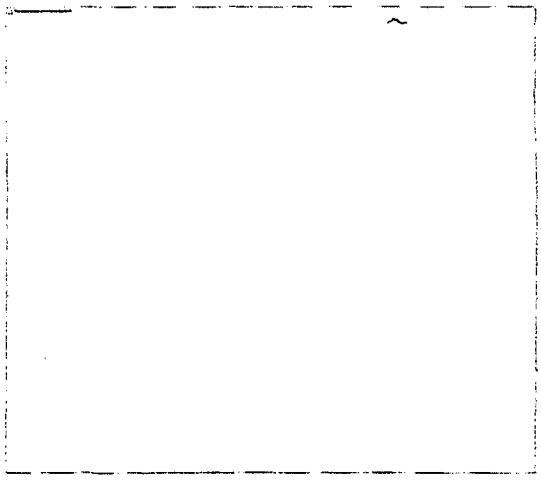

Project QUANTUM LEAP

After Action Report

v1.0 DRAFT 12 September 2012

QUANTUM LEAP takes its name from a three-year series of exercises and technology experiments conducted by Naval Special Warfare Group ONE (NSWG-1) in the late 1990s to examine ways to make Naval Special Warfare relevant in the 21st Century. Building upon this successful heritage, the reincarnation of QUANTUM LEAP is intended to accomplish the same mission but this time for all Special Operations Forces. QUANTUM LEAP will do this by following the example set by the British Special Operations Executive (SOE) during World War II - leveraging cutting-edge technology to enhance the conduct of operations. In many respects, this is

"... an old way to do new business."[1]

Admiral William H. McRaven, "The Plan," circa 2000.

Table of Contents

I. Introduction

Special Operations Command National Capital Region (SOCOM NCR) is the interagency coordination center for USSOCOM in the Washington DC area. Its stated mission is *"...to shape, coordinate, and support the synchronization of global SOF activities with the Interagency, Law Enforcement, Intelligence Community, TSOCs, multinational and private sector partners in order to integrate operational strategies and plans to achieve national security objectives, primarily along indirect lines of operations."*2 To this end, SOCOM NCR will facilitate and enable non-traditional capabilities, technologies, tactics, techniques and procedures (TTP), improve interagency cooperation and coordination with Washington DC-area organizations and agencies, and support the SOCOM global special operations mission. QUANTUM LEAP will be crucial to these tasks.

The new QUANTUM LEAP is a planned six-part experiment sponsored by SOCOM NCR. The first iteration of QUANTUM LEAP (QL) was held at the OSD AT&L open-source development laboratory in Crystal City, Virginia from 08-17 August 2012. Approximately 50 government and industry representatives attended this experiment.

The first three days of the experiment (Wed-Fri, 08-10 August) were focused on definition of requirements and exploration of the experiment scenario. The following week (Mon-Fri, 13-17 August) was devoted to actual exploration of tools, and TTP to support the SOCOM NCR mission, in this first iteration concentrating on use of unclassified and open source tools and information to support the counter-threat finance (CTF) mission.

The experiment scenario was based on an actual Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Bulk Cash Smuggling Center (BCSC) money laundering case. NDA's were signed among all participants to permit open sharing of proprietary and law enforcement sensitive information among the participants. The ICE/HSI Intelligence Analyst and case lead John Clifton provided background on the case, which included a wide range of examples and the tactics of advanced money laundering activity.

Against this scenario, various technologies were employed to identify and exploit the human, commercial and information networks associated with the moneylaundering case. The majority of these approaches utilized commonly available open sources and tools, in some cases integrated with specialized tools made available by the QL participants. From the use of these tools, new TTP were developed and explored.

SOCOM NCR Charter (Draft) 01 October 2012.

The most heavily used specialized tool employed in QL was Raptor X, a Government Off-the-shelf (GOTS) geospatial information system (GIS) developed by the Department of Energy (DOE) Special Technology Laboratory (STL) and operationally used by USSOCOM components. Raptor X is an open architecture that relies on "plug-ins" to import, exploit and display heterogeneous data. One of the tools developed as a Raptor X plug-in for QL was "Social Bubble," a tool which summons data via the Twitter API to display Twitter users, their geographic location, posted Tweets and related metadata in the Raptor X geospatial display. This tool was used heavily during QL to identify individuals and commercial entities associated with the money laundering network. Other participating tools and technologies included maritime and air surveillance networks, financial transaction analysis software, numerical analysis software and computer network monitoring and analysis tools and data visualization. None of the other third party tools were as heavily utilized as Raptor X (along with Social Bubble). This will be discussed at length in detail in section IV.

