SMALL WARS JOURNAL

smallwarsjournal.com

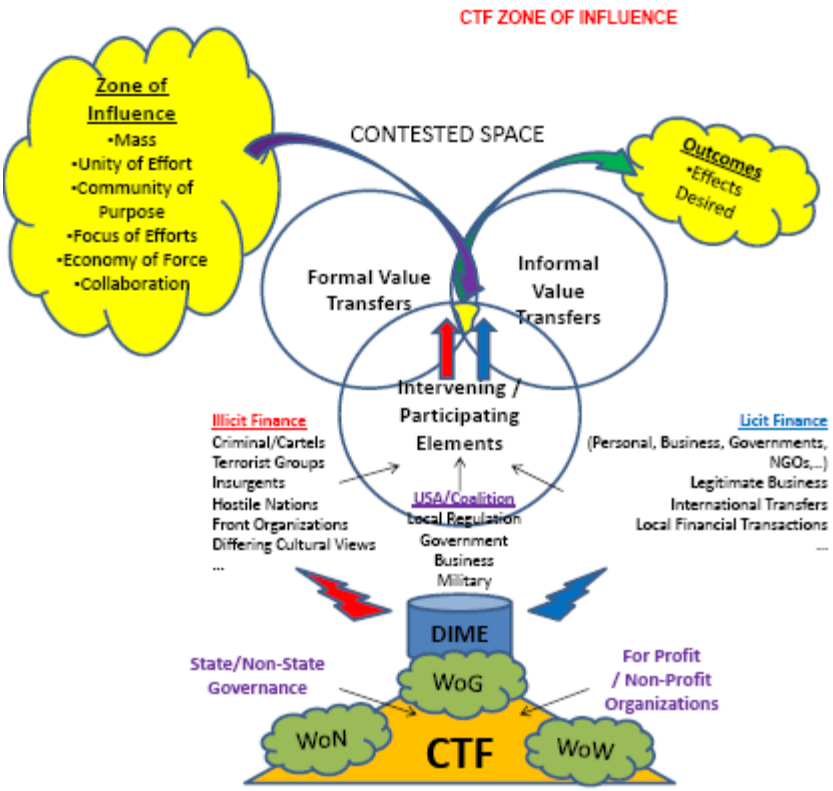
Assessing and Targeting Illicit Funding in Conflict Ecosystems: Irregular Warfare Correlations

David L. Grange and J.T. Patten

In December 2008, the Deputy Secretary of Defense issued a "Directive-Type Memorandum" whose subject was a DoD Counter-Threat Finance (CTF) Policy that included priority purposes to counter financing used by illicit trafficking networks in support of adversaries' activities, which may negatively affect U.S. interests. Countering threat finance included memorandum policy to deny, disrupt, destroy, degrade, and defeat these adversarial networks with many "counters" relying on tactics, techniques, and procedures (TTPs) that follow Irregular Warfare concepts. Targeting and assessing the greater illicit funding mechanism within conflict ecosystems demands the same below-the-waterline tacit knowledge, situational understanding, and intelligence creation that most complex and unconventional operations require while keeping local populations out of the fray.

CTF and other Irregular Warfare efforts need an accurate contextual assessment identifying the nature of specific activity and the culture of the various ethnic groups involved to precisely apply the use of force or countermeasures while gaining (and retaining) legitimacy in the eyes of the civilian population. This requires understanding and circumstantial application of history, society, economic infrastructure/ecosystems, local/regional politics, tribes and clans or social ties, and legal structures. Combining typical joint-oriented preparation of the environment/battle-space with CTF doctrine details will require going beyond the capabilities in traditional financing theory and forensic techniques of transactional dates, amounts, sources of transactions, and personalities involved to more accurately identify, detect, predict, target, and actively interdict threat, terrorist, and / or illicit criminal finance activities.

By employing a hybrid of IW, CTF, and shared operating concepts, intelligence and forensic investigative strategies can become complimentary at the joint and interagency community of interest levels. Based on the illicit groups or actions involved and those government agencies covering them, a Whole of Government (or beyond) network of efforts will improve support to operational strategies at ground level up to the prosecution needs at the Justice level. From this community of purpose standpoint, Zones of Influence can be better established to contest the space that is utilized by criminal and adversarial purposes.



