SMALL WARS JOURNAL

Analysis in Combat: The Deployed Threat Finance Analyst

By ***J. Edward Conway***
Journal Article | *Jul 5 2012 - 12:54am*

The author wishes to thank ***David Blum*** *(Stanford University) for his comments and suggestions on earlier versions of this article.*

Abstract

This paper traces a narrative behind small wars research that has yet to be developed fully within the community yet demands attention: the role of the deployed intelligence analyst, billeted to support the command staff or a specific task force in theater with analysis and course of action recommendations. Focusing specifically on the threat finance analyst (a subset discipline with the intelligence analysis community), the author follows the history of threat finance analysis from the post-9/11 call for intelligence reform up through the creation and operation of the Iraq Threat Finance Cell and the Afghan Threat Finance Cell in Baghdad and Bagram/Kabul, respectively. The paper captures key bureaucratic and analytical challenges for the deployed threat finance analyst and the larger community of deployed all-source intelligence analysts as they continue to support operators within the small wars community.

Introduction

In the wake of September 11, 2001, the Council on Foreign Relations (CFR) stood up an **independent task force to investigate U.S. efforts to disrupt terrorist financing**. The task force found that the U.S. national security community at the time was woefully unprepared to understand and attack adequately terrorist finance networks, noting among other failures the lack of coordination among the several national security agencies. Since then, there has been an exponential growth in the attention that the U.S. intelligence community has paid to global terrorist finance networks. Today all the **major intelligence and law enforcement agencies maintain a specific counter-threat finance mission**, defined in this article as the identification and degradation of financial networks used by militant groups. The position of "threat finance analyst" is now a fixture among the bureaucracy of intelligence analysts.

While in many ways this growth has only compounded the problems that the CFR identified – specifically with regard to coordination among agencies – the creation of the Iraq Threat Finance Cell (ITFC) (2005 – 2010) and subsequently the Afghan Threat Finance Cell (ATFC) (2008 – present) represent, whether deliberately or not, the successful implementation of many of the task force's recommendations. These threat finance cells (TFCs) are interagency organizations, co-led by the Department of Defense and the Department of the Treasury (and in the case of the ATFC, headed by the Drug Enforcement Administration), wherein several U.S. national security agencies are represented through analysts deployed to combat zones and detailed to support the cells. The ITFC was headquartered in Baghdad with liaison officers spread throughout Iraq and the ATFC is currently headquartered in Kabul with similar

liaison officers across Afghanistan.

This article begins with a brief history on the institutional development of the deployed threat finance analyst before providing a critical review of the unique combination of qualitative and quantitative methods that grew within the TFCs. Prior to the wars in Iraq and Afghanistan, never in such large numbers were civilian analysts (such as those within the TFCs) deployed to combat zones. The compressed distance between collections and analysis and analysis and operations created a new set of methodological opportunities and challenges for intelligence analysts – this article attempts to address critically those opportunities and challenges as experienced by threat finance analysts in the field.

To date *Small Wars Journal* has taken the lead in providing a forum for critical discourse on what works and what does not when COIN in the classroom transitions to COIN on the battlefield. This, I think we can all agree, has made the community of COIN practitioners more informed and better prepared for the next fight. But behind COIN outside the wire is COIN as practiced in spreadsheets, slide presentations and link charts on the FOBs across Iraq and Afghanistan. We too have our challenges in transitioning theory into practice, and while no doubt the narrative is less thrilling, the influence of deployed intelligence analysts and the viability (or lack thereof) of their course of action recommendations to command staff equally need to be captured in forums such as the *Small Wars Journal* for the very same reasons – to produce more informed, better prepared COIN analysts for their next deployment, wherever that may be.

The Creation of the TFCs

At around the same time the CFR report was published, the Bush Administration released the 2002 National Security Strategy (NSS), which equally recognized the significance of the counter-threat finance mission within the Global War on Terror (GWOT). The 2002 NSS provided added emphasis and visibility for targeting the financial networks of terrorists. “To defeat this threat [of terrorism],” the **2002 NSS reads**, “we must make use of every tool in our arsenal – military power, better homeland defenses, law enforcement, intelligence, and vigorous efforts to cut off terrorist financing.” Later the document goes into greater detail:

> The United States will continue to work with our allies to disrupt the financing of terrorism. We will identify and block the sources of funding for terrorism, freeze the assets of terrorists and those who support them, deny terrorists access to the international financial system, protect legitimate charities from being abused by terrorists, and prevent the movement of terrorists’ assets through alternative financial networks.

