.

Key to the execution of TOC-SC activities is the ability to share information among its members as well as fuse foreign intelligence with a wide spectrum of domestic information.

TOC-SC Information Technology Network

The TOC-SC information technology network has five core functions:

- Produce and orchestrate all-source intelligence analysis, including strategic and alternative analysis.
- Coordinate cross-community planning and integration efforts and develop common objectives and measures of effectiveness.
- Orchestrate and prioritize community information needs and establish processes for integrating and tracking information needs across agencies.
- Orchestrate all-source information acquisition and dissemination and adopt common standards and business processes (see Appendix 1 and 2 for more discussion on information sharing).
- Establish centralized and shared knowledge banks, intelligence integration and analytic tools, and information systems.

If military, intelligence, law enforcement, homeland security, and allied networks are integrated, robust information sharing can occur. TOC-SC analysts must be able to access their complete parent organizations' information network as well as the TOC-SC common network from their desks. Multiple networks should be accessible through a single log-on with established, secure mechanisms to ease data transfer between layers.

The TOC knowledge base should contain highly pertinent data

that is organized and standardized for ease of use from a variety of sources. The NCTC utilizes a system that could serve as a model for the TOC knowledge base. These network-based, information-sharing systems have a set of applications that transcend traditional government boundaries to provide users with centralized access to intelligence and analysis.

The TOC-SC analysis tools, optimized for the data within the environment, will provide the analysts with the ability to choose tools tailored to their tasks. U.S. Southern Command (SOUTHCOM) has one example of a successful tailored tool called Whole-of-Society Information Sharing for Regional Display (WISRD).[20] Ultimately, the TOC-SC should be able to provide 24/7 situational awareness, incident reporting, and information tracking in support of government-wide counter-TOC activities.

By providing a centralized, dedicated analytic center of excellence, the TOC-SC will enable thorough coordination among U.S. agencies, as well as international partners.

By providing a centralized, dedicated analytic center of excellence, the TOC-SC will enable thorough coordination among U.S. agencies, as well as international partners. It will provide clear identification of TOC networks, as well as the specific threats to U.S. and allied interests and permit efficient allocation of resources and prosecution of TOC threats in the international environment.

Finally, the TOC-SC must aid in building the capacity of partner nations. This is the capacity of intelligence, military, judiciary, and law enforcement assets to counter TOC threats and maintain the country's sovereignty. At the strategic level, TOC-SC can enable a whole-of-government approach to organize, train, and equip partner nations to more effectively combat TOC. For example, TOC-SC can leverage its multiagency capability to help develop doctrine and provide guidance on optimal institutional organization of partner-nation capabilities that enhance counter-TOC activities. Moreover, TOC-SC can coordinate and/or provide training opportunities to build and enhance necessary skills and tradecraft. Finally, TOC-SC may be positioned to provide equipment (hardware/software) that enhances intelligence operations and information sharing. Currently, many partner nations are missing access or lack understanding of the strategic TOC picture. Providing the geospatial capability to visualize threats will enable them to take action while understanding the impact that an operation might have on a network. The building of partner-nation capacity must be a focused effort by all elements of the U.S. government. The relationships that result are based on trust and are a long-term investment for the U.S. They are essential for the U.S. to remain the partner of choice.

Several key considerations must be addressed in establishing the TOC-SC, including who should be the NIM-TOC, what legal concerns must be addressed in creating the TOC-SC, where the funding should come from, and how does the concept of TOC-SC

gain acceptance in the various communities.

The title of National Intelligence Manager does not come with a government budget line or super powers. NIMs are the focal point within the Office of the Director of National Intelligence for the integration of all activities related to a certain function. They are successful because of their expertise and the relationships they have created with the various communities over the years. However, they cannot directly task an agency or organization to provide resources or accept a mission. The span of TOC activities is large and primarily falls into the law enforcement arena; therefore, it makes sense that either the NIM or the Deputy NIM for TOC is an individual with a law enforcement background. The other position could then be filled with an individual with an intelligence background. Ensuring the leadership of the TOC-SC has a broad span of expertise would assist in the acceptance and understanding of the various agencies and organizations that deal with an aspect of TOC.

The idea of sharing information between intelligence and law enforcement communities is always troublesome. The protection of sources, methods, and U.S. citizens is paramount for the TOC-SC to be successful. The passage of various executive orders and laws over the last twenty years has helped authorize collaboration between disparate agencies within the U.S. government. For instance, President Reagan's Executive Order 12333 authorized the CIA to "participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers or international terrorist or narcotics activity."[21] Other examples of legislation include the Patriot Act (and its amendments), the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the Western Hemisphere Security Cooperation Act of 2012, House Resolution 4303, and the Department of State Rewards Program Update and Technical Corrections Act of 2012.

