2009

Funding Bin Laden's Avatar: A Proposal for the Regulation of Virtual Hawalas

Stephen I. Landman

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr
Part of the Military, War, and Peace Commons, and the National Security Law Commons

Recommended Citation
Available at: http://open.mitchellhamline.edu/wmlr/vol35/iss5/15
FUNDING BIN LADEN’S AVATAR: 
A PROPOSAL FOR THE REGULATION OF VIRTUAL 
HAWALAS

Stephen I. Landman†

I. INTRODUCTION

"[T]he Metaverse is wide open and undefended, like airports in the
days before bombs and metal detectors, like elementary schools in the
days before maniacs with assault rifles. Anyone can go in and do anything they
want to. There are no cops. You can’t defend yourself, you can’t chase the
bad people.”

† J.D. Candidate, the Catholic University of America, Columbus School of
1. NEAL STEPHENSON, SNOW CRASH 328 (1992). Fiction author Stephenson is
credited with coining the phrase “metaverse,” a virtual world where individuals can
interact with each other through an online version of the real world. This article
For nearly a decade, the United States has conducted operations aimed at destroying suspected terrorist training camps from the deserts of Sudan to the mountains of Afghanistan and many places in between. Yet, one need only open a newspaper to see that groups such as al Qaeda, Hezbollah, Hamas, and their ilk still retain the ability to effectively plan, finance, and carry out attacks. This is due, in part, to an unintended consequence of the war on terrorism: the ability of terrorist groups to almost seamlessly transition from the battlefields of the Middle East and northern Africa to the virtual worlds of the Internet.

Although groups like al Qaeda consistently demonstrate an aptitude for adapting to changing technologies, the accessibility of the Internet has expanded every facet of their operations, from the spread of propaganda to the planning, financing, and preparation of terrorist attacks. As traditional modes of operation are identified, terrorism has evolved by exploiting many of the attributes for which the Internet has become so popular. The Internet's ease of access, fast flow of information, anonymity of communications, and dearth of regulation have revolutionized the command and control structure of modern terrorist organizations.

Once constrained by real-world impediments, terrorist groups now have unlimited resources at their disposal by shifting to the use

---


6. Id.
of developing technologies and exploiting a wide range of digital platforms in order to meet their organizational needs. From password-protected discussion forums to encrypted websites, the ability of terrorist groups to take advantage of technology is limited only by their creativity and the availability of the platforms. Terrorist groups have shifted from the battlefields and training camps of the Middle East to the virtual worlds of the Internet.

Virtual worlds are computer-based, simulated environments where millions of users can interact with each other on a daily basis. Once in-world, users participate in many of the same real-world activities of their daily lives. Because virtual worlds are meant to mirror the real world, many have virtual economies, allowing users to not only connect with one another, but also to conduct financial transactions. Two of the more popular, and arguably advanced, of the virtual words are Second Life (SL) and Entropia Universe (EU). Although the ability to buy, trade, and sell both tangible and intangible items in virtual worlds like SL and EU offers an entirely new marketplace for goods, these virtual economies are potentially vulnerable to exploitation by terrorist financiers.

One of the prime objectives of the war on terror is to prevent the free flow of money to international terrorist organizations. As

7. Virtual worlds go by many names, but, at their most basic level, they are "computer based, simulated, persistent environments that support synchronous interactions between users personified as avatars." Online Virtual Worlds: Applications and Avatars in a User-Generated Medium: Hearing Before the H. Subcomm. on Telecom. and the Internet, 110th Cong. 2 (Apr. 1, 2008) (statement of Dr. Colin J. Parris, Vice President, Digital Convergence, IBM Corp.).

8. See id. at 7 (discussing social networking and economic capabilities of virtual worlds).


11. President's Address Before a Joint Session of Congress on the United States Response to the Terrorist Attacks of September 11, 37 WEEKLY COMP. PRES. DOC. 1347 (Sept. 20, 2001) [hereinafter Presidential Address] ("We will direct every resource at our command, every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence . . . to the disruption and to the defeat of the global terror network.")
U.S. and international law enforcement officials continue to curb abuse of the formal financial sector—e.g., banks—terrorist financiers have shifted to underground banking.12 Broad in scope, "underground banking" refers to almost any type of informal value transfer system outside traditional banking.13 Underground banking attracts terrorist financiers with its anonymity and lack of regulation, two key attributes of the developing economies within virtual worlds. As financial transactions within virtual worlds become more accessible and widespread, law enforcement officials must recognize the potential for abuse by groups seeking to carry out acts of terrorism and respond vigorously. Accordingly, any counterterrorist financing policies must not only reduce the use of known underground banking methods, but also institute effective recordkeeping and reporting requirements to prevent the abuse of new methods of transferring funds.

