THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

VOLUME 12 NUMBER 4

OCTOBER 2013
FINANCIAL SERVICES

Market Resilience.....2
Cyber Threats.....7
Hacking Back.....11
Terrorism Financing.....16

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

This month's issue of *The CIP Report* highlights the Financial Services Sector, the backbone of the world economy. Our authors address the challenges of developing market resilience, the interplay with cybersecurity, and the related problem of terrorist financing.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

To begin, Professor John W. Bagby of the College of Information Sciences and Technology at Penn State discusses financial market resilience. Anthony Shaffer and Robert B. Newman, Jr. then evaluate public-private partnerships in the context of a recent tabletop exercise simulating an attack on the U.S. Financial Services Sector as part of the Cyber Analysis Strategic Wargaming Series at the U.S. Army War College. Next, Sean L. Harrington, a cybersecurity policy analyst and risk assessor for a U.S. financial institution, analyzes the extensive targeting of banks by hackers and explores the viability and legality of active defense, or "hack backs." Finally, Dennis M. Lormel addresses the tangential issue of terrorist financing, discussing both the threat to the integrity of the Financial Services Sector and the need for innovative cooperation between commercial banking entities and law enforcement.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Financial Market Resilience: Coping with Market Failure

by John W. Bagby
College of Information Sciences & Technology
The Pennsylvania State University

Financial markets periodically experience watershed changes that profoundly impact their "integrity." Many academics, policymakers, and some practitioners willingly examine such unsettling occurrences when they may arguably cause financial market failure. These include problems of liquidity, manipulation, fraud, information asymmetries, volatility, overvaluation from speculative frenzy, and transaction matching malfunction. This article reviews how such failures, including flash-crashes and the externalities produced by high frequency trading (HFT) impact resilience.

The article exhorts a search for models to bolster financial market resilience to avoid the devastation of broad and deep market failure. The National Market System (NMS), like other critical infrastructures, needs "hardening" to withstand volume-induced, algorithmic transaction overload. Due diligence requires that technical vulnerabilities of exchanges and other essential marketplace participants be continually reassessed to facilitate resilience and contingency planning. An important byproduct will be that risks of "social engineering" directed at the financial system will also be addressed.

Transaction Processing Resilience

Infrastructure failures in transaction processing capacity are vivid contemporary examples of resilience vulnerability. This can threaten industrial economies highly dependant on the Financial Services Sector. These problems may emerge slowly and incrementally, resulting in gradual overload beyond comfortable or seemingly affordable scalability. Wall Street's "back office" problem in the 1970s is the exemplar. However, incremental overload is a double-edged sword. A slow growing phenomenon permits more carefully considered and evolutionary responses, but may induce complacency. By contrast, when the transaction processing breakdown is abrupt, the resulting rise in trading volumes rather quickly exposes worrisome infrastructure failure.

The "clearance" process for securities or commodity transactions has a complex system architecture. It includes all activities starting with a customer's order, through the making of all commitments in various auction and order matching systems, and persists until that transaction is fully settled. Clearance is under increasing stress because high volume trading now greatly exceeds the time needed for completing each underlying transaction. Settlement of such transactions is a business process—documents and records are delivered. Settlement usually includes a simultaneous exchange of money payments, the closing of margin borrowing, or finalization of barter that constitutes adequate consideration payment(s) to fulfill contractual obligations.

The banking and finance sectors have long been viewed as critical infrastructures, nearly rising to the status of "public goods." Financial market failure may constitute a Tragedy of the Commons.[1] Indeed, some argue the 9/11 attacks on the World Trade Center were actually intended to debilitate capitalism's funding mechanism. This arguably makes Wall Street's "ground zero" designation both a very real, physical observation and a powerful metaphor because Wall Street remains the (financing)

(Continued on Page 3)

[1] Hardin Garrett, *The Tragedy of the Commons*, 13 Science 1243, 1243-1249 (1968).

(Continued from Page 2)

foundation for the American economy.

A "National Market System"

Congress originally envisioned the NMS mandated by the Securities Markets Amendments of 1975 as necessary to protect the "integrity" of the financial markets. This has been largely implemented in recent years to increase competition among exchanges, increase transaction processing efficiency, and confine broker/dealer conflicts of interest. Recent NMS implementation is even more narrowly focused on providing reliable trade opportunities for investors: best prices and fastest execution. However, this exceedingly narrow interpretation of "integrity" focuses primarily on conflicts of interest. The broader vision of integrity focuses on financial market stability and market resilience to continue accurate operations despite a wide variety of operational risks. The NMS was originally conceived to reverse the debilitating "back office problem" emerging as individual investors in the 1970s flooded into the stock market raising transaction volume beyond capacity. A logjam developed in the paper-based transaction-matching of broker/dealers' back offices. Transaction processing became a pinch-point that attenuated system efficiency.

Thus, the NMS was actually intended as a set of complex resilience design principles. A robust NMS would contribute to confidence in the financial market system's integrity and fulfill the expectations necessary to attract and allocate capital efficiently for the support of American industry and economic vibrancy. These NMS goals easily adapt to address predictable and unpredictable financial market failures, including the "mechanisms" of transaction processing. The Security Exchange Commission's (SEC) 2005 Regulation NMS reveals transaction processing "integrity" despite that it was prompted by growing Wall Street conflicts.[2] Indeed, the SEC's May 2012 "Joint Industry Plans" in Securities Exchange Act Release No. 34-67091 clearly confirms the NMS is about integrity as originally defined more broadly.

A litany of market failures in modern history have often been followed by market design changes, initiating many successful remedies driven by public policy. For example, the Panic of 1907 (Knickerbocker Crisis), triggered market design changes to address contagion, panic-induced runs, and conflicts from side bets made in bucket shops. Market regulations were soon instituted thereafter by Kansas in 1911 as state blue sky regulation. In the post-1929 crash era the Pecora Commission recommended the SEC's modern financial market regulation, including oversight of critical liquidity-contributing market intermediaries—specialists and market makers. Black Monday in October 1987 triggered circuit breakers to address volatility induced by (computer) program trading, a form of "cooling off." The dot.com bubble of 2000-2001 was reminiscent of the March 1637 speculative bubble in Dutch tulip bulbs. Speculative frenzy generally produces overvaluation, "irrational exuberance," largely unaddressed by regulation. Three notable market failures in recent years could coalesce into another perfect storm that would debilitate financial markets: flash crashes,[3] HFT, and software-induced trading failures. This liquidity squeeze from transaction processing lethargy would likely induce volatility from panic and speculation, most certainly vulnerable to exploitation by social engineering.

Conceptual Design to Address Financial Market Failure

Public policy plays an increasing role in the redesign of financial market resilience. The economics of security is instructive: consider how resilience in the payments system was incrementally "hardened." Members of the private sector, after centuries of incremental small scale experiences with theft by highwaymen, social engineering by fraudsters, and sudden/abrupt catastrophes attracted public attention. Both market pressure and self-interest compelled security enhancement. Now contrast that evolution with the modern

(Continued on Page 4)

[2] "Regulation NMS," SEC Exchange Act Rel. No. 51,808, June 9, 2005, *available at* www.sec.gov/rules/final/34-51808.pdf.
[3] *See, e.g.*, Joint Committee Staff Report, Findings Regarding the Market Events of May 6, 2010, Commodity Futures Trading Commission & Securities Exchange Commission (Sept.30, 2010), *available at* http://www.sec.gov/news/studies/2010/marketevents-report.pdf.