The 2002 NSS sparked significant restructuring within the Department of Defense (DoD) and the Department of Treasury (DoT) with respect to the war on terrorism in general and threat finance in particular. Within the DoD, **the Special Operations Command (SOCOM) was named the lead coordination organization for GWOT**, which included the military pursuit of terrorist finance networks. The DoT, whose counter-terrorism role until this time was mainly relegated to countering money laundering, **created an entirely new organization within the department, the Office of Terrorism and Financial Intelligence (TFI), led by an undersecretary for intelligence**. In the first few years following the 2002 NSS, DoD and the DoT would pursue their own objectives with minimal interaction between one another, but over time those two tracks would meet in an interagency endeavor known as the ITFC and later lead to the ATFC.

Institutionalizing Threat Finance Analysis

As the DoD's GWOT lead, SOCOM was specifically required to synchronize (among other priorities) "**efforts across the military to finds ways to choke off funding to terrorists**," according to Lieutenant General David Fridovich, an Army commander within the command at the time. Under this new role, the **geographic commands were now required to submit to SOCOM their plans for executing GWOT's newly outlined priorities**. While prior to the GWOT, counter-threat finance analysts existed in small, unorganized pockets across the geographic commands, SOCOM cemented the concept and ensured its continued development.

Meanwhile DoT was taking its own initiatives in meeting the challenge outlined in the 2002 NSS. The biggest development immediately following 9/11 that gave Treasury a direct authority in countering terrorist financing was President Bush's approval of **Executive Order 13224**, *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit, or Support Terrorism*, which authorized the U.S. to seize the assets of terrorist groups and supporters of terrorist groups outside the U.S. Through E.O. 13224 the U.S. gained access to terrorist assets beyond its borders by forcing foreign bank cooperation (the U.S. threatened to block a foreign bank's access to U.S. markets and financial institutions if it did not cooperate with the U.S. directive).

In 2004 Treasury created the Office of Terrorism and Financial Intelligence (TFI) as an umbrella organization for consolidating the various units within the department that had been working on threat finance related issues (such as, for instance, the Office of Foreign Asset Control, which has direct responsibility for proposing E.O. 13224 recommendations to the president). A key office set up under the TFI was the Office of Intelligence and Analysis (OIA), responsible for supporting the TFI with "expert analysis and intelligence production on financial and other support networks for terrorist groups, proliferators, and other key national security threats." Today OIA serves as the home for most intelligence analysis within the DoT but is perhaps **more widely known for becoming the primary human resource for Treasury's analytical support to the ITFC and the ATFC**.

The Deployed Threat Finance Analyst

In late 2005, the National Security Council called for the creation of an interagency cell based in Baghdad with a mission to "**enhance the collection, analysis, and dissemination of timely and relevant financial intelligence to combat the insurgency**" – the Iraq Threat Finance Cell (ITFC). The ITFC would build off the success of an existing intelligence group within CENTCOM known as the Threat Finance Exploitation Unit (TFEU) and be co-led by a CENTCOM colonel and a DoT OIA civilian but critically, staffed by intelligence analysts not only from OIA and CENTCOM but from the Defense Intelligence Agency (DIA), the Central Intelligence Agency (CIA), and eventually agents from the Federal Bureau of Investigations (FBI), the Secret Service, Immigrations and Customs Enforcement (ICE), and the Internal Revenue Service (IRS). **Over the course of its roughly 5 year tenure in Iraq, the cell peaked at over 30 individuals and had three main priorities**: increase the depth and breadth of intelligence collection on financial issues; process that intelligence to provide course of action recommendations to military commanders; and increase capacity with the Government of Iraq to handle counter-threat finance initiatives on its own.

By late 2008, U.S. national security priorities began to shift from Iraq to Afghanistan as the situation in the former improved while in the latter it became worse. What had been known as the "Other War" was now beginning to draw significant intelligence analysis resources from analysts rotating out – permanently – from Iraq. Gen. Petraeus at this time had moved from commander in Iraq to commander of CENTCOM writ large and saw as one of his priorities the establishment of a threat finance cell in Afghanistan akin to the ITFC. When he was asked at a **House of Representatives hearing in April of 2009** to comment on how forces in Afghanistan were combating threat finance networks, he responded that the key would be

getting the Afghan Threat Finance Cell set up because of the ITFC's success in Iraq. And in a hearing also in the House around that same time, Lt. Gen. Fridovich from SOCOM shared a similar perspective, noting that due to the successes of the ITFC – specifically the way in which the cell was able to fuse multiple forms of intelligence together for military operators – "**we are now eagerly participating in the establishment of the Afghanistan Threat Finance Cell**."