This article explores the use of the Internet by international terrorist organizations generally, concentrating on virtual worlds as a means for such organizations to plan, finance, and carry out attacks. Part I discusses numerous ways in which the Internet and other technological innovations have affected terrorist groups, tracing the platforms used and the activities engaged in by these organizations, broadly defined as the "virtualization of terrorism."14 Part II examines the evolution of terrorist financing, suggesting that, as terrorists continue to adapt to new and developing technologies, law enforcement officials and policymakers must recognize the vulnerability of virtual worlds as the new front in the war on terrorist financiers.15 Part III then analyzes the existing regulatory regime for countering terrorist financing, explaining that, as additional enforcement mechanisms have reduced the


14. See infra Part I.

15. See infra Part II.
vulnerability of formal financial institutions, informal systems such as virtual worlds remain largely open to terrorist dollars. This article concludes by proposing that law enforcement officials can more effectively curb the abuse of both formal and informal financial sectors by extending the existing regulatory regime to virtual worlds.

II. THE VIRTUALIZATION OF TERRORISM

"[Y]ou didn't have to speak Arabic in the mid 90's to know that terrorism had shifted its focus and you don't have to write code to understand that has changed again." 18

Before U.S. counterterrorism law and policy can begin to combat the ongoing virtualization of terrorism effectively, government officials must first understand how terrorist groups use the Internet. When considering use of the Internet by terrorist organizations, it is useful to distinguish two categories: (1) cyber-terrorism, attacks aimed primarily at Internet targets, 19 and (2) cyber-based terrorism, attacks that are undertaken in the real world, but planned and financed in the virtual world. While the threats posed to electronic infrastructure are significant, they are not the focus of this article. 20 Instead, this article concentrates on

16. See infra Part III.
17. See infra Part IV.
the equally troublesome use of new technologies to secretly undertake what was once accomplished, or at least attempted, in the real world.

A. The Marketplace of Terrorist Ideas Goes Digital

As cyber-based terrorism continues to expand, there are a few areas in which terrorist groups have shown both desire and ability to abuse otherwise legitimate systems to further their criminal ends. A recent study found that although only half of the thirty organizations designated as "Foreign Terrorist Organizations" maintained websites in 1998, "by 2000, virtually all terrorist groups had established their presence on the Internet."23 As these statistics reflect, the Internet has significantly expanded the opportunities available for terrorists to secure publicity and spread propaganda as well as revolutionized the process of enlistment.

Prior to being captured by British investigators in the fall of 2005, a key conduit for al Qaeda online was Younis Tsouli, better known as "Irhabi 007." As one news report declared: "Irhabi 007 had propelled the jihadists into a 21st century offensive through his ability to covertly and securely disseminate manuals of weaponry, videos of insurgents feats such as beheadings and other inflammatory material."24 By exploiting the Internet's anonymity and dearth of regulation, Irhabi 007 and, others like him, have not only expanded the ability of terrorist organizations to spread propaganda and recruit new fighters, but also to undertake more substantive offenses.25

---


22. WEIMANN, supra note 5, at 2.

23. Id. at 2; see also id. at 1-4 (conducting a thorough evaluation of terrorist presence on the Internet and breaking down the results by geographic location, with the majority of groups located in the Middle East and Asia).


25. See id.
B. Virtual Terrorist Training Camps

By exploiting technology, terrorists can use the Internet to plan and coordinate specific attacks. Primarily, the Internet serves as a tool for intelligence-gathering, providing access to a broad range of material on potential targets from simple maps to aerial photographs. Israeli officials reported last year that "[m]ilitant Palestinian groups who have been launching rockets into the Western Negev from the Gaza Strip have been using Google's popular satellite imagery program 'Google Earth' to reconnoiter areas in Israel to be targeted for attack."\(^{26}\)

As technology advances, computer-savvy terrorists can create password-protected forums that operate as virtual terrorist training camps. Roderick Jones, former member of the United Kingdom's Counter-Terrorism Command, explained that the worst-case scenario is "an expert bomb maker conducting a virtual lecture with his students all present and able to ask questions and check their knowledge and virtually manipulate the necessary parts."\(^{27}\)

More disconcerting, however, is that terrorist groups can now orchestrate training programs that would have been nearly impossible in many of the training camps based in the Afghan mountains and Federally Administered Tribal Areas of Pakistan. For example, Microsoft's new program "Photosynth" allows users to take a collection of photos of a location; have them analyzed for similarities; and display them in a reconstructed three-dimensional space.\(^{28}\) The potential for abuse of a program such as this is clear—it provides terrorist groups a virtual world in which to essentially "Red Team" potential attacks against a target prior to an attack.\(^{29}\)

---

27. Meta-Terror, supra note 18 (statement of Roderick Jones).
29. The opposing force in a simulated military conflict is known as the "Red Team" and is used to reveal weaknesses in current military readiness. See Marcus Spade, Army Approves Plan to Create School for Red Teaming, July 13, 2005, http://www.tradoc.army.mil/pao/nsarchives/July05/070205.htm. These same techniques could be used by terrorist groups. See Barton Gellman, FBI Fears al Qaeda Cyber Attacks, S.F. CHRON., June 28, 2002, at A1 (captured computer contained engineering and structural architectural features of a dam, enabling al Qaeda engineers and planners to simulate catastrophic failures).
C. Web-Based Terrorist Financing

The logistical implications of the virtualization of terrorism are not limited to propaganda, recruitment, and e-learning. In order to ensure continued survival, terrorists "need to raise funds [and] open and use bank accounts to transfer money."\(^{30}\) For financing, terrorist organizations historically have been attracted to operating in unregulated jurisdictions—those "places with limited bank supervision, no anti-money laundering laws, ineffective law enforcement institutions, and a culture of no-questions-asked bank secrecy."\(^{31}\) The Internet, with its relative ease of use and anonymity, satisfies many of these needs.