Countering Irregular Threats

The challenges related to countering irregular threats are multifaceted, dynamic, and often overwhelming. Effective solutions entail long-term, widespread methods in the appliance of proper tools and approaches—both direct and indirect. Irregular threats in warfare and finance include acts of a political, psychological, and economic nature, facilitated by both indigenous and non-state actors for the purpose of self-interests, eliminating or weakening authority, creating necessary processes to achieve "other" goals, or influencing an identified power, and often using asymmetric schemes. To counter such threats, the intercession element needs a comprehension of the mosaic environment that is characteristic to the area or group of interest that will have differing traits unique to each specific group's activity-based roles, sub-area, relationships, intersection points, pre-determined definitions or objects of trusts/agreements, and the dynamic time continuum that plays a part in shifting the system via environmental changes.

Complementary layers and sub-layers exist parallel to the identified network webs that enable additional relationships and behavior to meet unmet needs, resource constraints, and differing ideologies in the system. More often than not, these networks, sub-networks, and other inter-twined human terrain systems are resilient and adaptive to change, reorganization, or shifting linkages to avoid predictability or linear operations that can be identified and destroyed. In time, the network relationship links become more cloudlike encompassing multiple mutual association zones of influence that can be shuffled at any point due to emerging circumstances.

Assessments, therefore, must start off with both operations and intelligence analysts understanding how these groups can typically interrelate and disperse based on predictable

tendencies of the illicit nature, their licit activities that are above board and of legitimate nature, and the individuals involved. To reduce time constraints in potentially irrelevant social network analysis, and to improve dynamic targeting opportunities, the focus should be on identifying the critical recurring roles and supply-chain distribution chokepoints that are adopted by the illicit groups, based on the pre-assessed area-specific human terrain and typical actor-driven process flows. It is wasteful to chase every player and try to understand every link and role when all that matters are the key players and their critical process stifling points.

CTF efforts should cause financial pain but not mass financial carpet bombing. Understanding critical adversarial infrastructure and their exoskeleton, which consists of supporting roles defined as "rare and valuable skills," "strategic process-positioned individuals," or "highly vetted individuals of trust," in threat finance makes it easier to engage in more ad hoc targets to support the overall network-defeat-mechanism without throwing off a local business ecosystem.

IED "Role" System Similarities

As an example of similar role targeting, the IED system as of 2006 could be generally broken down by categories of: Information, Money, Personnel, Material, and Targets with a counter-engagement model split between *Attacking the IED Network* and *Defeating the IED Device*. The most pertinent social network component used by special operations at the time was focused on *Attacking the IED Network* through the various IED system stages, which enabled network destruction capabilities when role-actors could not be identified---but existed. The term "Network" was used because of the unstructured relational activities correlating to the IED repeatable action's nature that had common characteristics and could be analyzed collectively. The IED network was not always a formal organization in the same manner that threat finance is not always being part of a formal organization. Both IED and threat finance action-flow networks reflect the complex bodies of loose overlapping social partnerships that one would tap to facilitate core and supporting tasks. This process allows either of the repeatable activities to be accomplished successfully through systemic procurement channels. The names, places, and times may change, but the relatively stable process channel and illicit or legitimate duties to facilitate the processes remain the same.

Illicit social network-based trades and activities tend to have a process flow with a decentralized structure with a number of the so-called recurring roles being devoid of a hierarchical organizational model governing the transaction processes. Modular duties within the core of threat finance can be over-arching like the IED roles and can involve others acting along the Illicit Financial supply chain system for: drug trade, terrorism, banking, government, financial brokering, couriers, money buyers/sellers, bosses, workers, surrogates, legitimate business, cartels, etc. Fortunately, the financial aspect of illicit activities forces the finance-related individuals to be much less limited in external connectivity points (outside of the cell) than the actual crime or terror cell that may be operating in autonomous adaptive cells with independent orchestration, no central authority, or limited "non-group" connection points. To stress again, terror or threat financing only works with some form of link to the legitimate financial system, which cell financers are a part of, in most cases. Finding and disrupting that link is the key.