Unlike the ITFC, the ATFC would be led by a special agent within the Drug Enforcement Administration (DEA) – a nod to the fact that threat finance issues in Afghanistan were inextricably linked to the narcotics industry – with DoT and CENTCOM in deputy positions in charge of the intelligence and operations divisions, respectively. Further, the ATFC's guiding principle from the start would be a focus on capacity building with the Afghan government, a priority for the ITFC that came too late in the game. The ATFC continues to operate in Afghanistan today.

Analytical Challenges within the TFCs

To understand the methodological challenges facing analysts within the ITFC and ATFC, it is necessary to set the concept of the "deployed civilian intelligence analyst" within the context of Baghdad in 2006 when the ITFC began to hit its stride. As is now well documented, levels of violence in Iraq in 2006 forced a re-examination of U.S. strategy in the country under the auspices of the **Iraq Study Group**. Of the several recommendations within the group's final report, the section that would become the most famous focused on the need for significantly more troops in Iraq on a temporary basis – the so-called "surge."

While *Small Wars Journal* has dissected the myths and realities of the surge concept from **just about every angle**, the remaining piece of the puzzle that has yet to be addressed critically is the parallel (though less covered) call for a surge in analytical support. The influx of civilian intelligence analysts into Baghdad from 2007 onwards and into Bagram and Kandahar from 2009 onwards placed traditionally Beltway- or Tampa-based intelligence analysts much closer to intelligence collection efforts on the one hand and kinetic and non-kinetic military operations on the other, and as such these analysts found themselves in positions of much greater influence. With that increased influence came increased responsibility and accountability – to state it bluntly, briefing a series of slides to a flag officer was no longer an end in itself (the traditional metric of success); rather, it was the first step in a process that could very quickly lead to action. Concepts that to date had remained largely theoretically – from using social network analysis metrics to fracture an insurgent network to generating measures of effectiveness to determine post-operation success – began to be tested and to some degree, validated (or equally likely, rejected).

As it specifically regards the TFCs, these challenges can best be divided into three categories: intelligence collection; intelligence analysis; and course of action recommendation.

Challenges and gains in influencing intelligence collection

One of the unique benefits of the TFCs was the mixture of analysts with federal agents, the latter of which with significant previous interrogations experience. Particularly in the earlier stages of the wars, military interrogators had very little actual interrogation experience when they entered into Iraq or Afghanistan. Compounding the lack of experience was the weak detainee-to-interrogator ratio, meaning much of the potentially valuable information to be found in Baghdad or Bagram went unexploited.

Within the TFCs, an analyst could identify a detainee of interest and within 24-48 hours a TFC agent, a TFC interpreter, the analyst and the detainee would be in the booth together. Placing the analyst in the booth with the agent allowed for real-time course corrections in intelligence collection. Where under the traditional collection requirements process an analyst would need to submit a list of questions that the non-

subject matter expert interrogator would then ask a detainee, under the TFC system the analyst re-directed the agent in real time to push the detainee on a previously unanticipated theme within the interrogation (e.g. an off-hand remark about the detainee complaining that his wages were not paid on time, which in itself could lead to a greater understanding of motivational vulnerabilities within a cell). Placing the analyst in the booth also provided him or her with an unprecedented window into local life – highly skewed but nevertheless valuable cultural intelligence.

An additional benefit was the ability for analysts to exert considerable influence over all types of intelligence collection – HUMINT, yes, but more importantly MASINT (measures and signature intelligence), SIGINT (signals intelligence) and IMINT (imagery intelligence) capabilities that advanced rapidly over the course of the wars. Leveraging these latter three platforms was often the difference in making TFC recommendations "actionable" – the ability to provide detail down to a level in which the analyst's work could easily be transitioned into an actual operation. Admittedly, TFC use of these "other" INTs (i.e. beyond HUMINT) was highly idiosyncratic – some analysts grasped the concepts and their potential applications very quickly, others seemed lost in the technical lexicon – and as such future development of the TFC model should consider practical training in these platforms.