The idea of sharing information between intelligence and law enforcement communities is always troublesome. The protection of sources, methods, and U.S. citizens is paramount for the TOC-SC to be successful.

Initially, the NCTC faced the same challenges with respect to sharing information across various government organizations. The NCTC traces its authorities back to the National Security Act of 1947, the Homeland Security Act of 2002, the IRTPA, Executive Order 12333, and Executive Order 13388.[22] The IRTPA assigns primary missions to the NCTC and authorities/responsibilities to the Director to ensure those missions are executed. EO 13388, dated October 2005, provides for improved sharing of counterterrorism information across the U.S. government.[23] TOC-SC is a whole-of-government, partner nation focused approach that heavily relies on timely, effective information sharing. In order to effectively accomplish the TOC-SC mission, the center will need a legal foundation similar to what the NCTC and other national fusion centers already possess. Therefore, Congress and the President

should modify, adapt, and/or enhance existing legislative authorities and mandates to target various dimensions of the TOC problem. Such approaches may be region specific, group specific, or global in scope.

The current state of budget decreases and funding oversight has created a "competing priorities" environment within the federal government. Without belaboring the need and importance of TOC-SC, the center's realization will hinge on the funding made available to conduct activities. There are at least three funding options that should be explored.

- Increase the funding of federal law enforcement agencies working in more traditional crime-fighting manners that include organized crime. Administratively allocating these resources to criminal programs could potentially more closely align organized crime agent utilization without taking resources away from higher priority areas.[24]

- Provide direct funding for TOC matters to ensure that any increase in funding intended for criminal programs or TOC would be utilized in those areas.

- Share or redirect funding from counterterrorism to TOC. The ever-growing direct link between terrorism and TOC establishes the case to reevaluate the funding and resource allocation. Establishing and funding the TOC-SC would ensure Congress the most efficient use of funding and resources to enable a whole-of-government, partner nation collaborative approach.

No agency or organization within the U.S. government disputes that TOC is a national security threat. However, the current interagency process often hinders or even prevents the accomplishment of U.S. strategic and national objectives.

The acceptance of a new idea (TOC-SC) by a diverse group of individuals requires demonstrated benefits and inspiration. No agency or organization within the U.S. government disputes that TOC is a national security threat. However, the current interagency process often hinders or even prevents the accomplishment of U.S. strategic and national objectives. Agencies within the U.S. government work within varying cultures and foster contrasting attitudes that often result in bias or even resentment toward other organizations. To gain initial acceptance of the usefulness of TOC-SC, proponents must clearly show how its components will benefit each individual agency and organization that participates. One example is to show that added resources and analysis capabilities would be available for their use. Another example is to demonstrate how the TOC-SC capabilities will complement and assist an agency's primary mission.

As with any new idea seeking acceptance, dynamic leadership can inspire confidence. The idea of TOC-SC must be socialized throughout the U.S. government. Writing in various trade publications or holding persuasive conversations with TOC stakeholders can spread the concept of TOC-SC. To be successful, the concept must

have a clear vision and mission statement, demonstrate relevance against a current-day threat, and be built on accepted, successful components of other national fusion centers.

It will take concentrated and sustained effort by U.S. federal agencies and the international community to aid regional and local states in the disruption of transnational criminal organizations. TOC-SC can serve as the catalyst for changing the attitudes of the intelligence community by focusing on information sharing within the interagency community, partner nations, and other countries in question. By emphasizing sharing and disseminating information, TOC-SC can be seen as a resource aiding in the disruption of TOC in contrast to another organization seeking money, resources, and credit. ***IAP***

TOC-SC can serve as the catalyst for changing the attitudes of the intelligence community by focusing on information sharing within the interagency community, partner nations, and other countries in question.

Appendix 1: Intelligence Integration and Information Sharing

Intelligence integration and information sharing face significant challenges that include overcoming cultural differences, building and maintaining interagency trust, and establishing a common operational picture that supports visualizing and understanding complex and sophisticated adversaries. Improving interagency abilities to integrate and share information will help the U.S. realize the power of information as a strategic asset.