III. BY ANY MEANS NECESSARY: THE EVOLUTION OF TERRORIST FINANCING

"There are two things a brother must always have for jihad, the self and money."\(^{32}\)

Although opinions differ on the operating costs for terrorist organizations\(^{33}\) and the cost of an "average" terrorist attack,\(^{34}\) a


\(^{32}\) MONOGRAPH, supra note 4, at 17 n.5 (quoting an al Qaeda operative).

\(^{33}\) One source for deriving these estimates is the annual report of blocked terrorist assets pursuant to economic sanctions issued by the U.S. Treasury Department's Office of Foreign Asset Control. See, e.g., U.S. DEP'T OF TREASURY, OFFICE OF FOREIGN ASSET CONTROL, TERRORIST ASSETS REPORT: CALENDAR YEAR 2005, FOURTEENTH ANNUAL REPORT TO CONGRESS ON ASSETS IN THE UNITED STATES OF TERRORIST COUNTRIES AND INTERNATIONAL TERRORISM PROGRAM DESIGNEES 8 (showing that total assets blocked from seven terrorist groups totaled $13,793,102 in 2005), available at http://www.treas.gov/offices/enforcement/ofac/reports/tar2005.pdf.

\(^{34}\) See The Financing of Terror Organizations, Counterterror Initiatives in the Terror Finance Program: Organization of Terror Groups for Funding and Future U.S. Responses: Hearings Before the S. Comm. on Banking, Housing, and Urban Affairs, 108th Cong. 69 (2003) (statement of Dr. Louise Richardson, Executive Dean, Radcliffe Institute for Advanced Study, Harvard University) (arguing that while 9/11 cost an estimated half million dollars, the average terrorist attack costs much less); U.S. DEP'T OF STATE, 2003 INT'L. NARCOTICS CONTROL STRATEGY REPORT, PART II: MONEY
greater ability to track and restrict the sources of terrorist funding
would markedly deter the ability of terrorist groups to perpetrate
attacks. Consequently, in the fight against international
terrorism, a prime objective of law enforcement and intelligence
agencies is restricting the free flow of money to terrorist
organizations.

Despite law enforcement's best efforts, terrorists continue to
adapt and develop new methods of financing their organizations,
avoiding detection while maintaining a viable financial
infrastructure. Depending on operational needs and existing
risks, al Qaeda can employ a variety of mechanisms to transfer its
wealth to areas where it is needed. As Dennis Lormel explains,
"[o]ne of the true challenges in dealing with terrorist financing is
the recognition of the dynamics of change, and understanding
that... financing methodologies will constantly change to avoid
detection."
A. Formal Financial Institutions

The international banking system provides a broad array of financial services and convenience unmatched by any other monetary system in the world and, as a result, is the first choice for most international organizations—legitimate or otherwise—to move and store funds. The September 11 attacks are merely one example in which terrorist groups exploited the weaknesses of the formal financial system. Each of the hijackers maintained personal accounts at major financial institutions, such as Bank of America and SunTrust, as well as smaller regional banks. While in the United States, their expenses, including the actual cost of the attacks, were funded by approximately $300,000 deposited using a combination of wire transfers, traveler's checks, and debit or credit cards with access to funds held in foreign financial institutions.

Despite the administrative burdens, most financial institutions have contributed tremendously to the global financial war on terrorism. Recognizing the importance of inhibiting terrorist financing and the difficulty associated with monitoring individual transactions to determine the final destination of otherwise innocuous funds, formal financial institutions have begun to implement stricter oversight systems to better detect the financial activity of terrorist organizations. The results have been reduced


40. Cf. MONOGRAPH, supra note 4, at 3 ("The September 11 hijackers used U.S. and foreign financial institutions to hold, move, and retrieve their money.").

41. Id. at 131 ("The hijackers and their financial facilitators used the anonymity provided by the huge international and domestic financial system to move and store their money through a series of unremarkable transactions."); see also Linde v. Arab Bank PLC, 384 F. Supp. 2d 571 (E.D.N.Y. 2005) (alleging material support of terrorists, victims of attacks in Israel file suit against Jordanian bank); Weiss v. Nat'l Westminster Bank PLC, 453 F. Supp. 2d 609 (E.D.N.Y. 2006) (alleging material support of terrorists, victims of attacks in Israel file suit against British bank).