The TFCs also proved to be particularly adept at document exploitation (DOCEX) – drawing value from media picked up in the field. For example, TFC agents accompanying U.S. troops on a hawala office raid would seize forensic data such as financial ledgers, which TFC analysts could then process in a matter of days due to in-house TFC interpreters/translators. Benjamin Bahney (who was detailed to the ITFC in 2008 and 2009 while at **RAND**) along with several of his RAND colleagues affirmed the value of DOCEX in their open source **analysis of Al Qaeda financial ledgers**. Their analysis shows how in-depth exploitation of financial data can increase our understanding of an organization's decision-making hierarchy and vulnerable sources of revenue and expenditure, but most importantly, Bahney et al. make a strong case for the relationship between an organization's financial health and its ability to conduct attacks – validation of the need for threat finance analysts as originally proposed by the CFR back in the wake of 9/11.

A clear intelligence challenge for threat finance analysts was in convincing traditional HUMINT collection requirement officers that detailed intelligence on insurgent processes was more (or at least equally) valuable than intelligence on individual personalities. With the advent of so-called "manhunting" within both Iraq and Afghanistan came an over-emphasis on collecting intelligence that focused on "actionable" information – names, physical descriptions, and living locations. While no doubt valuable for the targeting process (e.g. **F3EA**), a prerequisite to targeting the vulnerabilities within a network is, quite obviously, understanding how that network functions. Compounding the problem was the fact that most "systems-oriented" collection requirements focused on small arms smuggling or improvised explosive device (IED) development, not sources and methods of financial support. TFC analysts spent considerable effort – with mixed results – in submitting formal intelligence collection requirements and intelligence evaluations to reorient priorities toward financial processes and logistic chains (i.e. systems) that would ultimately allow analysts to target threat finance networks more efficiently.

Fusing quantitative and qualitative approaches

The TFCs broke new ground in testing and evaluating at the time largely theoretical approaches to analyzing insurgent networks. Traditional intelligence analysis in Iraq and Afghanistan was highly qualitative and loosely structured: analysts read through raw intelligence on a given topic in order to author an intelligence assessment, build a brief or create a target package. Traditional analysts may have been familiar with graphical tools like **i2's Analyst Notebook** (an intelligence community staple) but only as a way to database information visually. A vocal but small community within the TFCs with more

quantitative backgrounds pushed the cells to incorporate new methods in **social network analysis** (SNA), multi-objective **decision analysis** (MODA), and **influence network modeling** (INM), with varying levels of success.

Social network analysis (SNA) became the preferred method for identifying network vulnerabilities – whether those networks were based on individual relationships or the flow of financial sources within an illicit organization. Metrics like "betweenness centrality" or "degree centrality" indicated individuals that served as bridges between cells or individuals deeply connected within a cell, each of which promoted discussions on associated targeting philosophies (do we target for information, i.e. intelligence collection, or target for removal, i.e. capture?). Measures of connectivity and flow were, somewhat controversially, used to forecast the extent of network fracture and reduction of available cash that would follow should a node be removed (e.g. an individual or a front company).

Inserting multi-objective decision analysis (MODA) techniques into daily intelligence analysis was perhaps the most successful application of quantitative methods within the TFCs. Leveraging private sector methods for assessing alternative decision paths (e.g. which product is more marketable, A, B or C?), TFC analysts designed a series of explicit hierarchies or trees in order to, for instance, prioritize financial targets within an insurgent group or prioritize hawala offices within an informal money exchange network. By explicitly defining "importance" as a function, for instance, of fund-raising success, accounting knowledge, laundering abilities, etc., and evaluating each target across these categories via a fixed scale (e.g. high, medium, low), positions taken by the TFC were defensible for their consistency and tractability (i.e. action officers could very easily see why one target or approach was deemed more significant than another).

Influence network modeling (INM) provided analysts with a means to articulate their beliefs regarding how sensitive certain variables were to changes in other variables, and to extrapolate systematically the probability that possible future scenarios would follow from courses of action under consideration. For example, an assessment of corruption at a given border crossing in Afghanistan may start with the desired future scenario of a "successfully functioning border crossing," and be broken down into a series of successively more specific contributing uncertainties. The INM methodology might find that the "successfully functioning border crossing" is most sensitive to one such uncertainty – e.g. the wages of the Afghan Border Police – because they were so low as to not afford basic living standards for a typical family, providing a clear incentive for bribe-taking.