Overall the experiment was successful in identifying strategies and techniques for exploiting open sources of information, particularly social media, in support of a counter threat finance mission. Major lessons learned were the pronounced utility of social media in exploiting human networks, including networks in which individual members actively seek to limit their exposure to the internet and social media; the need for a capability to collect, manage, and exploit "big data"; the importance of concentrating open-source collection on unique data sources vice unique exploitation tools; the need for specialized analytical expertise ("Subject Matter Experts" or SMEs) and the importance of developing a specific ontology of topics, terms and data types relevant to the specific threat model, in this case counter-threat finance.

II. QUANTUM LEAP Operational Concept

The QUANTUM LEAP operational concept envisions six separate iterations of the experiment over approximately six months, each with a different theme or scenario. The planned themes include:

- Counter-Threat Finance (CTF)
- Counter-Human Trafficking (CHT)
- Counter-Terrorism/Homemade Explosives (CT/HME)
- Counter-Narcotics/Drug Interdiction (CN)
- Counter-Proliferation (CP)
- Critical Infrastructure Protection (CIP)

The first theme, Counter Threat Finance (CTF), was explored in the first iteration of QL in August 2012. Subsequent themes are to be explored approximately monthly.

The themes of all of the planned QL experiments will be similar to the earlier Naval Special Warfare (NSW) *Trident Spectre* series, including "*Think-Do-Innovate*" and "*Evolving Threat – Technology Driven.*" Included among the goals for the initial experiment were an intent to leverage open-source, commercial, unclassified and law enforcement sources to gain increased insight into the scenario threat (moneylaundering) network and engage heavy use of social media sources to extrapolate, analyze and exploit the network. Additional goals were to evaluate network discovery processes and mechanisms and to capture and record the most effective technical applications and TTPs.

Evaluation of the QL experiment process will be conducted in four principal areas: technology, process (e.g. TTPs), legal and policy. For example, against a given problem associated with the scenario, such as *"identify entities associated with the money laundering network in a given geographic area,"* a technology would be identified, TTPs associated with the use of that technology developed, and legal and policy issues, concerns or requirements would be addressed. This process was followed through multiple dimensions of the threat scenario and various use-cases were developed and demonstrated. This methodology led to identification of a significant amount of new and actionable information associated with an actual ICE/HSI CTF investigation during the first iteration.

As part of this technology discovery process, tools and technologies were evaluated for maturity, including usability, versatility and effectiveness; availability, including classification, ITAR restriction, etc; and practicality, including cost, license schema, etc. It was noted that adherence to traditional DOD software procurement models, including a procurement TRM/CMMI level, etc, can be an impediment to obtaining the most modern and effective tools available.

Tools and technologies were also evaluated for their applicability. The specific goal was to identify open, commercial, and unclassified sources relevant to counter threat finance (CTF)

requirements. Eight "*Categories of Information*" were identified as characteristic of the CTF network exploitation problem. These are:

- Business Networks
- Human Networks
- Communications
- Financial interactions
- Property/Real Estate
- Assets
- Transport and Logistics
- Value Transfer/Movement of Goods

It was also noted that it was essential to systematically assess and understand the nature and structure of CFT networks in order to identify likely multiple high value sources of information. This type of analysis requires specialized knowledge and expertise on the part of analysts and subject matter experts ("SME's") as well as access to tools tailored to each of the 8 major information categories listed above.

One of the major issues identified was the need for improved capabilities to acquire raw data from open sources for further reduction. One of the key types of data (under "financial interactions"#4 above) is banking secrecy data (BSA) obtained by law enforcement pursuant to a warrant. Transactional data obtained through other sources – law enforcement investigation and forensic exploitation of seized or otherwise obtained media - is also key to unraveling deliberately obfuscated transactions and relationships.

Some data in other categories is available but not necessarily efficient to obtain unilaterally, such as real estate information (almost always public record) and transportation and logistics data. These types of data may be most efficiently obtained on a commercial or "subscription" basis from industry sectors that focus on the type of data in question.

Network and communication data can be more complex to obtain and may require more sophisticated tools to exploit. On one hand, simply scraping the Internet can obtain a huge amount of data but the infrastructure required to perform the scraping is a highly complex effort.