(Continued from Page 3)

systemic vulnerabilities of the financial system.[4] Systemic resilience vulnerabilities may prevent public policy from indulging in the libertarian, incremental approach. Financial failures externalize costs on investors, industry, the whole economy, and world. When left to their own devices, the private sector is reliably beset by moral hazards, asymmetric information, externalities, and free riding. Indeed, financial system security investment exhibits most of the characteristics of a weakest-link (in-chain) security game.[5]

Few domain experts have serious confidence in domination by regulator-imposed design standards. Because they risk stagnancy, obsolete technologies become locked-in and revolutionary innovation is locked-out. This tension between prescriptive approaches and libertarian experimentation produces a middle way. Regulatory approaches are imposed mostly when private sector security controls either fail or are unlikely given failures in the markets for security controls. Public policy generally prefers industry-led resilience derived from standardization by self-regulatory organizations (SRO) comprised of professional domain experts.

Should financial system resilience be initiated at the grassroots level in the private sector? Are resilience mechanisms doomed to political failure when imposed by government? Not exactly! Remedy development for financial market failure follows a hybrid approach. For example, consider the high degree of order transaction processing reliability developed for the payment system (e.g., negotiable instruments, electronic funds transfer). Industry practices developed incrementally, evolving over hundreds of years. They were eventually made more efficient when enabled by public policy. This hybrid approach is complex, an iterative process of vulnerability analyses and remediation. Most constituents should participate by identifying weaknesses, proposing controls and monitoring experience. The 2009 Dodd-Frank law and other nations' post-2008 financial crisis remediation[6] does just this. Furthermore, investment in contingency planning is strongly indicated.[7]

Information Technology—Both a Cause and a Cure

Information technology (IT) may cause some financial market transaction process failures. However, IT also serves to rescue the financial system. IT is likely to become the least cost provider of such remediation. IT permits low-cost redundancy for transaction recordkeeping and provides alternative reconciliation mechanisms.

IT is prevalent in the paradigm of modern transaction unwinding procedures: insolvency proceedings. The Lehman Brothers bankruptcy, like other unwinding regimes required in the post-2008 financial crisis, relied on IT to support unwinding "positions." Indeed, the two August 2013 disasters, the NASDAQ "freeze" and the Goldman-Sachs options trading "errors," are now classic methods to "set things right." Furthermore, these regimes inspire network science approaches to discover and remediate centrality risk for the vulnerabilities imposed by "systemically important financial institutions" that may remain "too big to fail."[8]

Consider how the paper order ticket and the telephone were the twentieth century's transaction processing backbone. Today, software running network data is the

(Continued on Page 5)

---

[4] *See, e.g.,* Marc Labonte, *Systemically Important or "Too Big to Fail" Financial Institutions*, Cong. Res. Serv. No. R42150 (July 30, 2013), *available at* www.fas.org/sgp/crs/misc/R42150.pdf.

[5] *See generally*, Jens Grossklags & Benjamin Johnson, *Uncertainty in the weakest-link security game*, Proceedings of the First ICST Int'l Conference on Game Theory for Networks (GameNets'09) (2009 IEEE Press, Piscataway NJ) at 673-682.

[6] *See, e.g.*, Alessandro Beber & Marco Pagano, *Short-Selling Bans Around the World: Evidence from the 2007–09 Crisis*, 68 J. Fin. 343, 343-81 (2013) *available at* http://www.afajof.org/details/journalArticle/4240281/ShortSelling-Bans-Around-the-World-Evidence-from-the-200709-Crisis.html.

[7] Consultative Document, *Recovery and Resolution Planning: Making the Key Attributes Requirements Operational*, Financial Stability Board (Nov. 2012) *available at* https://www.financialstabilityboard.org/publications/r_121102.pdf.

[8] *But see*, David A. Skeel et al., The New Financial Deal: Understanding the Dodd-Frank Act and its (Unintended) Consequences, (John Wiley, New York, 2011).

(Continued from Page 4)

financial system's transactional backbone. The American software industry has little legal responsibility for product quality outside privity under breach of contract. However, other nations are far less forgiving; some European nations do not support the software industry with nationalistic and protectionist goals. Whether software causes or simply contributes to unintended consequences of HFT remains widely misunderstood. While this understanding gap should delay imposition of abrupt regulatory design choices, it should never delay the identification and analysis of HFT causes and their systemic mechanisms.

Drawing from a Palette of Market Failure Remedies

In the past, financial market failures were addressed largely by regulator imposition of new controls, often fiercely opposed by industry. Predictibly, investors criticize some other provisions as insufficient "window dressing." Financial market regulation must survive a gauntlet of lobbyists and rivalry among private interests.[9] Consider how robust opposition delayed Dodd-Frank's Volker Rule addressing conflicts by banning proprietary trading. Contrawise, Dodd-Frank critics argue that battalions of regulatory lawyers burrowed deeply into the federal financial (functional) regulators to prevent further real reforms. Still, longevity and independent empirical validation of many reforms illustrate how a lasting and positive impact is possible for useful remediation.

Three clusters of reforms emerge: emergency powers, preventative structures, and curative remedies. First, emergency powers have a long and proven tradition, although not without criticism. For example, the post-1987 crash circuit breakers clearly attenuate panic, yet temporarily make markets illiquid. Liquidity remains a problem for smaller issuers. Similarly, temporary trading halts can focus on particular instruments or on issuers (e.g., impending material news release), and sometimes on the whole market. The uptick rule is a micro-trading ban that prevents manipulation by bear raiders.

The second cluster aggregates preventative measures, typically targeted at adverse market practices that precipitated significant negative regulatory and legislative findings. For example, the aforementioned Volker Rule resulted from such evidence. Transparency requirements can function as preventative, particularly when intended to harness pressures from analysts and traders informed by mandatory disclosures. Planning has taken firm hold in the "tool kits" of financial and banking regulatory authorities, particularly for disaster recovery. For example, top U.S. financial institutions were required in 2013 to study, devise, and file contingency plans to aid in orderly "resolution," the unwinding of transactions to preserve financial stability.[10]

The third cluster includes regulatory tools to provide curative remedies. Liability is a classic under banking and financial services laws. Of course, litigation is unpopular in the industry—admittedly costly and susceptible to gaming. The widespread private-sector-designed securities arbitration is a reaction that addresses the harassment and abuse of process aspects of unwinding individual trades. Insurance patterned on the Federal Deposit Insurance Corporation by the Securities Investors Protection Corporation is also a curative remedy. SROs may continue to embrace insurance, essentially a transaction tax that spreads such risks. The Financial Industry Regulatory Authority (FINRA)

(Continued on Page 6)

---

[9] Gary Rivlin, *How Wall Street Defanged Dodd-Frank*, The Nation, May 20, 2013, *available at* http://www.thenation.com/article/174113/how-wall-street-defanged-dodd-frank.

[10] Reg. QQ, 12 C.F.R. §243.8(c) (2013)(living will).

> [The]Dodd-Frank Wall Street Reform and Consumer Protection Act requires that bank holding companies with total consolidated as sets of $50 billion or more and nonbank financial companies designated by the Financial Stability Oversight Council for supervision by the Federal Reserve submit resolution plans annually to the Federal Reserve and the Federal Deposit Insurance Corporation (FDIC). Each plan, commonly known as a living will, must describe the company's strategy for rapid and orderly resolution in the event of material financial distress or failure of the company.

http://www.federalreserve.gov/bankinforeg/resolution-plans.htm.

(Continued from Page 5)

has recently proposed additional insurance schemes to address other financial market failures.[11]

Final Observations: Please Do No Further Harm!