Many of the threat finance roles have ties outside of their member cluster. For example, they often foster connections to prior contacts formed in school, neighborhoods, mosques, training camps, business relationships, and family extensions. It is through this window that penetration to a financial network is somewhat easier than that of the closed or cloaked terror or IED-specific cell, and just as cells or factions share information, techniques, and trusted sources, so too does the illicit finance activity. Often this financial resource-sharing links to other financial bases in support of illicit activity: national charities, private donors, mosques, front organizations or businesses, 'Zakat' alms, corrupt government organizations or officials, and informal or formal value transfer agents.

In formal financial system interactions, the relationships can align to cross-over roles as: *users* (dealers, businessmen, traders); *regulators* (government, banking personnel); and *service providers* (private bankers, accountants). In the case of insurgency and terror, it is not uncommon to find an accountant or business front member within the process-chain who crosses connections to formal and informal exchanges as well as legitimate and illicit activities, and loves to associate with the radical and violent individuals, but who loves his money even more. This trait opens the network disruption opportunity wider.

Identifying Illicit within Legitimate

True to the art of counterinsurgency, the way to disrupt illicit finance activities is to simultaneously attack the adversary, keep the population's hearts and minds at the forefront for pacification initiatives, and thwart civil mobilization attempts by the enemy. Cutting off the sources of illicit funding in informal banking environments has historically meant shutting down the local informal (often *Hawala)* systems of transferring money. Disrupting these sources of funds is risky due to the interconnectedness of illicit and legitimate financial activity. Operations intended to defend locals and attack illicit activities often have the unintended consequence of harming or alienating the people it had intended to protect. The hawala system is central to economic survival and continues to be the system of choice for most cash payments, transfers, currency exchange, and remittances in many foreign countries, especially those in a civil conflict or reconstruction process.

The informal business ecosystem is the largest portion of these countries' economy and without its informal value transfer mechanisms, basic assistance cannot be delivered to those in need or in rural areas of the country. Most local businesses in these locations operate on a cash basis or on equal value exchange mechanisms that are fostered by the informal banking system. In most cases, promissory instruments are not used because transactions are based on honor and reputation. With a widespread distrust of banking systems and corrupt government, many locals also use the hawala system for short-term micro-finance loans to fund working capital needs, get out of poverty or debt, access credit, obtain common life-sustainment or luxury goods, cover wedding expenses, and procure agriculture inputs. Destroying and disrupting the legitimate flow in an attempt to stop illegitimate flows can be perceived as a direct infraction on the civil population whose support is needed to counter terror, criminal activity, or insurgency.

In similar environmental business dynamics, it is important to recognize culturally that what may be considered to be illicit trade in a Western context may be viewed as an acceptable business

practice in the foreign land. Many law abiding citizens use illicit economies as the only available source of income. With criminal activity tied directly to standard trade, citizens in Afghanistan, or similar places, have to turn to illicit crops or trades to obtain income or credit. Eradication programs in Afghanistan that were not attuned to this correlation initially caused many poor farmers to lose their crops, forcing them to deplete their meager assets to repay debts. They had to turn to criminals for short-term loans at usury rates (available only against another poppy crop), and some poverty stricken homes paid debts with their daughters. In such cases, hearts and minds follow rules of survival. Insurgents and criminals take advantage of this to mobilize the population at the local levels by exploiting economic, social, and political grievances.

Threat finance disruption, therefore, can be viewed in similar blowback terms where major sources of funds being exchanged in systems targeted as "Illicit" likely host great quantities of funds that come from people working abroad who could not find legitimate work elsewhere and are now sending sustainment back to their families. Shutting down the system can inadvertently hurt legitimate individuals, leaving them less than motivated to support reprisals against terrorists and criminals who are indirectly responsible for the targeted closures as a counter-mechanism; the disruption is focused on the authority directly blocking financial life-lines to legitimate recipients. Plus, most informal networks, when officially shut down, only go deeper "underground" and become much harder to identify, penetrate, and disrupt.