The greatest challenge to information sharing is cultural. Each agency, department, and partner nation must move from a ''need to know'' mindset toward a culture of "responsibility to share'' mindset.[25] Establishing and enforcing policies and practices, providing incentives, and training the workforce to effectively share information are critical to effectively making this transition. Institutionalizing an information-sharing culture will set the conditions to effectively and securely share information; lead to greater levels of intelligence integration, analysis, and operational success; and naturally build trust among agencies and departments within the U.S. government.

Arguably, no interagency trusted information network currently exists where participants can post, store, share, and collaborate on information pertaining to TOC. Concerns regarding data sharing and mitigating leaks is shared by all agencies and departments, but also serves to impede sharing efforts and bolstering operations. Each agency and department must break through sharing barriers and collaboratively counter the effects and influences of TOC. One example of this effort includes SOUTHCOM's use of the WISRD program, developed to create a comprehensive common visualization of the TOC environment.[26] This system cultivates and reinforces the ''responsibility to share'' mindset.

Improving the U.S. government's interagency abilities to integrate and share information will help it realize the power of information as a strategic asset to combat transnational criminal organizations. Benefits include but are not limited to: (1) achieving unity of effort across mission and interagency operations, (2) improving the speed and execution of decisions, (3) achieving rapid adaptability across mission and interagency operations; and (4) improving the ability to anticipate events and resource needs, which provides an initial situational advantage and sets the conditions for success.[27]

Integrating intelligence and sharing of information is an increasingly important element of interagency mission success. It is imperative to exchange information effectively among federal agencies, departments, and partner nations, and it represents a critical element of U.S. government efforts to defend the nation and execute the President's strategy to combat TOC. Overcoming challenges associated with culture and trust and establishing a common information network will bolster information sharing and improve operations to combat organized crime.

Appendix 2: Digital Data Sharing

Of the three barriers to information sharing, technology may be the one most easily addressed. The U.S. has tremendous resources at its disposal, including leading edge technologies and an unparalleled research ability. Among the problems of harnessing and sharing information are the needs to:

- Develop a means to access varying databases of different classification levels and seamlessly integrate and share information among interagency, DoD, the intelligence community, and law enforcement agencies.
- Develop a means to automatically integrate and share intelligence and law enforcement-related information concerning relevant and credible terrorist/criminal threats.
- Guard "upper level" sources and methods while making vital information and intelligence available to agencies/individuals with lower security clearances but a pressing "need-to-know and need-to-share."
- Develop uniform certification and accreditation (C&A) policies and standards across the individual departments and agencies. The lack of standards impedes the speed and agility of today's information-sharing environment. Reducing the time needed to certify and accredit systems and promoting the reciprocity of C&A decisions are crucial to information sharing and inter-connectivity.

Four proposals, currently in development, exemplify the directions required in overcoming the information-sharing hurdles:

- Protect America. This effort is an integrated homeland defense information-sharing initiative sponsored jointly by U.S. Northern Command and the Joint Staff.[28]
- Net-Centric Enterprise Services (NCES). The NCES is a pilot project being run by the Defense Information Systems Agency that would enable the military and intelligence communities to access information relevant to their missions regardless of what agency operates the network where the data resides. In a network-centric environment, data would be made available as quickly as possible to those who need it, across an organization or on the battlefield.[29]
- Trusted Control Interfaces. While sharing information and intelligence is a growing mandate in battling terrorism, one of the technological challenges remaining for the government is ensuring that information is still disseminated only to authorized users in the process.[30] To that end, the NSA is developing "trusted control interfaces," designed to strip classified information from messages before passing them to someone in a lower security class.[31]
- Terrorism Information Awareness (TIA). One of the manifestations of recurring attempts to "build machines that think like human beings," the Defense Advanced Research Project Agency's Terrorism Information Awareness (formerly Total Information Awareness) initiative is focused on an ultimate goal of predicting terrorist attacks before they happen. The system is designed to basically "scan" diverse public and private databases, as well as the Internet, for pieces of information that might be associated with a terrorist attack or intent.[32]

Appendix 3: Legal Considerations

The interagency and international nature of the approach needed to effectively counter the TOC threat presents specific legal challenges. These challenges must be addressed prior to operations in order to ensure timely and efficient operations to counter the threats presented by this complex problem. Two of the most significant legal considerations related to countering TOC are intelligence oversight and information sharing. By addressing these issues prior to operations, TOC-SC will avoid timely and potentially disastrous delays in addressing emerging threats.