Some final observations on financial market resilience. First, please do no further harm than was suffered in the last financial crisis. Recognize that nearly every regulatory response inspires work-arounds by regulated entities. Work-arounds should be anticipated much more diligently than in the aftermath of several recent financial crises. Regulation, like any obstruction, spurs innovation in new trading strategies, revealing new weaknesses and making new vulnerabilities. Consultation that forges consensus is optimal, but inevitably some market failure remedies eviscerate trading strategies, perhaps whole lines of (profitable) business. These casualties should survive a societal risk-benefit analysis.

Second, some of Dodd-Frank's financial stability remedies include mapping the entire network of transactions among all trading parties and their clients. While this enables systemic vulnerability analysis using network science, the resulting transparency threatens proprietary trading strategies widely believed to offer at least temporary economic advantage. Furthermore, comprehensive transaction disclosure is likely suspected to offer regulators and plaintiffs' lawyers an evidentiary trail that could chill innovation and curb profitability.

Finally, it is a widely shared financial industry ethic that liquidity must remain king.[12] Price discovery and near instantaneous trade matching appear to sometimes benefit investor clients but nearly always benefits the financial services industry's twin business models of commission income and proprietary trading (for their own account). The liquidity quest can also induce conflicts evident in the 2008 financial crisis that prompted the Volker Rule. Consider that liquidity is argued as a primary cause of market failure at both ends of the liquidity spectrum: illiquid markets demonstrate failure, as does HFT that exploits a seemingly infinite supply of transaction opportunities. When the liquidity goal is over-satisfied and this coincides with poorly understood HFT "black-box" proprietary algorithms, then systemic risk of financial market failure through transaction processing reemerges.[13] ❖

[11] Jean Eaglesham & Rob Barry, *Finra to Consider Requiring Brokerages to Carry Arbitration Insurance,* Wall St. J., Oct. 4, 2013, *available at* http://www.thenation.com/article/174113/how-wall-street-defanged-dodd-frank.

[12] *See, e.g.*, Burcu Duygan-Bump et al., *How Effective Were the Federal Reserve Emergency Liquidity Facilities? Evidence from the Asset-Backed Commercial Paper Money Market Mutual Fund Liquidity Facility*, 68 J. Fin. 715, 715-737 (2013).

[13] Jenkins, Holman W., *How to Think about the NASDAQ Freeze*, Wall St. J., Aug. 23, 2013, at A11, *available at* http://online.wsj.com/article/SB10001424127887324165204579030880774245124.html.

Software Assurance Workshop

Presented by the Cyber Security and Information Systems Information Analysis Center (CSIAC)
Sponsored by George Mason University's Center for Infrastructure Protection and Homeland Security (CIP/HS)
Presenter: Taz Daughtrey, Senior Scientist at Quanterion Solutions

To register, please visit:
https://www.regonline.com/Register/Checkin.aspx?EventID=1316007

George Mason University
Center for Infrastructure Protection and Homeland Security

CSIAC
Cyber Security & Information Systems Information Analysis Center

Cyber Threats and the U.S. Financial System: A Table Top Exercise at the U.S. Army War College[1]

by Anthony Shaffer and Robert B. Newman, Jr.

Across the board, private-public partnerships are not just a good idea, they are a fact of life. In all sectors of the economy, the business community is partnering with government to address emergency situations. Yet this rise of private-public partnerships, while pervasive, has not always been welcomed by some of the nation's stakeholders —in particular the Department of Defense (DOD). In a military context, it is critical to understand this paradigm for purposes of preparation and resilience, particularly as the possibility of defense support to civil authorities (DSCA) becomes more likely as the significance of an event escalates.

There was a time during the Cold War when the government had created sufficient capacity to ensure it could run without the civil infrastructure backbone for an extended period. Many military bases were built with their own power plants, water purification, and telecommunications capabilities. This sort of capacity redundancy is now limited, and in most bases, eliminated.

Due to our victory in the Cold War and significant budget constraints, the military has become increasingly reliant on having continuous and often priority access to private sector capacity, which is by nature commercial and not necessarily available in a time of crisis. Besides the military, all other departments of the federal, state, and local governments will become competitors for the same private sector/commercial capacity during an emergency, be it for fuel, electricity, or Internet bandwidth (and that is assuming that these commodities are still available).

The Army War College (AWC), a graduate school for senior army officers, has taken the lead regarding this critical issue. Ultimately, the military's mission is to protect and defend the people of this great nation, and while there is concern about the full spectrum of resilience, the AWC has prioritized focus on cyber with specific attention to the protection of critical banking infrastructure. The Army's mission to protect the nation must include and extend to cyberspace. As much as mountain operations, cyberspace has developed into a legitimate component of land warfare, but one that must be better-defined and prepared for battle.

Transition to digital society, while hugely beneficial, has simultaneously created a sword of Damocles resulting from the development of significant vulnerabilities. Banking and our reliance on its current digital form now requires special examination and understanding.

One key issue is how the whole of government, and society in general, would survive in an environment of diminished digital capabilities (i.e., lack of Internet, or loss of bulk power grid). Further, within the context of technology, based on the military's reliance on commercial systems, how would the military carry on in this diminished resource environment?

Far away from the paneled board rooms of U.S. banks, a diverse group of financial, cyber, and defense experts gathered at the historic AWC in Carlisle Barracks, Pennsylvania, to discuss and debate preparations for and responses to a cyber attack against the U.S. Financial Services Sector.

Banks around the world and U.S. banks in particular are no strangers to cyber attacks. While most attacks have focused on distributed denial of service (DDOS), in recent months more intense attempts at DDOS, along with the theft of customer information and money

(Continued on Page 8)

[1] This article was adapted from the after action report of the Cyber Analysis Strategic Wargaming Series. 27-28 March 2013, Center for Strategic Leadership Development, US Army War College, Carlisle Barracks, PA 17013.

(Continued from Page 7)

have led banking institutions to focus even harder on protecting their systems against cyber attacks.[2] As one banker put it, "the banks are getting tired of being hit in the face."

Financial institutions have long been a favorite target for cyber hackers and thieves and employ some of the most modern technical systems to protect their assets. They also regularly host exercises to test their systems and share information with regulators, the Federal Reserve, and state banking commissions. However, the AWC exercise was unique in that the setting and the host had nothing to do with banking, at least in the traditional sense.

Stressing the potential for significant physical casualties and economic loss from a successful attack against this sector, former Secretary of Defense Leon Panetta and former Secretary of Homeland Security Janet Napolitano recently addressed the need for a more dynamic public-private partnership focused on responsive national cybersecurity. The participant diversity demonstrated an understanding of the importance of a strong working relationship between both public and private partners.

The Army is used to thinking of kinetic actions involving moving troops in combat and countering a threat or attack with physical force. Many soldiers questioned the relevancy of an exercise to develop tactics and protocols to respond to and recover from a cyber attack. The financial professionals likewise had a hard time understanding the need for such a partnership since most of the cyber attacks that they had experienced were DDOS attacks with no harm to people or systems, leading many to wonder how a kinetic attack might ever be justified. Nonetheless, as the exercise continued, it became evident that the cascading effects of an attack against the U.S. financial system would most likely require support and response from the military.

The Center for Strategic Leadership and Development (CSLD) at the AWC conducted a cyber war game as part of the AWC Strategic War gaming series. The purpose of this war game was to identify deficiencies in current U.S. policy, and conduct in-depth analysis of strategic issues concerning a whole-of-government response to cyber aggression directed against the U.S. Financial Services Sector, and to specifically identify the Army's doctrinal equities and interests.