Targeting Illicit Financial Networks

Recognizing that negative outcomes of action affecting legitimate transactions often outweigh the positives of affecting some illicit transactions, other soft-approaches must be used as initiatives that will not exasperate already tenuous societies. The supporting information to foster these decisions must come, at a minimum, from intelligence assessments, area intelligence fusion cells, the local HTT Anthropologist, the local police officer working with the US or coalitions, PSYOPerators, CoIST members, CAT members, the local SF team, or from local source networks and business groups. Lessons learned from Vietnam's Marine Corps Combined Action Program (CAP) irregular warfare mission strategy can be applied to today's Illicit Finance networks:

- Destroy VC [adversary] infrastructure within the [micro/macro-] area of responsibility
- Provide public [financial] security and help maintain law and order
- Protect friendly [value transfer] infrastructure
- Protect bases and communications within the villages and hamlets
- Organize indigenous intelligence nets
- Participate in civic action and conduct propaganda against the VC [threat finance networks]

Identifying Fund Segments

Investigations and intelligence collection in combined action programs can be directed against critical points in the social finance flows to ascertain tacit knowledge for operational interdiction strategy that can destroy the adversarial infrastructure. To this point in time, most identified

source patterns of illicit finance have materialized along the lines of government aid, charities, legitimate transactions, market exploitation, trade, and all forms of illicit activities. Intelligence collection and analysis often has the greatest difficulty in determining the junction points at which each action links with the other to form a nexus between money, geography, arms, social-networks, economics, politics, illicit activity, and ideology, especially with adversarial concealment, denial, and deception activities in place.

Further examination shows that illicit entities often dedicate operational and infrastructure funds to safe havens (including housing/food); communications (devices, couriers, etc.); documentation (identity, travel, etc.); facilities (processing, distribution hubs, bases, training camps); mobilization (recruitment, inducements, bribery); intelligence collection; arms (explosives, weapons, ammunition, detonation devices, etc.); vehicles; and business fronts. All of these areas should be identified, but in the context of the local terrain and the micro- macro-business ecosystem, to prepare the complete operational environment for CTF operations and assessment.

Public Financial Security

Threat finance is embedded within most war torn economies where special operations are involved today. In Iraq, Afghanistan, and parts of Africa, it is not uncommon for citizens to pay for protection under the pretenses of "war or brotherhood taxes." Extortionists using real-estate fraud, road block and trade route taxes, public service extortion, rebuilding contract up charges, price gouging, short-term loan financing at usury rates, oil/fuel smuggling, and middlemen up charges are all working to the detriment of public financial safety. These criminal financial acts can be discovered through public elicitation once civilians know, and are shown, that they can be safe from reprisals.

When illicit financial crime is exposed in communities, programs can be designed to further demonstrate the unjust and greedy nature of the criminals, insurgents, or terrorists. Building trust within the community will expose opportunities to identify more heinous dealings of hawala brokers, front companies, corrupt officials, couriers that transfer cash to criminals or insurgents, trading routes that are most often used for value goods, smuggling, and cash transfers for transactional settlement.

Organize informants netted around indicators

Access is the key to penetrating networks for accurate, relevant, and timely intelligence collection and, ultimately, network disruption. A network of local informants and existing relationships within the area's business community is fundamental to providing the initial financial ecosystem mapping through their particular neighborhood knowledge and social network relationships. The informant network is also vital for updates and shifts in the financial terrain that can be captured in databases as elements shift dynamically. For informants to provide the most reliable information, their handlers need to understand the financial issues and transactional process mechanisms so they can better direct tasking and appreciate sensitivities in inquiring about matters that are often left to blind trust. A set of indicators should be compiled that relate to the typical structure and local history of transactions.

As a sample, for informal value transfers/exchanges, most brokers and those conducting hawala transactions on behalf of themselves or the larger hawala association, there is no standard documentary requirement for transactions or inspection. Reporting and documentation is considered unnecessary based on the very virtue of hawala, which is based on trust. Those failing to honor contracts are immediately shunned, expelled from markets, or physically punished and, in some cases, killed. Individual hawaladars and book-keepers design, develop, and maintain their own records for purposes of remittance and settlement that are adapted to their nature and that of their business clientele or operations. These dealers are very well attuned to the cash they have on hand, how much is available to them, how much has been transferred, how much is owed to them, and how much of a percentage they earned per transaction.