42. See MONOGRAPH, supra note 4, at 140.

43. See id. at 3.

44. See, e.g., Joseph M. Myers, The Silent Struggle Against Terrorist Financing, 6 GEO. J. INT'L AFF. 33, 35 (2005) ("The financial services sector, which had previously opposed many of the PATRIOT Act provisions, was extraordinarily cooperative and patient with the United States and other countries trying to unravel the financial trail left by the 9/11 hijackers."); Leo Wolosky & Stephen Heifetz, Regulating Terrorism, 34 L. & POL'Y INT'L Bus. 1, 1 (2002) (regulations now require financial institutions to report on suspicious transactions).

45. See Adam Rombel, Banks Battle Terror Financing with Software, 16 GLOBAL FINANCE 44 (2002) (discussing the niche industry born out of new compliance
vulnerability within the formal financial sector to terrorist financing schemes.\textsuperscript{46} Despite these successes, the informal banking system remains open for business to terrorist dollars.\textsuperscript{47}

B. Informal Financial Institutions

Although existing regulatory mechanisms have been very effective, terrorist organizations and their financiers remain highly adaptive entities.\textsuperscript{48} Since they can no longer safely use the international banking system, terrorist financiers have turned to underground banking systems.\textsuperscript{49} Informal financial networks,
collectively referred to as "informal value transfer systems" (IVTS),
exist outside of the modern banking system but serve a similar
purpose—to facilitate the transfer of valued goods and money.

Although one obvious benefit of IVTS for terrorist financiers is
that it operates outside the bounds of the traditional financial
system, there are many other reasons why IVTS may be preferred to
ordinary banks. IVTS are reliable, efficient, anonymous, and
available twenty-four hours a day, seven days a week. The true
extent of terrorist use of these systems is unknown, a result of both
the criminal nature of the activity and the lack of systematic data
collection and analysis. Estimates regarding the annual flow of
transactions through informal banking systems range from $200
billion to "tens of billions." Others believe the amount cannot be
quantified with any certainty.

The most well-known IVTS is hawala. Groups like al Qaeda

50. Informal Value Transfer System is defined as a "system or network of
people facilitating, on a full-time or part-time basis, the transfer of value
domestically or internationally outside the conventional, regulated financial
institutional systems." Nikos Passas, WODC, Informal Value Transfer Systems &
Criminal Organizations; A Study Into So-Called Underground Banking

51. Cf. Amos N. Guiora & Brian J. Field, Using and Abusing the Financial
Markets: Money Laundering as the Achilles' Heel of Terrorism, 29 U. PA. J. Int'l L. 59, 62
(2007) ("[T]he use of Informal Value Transfer Systems ("IVTS") is commonly
referred to as 'underground banking' because, although operating akin to a
banking system, the IVTS does so without the formal requirements of institutional
banking.").

regulatory scrutiny, and tend to have fleeting relationships with their customers,
making customer due diligence very difficult."); U.S. Dep't of Treasury Fin.
Crimes Enforcement Network, FinCEN Advisory, Informal Value Transfer
benefits to IVTS users).

53. See FinCEN Advisory, supra note 52, at 3; see also Alan Lambert,

54. Use of Alternative Financing Mechanisms, supra note 12, at 3 ("[The
FBI] do[es] not systematically collect and analyze data on alternative financing
mechanisms.").

55. Id. at 24.

56. Id.

57. Passas, supra note 50, at 13-25 (outlining a family of traditional IVTS
systems with different names depending on geographic location and ethnic group
and identifying many varieties).
have systematically used hawala because, unlike formal financial institutions, they neither were traditionally subject to potential government oversight nor did they keep detailed records.\(^58\) Evidence shows "the hawala network has been used to funnel money to terrorist groups in the disputed Kashmir valley... [and] as a conduit for funding the 1998 bombings of U.S. embassies in Kenya and Tanzania."\(^59\) Recently, the U.S. Government, in cooperation with international law enforcement, has worked to curb the abuse of hawala, forcing terrorist financiers to find new methods for transmitting money.\(^60\)

C. Virtual Worlds: The New Front in the War on Terrorist Financing

The expansion of the Internet and the evolution of IVTS have opened up virtual worlds as potentially useful mechanisms for transferring funds to cells around the world. Virtual worlds provide many of the same characteristics as the existing IVTS network: they are fast, inexpensive, reliable, convenient, and—most notably—discreet.\(^61\) Moreover, financiers no longer need to leave the comfort of their own homes to successfully transfer large sums of money to those looking to carry out horrific attacks. The development of virtual economies, along with the dearth of regulation, makes virtual worlds the new frontier in IVTS.

The ability to conduct real-time, in-world transactions in

---

\(^58\) Monograph, supra note 4, at 25; see also USA PATRIOT Act/Terrorism Financing Operations Section: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the S. Comm. on the Judiciary, 107th Cong. (Oct. 9, 2002) (testimony of Dennis Lormel, Chief, Terrorist Financing Operations Section, Counterterrorism Division, FBI) ("Informal Value Transfer systems, such as 'Hawalas,' also present problems for law enforcement. They permit terrorists a means of transferring funds that is difficult to detect and trace. These informal systems are commonplace and appear to serve as an efficient means of transacting in mostly 'cash' societies such as Pakistan, Afghanistan, and the Philippines [sic].")