Ultimately all of these modeling approaches were successful because they offered an explicit, "structured analytic technique" to an otherwise largely qualitative problem (to borrow a phrase from **veteran CIA analyst Richards Heuer**). In other words, they were methods for making sense of messy problems. Though the development of these analytic methods no doubt predated the wars in Iraq and Afghanistan, the TFCs provided a welcoming laboratory environment to put them into practice in real-time, sensitizing the military and interagency communities to their value. However, validation of these previously unproven techniques was not without difficulty, suffering from the high operations tempo of being a deployed analyst with an action-oriented customer. Under ideal conditions, when a TFC analyst recommended a particular hawala office for kinetic targeting due, for instance, to a series of social network analysis metrics, following the kinetic operations (e.g. closure of the office), the analyst would confirm that the network's fracture, as hypothesized beforehand, actually occurred. In reality, this was almost never possible due to time constraints.

Generating course of action recommendations

For TFC analysts in Iraq and Afghanistan, the traditional intelligence assessment was only step one in a

process that ultimately led to some form of action, kinetic or non-kinetic. In this sense TFC analysts found themselves closer to the operations side of the wars than previously experienced and as such were required to transition assessments into course of action recommendations. Two challenges quickly emerged in taking on this new responsibility: recognizing that inaction is as important as action; and when to recommend kinetic force over non-kinetic force (or the reverse). Both challenges were closely related.

The greatest debate within the TFCs revolved around course of action recommendations for hawalas – informal money exchange networks typical in the Middle East and South Asia. Quantitative and qualitative analyses would often point to hawala brokers as critical nodes within an insurgent group's network, which initially led to kinetic courses of action – quite literally, kicking down the door of the hawala office and shutting down the operation. Such an approach proved to be highly controversial and underscores a key point of friction between counter-threat finance analysis and traditional COIN analysis that has yet to be fully explored. While there might have been little doubt to a particular hawala office's involvement in an illicit network, the fact remained that the vast majority of the hawalador's business was likely legitimate and relied upon by the region's populace. Shutting down a hawala node may temporarily degrade the financial network of an insurgent group (good) but at the cost of upsetting an entire village (bad).

In terms of non-kinetic operations, the TFCs tended to focus heavily on E.O. 13224, the aforementioned executive order that allowed the U.S. to seize the assets of terrorist and/or insurgent groups. Reliance on E.O. 13224 was a natural extension of the TFCs' institutional connection to the DoT, but the value of an E.O. 13224 designation continues to be debated. Specifically, E.O. 13224's "punch" is relegated to militant groups (and their supporters) that use formal channels of banking. Designating an insurgent group that draws most of its financing from informal taxes on the populace and/or local businesses (e.g. narcotics in Afghanistan) would not result in the ultimate aim of the executive order – to recover significant quantities of cash and therefore degrade the group's financial operations.

Proponents of E.O. 13224 will claim that there is secondary value in the "name and shame" association of being designated, but this too is questionable. Insurgent groups derive a component of their legitimacy from the level of importance the enemy places on their existence. When in 2009 the U.S. government designated Kata'ib Hizballah under E.O. 13224, the group was described in the **State Department's press release** as "a radical Shia Islamist group with an anti-Western establishment and jihadist ideology…responsible for numerous violent terrorist attacks since 2007, including improvised explosive device bombings, rocket propelled grenade attacks, and sniper operations." Such a statement might sound "shameful" to a U.S. citizen but to an Iraqi it might resonate loudly and actually increase the group's local legitimacy.

Conclusion

The imperative to deploy civilian analysts to combat zones is quickly diminishing. The mistake at risk is to assume the concept of the TFC is equally becoming irrelevant as the U.S. national security community looks beyond Iraq and Afghanistan. Though the TFCs represent a fraction of the deployed civilian analyst population, within that fraction great progress has been made in influencing intelligence collections, in fusing quantitative and qualitative methods for solving complex, multifaceted problems, and in becoming more active in recommending courses of action on the battlefield. While the battlefield will change – perhaps, for instance, to drug cartels in Latin America, or insurgent groups in North Africa – the concept of a small, forward-deployed interagency cell that on an operational level combines analysts with agents, collectors and interpreters, and on an analytic level combines qualitative and quantitative approaches, is a concept worth replicating across the spectrum of U.S. national security challenges. This article begins to make the case for that replication by unfolding the role (and significance) of the deployed threat finance

analyst to date. The next steps in evaluating the concept of the deployed civilian analyst are threefold:

First, to capture more completely the advances of the TFCs so that they may be replicated. How exactly can an analyst use influence network modeling or multi-objective decision analysis in his or her daily routine? How exactly does one evaluate the costs and benefits of recommending an individual as a target for capture as opposed to a target for collection?