Crowd-sourcing was also identified as another efficient way to obtain data. In the scenario of a money laundering network, various individuals around the world were identified with rich and highly specific knowledge of the network. Finding and leveraging such individuals can be a productive and effective strategy, but requires various forms of subject matter expertise to conduct.

Human entity resolution is a requirement that will be common to almost any of the scenario categories proposed for the QUANTUM LEAP (QL) experiment series. Fortunately, penetration of social media, preponderance of publicly available Personal Identifying Information (PII) databases and sources, and advancements in available analytical tools

significantly improves the ability to rapidly and accurately do human entity resolution from open sources.

Various (over 300) other traditional and non-traditional open sources were identified with potential relevancy to the CTF mission. These include public sources such as the Patent Classification System, which has tremendous amounts of business information contained in patent applications, or subscription-based sources like Revere Data, who sell specialized financial and business data. Two sample lists of sources are included as Appendices C and D.

An important dimension of the QL experiment was the evaluation of the policy and strategic considerations associated with open-source discovery and analysis of CTF data as well as the larger implications of the applications of technologies and TTPs developed as part of QL. The discussion included consideration of the strategic goals of the emerging capability to be created by QL: What is it trying to accomplish? Who are the likely customers? Who are likely partners, collaborators, suppliers, and participants? Are there security or OPSEC considerations from advanced applications of open source collection and analysis capabilities? Although many of the types of issues were discussed, in general, no firm conclusions were drawn. Stated goals, however, were included to make the resultant capabilities applicable to and usable by the Theater Special Operations Commands (TSOC's, e.g. SOCCENT, SOCPAC, etc) and to make the technical capabilities interoperable with the proposed "Digital Joint Task Forces" (Digital JTFs) being created to support the transformed TSOC organizations. Another hypothesized goal is "parallel discovery," whereby open-source and commercial capabilities are identified or developed in parallel with government-owned capabilities and systems, in order to capitalize on the sharing of tools and information with interagency and international partners.

III. Scenario

The scenario for the first iteration of QUANTUM LEAP, Counter Threat Finance (CTF), involved an actual major money laundering case being investigated by the Department of Homeland (DHS) Security Bureau of Immigration and Customs Enforcement (ICE) Homeland Security Investigations Division (HSI) Bulk Cash Smuggling Center (BCSC). Details of the case are Law Enforcement Activity Sensitive (LEAS) and involve a wide range of real-world money laundering tactics, to include informal value transfer systems, unlicensed money services, conspiracy, wire fraud, layered transactions, masked ownership and beneficiary relationships, shell and shelf companies and the use of bank secrecy havens.

The scenario threat network included several multi-national and US-based corporate entities, shell and shelf companies, dozens of individuals, and millions to billions of USD in assets. The total identified scope of the money laundering activity thus far identified is approximately $2.5 billion USD in five separate law enforcement cases.

The purpose of the money laundering activity is to transfer and launder proceeds in the United States of illicit (and probably licit) activities in a country unfriendly to the US. The funds are licitly or illicitly transferred to the US where they are then used in informal value transfer systems (IVTS), trade-based money laundering, fraudulent payments, wire fraud, bribes and kickbacks and possibly the black market peso exchange.

The money laundering network includes several major groups in the US, which are all connected to financial and wealthy commercial interests in their home country. They all share various characteristics, including intricate networks of shell and shelf companies, large numbers of suspect illicit wire transfers, and use of unwitting or semi-witting proxies (often US citizens) and a heavy reliance on family and personal relationships.

The various components of this scenario for this particular threat finance network operate globally, conducting large-scale business transactions in many different countries, relying on banking secrecy havens such as the British Virgin Islands, the Madeira Islands, Switzerland, and Bermuda.

The success of the scenario network is enabled by the unfriendly relations between their home country and the US, as well as heavy reliance on layered transactions, large numbers of wire transfers, including to/from bank secrecy havens, masked ownership and beneficiary relationship of many transactions, close relationships with the home country's government, and common use of inflated-value transactions, often offshore, with institutions in the home country.

Facilitators in the threat network include registered agents, attorneys and accountants, uncooperative banks, limited liability corporations (LLCs), shell and shelf companies, and family members and close friends of the key participants. To exploit this network, heavy use was made of open-source information and social media, including the exploitation of publicly available personal identifying information (PII), web log (blog) postings about the network and its

members, as well as publicly reported data about companies, banks or other entities associated with the network.