\(^59\) Lambert, supra note 53, at 12 (emphasis added).

\(^60\) See Report to Congress, supra note 13, at 6–10 (explaining that the Bank Secrecy Act's recordkeeping and reporting requirements reach the types of informal unconventional entities operating outside of the mainstream financial system like hawala); see also supra Part III.A (discussing existing counterterrorist financing regulations and their application to informal financial networks).

virtual currency that can then be exchanged for U.S. dollars or other regional currencies has made virtual worlds widely popular. Virtual worlds allow users to transfer real funds in a variety of ways, including credit cards, traditional bank accounts, pre-paid debit cards, and PayPal accounts. Despite the obvious benefits of an expanding virtual economy, officials must acknowledge that this economy is no different than the real-world economy when it comes to financial crime. Virtual worlds are especially susceptible to manipulation by terrorist financiers because they escape regulation and observation by law enforcement.

The primary concern is paltry customer identification rules associated with virtual worlds. In traditional banking, customer identification procedures are implemented both during account origination and in subsequent transactions. However, the nature of virtual worlds limits the ability to accurately identify customers at each of these stages, rendering all customers more vulnerable to financial crimes.

Currently, the virtual worlds of SL and EU have limited abilities to verify their residents' identities. SL, for instance, maintains few verification procedures for accurately confirming the personal information of individuals who buy, sell, and transfer Lindens in-world. To the extent that Linden Labs was interested

62. See Meta-Terror, supra note 18.
66. See supra Part II.B.
in identifying its customers, they would have to turn to either the e-mail address provided during registration or the Internet Protocol (IP) address associated with the account. Yet, neither of these approaches provides any actionable intelligence if the user intends to keep his identity secret. In contrast, EU maintains relatively strict customer identification procedures, and, to the extent that customer identities are accurately verified, fake accounts can be reduced.

Virtual worlds are also limited in their ability to monitor individual financial transactions. Residents can buy, sell, and exchange currency in nearly unlimited amounts without any questions asked. Presently, there is nothing to indicate that either EU or SL maintains records of individual financial transactions between residents. Moreover, once a resident seeks to move funds from the virtual world and back into the real world, there are limits on the ability to properly identify the recipient of those funds.

Although vulnerabilities exist, without a documented instance

https://support.secondlife.com/ics/support/default.asp?deptID=4417 (last visited Apr. 3, 2009) (follow “Linden Dollars” hyperlink; then follow “General LS Information” hyperlink; then follow “How can I use my US dollar balance?”) (to make withdrawals, users must “have accurate and complete registration information, including verifiable billing information”). There does not appear to be any verification of individual customer identity.


69. Methods used to conceal identity range from using fake e-mail and PayPal accounts to masking an IP address by moving from server to server. See, e.g., Benjamin R. Davis, Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance, 15 COMM.LAW CONSPECTUS 119, 129 (2006) (“Like any Internet user, a terrorist operative will find setting up a Website or e-mail account to be a very simple and inexpensive process. With minimal disclosure requirements (which are difficult, if not impossible, for providers to verify for accuracy), a cyber jihadist can set up any number of free e-mail accounts within a matter of minutes.”); Kohlmann, supra note 63 (“[E]nd users often use Internet proxy servers to obscure their location. These days, they also layer their communications internally to provide an additional cover.”).


71. Certain limits apply depending on the type of account and how long it has been open. See, e.g., LindeX Exchange: Billing and Trading Limits, http://secondlife.com/currency/describe-limits.php (last visited Apr. 3, 2009) (explaining that for residents, during the first thirty days, limits gradually rise from $10 to $500, and after thirty days, limits can reach between $2500 and $10,000; for business owners, the limits range from $5000 to $320,000 monthly).
of virtual terrorist financing, the methodology remains largely academic. However, as with the spread of other IVTS, an absence of evidence is not evidence of absence. By combining the recognized vulnerabilities of virtual worlds with the known traits of terrorist financing, it is possible to illustrate a hypothetical terrorist financing scheme in a developing virtual world (VW).

Over the course of two weeks, suppose that sixteen individuals in five different U.S. cities register to join VW from local coffee shops. After downloading the required programming, these users are prompted to register. Although all are men from countries in the Middle East, southeast Asia, and northern Africa, they supply nondescript, anglicized names and about half self-identify as female. To fulfill the requisite identity confirmation, they then provide the free, web-based e-mail address they each created the day before at another coffee shop. After confirming their new virtual accounts, all of the men shut down their e-mail accounts and allow their VW accounts to remain dormant for the rest of the two-week period.