The first significant legal issue that must be addressed is intelligence oversight. While this is an existing consideration throughout the law enforcement and intelligence communities, the interagency and international nature of the TOC-SC demands additional consideration be given to this issue to ensure intelligence oversight compliance is handled as quickly as possible. The nature of the TOC threat virtually guarantees that routine operations will confront intelligence oversight issues as TOC-SC investigates the nexus between transnational criminal organizations and legally defined U.S. persons. Failure to institutionalize legal procedures within TOC-SC will almost certainly result in either loss of opportunity to prosecute targets due to delays or inadvertent violations as members of the TOC-SC share information with their partners in an effort to accomplish the mission. Including dedicated legal staff in the organizational structure of the TOC-SC and providing robust intelligence oversight training to all members of the TOC-SC will avoid these issues. Additionally, the different charters and legal authorities of various member organizations within TOC will present challenges in planning and executing missions.

The different legal authorities, jurisdictions, and charters of member organizations within TOC-SC will present specific legal issues with regard to information sharing. The most obvious example of these issues is found in the sharing of information gathered via the intelligence community with the law enforcement community. This scenario presents several potential issues. While law enforcement officials are often focused on building an effective prosecution, the intelligence community is often more interested in long-term intelligence collection. Additionally, when information gathered via intelligence channels is well suited for use in prosecution of criminal activity, the sources and methods used to collect this information may prevent its use in legal proceedings. Finally, the Posse Comitatus Act makes sharing of information collected by the military with the law enforcement community subject to specific legal considerations in order to avoid potential abuses.[33] As with intelligence oversight, the demands of rapid information sharing within TOC-SC will require that a dedicated legal staff is resident within the organization to address information-sharing challenges in a timely manner.

While legal considerations are always a concern in law enforcement and intelligence operations, the complex global nature of TOC presents additional concerns for an organization designed to counter threats presented by these organizations. By incorporating a dedicated legal staff with the appropriate authorities to address and make determinations on legal issues within the organization, the TOC-SC will be able to effectively prosecute and counter threats to U.S. national security. Failure to address these concerns before they arise will result in costly delays in operations, potential legal violations, and, ultimately, a degradation of TOC-SC ability to accomplish its mission of countering threats to national security presented by TOC.

Appendix 4:
Department of Defense Roles

DoD has unique capabilities and resources to support efforts to counter TOC. The DoD's role in countering TOC can be leveraged and used as a force multiplier when paired with U.S. and partner nation law enforcement. With conscious legal parameters being realized, the DoD should serve as a supporting entity to enhance the capacity of both the warfighter and law enforcement agency. A March 2013 study conducted by the Joint Chiefs of Staff listed five interlinked strategic objectives for institutionalizing, operationalizing, and advancing counter transnational criminal organizations (CTCO) operations within DoD. DoD's approach to achieving these strategic objectives listed below exemplifies how its policy supports broader U.S. government efforts.

- Actively support a whole-of-government, full-spectrum approach to transnational criminal organizations. "DoD should serve as an enabling platform for interagency partners to work together against financial threats, synchronizing and sequencing policy, diplomatic, intelligence, law enforcement, and military authorities and capabilities."[34] Transnational criminal organizations conduct illegal activities such as drug, human, and weapons trafficking to gain funding and power for their organizations, and it is imperative that DoD efforts focus on the whole-of-government approach to develop sufficient ends, ways, and means to support interagency CTCO operations.

- Enhance support for law enforcement against top-priority transnational threats. "DoD must work closely with U.S. and foreign law enforcement partners supporting efforts to provide strategic, operational, and analytical support for their respective judicial missions."[35] DoD can use its unique capabilities and resources to detect and disrupt transnational criminal organizations. Working to find, follow, freeze, and seize illicit funds; prosecute financiers; and target complex criminal revenue generating and laundering mechanisms, DoD will reduce the threat to national security to a lower level that can then be engaged by law enforcement agencies.

- Organize, train, equip, and support CTCO units. "DoD must work in tandem with its interagency partners to build CTCO offices or units with the full range of capabilities at each of the combatant commands to complement the Office of the Under Secretary of Defense for Policy guidance based on the President's policy."[36] These CTCO units should focus on strategic and operational planning and mission analysis based on intelligence collection, analysis, and distribution.

- Develop core DoD CTCO capabilities:

  – Interagency campaign strategies.

  – CTCO operational capabilities including the development of deployable operational capabilities.

  – Military strategic plans that include CTCO strategic annexes for major military plans.

  – CTCO lines of operation and effort.