The scenario investigation is a large interagency effort with participants from many non-DOD law enforcement and regulatory agencies, led by ICE/HSI. The main goals of the investigation includes the criminal prosecution of key leaders of the money laundering network, and possibly regulatory reform to make it more difficult for this type of activity to be conducted in the future.

IV. Experiments and Participants

Several industry representatives were invited to participate in QL to demonstrate their particular technologies or capabilities. Most of the industry participants were developers or providers of software tools, chosen for their potential applicability to the CTF scenario.

Raptor X/Creative Radicals

The backbone of the open source analytical effort was Raptor X, a GOTS GIS architecture designed to incorporate a wide range of "plug-ins" or software modules from third parties to enhance the ability to discover relationships, human networks, and geospatial features.

The key plug-in used with Raptor X in the first iteration of QL was called "Social Bubble," developed by Creative Radicals, Inc. (http://creativeradicals.com/) Social Bubble enabled search via the Twitter API and display of Twitter-related content associated with the search query within Raptor X. This tool was heavily used to explore human networks associated with the CTF scenario and enabled identification of various entities: people, businesses and locations associated with the moneylaundering network.

Information Systems Worldwide (i_SW)

i_SW (http://www.iswcorp.com/) is one of the principal contractors building the "Digital JTF" concept on behalf of SOCOM NCR to support the "TSOC transformation". I_SW engineers and developers participated in QL to evaluate the process and tools developed for subsequent integration into the Digital JTF concept.

Cybertap

The Cybertap Corporation (http://www.cybertapllc.com/) produces a tool called "Recon"that can be used to recreate data streams from an Ethernet "tap" or packet capture file. The tool is effective at recreating documents and pages from a raw TCP/IP packet stream. Documents are re-created in their native format, .html, .pdf, etc. While there are many other tools, including many open source programs, that will recreate a TCP/IP stream, Rr tap to provide data for it to process.

Red Cell Intelligence Group

Red Cell Intelligence Group (http://www.redcellig.com/) is a financial intelligence company who specialize in characterizing global correspondent banking relationships. They collect data from several public or commercial sources, including comparatively expensive financial industry data subscriptions, to create a searchable database of international banking relationships. This data is potentially highly applicable to the CFT scenario although no sample data related to the scenario was introduced during QL.

Lockheed Martin Inc

Lockheed Martin (http://www.lockheedmartin.com/) primarily participated by having representatives to observe and advise on organizational issues. They did not demonstrate any software tools.

Green Line

Green Line Systems (http://greenlinesystems.com/index.php) is a commercial maritime tracking and analysis company. Their "MDA WatchKeeper" product delivers comprehensive global ship tracking and analytical services in a Software as a Service (SaaS) format. For QL they demonstrated the ability to track a particular ship or ships associated with a named company or other commercial entity including transoceanic transits.

G. Intrusion, Inc.

Intrusion, Inc. (http://www.intrusion.com/) specializes in large scale open-source monitoring and analysis. They have a nearly unique capability (shared only with large search engines such as Google) to index the internet and establish network relationships, status, and topography over time, as well as collect large quantities of data from the "deep web", or sources which are accessible via the internet but not necessarily indexed or linked via a WorldWide Web (WWW) page. Intrusion's capabilities include several software tools:

- Savant: the principal data accumulator or engine that indexes the internet on a constant basis
- Resume Harvest: a tool to collect individual resumes posted on the internet
- TraceViewer: a tool to geolocate IP addresses and map the global IP space
- Global Harvest: a large repository of WWW and web server data
- GeoObjects: a tool to fuse multi-source locative data
- TraceCop: monthly survey of internet topography
- TraceViewer: global IP space mapping via traceroute

They did not provide any sample data sets during the first iteration of QL but would probably be able to provide some sample data for future iterations, if given some advance indication of the subjects of interest.

Numerica Corporation.

Numerica Corporation (http://www.numerica.us/) produces computational software for compressing and evaluating geospatial data. Their tool is capable of real-time signal processing on networks and potential detection of anomalous behavior, but use of the Numerica tool against a digital file containing steganography might erase the steganographic payload, similar to other compression tools. During QL, the Numerica tool was not used significantly, likely due to the lack of a candidate dataset to process.