Dealers commonly have a form of documentation which indicates something about their network. Hawala slips denote a code or number to identify the customer and settlement. Secondary information notes may be presented for the cashing of the exchange. To facilitate organization, some hawaladars maintain information on their customers, to include a date of transaction; name and address or phone number for the sender and recipient; hawala number; name of counterpart dealer; and, in some cases, another identification number, which may relate to a passport. Fees can be noted where a commission charge ranges from 0.25-1.25% of the amount involved, but where illicit activity is concerned, the fee charged may be between 15-25%.

The informal value transfer accounting records can differ from the actual transaction books or computer files. When conducted by a business-minded individual, these records often correlate to common local accounting practices with maintained debit and credit columns. More often than not, these dealers maintain one or more formal financial institution accounts in the area. Outstanding accounts can be balanced daily, weekly or monthly depending on volume with the nature of the business or dealer relationship determining frequency. Balancing tends to be based on local custom, whether in cash, the purchasing of commodities, or capital flight.

As illicit activities and networks converge, lucrative trades in drugs, stolen cars, motorbikes, gemstones, food goods, appliances, alcohol, or arms are common exchanges and money laundering opportunities. In Afghanistan, CTF money trail efforts may at times be incorrectly aimed at “bongo” vehicle purchases when the reality could be that they were coming from neighboring countries through unofficial channels like Pakistani religious school or organization “donations” that either addressed a transactional need or ideological aim. Similarly, the illicit finance industry and illicit traffic share characteristics of fluctuations based on the illicit activity nature and months of the year that also can serve as an indicator. In the case of the heroin business, little money flows during February, March, and April in Afghanistan when opium poppy is in the growing stage. Activity spikes during cultivation when farmers receive advance payments. Later when the crop is ready for harvesting and purchase, the exchanges spike again.

Again, this largely depends on the needs, beliefs, and transactional history within the human terrain and the networks therein. In some areas of the world, there may not be any monetary flow at the micro-level, especially where pastoralists are the majority. In those situations, selling or buying livestock during certain periods may be the most relevant and safe investment to store

wealth. Such complex systems and social organization systems must be identified for threat finance situational awareness.

With enhanced indicators and key process collection tasking, human intelligence assets can be better directed and non-specific accusations that could simply settle tribal vendetta scores will be taken in context with the evidence required to support claims. Similarly, Sheiks who often receive local information from tribal members regarding unfair commercial practices and price gouging can be more specifically debriefed on where occurrences are taking place in the value exchange supply chain. While the military has taken strides to understand the anthropological and cultural nuances, so too, must they incorporate an understanding of the economic and financial ecosystems into their intelligence requirements or area studies.

Destroy the Adversary

Akin to the IED social network destruction in Iraq, viral-targeting through misinformation morale operations directed to the threat finance subjects' inherent issues around trust, inferiority, identity, role confusions, etc., can disrupt illicit activity in a manner that can be activated from the outside of a network that travels both internally to the cell and externally in the community for maximum correlating efforts to support the message uptake in a viral-like spread. Most of the so-called "virus" frontline recipients in Iraq often initially demonstrate a defensive response to accusations because they perceive or anticipate a threat being directed at them from within their own network, hence questioning their motives, loyalty, trustworthiness, etc. Their initial energy and resources are spent in defensive posturing to mitigate further trust attacks in order to re-posture one's self, escape punishment, and win group information dominance. During this period, defensive viral targets will also distort the messages by their responses an attempt to regain trust, which further warps and reinforces some viral communications.

Such distortions can create social disturbances between groups and impact transactional processes, common purpose, unity of effort, and trust when directed at roles at financial process flow choke points. Most virus details will require action on a psychological and transactional process or communication level. The concept is simply based on the illicit organization's activities, fraud, deceptive network intrusion, mistruths, and scheme disruption forced on the strategic link of a cell and social network.