With their accounts set up and avatars selected, these fifteen individuals begin blending into VW. They attend social functions and meet other avatars, and, looking to capitalize on VW's virtual economy, five of them open in-world businesses. One avatar acts

72. This hypothetical presents VW as a "worst case scenario" in terms of regulations within virtual worlds so as to highlight the potential for exploitation by terrorist financiers. While many of the vulnerabilities identified are based on existing problems in SL and EU, they are not meant to imply that such a scenario could occur in either of those worlds, but, rather, illustrate the potential for abuse in future virtual worlds. See generally supra Part II (discussing characteristics of terrorist financing schemes and the vulnerabilities of virtual worlds).

73. The VW registration process simulates methods used by SL and EU. However, in VW, there are no attempts to verify the actual identity of the users. Cf. supra notes 67–70 and accompanying text (discussing registration procedures in SL and EU).

74. Self-selection is just one way of preserving anonymity—a highly attractive quality of virtual worlds. See Robert O'Harrow, Jr., Spies' Battleground Turns Virtual, WASH. POST, Feb. 6, 2008, at D01 ("Intelligence officials who have examined these systems say they're convinced that the qualities that many computer users find so attractive about virtual worlds—including anonymity . . . —have turned them into seedbeds for transnational threats."); Meta-Terror, supra note 18 (statement of Roderick Jones) ("Anonymity has been a key feature in gaming. Everyone is anonymous and everyone accepts that. . . . Once you have that anonymity you open it to [ ]being misused.").

75. By changing locations, the users effectively mask their IP addresses. See supra note 69 and accompanying text (discussing methods to mask identity while in-world).

76. The ease of opening in-world businesses, combined with the increased
as a virtual real estate broker; one sells virtual lingerie; one runs a virtual coffee shop; and the other two run stores that transfer real-world books and paintings, respectively. To handle the anticipated demand for the virtual and real-world products their avatars are selling, each of these businesses hires two staff members who applied by contacting them and providing a pre-approved word. With their businesses established, the avatars go about their everyday, in-world business, selling their wares and earning VW dollars (VW$).

Two months after setting up his account, and having given the others time to establish their new businesses, the last remaining avatar begins customizing his own virtual life. Having spent the past eight weeks converting $500 per week into VW$ from a PayPal account, this avatar now has VW$4000. Over the next week, the avatar conducts the following transactions with the aforementioned businesses: he purchases a virtual island home for VW$1000, of which the real estate broker takes a commission of 50%; he buys VW$200 worth of lingerie for his virtual girlfriend; each day he purchases three cups of virtual coffee for VW$5 per cup, for a total of VW$75; and, with the remaining money, he purchases countless books and paintings, none of which are ever delivered despite the transfer of VW$. Within nine weeks, the initial VW$4000 is

spending limits for business owners, make these attractive “fronts” for illegal activity. See, e.g., Igor Mutlik, McAfee, Securing Virtual Worlds Against Real Attacks: The Challenges of Online Game Development 4 (Aug. 2008), available at http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_online_gaming.pdf (“Virtual objects are traded in two connected markets—fully virtual and real. The intertwining of real and virtual markets is growing, and there are now real shops in virtual worlds (where you can buy real goods for virtual money). Both of these markets attract criminal elements.”).


78. As discussed supra note 71, to the extent transaction limits exist, they would not catch these small transactions, especially if the account has been open for an extended period. But see Catherine Holahan, Policing Online Money Laundering, BusinessWeek, Nov. 6, 2006, http://www.businessweek.com/technology/content/nov2006/tc20061106_986949.htm?campaign_id=bie_rtv_g3a_rssf1l06u (recommending “imposing limits on the amounts that can be held in online accounts, thus limiting the potential for large amounts to be laundered, and implementing ‘suspicious activity’ reporting practices”).

Published by Mitchell Hamline Open Access, 2009
transferred into the accounts of the other fifteen avatars. Each person then exchanges the VW$ back into real-world currency through PayPal and pre-paid debit cards, and cancels his VW account. 79

Back in the real world, the individuals gather in groups of three in each of the five cities. With their funds combined, each group has a little under $1000. They immediately work toward implementing their “mission,” purchasing the materials to create one improvised explosive device per person. 80 By the end of the week—less than three months after first signing onto VW—the fifteen men carry out fifteen suicide bombings in five major cities throughout the United States. Unable to identify or trace the source of the funds, or locate the sixteenth avatar that financed the attacks, law enforcement and intelligence officials are left with limited leads to investigate the bombings.

As this hypothetical demonstrates, the use of virtual worlds to finance terrorist attacks is more than merely academic.

IV. REGULATING THE VIRTUAL HAWALA

“We will direct every resource at our command [to win the war against terrorism], every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence . . . .” 81

“The environment in which terrorists raise, launder, and transfer funds to further their activities remains all too permissive . . . .” 82 The complexity and variety of methods available to terrorist financiers, combined with the difficulties of identifying these otherwise innocuous financial transactions, requires broader regulation and enforcement. 83 In particular, the ability of terrorist

79. Through the use of fraudulent PayPal accounts or fake identification, this money may become effectively untraceable once it leaves the virtual world. See Holahan, supra note 78 (“Once flush with funds, the [online] accounts can be used to make purchases without leaving a paper trail to the user the way a credit card or check would.”).