Semantic Research Inc (SRI)

Semantic Research Inc. (SRI) (http://www.semanticresearch.com/) produces the *Semantica* visual analytics tool. Semantica is capable of ingesting structured and semi-structured data and displaying it in a "triplet" format, e.g. two entities and a relationship, such as "*Acme Widgets is owned by Wile E. Coyote.*" Triplet datablocks can then be interrelated to identify and visualize networks. Semantica is capable of processing and visualizing live data, if the data is structured in a format that the tool can ingest.

SRI provided a limited demonstration of the Semantica visual analytics tool. It was proposed that SRI develop a "plug-in" version of Semantica to interoperate with Raptor X for future iterations of QL.

Sherpa Analytics

Sherpa Analytics (http://www.sherpaanalytics.com/) specializes in the near real time and automated analysis of publicly available data in all media channels, especially the social media, in many languages, to extract indicators and assess insights that impact target audiences. Sherpa discussed but did not demonstrate their capabilities. It appears they mainly offer a consulting service using off-the-shelf tools, vice providing a tool of their own. Their capabilities, focusing on social media collection and analysis, appear to be a very good fit for QL requirements, however.

Cypherpath

Cypherpath (http://cypherpath.com/) participated in QL principally by providing a financial crimes subject matter expert who was able to guide the open source data collection effort as well as providing a comprehensive overview of the mechanics of moneylaundering.

Basis Technology

Basis Technology (http://www.basistech.com/) provides text analytics and digital forensics tools potentially useful for media exploitation or analytics particularly of foreign language text sources. They are supporting the Digital JTF effort and their capabilities are probably desirable for QL requirements as well, although they did not specifically demonstrate applicability of any of their tools to the QL scenario in this interation.

Actionable Intelligence Technologies (AIT)

Actionable Intelligence Technologies (http://www.aitfis.com/) produces a financial analysis tool called "FIS" (for Financial Intelligence System). It is, in effect, an accounting

software package similar to Quicken or Peachtree but modified and optimized for financial investigations. It is used by many financial crimes investigatory agencies, including IRS, FBI, Secret Service, etc, to reconstruct and analyze large-scale financial records. AIS advertises that an investigative agency can perform an entire investigation in FIS, including importing and managing documents, records analysis, intelligence data capture, and automated analytics. AIS demonstrated FIS during QL and it appeared to be one of the most relevant and valuable tools to CTF requirements.

More than 200 additional open-source tools and sources were identified relevant to counter threat finance. Some were investigated or used during QL while others were identified as desirable but not available during the experiment. These additional sources are described in Appendices C and D.

V. Conclusions

The first iteration of QUANTUM LEAP 2012 (QL) successfully developed and identified technologies, sources, TTPs, policy and legal issues and strategies for developing a capability to support Counter Threat Finance (CTF) requirements and missions.

With over 50 participants in the initial experiment over the course of 8 days, there was a wealth of valuable input, resulting in development of a coherent methodology for approaching CTF missions.

This methodology is described as an iterative cycle, with an initial input of known and unknown indicators of CTF-related activity. Subsequently a phase of mapping and discovery is initiated, identifying people, assets, money, criminal activity, etc. This is followed by forensic development of a movement and chronology narrative of transactions, goods exchanged, communications, and transportation. Subsequently the narrative is mapped against targeted outcomes, e.g. desired end game, etc, to inform specific actions to be taken. Every time a new entity is identified associated with the CTF network or activity, the cycle is repeated. This cycle is illustrated in Figure 8 of Appendix B.

Also identified as part of the initial QL effort were broad categories of functions needed for SOCOM NCR. These include:

- Training
- Processes
- Protocols
- Data
- Technology
    - Discovery
    - Maturation
    - Transition
- Cooperation between stakeholders
- Strategy
- Risk Mitigation
- Liability
- Counterintelligence
- Work Processes
- Interagency Collaboration
- Information Sharing
- Communications
- Funding
- Feedback loops/Lessons Learned
- Resiliency, Robustness, and Repeatability
- Research and Development

These categories, described as "nodes in the solution set", were not completely developed during the first iteration but will be subjects for continued discussion at the next and subsequent QL experiments. Some additional requirements or needs identified for future QL iterations were also identified, including:

- Need to identify and prioritize target datasets within the 8 major categories (see Section II above)
- Need to identify strategies for rapid large-scale data reduction, to "zero in" in on potential targets in a timely way.
- Need to develop strategies for "triage" of targets, especially in CTF investigations, to avoid inaccurate targeting and wasted effort.
- A strategy is needed for development of measures of effectiveness (MOE). These may be different depending on the mission (CTF vs CT, CP, etc) but the metrics should be clear, unambiguous, and agreed upon with interagency partners.
- Also needed are ontologies for technical and social media collection, to clearly enumerate what data is sought from what sources, relevant to the eight categories of CTF-related information and the CTF exploitation cycle.