How it Works

Network disruption activities capitalize on the typical social network strengths which can be exploited as weaknesses. As networks are self-enforcing, trust is a core requirement to foster the relationships at all levels of an organization. The abilities to close distances, coordinate activities, and ensure security within the community is based on the faith that all individuals will be diligent within the distributed system. Stopgaps, however, are often constructed within illicit "dark networks" to ensure security in supply chain distribution networks where individuals, commodities, and knowledge travel along dispersed contacts. Other times, a hub and spoke network structure is used to revolve around the central orb for communication and extended network connectivity that ties compartmentalized nodes (cells) together.

In both cases, the network structure is a barrier to effective contact and communication within nodes. Security prevents open sharing about activities that do not concern other members. The shroud of "need to know" activities makes contact limited and questions for addressing concerns are often tied back to trust. Because of the lack of a central authority to sanction all decisions, there are many contradictions that occur, and some activities that individual groups may participate in do not always link back to the whole group's strategy. Individual groups may not openly discuss their intentions with the larger audience due to the fact that the norms of collective decision making often suggest that those who are not in consensus may be deemed as disloyal.

Some illicit networks that are routinely disrupted over an extended period of time through shipment seizures and periodic safe haven raids reveal that the psychological stress on the network causes internal finger-pointing and individual reputational posturing as a priority to mitigate future disruptions and raids. Acts of recklessness and fear prompted faster compensation attempts to return in good favor with the illicit network and avoid internal repercussions. Ancillary effects disturbed the group unity, cohesion, and collective-action capacity, plus it added greater security vulnerabilities as groups opened their network exposure. Without a hierarchical system to resolve disputes, the network recognizes that individual or group think could decide a fate without greater debate if trust was compromised. If a node is cut off, again referring to requirements of trust, critical roles within the network are harder to replace unless they defer to other preexisting personal relationship networks.

The misinformation campaign, or covertly orchestrated disruption event, applied to this theory is pushed unwittingly by the cell members to other cell members, cells, family, and social contacts along the threat finance process supply chain. The push of perceptions and rumor is what carries the "virus" in a lytic cycle created by a contrived solution that directly correlates to the target and damages or ostracizes the group from within. While it damages an individual's credibility and trust, it also decelerates the flow of knowledge and information, creates some bottlenecks, and reduces innovation that would otherwise dynamically shift the process flow to compensate for disruption. Also at hand in the illicit trades, are significantly differing ideologies within the often overlapping criminal or terror relationships that are initially cohesive based on a centralized goods or service value perception. In reality, each of the many illicit groups globally remains in constant distrust of the others despite the business convenience, profit, or necessary conduit. It does not take much for any particular group to attack a traitor.

By understanding an area's environmental factors at the micro-level, they can be manipulated on the large scale while criminal cartels and terror cells limit themselves to specific places of influence for finite periods of time. Therefore, messaging for viral attacks has to be compelling enough for the network to push communications fast and with decisive measures across their areas of influence and within their immediate center of gravity to change a flow of operations. Viral approaches or other "soft" non-kinetic activities that enable civilian discontent directed against the informal value exchange system or adversary is the best method to ensure local authorities or coalition militaries are not the scapegoat. This is why the efforts of CTF disruption can be effectively based or exploited against the same reasons individuals use informal value transfers in the first place:

- Lack of access to conventional banking system
- Local banks ill-equipped for overseas transfers
- Inefficient, costly, bureaucratic banking system
- Lack of legitimacy in tax system
- Perception of over-regulation and costly compliance to government
- Cultural traditions
- Lower costs
- Faster service
- Avoid reporting and ensure secrecy
- Protect assets from nationalization
- Make effective discreet payments to illicit network abroad
- Pass currency controls
- Criminal purposes

Conclusion

Breaking down the individual transactions that may, or may not, yield a link to illicit activity is nearly impossible in difficult operating environments with already constrained resources, unless experts who are globally networked are involved throughout the formal and informal value exchanges and business ecosystem. With such experts who can guide effective identification of the afore-mentioned role based targeting, individuals and groups can be targeted more efficiently and effectively. Further, intelligence and informant operations that are tasked to SOF elements that regularly interact with family head sheiks (bloodline and emplaced), citizens, business owners, market vendors, farmers, imam religious leaders, local politicians, militia, military, and local law enforcement, can also be enhanced with improved contextual framing of the entire human terrain.