  – Expand the collection, analysis, dissemination, and database development of CTCO intelligence.

– Enhance the ways and means to defend against foreign threats.

– Define and incorporate CTCO within DoD doctrine, strategy, and operational planning.

"All of the strategic objectives listed above will depend on DoD incorporating CTCO as an element within DoD doctrine. This integration will include defense planning procedures and revisions of the Quadrennial Defense Review (QDR), and personnel, training and education programs."[37]

The rapid pace of change, easier access to technology, and flourishing globalization enable transnational criminal organizations greater ease to conduct criminal activities. The DoD's unique capabilities and resources coupled with a whole-of-government approach provide law enforcement agencies a better chance to disrupt and degrade TOC networks. Through focused activities and sustained efforts, DoD will continue to prove its role as a key enabler in the support of combating TOC.

Appendix 5: Partner Nations

If we are together nothing is impossible.
If we are divided all will fail.
Winston Churchill

The threat of TOC to the national security of the U.S. did not occur overnight. The transformation of TOC from a national security-level problem to a manageable public-safety problem will likewise not occur overnight. More importantly, it will not occur without the help of other nations. It will take both regional and global efforts to destroy their capabilities.

Partner nation inclusion within the TOC-SC is critical to mission success. Any actions that the U.S. takes to counter TOC must be part of a larger strategy to destroy the networks that support and facilitate these organizations. Not only must the U.S. destroy the network within the U.S., it must also help facilitate the destruction of the network that exists beyond its borders. This requires cooperation and collaboration with partner nations. Situational awareness and understanding of the TOC threat will only be achieved by examining the entire picture. Each U.S. agency and organization within the TOC-SC has a slice of that picture, but other nations do as well. What is required is the successful fusion of that information.

An additional concern is that a significant portion of TOC networks operate within weak states because they are able to operate with impunity. The U.S. must work with its partners to improve local government, judiciary, military, and law enforcement capabilities to maintain law and order. The West Africa Cooperative Security Initiative (WACSI) is a great example of a U.S. Department of State program that focuses on building partner nation capacity in rule of law and regional security. It provides technical assistance in creating the institutions, doctrine, units, and training to combat a country's local TOC threats.

Partner nations have a vital role to play in reducing global and regional TOC threats. The U.S. must enable their success by providing the assistance that they need to counter these threats within their own unique environments. If, instead, the U.S. chooses to ignore their capabilities and concerns, TOC will continue to be a national security threat for generations to come.

Endnotes

1 "National Strategy to Combat Transnational Organized Crime, Addressing Converging Threats to National Security," <http://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf>, July 2011, accessed on May 1, 2013.

2 Ibid., p. 3.

3 Ibid., p. 5.

4 Ibid., p. 6.

5 Ibid., p. 14.

6 Douglas Farah, "A Line in the Sand: Assessing Dangerous Threats to Our Nation's Borders," testimony of Douglas Farah, Senior Fellow, International Assessment and Strategy Center, before the House Committee on Homeland Security Subcommittee on Oversight, Investigations, and Management, November 16, 2012, <http://homeland.house.gov/sites/homeland.house .gov/files/Testimony-Farah.pdf>, accessed on May 1, 2013.

7 "National Strategy to Combat Transnational Organized Crime," p. 13.

8 The World Ministerial Conference on Organized Transnational Crime, United Nations Crime Prevention and Criminal Justice Newsletters, Nos. 26–27,Vienna, Austria, November 1995, p. 22.

9 "National Strategy to Combat Transnational Organized Crime," p. 15.

10 *The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States*, authorized edition, WW Norton & Company, New York, 2004, p. 194.

11 Ibid., p. 401.

12 Ibid.

13 Douglas M. Fraser and Renee P. Novakoff, "Confronting Transnational Organized Crime: Getting It Right to Forestall a New National Security Threat," *Joint Forces Quarterly*, Vol. 69, April 2013, <http://www.ndu.edu/press/transnational-organized-crime.html>, accessed on May 1, 2013.

14 "National Strategy to Combat Transnational Organized Crime," p. 5.

15 Ibid., p. 9.

16 Joint Publication (JP) 3-0, *Doctrine for Joint Operations*, U.S. Joint Chiefs of Staff, U.S. Government Printing Office, Washington, August 2011, p. IV-4.

17 Dale C. Eikmeier, "Center of Gravity Analysis," *Military Review*, July-August 2004.

18 Ibid.

19 John Rollins, "Fusion Centers: Issues and Options for Congress," Congressional Research Service report for Congress, January 18, 2008, <http://www.fas.org/sgp/crs/intel/RL34070.pdf>, accessed on May 1, 2013.