Some generalized additional conclusions:

- It would be highly desirable to recruit additional participants from the social media monitoring industry. Social media monitoring is a rapidly growing commercial sector, primarily focused on private sector marketing. But the same tools and technologies would apparently be highly applicable to QL requirements as well.
- Future participants in QL experiments should be "primed" with information about the theme and scenario for the experiment and encouraged to develop or modify their technologies or capabilities for demonstration against the specific scenario for that iteration. Ideally, participants should be provided in advance with some sample data as an example or for use with tools that do not collect data organically.
- We are currently in a "window" of opportunity for exploitation of social media sources for application to CTF or other SOCOM NCR missions. This window could be as narrow as 18-24 months before the social media phenomenon transforms. This future transformation is unknown and could offer additional opportunities, or existing opportunities could be closed, but the only thing that is certain is that there will continue to be rapid change.
- Legal review of the appropriate use and application of social media data is in its infancy. Social media is transforming notions of privacy and distinctions between personally identifiable information (PII) and self-reported public information will have to be established by precedent in case law.
- Almost all information relevant to the QL experiment has a locative context. Location based services (LBS) are becoming integrated into every facet of our lives and are becoming much more accepted. There is a cultural/generational component to acceptance of LBS in social media.
- Strategies and tactics to protect operational security (OPSEC) in the open-source exploitation process are very important and can be very difficult. But use of open sources

is a "double edged sword" that can compromise OPSEC as readily as it can contribute to the mission.

QUANTUM LEAP (QL) intends to use a secure workspace and collaboration capabilities in the performance of future advanced, cutting edge technology demonstrations. The SOCOM NCR Collaboration Portal (SNCP) will be specially tailored to provide a Secure Work Environment (SWE) to enhance the performance of QL by offering government, industry, interagency and academic partners the capability to share information and work asynchronously from remote locations when required – all secured by the portal. There are three stages to this process of SWE integration:

- Stage one consists of mapping the integration methodology needed to ensure that the developing Innovation can be readily transitioned to a secure work environment (SWE)
- Stage two is formatted as pre-deployment zone which mirrors portal hardware, software and network environment while only allowing access to limited users -to include original developers and beta-testers as required
- Stage three is a fully-operational enclave that addresses the security concerns related to the innovation product, allows remote web access, is part of a collaborative environment

To complete the creation of the SWE, an Innovations server will be connected to the Portal server enclave which will be accessible via a public-facing web address and/or the collaboration layer, as required. The work spaces will pull information into data groups which will be accessed by Innovations and also be able to export results in multiple formats. A risk assessment of each innovation package will be prepared and provided to the appropriate decision makers. The SWE will allow an Innovation to be held in the pre-deployment zone or cycled back to the QL for further development. Users can be segmented and all users on the network will have visibility as to who is on the network. A future enhancement will allow the creation of special classes of users, to enable secure yet limited access and functionality for trusted but un-vetted foreign partners.

VI. Summary and Thoughts on the Way Ahead

In summary, the August 2012 QUANTUM LEAP experiment yielded some vital insights into the process of exploiting social media and other open sources within a Counter Threat Finance (CTF) scenario, as well as highlighting many of the technical, organizational, legal, policy and procedural issues important to the development of the SOCOM NCR organization. There were numerous "Lessons Learned" for future iterations of the QL which will inform and improve each successive experiment. As a result of this experience, the next QL iteration should be even more productive and effective in addressing SOCOM NCR's unique needs and requirements.