80. It costs very little to gather the materials and create an improvised explosive device. See LORETTA NAPOLEONI, MODERN JIHAD: TRACING THE DOLLARS BEHIND THE TERROR NETWORKS 178-79 (2003) (explaining that the cost of making a suicide bomb can be as low as $5 while deployment of a suicide bomber, including transportation and reconnaissance, can cost between $100 and $200).

81. Presidential Address, supra note 11.


83. See Lormel, supra note 39 (“Developing mechanisms to identify emerging
financiers to move between the formal/real-world and informal/virtual-world financial sectors must be curtailed, and any policy aimed at doing so must be "all-encompassing . . . to have any chance of successfully disrupting terrorist activity."\textsuperscript{84}

A. Developing a Framework to Combat Terrorist Financing

Terrorist financing is a global problem that must be fought both domestically and internationally.\textsuperscript{85} At the forefront in the global war on terrorist financing is the Financial Action Task Force (FATF), an international body dedicated to eradicating money laundering and terrorist financing.\textsuperscript{86} The FATF has led the charge for greater regulation and accountability, offering a list of forty recommendations that should be implemented world-wide by both the formal and informal financial sectors.\textsuperscript{87} Recommendations integral to developing successful programs to combat terrorist financing include:

i. identifying all individuals and businesses engaged in financial transactions, both formal and informal;

ii. obtaining accurate and verifiable information

\textsuperscript{84} Levitt, supra note 82, at 61.


\textsuperscript{87} Id. Among the recommendations the FATF suggests:

1) ratifying the 1999 UN Convention on the Suppression of Terrorist Financing;
2) criminalizing the financing of terrorism, terrorist acts, and terrorist organizations;
3) freezing and confiscating terrorists' assets;
4) requiring financial institutions to report suspicious transactions that may be linked with terrorism;
5) assisting in investigations with other countries of terrorist financing networks;
6) imposing anti-money laundering on alternative remittance systems; and
7) taking steps to ensure that non-profit organizations are not misused to finance terrorist groups.

\textit{Id.} (follow "40 Recommendations" hyperlink under "Quick Links").
According to reviews by the FATF and the U.S. Department of the Treasury, the combined implementation of these programs has had marked success in reducing the abuse of formal financial institutions by terrorist financiers. 

Domestically, many of the FATF’s recommendations have been implemented through the Bank Secrecy Act of 1970 (BSA).90 “The principal policy goal of the [BSA] is to protect the international gateways to the United States financial system and to safeguard our financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity.”91 To that end, the BSA requires banks to establish and maintain effective anti-money laundering programs, implement customer identification programs, and maintain transactional records.92

Intended to have a broad reach, the BSA applies to both

---

88. Id. (primarily relying on Recommendations 5–11).
formal and informal financial service providers.93 Formal service providers are generally referred to as "financial institutions" and, although construed relatively narrowly in 1970 when the BSA was passed, Congress has repeatedly expanded the meaning of "financial institution" to keep pace with the ingenuity of criminal organizations.94 Despite the expansion covering formal financial institutions, the BSA historically ignored loopholes that prevented regulation of the vulnerable informal financial sector.95

Less than two months after the September 11 terrorist attacks, President Bush signed into law, as Title III of the USA PATRIOT Act,96 the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.97 Recognizing the need "to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities,"98 Congress sought to patch many of the holes through which terror financiers had slipped.99 Title III expanded existing BSA regulations by ensuring that all individuals or entities that transfer money, no matter how formal or informal, must comply with all anti-money laundering and counter terrorist financing regulations.100

In its post-PATRIOT Act coverage, the BSA provides greater regulation of the informal banking system. Section 359 of the PATRIOT Act specifically addresses underground banking and


94. See id. ("financial institution" includes banks and depository institutions, casinos and card clubs, broker-dealers, and investment companies). The regulations promulgated by the Department of the Treasury under the BSA are found at 31 C.F.R. § 103.22(b)(1) (2002).

95. See Gouvin, supra note 48, at 964 ("[W]hile coverage under the BSA was far-reaching, it was far from universal. Some financial intermediaries were subject to it, but others were not.").


97. Id. §§ 301–377.

98. Id. § 302(b)(11).

99. Weiss, supra note 89, at 6 ("Given that funds used to finance terrorist activities are often not derived from illegal activities, prosecution for funding terrorist activities under the pre-USA PATRIOT Act money laundering laws was difficult.").

expands the definition of "financial institution" to cover IVTS. The BSA and subsequent Treasury Department regulations describe these non-bank entities as "money transmitters" or "money services businesses" (MSB). Despite the expanded coverage, it is unclear whether virtual worlds qualify as MSBs, and thus are subject to BSA regulations.

B. Expanding Current Law to Cover Virtual Worlds

Virtual worlds remain vulnerable to abuse by terrorist financiers. Additional measures must be taken to effectively curb the use of IVTS by terrorist organizations. Bringing virtual worlds under the umbrella of institutions covered by the BSA is the most effective method. Once virtual worlds, like all others who engage in the transfer of money, have a clear responsibility to ensure the sanctity of the markets, businesses working with regulators can begin crafting procedures for compliance with the BSA.