This cyber war game considered an attack scenario on the financial industry that started with an indications and warnings (I&W) phase, escalated to an early hostilities phase, and culminated with a full hostile engagement. Three groups assessed policy requirements from the perspectives of DOD, DHS, and DOJ. Each group was represented by experts from the Army, other DOD organizations, government agencies, the Federal Reserve Board of Governors, and private sector institutions.

Participants responded to hostile action in accordance with the roles and missions of the government organization they represented in the war game and identified policy, legal, and strategic issues associated with response to aggressor actions. Groups then developed policy options.

The I&W phase focused on policy and legal issues related to preemption and deterrence. Initial decisions participants identified as essential included: designation of supported/supporting relationships; clear identification of type of conflict (criminal, national security, or national defense); and policy and legal changes needed to counter the threat.

The second phase expanded to early hostilities of an impending cyber conflict. Discussions continued to focus on policy and legal issues related to preemption and deterrence.

A key decision identified by participants involved the development of metrics on when lead authority should change from a homeland security-led criminal response to a national defense response. This change in authorities requires clear understanding of the type of cyber aggression. War game participants

(Continued on Page 9)

[2] *Cyber attacks against banks more severe than realized*, Reuters, May 16, 2013, http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518.

(Continued from Page 8)

again considered the policy and legal changes needed to counter the aggression, identified second and third order effects of likely response decisions, and identified appropriate response thresholds as the situation developed.

The war game then escalated to full hostile engagement against U.S. financial networks by an aggressor nation that included attacks to deny service, malware insertion, exploitation of zero day vulnerabilities, and other types of Advanced Persistent Threat (APT). This drove discussions focused on restoration, retaliation, and escalation avoidance. The escalation to cyber warfare caused war game participants to consider international legal considerations (*jus in bello* and *jus ad bellum*) and develop appropriate response options.

At the conclusion of the two-day event, participants met for an in-depth review and "hotwash" of the exercise. A brief summary of recommendations, themes, and observations follows.

• There is Need for a Common Lexicon: Words matter. A recurring theme throughout the war game and across the groups was the need to develop a catalog of words and definitions related to cyber. Cyber terminology and definitions must be standardized throughout government and private organizations to enable a more coordinated response.

• Cyber Effects Can "Go Global": Participants readily acknowledged that even if not specifically targeted, the effects of a cyber attack against the Financial Services Sector could quickly spread to other sectors, leading to a national and global crisis. A new national policy to structure response to such a national crisis may be needed. Under current policies and processes, response to large-scale, large-region disasters may be unsustainable because they rely on partnerships which shuttle resources from unaffected areas to those areas under crisis. Yet cyber effects, unlike natural disasters, do not remain localized to a specific area of attack.

• Stakeholder Equities are Barriers to Cooperation: Private sector equities may directly conflict with government objectives, particularly since government controls can interfere with a response that is timely and robust enough to maintain the private sector entity's viability. This perception of an unresponsive national cyber defense structure frequently results in a lack of trust and often impedes information sharing. This necessitates a policy to address incentives, legal exemptions, regulatory concerns, and timeliness of response. Private sector involvement could be encouraged by reducing confusion as well as the fears related to liability and cost. Other possible private sector incentives include positive reinforcement options such as: cyber ratings indicating the cyber efficacy of a company, tax breaks for cybersecurity, indemnity from prosecution, and financial liability protection. Some participants suggested legislation mandating that companies report cyber intrusions.

(Continued on Page 10)

*Image courtesy of Naypong/FreeDigitalPhotos.net.

(Continued from Page 9)

• U.S. Policy Objectives: Group discussions reflected the immaturity and lack of policy assertiveness without consensus. Some felt it lacked enforcement (no legislative backing) and robustness, while others felt that it provided a substantial principle of government action. Participants acknowledged that timely and actionable information sharing represents a fundamental problem, and it is not clear if the mandates of PPD-21 (Critical Infrastructure Security and Resilience) will correct this issue. Nor was it concluded that this policy adequately addresses the need to strengthen resilience and address national risk mitigation. Participants repeatedly addressed the global aspects of an attack on the Financial Services Sector and the need for a "whole of community" response that includes international partners.

• Interagency Roles and Responsibilities: PPD-21 and the National Cyber Incident Response Plan (NCIRP) establish public sector roles and responsibilities to respond to the challenges of an attack in the cyber domain. DOJ, DHS, and DOD have well-defined roles and responsibilities to execute a joint and supporting response to hostile cyber activities directed against the Financial Services Sector. Each agency retains its roles and responsibilities designated under existing policies. Accordingly, agencies will task, organize, and assume appropriate "Lead For" roles, with other agencies in support.

• Attack Attribution and Intent: Establishing attribution and intent for a cyber attack is critical both to DOJ prosecution and DOD response. Determining the perpetrator of the cyber attack drives appropriate interagency response as well as the supported and supporting relationships. On the other hand, the private sector simply wants to "stop the bleeding" as quickly as possible, get back to business, and prevent further disruptions.

• Policy and Process Needs: Clearly stated and enforceable policy, doctrine, and processes are needed to assist in the timely analysis, categorization, and evaluation of any cyber threat. These must include clear guidelines for the transition of a cyber event from criminal (DOJ) to national/homeland security (DHS) to national defense (DOD). Policy should encompass all critical infrastructure sectors and consider private stakeholders. Policy should establish centralized command and control, and a well-defined reporting system for both governmental agencies and the private sector.

• Criminal Intent: Participants treated initial cyber actions against the Financial Services Sector as a crime with DOJ in the lead and agreed that many of the actions should continue to be treated as a crime throughout the entire scenario. As subsequent actions increased the threat to the United States, the lead transitioned to DHS and remained there for actions in the homeland. DOD maintained situational awareness and planned response options for action outside the homeland. One group made the point that there exists no means to prosecute cyber criminals outside the United States and this dilemma might warrant a DOD response option in lieu of prosecution.

With the cyber interconnectivity of our modern society, a significant attack against a critical infrastructure sector will likely cascade throughout other sectors, threatening the health of the U.S. economy and the lives of American citizens. This exercise brought to light many of the challenges that must be faced following a cyber attack against the Financial Services Sector. While much was gained from the interaction of the diverse group in attendance, more needs to be done to assure our country survives the potentially devastating effects of a cyber attack against American society. ❖

"Hacking Back": Legitimate Corporate Security or Risky Business?[1]

by Sean L. Harrington*

Trying to change its program
Trying to change the mode, crack the code
Images conflicting into data overload[2]

Introduction

"Banks Remain the Top Target for Hackers, Report Says." That is the title of an April, 2013 *American Banker* article,[3] and as information security risk assessor for a major bank and a legal scholar, I do my best to stay informed about cyber security developments. Although no new comprehensive legislation has been enacted since 2002, staying informed has been challenging, because the statutory language of the Computer Fraud and Abuse Act (CFAA) and Electronic Communications Privacy Act (ECPA) and its legislative history makes no reference to the Internet,[4] and courts have filled in the gaps with sometimes surprising results. State law, federal legislative proposals, and case law all are in a continuing state of flux, and practitioners must follow these developments carefully, forecast, and adapt.