With regard to the way ahead, it would be prudent for SOCOM NCR and SOCOM writ large to take a hard look at the way CTF is currently conceptualized and executed within DoD

and a wider interagency context. Terrorist, insurgent, weapons proliferation and Transnational Organized Crime (TOC) networks all rely on irregular ways and illicit means to fund their activities, to include donations from non-governmental organizations (NGOs) and clandestine financial support from hostile foreign governments. As we witnessed in the QL scenario, sophisticated front companies—established by an adversary as part and parcel of an Irregular Warfare (IW) strategy—are another important financial source, generating self-sustaining streams of revenue, laundering illicit money, and providing covert means to penetrate economies, states and societies. Such legitimate looking companies can be used to cloak less-sophisticated, large-scale means of transferring illicit funds, such as bulk cash shipment and trade-based money laundering. Protecting or attacking these networks— including their financial bases of support, means of sustainment and lines of communication—has always played an important role in the history of warfare. Yet, in the 21st-century era of globalization and IW, the challenge of countering the financial and economic depth of our adversaries in conflict has become remarkably complex. Early on in the QL first iteration, a couple of points became apparent:

- There is a need to develop or identify USSOCOM policy relevant to Counter Threat Finance (CTF) missions. It was unclear to the QL participants if SOCOM has a command-wide policy or instruction governing CTF outside existing DOD instructions and directives.
- A "policy roadmap" for CTF in the USSOCOM claimancy is needed, which will probably need to be coordinated or staffed with OSD USD(I) and ASD(SOLIC)

Given the complexity of today's threat and IW financial networks, CTF as it currently exists may be too narrowly defined. From the current strategy, this is:

> *"CTF is defined as the means to detect, counter, contain, disrupt, deter or dismantle the transitional financing of state and non-state adversaries threatening US national security. Monitoring, assessing, analyzing and exploiting financial information are key support functions of CTF activities."*[3]

The scope of DOD interests in preventing US adversaries access to resources to support their activities goes far beyond financing. We should also consider non-financial resources as targets for coordinated, "whole of government" action to include:

- Counter trafficking – narcotics, illicit goods (e.g., counterfeited contraband, blood diamonds, etc.), weapons transfers, human trafficking and weapons of mass destruction and subcomponents (the latter two are subjects of future QL experiments)
- Facilitating US and allied law enforcement actions to undermine TOC networks (i.e., arrests, prosecutions, asset seizures)
- Economic activity and lines of communication ("ratlines") disruption

---

Department of Defense Counter Threat Financing Strategy, p. vi.

- Disrupting/undermining adversary critical infrastructure and economies (Economic Warfare)
- Support for economic development programs to undermine insurgencies (e.g. alternative crop programs in Colombia and Afghanistan)
- Counter transfer of dual-use technologies

While strategy and policy formulations refer to most if not all of the above, there is no coherent DOD strategy that is all-encompassing, and provides the capability for DOD to provide support to counter IW adversaries in peacetime, as well as war. In the larger view, perhaps a better terminology is "Countering Threat Resources (CTR)" vice purely CTF. As such, CTR may be more broadly defined as follows:

> *"CTR is the strategy of undermining the economic activities that generate financial resources for adversary nation states, insurgent groups, terrorist organizations and individuals who are part of or supporting forces engaged in hostilities against the US, its collation partners and allies. This includes actions taken against persons who have committed a belligerent act or supported hostilities in the aid of enemy forces, to include criminal enterprises linked to these activities."*

Given the seamless nature of adversary economic activities, it is also our view that the future design of CTF/CTR should take a global view, and not piecemeal the problem by limiting the spectrum of action or carving CTF/CTR up along Geographic Combatant Commander (GCC) lines. This will yield a system that will have too narrow a mission focus, will thus "miss the bigger picture" with regards to enemy economic activity, will not have the agility to act or coordinate action in response to disruption actions and will not be able to measure and assess the effects of disruption activities and their impact on adversary networks, not to mention on our collation partners and allies. Therefore it is the view of the QL participants that SOCOM should advocate for the following:

- Develop a more encompassing CTF/CTR strategy that incorporates a "whole of government" or more broadly "whole of nation(s)" that provides DOD the flexibility to support CTF/CTR and Economic Warfare activities in both peace and war
- Clearly define DOD (and SOCOM's role) in CT, CN and CTF/CTR activities and the derivative authorities involved
- CTF/CTR should be a national priority and directed at the national level, with a national interagency center directing the action worldwide (central planning/de-centralized execution), supported by technology that can be brought to bear on the problem to provide global situational awareness
- Examine the JIATF-South military - law enforcement – international cooperation model for a combined interagency CTF/CTR operations center that would work in conjunction with SOCOM NCR