Second, to dig deeper into the application of quantitative methods with an aim for assessing the validity of these approaches. Can we truly predict network fracture via social network analysis algorithms? What are some of the assumptions of quantitative approaches that military commanders may be unwilling to accept?

Third, to widen the aperture. While the TFCs represent a convenient microcosm for studying both the intellectual and bureaucratic challenges of deploying analysts to a combat zone, particularly against a subject matter focus of increasing importance, the TFCs were but a part of a much larger community centered in Baghdad, Bagram, Kabul and Kandahar. Capturing the successes and failures of IED analysts as they built and targeted logistic networks of insurgent groups in Iraq or the successes and failures of command and control (C2) analysts as they struggled to identify key leaders within a sea of shadow governors in Afghanistan are all equally critical.

All in all capturing the challenges and institutionalizing the successful approaches associated with analysts in combat zones will lead to better, more informed analysts overall, whether in CONUS or OCONUS, and therefore ultimately lead to more informed operators and operations, wherever they may be.

About the Author

J. Edward Conway

J. Edward Conway is a doctoral candidate and postgraduate researcher at the **Institute for Middle East, Central Asia and Caucasus Studies** at the University of St Andrews in Scotland and a former analyst for the U.S. Department of Defense. He deployed to Baghdad, Iraq in 2007 to support the Iraq Threat Finance Cell and to Balad, Iraq in 2009 to support a joint task force as the resident threat finance analyst.

Available online at : http://smallwarsjournal.com/jrnl/art/analysis-in-combat-the-deployed-threat-finance-analyst

Links:
{1} http://smallwarsjournal.com/author/j-edward-conway
{2} http://fsi.stanford.edu/people/David_Blum/
{3} http://www.cfr.org/economics/terrorist-financing/p5080
{4} http://projects.washingtonpost.com/top-secret-america/
{5} http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/
{6} http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg33596/html/CHRG-109hhrg33596.htm
{7} http://www.treasury.gov/press-center/press-releases/Pages/tg1291.aspx
{8}

http://defensenewsstand.com/index.php?option=com_ppvuser&view=login&return=aHR0cDovL2RlZmVuc2VuZ
{9} http://defensenewsstand.com/Inside-the-Navy/Inside-the-Navy-03/20/2006/menu-id-289.html
{10} http://www.fas.org/irp/offdocs/eo/eo-13224.htm
{11} http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Intelligence-Analysis.aspx
{12} http://www.treasury.gov/press-center/press-releases/Pages/hp898.aspx
{13} http://defensenewsstand.com/index.php?option=com_ppvuser&view=login&return=aHR0cDovL2RlZmVuc2VuZ
{14} http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg53056/pdf/CHRG-111hhrg53056.pdf
{15} http://www.usip.org/isg/iraq_study_group_report/report/1206/index.html
{16} http://smallwarsjournal.com/blog/as-the-iraq-war-ends-reassessing-the-us-surge
{17} http://www.rand.org/topics/terrorism-financing.html
{18} http://www.rand.org/pubs/monographs/MG1026.html
{19} http://smallwarsjournal.com/topics/F3EA
{20} http://www.i2group.com/us/products/analysis-product-line/ibm-i2-analysts-notebook
{21} http://www.journals.elsevier.com/social-networks/
{22} http://da.journal.informs.org/
{23} http://www.inet.saic.com/docs/_docs_/math.pdf
{24} http://www.saic.com/business/technologies/license/it/causeway.pdf
{25} http://www.cqpress.com/product/HeuerPherson.html
{26} http://www.state.gov/r/pa/prs/ps/2009/july/125582.htm
{27} http://smallwarsjournal.com/jrnl/art/us-efforts-to-combat-terrorism-financing
{28} http://www.st-andrews.ac.uk/intrel/staff/index.php/jc555.html
{29} http://www.st-andrews.ac.uk/intrel/mecacs/

Copyright © 2017, Small Wars Foundation.

Select uses allowed by Creative Commons BY-NC-SA 3.0 license per our **Terms of Use**.
Please help us support the **Small Wars Community**.