One of the latest techno-phrases *du jour* is "Hack back."[5] The concept isn't new, and the term has been "common" parlance as far

(Continued on Page 12)

[1] This is an abbreviated form of an article the author will seek to have published in the near future.
[2] Rush, *The Body Electric*, on Grace Under Pressure (Mercury 1984).
[3] Sean Sposito, *Banks Remain the Top Target for Hackers, Report Says*. Am. Banker, April 23, 2013, http://www.americanbanker.com/issues/178_78/banks-remain-the-top-target-for-hackers-report-says-1058543-1.html (last retrieved Oct. 12, 2013).
[4] Yonatan Lupu, *The Wiretap Act and Web Monitoring: A Breakthrough for Privacy Rights?*, 9 Va. J. L. & Tech. 3 (2004); *see also The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age.* Hearing of the Senate Committee on the Judiciary, September 22, 2010 ("[b]ringing this privacy law into the Digital Age will be one of Congress's greatest challenges... the ECPA is a law that is often hampered by conflicting privacy standards that create uncertainty and confusion for law enforcement, the business community and American consumers.") (Statement of Senator Patrick Leahy (D-Vt.), Chairman, Senate Committee on the Judiciary); Bosset, Frankel, Friedman & Satterfield, *Private Actions Challenging Online Data Collection Practices are Increasing: Assessing The Legal Landscape*, Intellectual Property & Technology L.J. (2011) ("[F]ederal statutes such as the Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA) . . . were drafted long before today's online environment could be envisioned"); *see also* Helft & Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. Times (January 09, 2011); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, Geo. Wash L. Rev. 72 (2004): 1208.
[5] *See, e.g.,* Ken Dilanian, "A New Brand of Cyber Security: Hacking the Hackers" L.A. Times, Dec. 04, 2012.

(Continued from Page 11)

back as 2003.[6] Also termed "active defense," back hacking has been variously defined as the "process of identifying attacks on a system and, if possible, identifying the origin of the attacks. Back hacking can be thought of as a kind of reverse engineering of hacking efforts, where security consultants and other professionals try to anticipate attacks and work on adequate responses."[7] A more accurate and concise definition might be "turning the tables on a cyberhacking assailant: thwarting or stopping the crime, or perhaps even trying to steal back what was taken."[8] The most common active defense techniques include beaconing, sinkholing, and honeypot traps. Beaconing is used as a way to enhance electronic files to "allow for awareness of whether protected information has left an authorized network and can potentially identify the location of files in the event that they are stolen."[9] Sinkholing is the impersonation of a botnet command-and-control server in order to intercept and receive malicious traffic from its clients,[10] and a honeypot is "a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers."[11] These and other "hack back" techniques incur the risks of criminal liability, civil liability, regulatory liability, professional discipline, compromise of corporate ethics, injury to brand image, and escalation.

Retaliatory Hacking

A common belief for why corporations have little to fear in the way of prosecution for retaliatory hacking is, "Criminals don't call the cops."[12] Nevertheless, there is little debate that affirmative hacking back is unlawful.[13]

Obtaining evidence by use of a keylogger, spyware, or persistent cookies may violate state or federal law (e.g., the ECPA).[14] And under the CFAA, offenses include knowingly accessing without authorization a protected computer (for delineated purposes) or intentionally accessing a computer without authorization (for separately delineated purposes). Relevant statutory phrases, such as "without authorization" and "access," have been the continuing subject of appellate review.[15] One federal court, referring to both the ECPA and CFAA, pointed out that "the histories of these statutes reveal specific Congressional goals—*punishing destructive hacking*, preventing wiretapping for criminal or tortious purposes, securing the operations of electronic communication service providers— that are carefully embodied in these criminal statutes and their corresponding civil rights of action."[16] And at least one court has held that the use of persistent tracking cookies is a violation of the

(Continued on Page 13)

---

[6] Scott Carle, *Crossing the Line: Ethics for the Security Professional*, Sans Inst. (2003).
[7] Techopedia.com, http://www.techopedia.com/definition/23172/back-hack (last retrieved Oct. 09, 2013).
[8] Melissa Riofrio, *Hacking back: Digital revenge is sweet, but risky*, PCWorld, May 9, 2013, http://www.pcworld.com/article/2038226/hacking-back-digital-revenge-is-sweet-but-risky.html (last retrieved Oct. 09, 2013).
[9] IP Commission Report at 81, http://ipcommission.org/report/IP_Commission_Report_052213.pdf (last retrieved Oct. 09, 2013).
[10] David Sancho & Rainer Link, *Sinkholing Botnets*, Trend Micro, Feb. 2011.
[11] http://en.wikipedia.org/wiki/Honeypot_(computing) (last retrieved Oct. 10, 2013).
[12] Joel Reidenberg, *Companies Battle Cyberattacks Using 'Hack Back',* CNBC, June 04, 2013 ("[L]aw enforcement is unlikely to detect or prosecute a hack back. . . . If the only organization that gets harmed is a number of criminals' computers, I don't think it would be of great interest to law enforcement.").
[13] *Id.* ("'Reverse hacking is a felony in the United States, just as the initial hacking was. It's sort of like, if someone steals your phone, it doesn't mean you're allowed to break into their house and take it back,' Fordham University law professor Joel Reidenberg told CNBC.").
[14] Sean L. Harrington, *Why Divorce Lawyers Should Get Up to Speed on CyberCrime Law*, Minn. St. B. Ass'n Computer & Tech. L. Sec, Mar. 24, 2010, 9:40 PM, http://mntech.typepad.com/msba/2010/03/why-divorce-lawyers-should-get-up-to-speed-on-cybercrime-law.html (last retrieved Oct. 15, 2013) (collecting cases regarding unauthorized computer access).
[15] *See, e.g.*, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1624–42 (2003) (showing how and why courts have construed unauthorized access statutes in an overly broad manner that threatens to criminalize a surprising range of innocuous conduct involving computers).
[16] *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001)[emphasis added].

(Continued from Page 12)

ECPA.[17]

Another much-more-frequently discussed liability is that of misattribution and collateral damage. Rep. Mike Rogers (R-MI), sponsor for the Cyberintellence Sharing and Protection Act (CISPA) and Chair of the House Permanent Select Committee on Intelligence, has warned private corporations against going on the offensive as part of their cyber security programs: "You don't want to attack the wrong place or disrupt the wrong place for somebody who didn't perpetrate a crime," said Rogers, speaking at an event at The George Washington University last year. Contemplate the civil liabilities that could be incurred if, in an effort to take down a botnet through self-help and vigilantism, the damaged computers belonged to customers, competitors', or competitors' customers. Aside from the financial losses and injury to brand reputation and goodwill, implicated financial institutions could expect increased regulatory scrutiny and could compromise Government contracts subject to FISMA.

Yet another frequently discussed liability is that of escalation: cybercrime is perpetrated by many different profiles of persons and entities, including cyber-terrorists, cyber-spies, cyber-thieves, cyber-warriors, and cyber-hactivists.[18] Because the purported motivation of a cyber-hactivist is *principle*, a retaliation by the corporate victim may be received as an invitation to return fire and escalate. Similarly, "Encouraging corporations to compete with the Russian mafia or Chinese military hackers to see who can go further in violating the law . . . is not a contest American companies can win."[19] Conversely, the motivation of a cyber-thief is *principal and interest*, so retaliation by the target might be taken as a suggestion to move on to an easier target. Because the perpetrators are usually anonymous, the corporate victim has no way to make a risk-based and proportional response premised upon the classification of the attacker as nation-state, thief, or hactivist.

If, without conclusive attribution and intelligence, the corporate victim is unable to make a risk-based and proportional response, is it fair to conclude that hacking back is to abandon the risk-based approach to business problems required by FFIEC,[20] PCI,[21] and the forthcoming Cybersecurity Framework?[22] "If we start using those sort of [cyber weapons], it doesn't take much to turn them against us, and we are tremendously vulnerable," said Howard Schmidt, former White House cyber security coordinator.[23]

(Continued on Page 14)

---

[17] *In re Pharmatrak, Inc. Privacy Litigation*, 13 ILR 436, 329 F.3d 9 (1st Cir. 2003) (use of tracking cookies to intercept electronic communications was within the meaning of the ECPA, because the acquisition occurred simultaneously with the communication).