To then disrupt the patterns, the next step is to synthesize and coordinate joint operational activities around (based on a model of Destabilizing Networks Carnegie Mellon University, 2001):

1. The basic components that account for the network's structure (e.g. - the number and types of sub-groups, or the number of triads, stars, and the extent of reciprocity)
2. The central tendency and similar or differing ideology within a set of networks, and the networks that are anomalous when contrasted with the other networks in the set.
3. Critical differences between two or more sets of networks.
4. Which components in the network are structured significantly differently from the rest of the overall network
5. How cells contribute or control behavior, emotion, or attitudes of individual members
6. What makes some groups hostile to one another and others neutral or civil
7. Whether the existing network is coherent (i.e. - What is the likelihood that there are key missing nodes or relations?)

At a minimum, interagency/military fusion cells can create a comprehensive matrix around Actors, Knowledge, and Tasks. All segments will cross-relate as "Actors" and are contrived of the individuals who are a part of the varying social networks and illicit activity. The financial

actors are affiliated with specific banking, value items, or transactional "knowledge" and information available on the networks and elements of the tasks. Financial-processes knowledge and actors also fit into "tasks" based on assignment, needs, and task-precedence. Since it can be difficult to fully identify or penetrate these segments, specific social viruses (or similar deception operations) can be sewn in the form of financial transaction disruptive sabotage, communications denial, key individual distrust, persuasion, impersonation, ingratiation, and conformity. Operations may be conducted in the form of DoD operations and campaign plans; Civil Affairs or UN designation processes tied to banking, lending, commerce, regulations, laws, etc; PSYOPS; black or overt SOF; Partner Nation efforts; Internal Agency collaboration; Information Operations; and associated financial instruments of power or policy. The cornerstone is SOF and/or other Agency HUMINT, surrogates for denied spaces access, and intelligence support work.

Affirmative action or more nebulous social network attacks can be directed at the individual level, process chokepoint, or group affiliations and is constructed with actors' social culture in mind based on continuous understanding of the battle-space and financial ecosystem appreciation. Creating virus-like spreadable disruptors that can damage hard to reach social networks from within are among the few effective ways to cripple or minimize threat finance closed-network activity and minimize the adjoining illicit system activities (credibility, recruitment, motivation, procurement, sanctuary, and funds), if we cannot penetrate the cells directly. When CTF efforts are fused to include Whole of "X" ("X" being Government, Nation, or World), sustained proactive man-hunting and disruption operations can also be spawned globally based on the financial transaction domino effects which correlate to community of interest/purpose opportunities in building partner capacity and persistence surveillance across governed and ungoverned domains.

From this stance, the DoD Directive can be realized through the enhanced CTF alignment of analysis, collection, intelligence, surveillance, and reconnaissance activities with operations.

Brigadier David L. Grange (USA Ret.) was the president and chief executive officer of the Robert R. McCormick Foundation until June 2009. During his military career, Grange served as a Ranger, Green Beret, Aviator, Infantryman, and as a CT Unit member, with his final position as Commanding General of the First Infantry Division. Assignments took him to Vietnam, the DMZ of Korea, Grenada, Russia, Africa, former Warsaw Pact countries, Central and South America, and the Middle East, to include the Gulf War.

J.T. Patten supports various hybrid conflict activities within the special operations and intelligence community. Specialty areas include Irregular Warfare mission support in intelligence analysis, assessing complex conflict ecosystems and informal/formal dynamic relationships. He can be reached at jtp@irregularwarfare.org.

Other *Confronting Irregular Challenges in the 21st Century* series publications:

Attaining and Retaining Positional Advantage
Confronting Iran, Securing Iraq's Border: An Irregular Warfare Concept
Executive Summary, Irregular Warfare Leadership

From Gun Violence to Civic Health: A "Whole of City" Approach to Creating Chicago's Future
Irregular Warfare Leadership in the 21st Century
Irregular Warfare Support Operations
Russia's Attack on Georgia: What to do with the Awakened Bear
Whole of Nation Approach to Irregular Conflict/Warfare
Whole of Nation Global Engagement
Whole of World Collaboration
Winning Damaged Hearts and Minds
Contact iwc@irregularwarfare.org with questions.