20 "The 'New' Face of Transnational Crime Organizations (TCOs): A Geopolitical Perspective and Implications to U.S. National Security," <https://www.hsdl.org/?view&did=733208>, accessed on May 1, 2013.

21 Executive Order 12333, "United States Intelligence Activities," December 4, 1981, <http://www.archives.gov/federal-register/codification/executive-order/12333.html>, accessed on May 1, 2013.

22 National Counterterrorism Center website, <http://fas.org/irp/offdocs/eo/eo-13388.htm>, accessed on May 1, 2013.

23 Executive Order 12388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005.

24 Kristin M. Finklea, "Organized Crime in the United States: Trends and Issues for Congress," April 16, 2009, <http://fpc.state.gov/documents/organization/122948.pdf>, accessed on May 1, 2013.

25 "National Strategy for Information Sharing and Safeguarding," <http://www.ise.gov>, accessed on May 1, 2013.

26 "The 'New' Face of Transnational Crime Organizations (TCOs): A Geopolitical Perspective and Implications to U.S. National Security," p. 64.

27 DOD Information Sharing Strategy, <http://dodcio.defense.gov/Portals/0/Documents /InfoSharingStrategy.pdf>, accessed on May 1, 2013.

28 Bert B. Tussing, "Meeting the Security Challenges of the 21st Century," in "Sharing Information for Homeland Security: Overcoming Obstacles of Technology, Process, and Culture," Center for Unconventional Security Affairs, Occasional Paper Series No. 3, January 2004.

29 Ibid.

30 Ibid.

31 Michael Hardy, "Info Sharing Hobbled by Tech and Culture." *Federal Computer Week*, February 26, 2003, <http://www.fcw.com/fcw/articles/2003/0224/web-info-02-26-03.asp>, accessed on May 1, 2013.

32 Tussing.

33 18 U.S. Code § 1385, "Use of Army and Air Force as Posse Comitatus," 1978 and 1981.

34 "The 'New' Face of Transnational Crime Organizations (TCOs): A Geopolitical Perspective and Implications to U.S. National Security," pp. 28–38.

35 Ibid.

36 Ibid.

37 Ibid.

InterAgency Paper Series

The ***InterAgency Paper*** (*IAP*) series is published by the Simons Center for Interagency Cooperation. A work selected for publication as an ***IAP*** represents research by the author which, in the opinion of the Simons Center editorial board, will contribute to a better understand of a particular national security issue involving the cooperation, collaboration, and coordination between governmental departments, agencies, and offices.

Publication of an occasional ***InterAgency Paper*** does not indicate that the Simons Center agrees with the content or position of the author, but does suggest that the Center believes the paper will stimulate the thinking and discourse concerning important interagency security issues.

Contributions: The Simons Center encourages the submission of original papers based on research from primary sources or which stem from lessons learned via personal experiences. For additional information see "Simons Center Writer's Submission Guidelines" on the Simons Center website at www.TheSimonsCenter.org/publications.

About the Simons Center

The Arthur D. Simons Center for Interagency Cooperation is a major program of the Command and General Staff College Foundation. The Center's mission is to advance scholarship pat the U.S. Army Command and General Staff College; develop interagency leaders; improve interagency operations; and build a body of interagency knowledge.

About the CGSC Foundation

The Command and General Staff College Foundation, Inc., was established on December 28, 2005 as a tax-exempt, non-profit educational foundation that provides resources and support to the U.S. Army Command and General Staff College in the development of tomorrow's military leaders. The CGSC Foundation helps to advance the profession of military art and science by promoting the welfare and enhancing the prestigious educational programs of the CGSC. The CGSC Foundation supports the College's many areas of focus by providing financial and research support for major programs such as the Simons Center, symposia, conferences, and lectures, as well as funding and organizing community outreach activities that help connect the American public to their Army. All Simons Center works are published by the "CGSC Foundation Press."

The Simons Center
PO Box 3429
Fort Leavenworth, Kansas 66027
ph: 913-682-7244
www.simonscenter.org
facebook.com/TheSimonsCenter

CGSC Foundation, Inc.
100 Stimson Avenue, Suite 1149
Fort Leavenworth, Kansas 66027
ph: 913-651-0624
www.cgscfoundation.org
facebook.com/CGSCFoundation
LinkedIn.com >> CGSC Foundation, Inc.