[18] For definitions and discussion of these terms, *see* Fischer, Liu, Rollins, & Theohary, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, Cong. Res. Serv.(March 1, 2013).

[19] Max Fisher, *Should the U.S. allow companies to 'hack back' against foreign cyber spies?* Wash. Post, May 23, 2013 (quoting James Andrew Lewis, *Private Retaliation in Cyberspace*, Center for Strategic & Int'l Studies (May 22, 2013). http://csis.org/publication/private-retaliation-cyberspace (last retrieved Oct. 20, 2013) (quotations omitted).

[20] Fahmida Y. Rashid, *Layered Security Essential Tactic of Latest FFIEC Banking Guidelines*, EWeek. June 30, 2011 ("Banks must adopt a layered approach to security in order to combat highly sophisticated cyber-attacks, the Federal Financial Institutions Examination Council said in a supplement released June 28. The new rules update the 2005 *Authentication in an Internet Banking Environment* guidance to reflect new security measures banks need to fend off increasingly sophisticated attacks. . . The guidance . . . emphasized a risk-based approach in which controls are strengthened as risks increase.") http://www.eweek.com/c/a/IT-Infrastructure/Layered-Security-Essential-Tactic-of-Latest-FFIEC-Banking-Guidelines-557743/(last retrieved Oct. 12, 2013).

[21] *See, PCI 2.0 encourages risk-based process: Three things you need to know*, The Technology Side of Grc (Aug. 23, 2010) http://itgrcblog.com/2010/08/23/pci-2-0-encourages-risk-based-process-three-things-you-need-to-know/ (last retrieved Oct. 12, 2013).

[22] Lee Vorthman, *IT Security: NIST's Cybersecurity Framework,* NetApp, July 16, 2013 ("It is widely anticipated that the Cybersecurity Framework will improve upon the current shortcomings of FISMA by adopting several controls for continuous monitoring and by allowing agencies to move away from compliance-based assessments towards a real-time risk-based approach"). https://communities.netapp.com/community/netapp-blogs/government-gurus/blog/2013/07/16/it-security-nists-cybersecurity-framework (last retrieved Oct. 12, 2013).

[23] John Reed, *Mike Rogers: Cool it with Offensive Cyber ops*, Foreign Policy, Dec. 14, 2012.

(Continued from Page 13)

Then there is the often overlooked issue of professional ethics for the information security professional, as many are certified by the International Information Systems Security Certification Consortium® (ISC)². The (ISC)² Committee has recognized its responsibility to provide guidance for "resolving good versus good, and bad versus bad, dilemmas," and "to encourage right behavior." The Committee also has the responsibility to discourage certain behaviors, such as raising unnecessary alarm, fear, uncertainty, or doubt; giving unwarranted comfort or reassurance; consenting to bad practice; attaching weak systems to the public network; professional association with non-professionals; professional recognition of or association with amateurs; or associating or appearing to associate with criminals or criminal behavior. Therefore, an information security professional bound by this code who undertakes active defense activities that he or she knows or should know are unlawful, or proceeds where the legality of such behavior is not clear, may be in violation of the Code.

It would stand to reason that, an organization that empowers, directs, or acquiesces to conduct by its employees that violates the (ISC)² Code of Ethics may violate its own corporate ethics or otherwise compromise its ethical standing in the corporate community—or not. When Google launched a "secret counter-offensive" and "managed to gain access to a computer in Taiwan that it suspected of being the source of the attacks,"[24] tech sources praised Google's bold action.[25] Regardless, corporate ethics is an indispensable consideration in the hack back debate.

Alternatives to Back Hacking

The obvious argument in support of active defense is that the law and governments are doing little to protect private corporations and persons from cyber crime, which has inexorably resulted in resort to self help,[26] and those who vociferously counsel to refrain from active defense often have little advice on alternatives. At the risk of pointing out the obvious, one counsels, "When you look at active defense, we need to focus on reducing our vulnerabilities."[27]

Alternatives to hacking back are evolving, and one of the more promising is the pioneering threat intelligence gathering and sharing from the Financial Services Information Sharing and Analysis Center (FS-ISAC), which collects information about threats and vulnerabilities from its 4,400 industry members, government partners, and special relationships with Microsoft, iSIGHT partners, Secunia, et al., then anonymizes the data and distributes it back to members. In addition to e-mail alerts and a Web portal, FS-ISAC holds regular tele-conferences during which vulnerability and threat information is discussed, and during which presentations on current topics are given. The FS-ISAC recently launched a security automation project to eliminate manual processes to collect and distribute cyber threat information, according to Bill Nelson, the Center's director. The objective of the project is to "significantly reduce operating costs and lower fraud losses for financial institutions," by consuming threat information on a real-time basis, explained Nelson.

The FS-ISAC cooperative model—even before its current ambitious automation project— has some demonstrable benefits. An illustrative example is the Citadel malware botnet takedown, where Microsoft's Digital Crimes Unit, in collaboration with the FS-ISAC, the Federal Bureau of Investigation, the American Bankers Association, NACHA—The Electronic Payments Association, and others, executed a simultaneous operation to disrupt more than 1,400 Citadel botnets reportedly responsible for over half a billion dollars in

(Continued on Page 15)

[24] David E. Sanger, *After Google's Stand on China, U.S. Treads Lightly*, N.Y. Times, Jan. 14, 2010, http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?_r=0.

[25] Skipper Eye, *Google Gives Chinese Hackers a Tit for Tat*, Redmond Pie, Jan. 16, 2010, http://www.redmondpie.com/google-gives-chinese-hackers-a-tit-for-tat-9140352/.

[26] James Andrew Lewis, *Private Retaliation in Cyberspace*, Center for Strategic & Int'l Studies (2013), http://csis.org/publication/private-retaliation-cyberspace (last retrieved Oct. 20, 2013)("Another argument is that governments are not taking action, and therefore private actors must step in.").

[27] John Reed, *The cyber security recommendations of Blair and Huntsman's report on Chinese IP theft*, Foreign Policy, May 22, 2012 (quoting Howard Schmidt).

(Continued from Page 14)

losses worldwide.[28] With the assistance of U.S. Marshals, data and evidence, including servers, was seized from data hosting facilities in New Jersey and Pennsylvania, and was made possible by a court ordered civil seizure warrant from a U.S. federal court. Microsoft also reported that it shared information about the botnets operations with international CERTs to tackle the botnets outside U.S. jurisdiction, and the FBI informed enforcement agencies in those countries. Likewise, *American Banker* just published an article discussing how "Bankers have never been too keen on sharing secrets with one another," but that dire circumstances have catalyzed a new era of cooperation.[29] And vendors, such as Guardian Analytics, have come to market with information sharing tools.[30]

Another promising option is the partnership that financial institutions have formed (or should investigate forming) with ISPs for passive defense. For example, ISPs currently provide DDOS mitigation services that, although not particularly effective in application vulnerability (OSI model layer 7) attacks, are very capable in responding to volume-based attacks. ISPs are, of course, subject to regulatory oversight, and the laws and regulations that limit what actions an ISP can take would be the subject of another lengthy article. Nevertheless, several researchers urge that ISPs should assume a "larger security role," and are in a good position "to cost-effectively prevent certain types of malicious cyber behavior, such as the operation of botnets on home users' and small businesses' computers."[31] One 2010 study found that just 10 ISPs accounted for 30 percent of IP addresses sending out spam worldwide.[32] In 2011, the same researchers reported that over 80 percent of infected machines were located within networks of ISPs, and that fifty ISPs control about 50 percent of all botnet infected machines worldwide.

Conclusion

Hack back or active defense, depending on how you define each—and everything in between—consists of activities that are both lawful and unlawful, and which carry all the business and professional risks associated with deceptive practices, misattribution, and escalation. To urge a risk-based approach to using even lawful active defense tactics would be to state the obvious, and the use of certain types of active defense where misattribution is possible, may be to entirely abandon the risk-based approach to problem solving. Moreover, at the time of this writing, a qualified privilege to hack back through legislative reform seems unlikely, and would be difficult because the holder of such a privilege would not only have to establish proper intent, but also attribution. However, the tools, technologies, partnerships, and information sharing between corporations, governments, vendors, and trade associations are promising; they have already proven effective, and are steadily improving.

** Sean Harrington is a cyber security policy analyst and information security risk assessor in the banking industry, as well as a digital forensics examiner in private practice. He is a graduate with honors from Taft Law School, and holds the MCSE, CISSP, CHFI, and CSOXP certifications. He has served on the board of the Minnesota Chapter of the High Technology Crime Investigation Association, is a current member of InfraGard, the Financial Services Roundtable's legislative and regulatory working groups, FS-ISAC, and is a council member of the Minnesota State Bar Association's Computer & Technology Law Section. Harrington teaches computer forensics for Century College in Minnesota, and recently contributed a chapter on the Code of Ethics for the forthcoming Official (ISC)²® Guide to the Cyber Forensics Certified Professional CBK®, and will be an instructor for the new CCFP certification.* ❖

[28] Tracy Kitten, Microsoft, *FBI Take Down Citadel Botnets*, Bankinfosecurity, June 6, 2013, http://www.bankinfosecurity.com/microsoft-fbi-takedown-citadel-botnets-a-5819/op-1. (quoting Howard Schmidt)

[29] Sean Sposito, *In Cyber Security Fight, Collaboration Is Key: Guardian Analytics*, Am. Banker, Oct. 8, 2013, http://www.americanbanker.com/issues/178_195/in-cyber-security-fight-collaboration-is-key-guardian-analytics-1062688-1.html.

[30] *Id.*

[31] Rowe, Wood, Reeves, & Braun, *The Role of Internet Service Providers in Cyber Security*. Inst. for Homeland Sec. Solutions (June, 2011).

[32] Van Eeten, M., Bauer, J., Asghari, H., Tabatabaie, S., Rand, D. (2010). *The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data.*

The Challenges of Terrorist Financing in 2013 and Beyond

by Dennis M. Lormel

Introduction

On October 3, 2001 in testimony before the House Financial Services Committee I stated: "***Funding is the lifeblood of terrorist organizations.***" Many factors regarding terrorism have changed significantly since 2001. One constant remains: ***Funding is the lifeblood of terrorist organizations***. Terrorists require financial support in order to succeed. They must have effective financial infrastructures and support mechanisms to ensure they have a steady flow of funds.

An unfortunate reality is that there will be more successful terrorist attacks in the United States. The increasing threat posed by homegrown or lone wolf militants and the simple nature of constructing an explosive device, as evidenced by the Boston bombing, makes detecting and preventing such attacks extremely challenging. The best chance to prevent terrorists from succeeding is to disrupt their ability to raise, move, and access money.

Terrorist financing is extremely difficult to identify. The ability to disrupt it begins with a strong foundation that includes three elements:

- Coordination
- Innovation
- Training

There must be coordination between U.S. government agencies; the public and private sectors; and the U.S. government and nations throughout the world. The greater the level of cooperation and communication, the more effective the level of coordination will be.

There are significant changes taking place regarding terrorism. The public and private sectors must develop new and innovative mechanisms to identify and disrupt terrorist financing, including targeted and proactive transaction monitoring and investigative techniques.

Training to promote a sense of awareness and understanding of who terrorists are; how they operate; and how they raise, access, move, and spend money is essential. To better understand terrorist financing, four factors must be considered: the terrorist groups themselves; their funding capacity; the financial mechanisms they use; and the individuals, entities, and cells that comprise the terrorist groups. They each have their own financial requirements, which leave a traceable trail.

Partnerships and perspectives are important in accessing and assessing financial information. Government and industry have different perspectives, but they share the same end game: deny terrorists the ability to move and access funds unencumbered. As criminals, terrorists and our financial system continue to become more sophisticated, financial transactional information becomes more relevant as a critically important investigative mechanism. All investigators can benefit from knowing what financial information is relevant, where to collect it, and how to use it.

Current and Emerging Financial Trends

In assessing current and emerging financial trends, it is important to understand the local, regional, and global nature of funding catalysts. World events lead to change. Change leads to opportunity. Opportunity drives corridors used to facilitate activities and funding flows. The availability of money based on the flow of funds influences the level of threat generated.

Facilitation tools used by terrorist and criminal organizations include:

- Corresponding banking
- Wire transfers
- Remote deposit capture
- Depository accounts
- Debit/credit/prepaid cards
- Use of nominees
- Use of false identification
- Shell companies
- Money services businesses
- Illegal money remitters

(Continued on Page 17)

(Continued from 16)

- Electronic mechanisms
- Bulk cash shipment
- Trade-based finance

A common thread between the above facilitation tools exploited by malicious actors is anonymity. When terrorists and criminals can conceal beneficial ownership, they can operate more freely and use facilitation tools more openly and effectively.

As financial institutions and regional governance in traditional financial systems becomes more rigorous, terrorists and criminals rely more on the alternative mechanisms of bulk cash smuggling and trade-based money laundering. Bulk cash smuggling is a method that keeps illicit proceeds and related activity away from the scrutiny of financial regulators and law enforcement. Trade-based money laundering relies on international trade to move money around the world and is more prevalent in cases where terrorist and criminal organizations act collaboratively in global schemes to launder the proceeds of illicit activity, such as drug trafficking.

Understanding Funding Flows

Due to the diverse nature of terrorist financing, there is a wide range of terrorist financing cases, including fundraising and financing for operations. Fundraising generally involves larger funding streams, while operations involve more minimal amounts of funding.

The funding cycle begins with money-raising, progresses to money movement and/or storage, and ultimately to spending. Disrupting funding flows to terrorists requires understanding in four dimensions:

1. **The terrorist organization:** Who are they? How large are they? Where do they operate? What type of infrastructure do they have? How do they raise money? What are their funding requirements?

2. **Funding capacity:** What are their sources of funds? How do they launder money? What is the availability of funds?

3. **Funding mechanisms:** Do they deal in the formal financial system, the informal system, or a combination of the two?

4. **Group members:** What are their individual financial requirements?

Working with this understanding, it is best to go back to the point of origin and forward to terrorist strike teams. In that context, there are three funding tracks. The first is funding to a network or organization. This funding stream ranges from hundreds of dollars to millions of dollars. The next track is funding to operations. This funding stream ranges from thousands to hundreds of thousands of dollars. The last track is funding to individuals, cells or groups. This funding stream ranges from hundreds to thousands of dollars.

Thinking Forward Beyond 2013

In looking beyond 2013, we need to develop mechanisms to identify and address the convergence and diversification of terrorist and criminal groups.

As these groups continue to collaborate and benefit from each other, transaction monitoring and investigative techniques must be calibrated to identify the point of the nexus. In addition, as terrorist and criminal organizations mature, they diversify. This requires more vigilance in the process of identifying the totality of organizational operations.

As we look forward, we must assess emerging threats, financial requirements associated with those threats, and the transformation of the terrorist landscape. As chaos continues in the Arab world, a number of questions will need to be answered, to include:

- How will the ongoing and future unrest and conflict affect terrorist and criminal groups?

- How will E.U. sanctions affect Hezbollah's operations?

- Will the core al-Qaeda group experience a significant resurgence?

- Will al-Qaeda-related groups such as al-Qaeda in the Arabian Peninsula and al-Qaeda in Iraq pose a threat to the United States?

- How can the United States diminish the growing homegrown terrorist threat?

New strategies to deal with the emergence of convergence and diversification, as well as the changing dynamics of terrorism require specialized

(Continued on Page 18)

(Continued from Page 17)

training. This training should focus on the transformation of terrorist groups, their affiliation with transnational criminal groups, their funding sources, and how they use money to support their operations. The training should contain specific case typologies and examples where the convergence, diversification, and transformation are dissected and analyzed. A good example of such a case study is the Lebanese Canadian Bank case, where the Joumma criminal organization, Los Zetas drug cartel, and Hezbollah aligned in a global drug trafficking and money laundering operation.

Countermeasures

Countermeasures in terms of terrorist financing begin with public-private partnerships. Law enforcement and the Financial Services Sector each possess financial intelligence information the other can significantly benefit from. Meaningful and sustainable information sharing requires three elements:

1. **Understanding perspectives:** Law enforcement and financial institutions have different perspectives. Traditionally, law enforcement focuses on criminal prosecutions, whereas financial institutions focus on regulatory concerns. When it comes to terrorist financing, both want to detect, disrupt, and prevent terrorism.

2. **Partnerships:** Partnerships form the gateway to meaningful and sustainable information sharing.

3. **Innovation:** Developing proactive methodologies, such as targeted monitoring for patterns of activity recognizable with the identified crime problem. This requires information sharing among partners.

Financial institutions are the repositories for significant financial intelligence information, while law enforcement is the beneficiary of financial intelligence. The ability of financial institutions and law enforcement to collaborate and identify actionable financial intelligence information in a timely manner is a powerful tool.

Law enforcement conducts financially focused investigations to disrupt and/or prevent the flow of funds to terrorists. These investigations are conducted to support the broader U.S. government counterterrorism mission. In terrorist financing investigations, law enforcement is the collector and producer of actionable financial intelligence and the direct beneficiary of Bank Secrecy Act (BSA) data. When it comes to suspicious activity reports (SARs), the perspective of law enforcement is focused on the "why." Why did the financial institution consider activity suspicious?

Financial institutions are required by the BSA to maintain robust anti-money laundering programs to safeguard the system from money laundering and terrorist financing. They originate BSA reports. Regarding SARs, the perspective of financial institutions is focused on the "how." How did terrorists and/or criminals use the financial institution to facilitate their nefarious activity?

Law enforcement must understand the importance of the "how" and provide financial institutions with feedback regarding how the institution was used. Conversely, financial institutions must emphasize the "why" to law enforcement when filing SARs and through follow-up contacts. Dealing with the how and why sets the stage for financial institutions and law enforcement to develop innovative ideas and proactive countermeasures. This requires coordination, cooperation, and communication.

Using financial intelligence to develop actionable information for monitoring and/or investigating terrorist financing in a timely manner is essential. The better the financial intelligence and understanding of terrorist money flows, the better the prospect for developing targeted monitoring and/or investigative initiatives.

Financial intelligence can be used effectively in three investigative methodologies:

- *Strategic investigations:* Analysis used to identify emerging trends.

- *Tactical investigations:* Proactive targeted operations intended to disrupt funding flows.

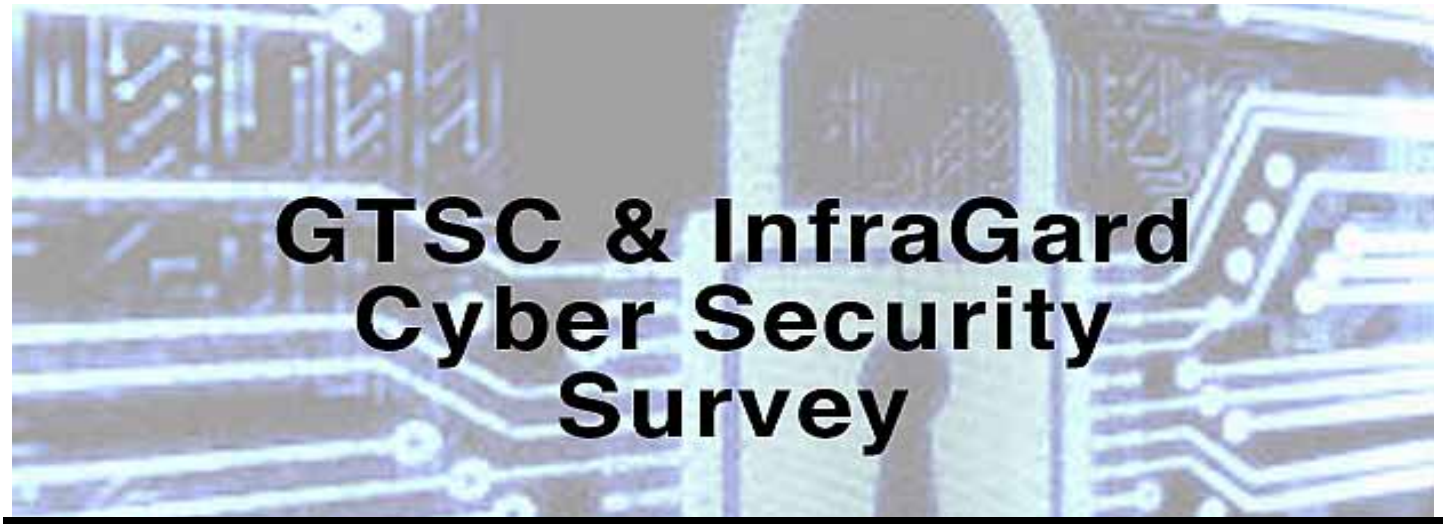
- *Historic investigations:* Reactive traditional investigations conducted to follow the money.

(Continued on Page 19)

(Continued from Page 18)

Conclusion

Funding remains the lifeblood of terrorist organizations. Yet, it is one of their most significant vulnerabilities. The better we understand the flow of funds, the higher the quality of actionable financial intelligence we exchange, and the more innovative we become, the more likely we will be positioned to prevent and/or disrupt the financing required to support terrorist activities. ❖



Recognizing National Cyber Security Awareness Month, InfraGard, in partnership with the Government Technology & Services Coalition (GTSC) and the FBI-Washington Field Office, has launched the following survey to increase collaboration between the public and private sectors to mitigate and lessen the impact of cyber indents, hacking, viruses, and other kinds of malicious attacks. We are working jointly to find what kinds of tools and resources can be most valuable to help industry be more prepared.

This survey will take approximately 30 minutes of your time and collects data to help us enhance and/or initiate efforts to strengthen our awareness, encourage mutually beneficial information sharing, and create meaningful programming and tools to combat cyber threats. Please feel free to forward the survey to colleagues who may also be in a position to respond.

Survey link options:
GTSC website: http://www.gtscoalition.com/cyber-survey/
Survey Monkey: https://www.surveymonkey.com/s/gtscinfragardcybersurvey

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1