1. Declare Virtual Worlds to be an IVTS and Require Registration

Under the existing regulatory framework, every IVTS must register with the Treasury Department. The first step in reducing the potential for abuse of virtual economies is to extend the scope of coverage to include virtual worlds. Although not traditional "financial institutions," virtual worlds can reasonably fit within the broad MSB category of covered financial systems.

The present interpretation of MSB encompasses "any person doing business, whether or not on a regular basis or as an organized business, which engages in the transfer of funds." Virtual worlds like SL and EU not only engage in the transfer of funds by allowing residents to exchange real-world currency with

101. PATRIOT Act, supra note 96, § 359 (expanding coverage of the BSA by broadening the definition of "Money Transmitting Businessess").
102. Posting of Dennis Lormel to Counterterrorism Blog, Two Easily Exploitable Vulnerabilities of Money Services Businesses, http://counterterrorismblog.org/2008/05/two_easily_exploitable_vulnerabilities_money_services_businesses.php (May 21, 2008, 15:41 EST) ("MSBs refer to five distinct types of financial services providers: currency exchangers; check cashers; issuers, sellers, or redeemers of traveler’s checks, money orders or stored value; the United States Postal Service; and money transmitters.").
103. See supra Part II.C (discussing the vulnerabilities of virtual worlds).
virtual currency, they have built systems in which a virtual economy is an integral part of their business. Neither new laws nor amended regulations are necessary to apply existing BSA regulations to virtual worlds. Rather, the Department of the Treasury merely has to issue an administrative ruling designating virtual worlds as covered institutions since a plain reading of current regulations arguably covers virtual worlds as IVTS. Once existing BSA regulations are expanded to cover virtual worlds, law enforcement and intelligence officials can begin cracking down on one of the last remaining unregulated methods for transferring terrorist funds.

2. Implement Know-Your-Customer Procedures

Once virtual worlds are placed on notice that they are subject to BSA regulations, they must implement comprehensive anti-money laundering and terrorist financing programs. Such compliance programs are required of brick-and-mortar financial institutions and, while admittedly more complicated, expanding them to virtual worlds will reduce criminal abuse of these systems. Recognizing the critical role that both formal and informal financial systems play in the effort to find terrorists, a key compliance mechanism is that all covered institutions "know their customer." Under existing regulations, covered institutions must:

   i. identify customers as they open accounts by obtaining information such as the customer's name, address, date of birth, and taxpayer


\[\text{107. Despite initial skepticism and opposition to the PATRIOT Act provisions, increased regulation has been effective in curbing the abuse of formal financial institutions. See Joseph M. Myers, The Silent Struggle Against Terrorist Financing, 6 GEO. J. INT'L AFF. 33, 35 (2005).}\]

\[\text{108. MONOGRAPH, supra note 4, at 61. "To fulfill this role properly in the life-and-death emergencies that can arise, financial institutions must (1) know their customers by their real names and possess other essential identifying information, (2) have the ability to access this information in a timely fashion, and (3) quickly provide this information to the government in a format in which it can be effectively used." Id. Law enforcement will not be able to develop a comprehensive strategy for countering terrorist financing until individuals can be openly identified.}\]
identification number;
ii. exercise reasonable efforts to verify the customer's identity;
iii. maintain records and information obtained during the identification and verification process; and
iv. consult lists of individuals whose assets have been blocked or frozen. 109

Like their brick-and-mortar counterparts, virtual worlds must ensure that every avatar with virtual currency can be linked back to a verifiable name, address, and real-world bank account. 110 Absent this basic know-your-customer requirement, anti-terrorist financing efforts will not be effective. 111

These customer identification and verification procedures, while potentially costly and time-consuming, are a necessary expense for virtual worlds looking to profit from the spread of their economies. 112 Although this is a developing area of regulation, traditional banks implemented similar programs when shifting to online banking. 113 Any effective program must ensure proper

110. Todd M. Hinnen, The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet, 5 COLUM. SCI. & TECH. L. REV. 5, ¶ 66 (2004) ("For traditional brick-and-mortar banking, this process often involves meeting the customer, obtaining identifying documents that have photographs or list physical characteristics that match the customer's characteristics, and observing the customer's behavior. In an Internet banking context, none of these traditional techniques is possible.").
111. MONOGRAPH, supra note 4, at 61 (Section 326 of the PATRIOT Act, which "requires financial institutions to 'enhance the financial footprint' of their customers by ensuring effective measures for verifying their identity," recognizes that "effective customer identification may deter the use of financial institutions by terrorist financiers and money launderers and also assist in leaving an audit trail that law enforcement can use to identify and track terrorist suspects when they conduct financial transactions").
112. Many of the same arguments likely made by virtual worlds have already been proffered by formal financial institutions and rejected by regulators. See, e.g., Joseph J. Norton & Heba Shams, Money Laundering Law and Terrorist Financing: Post September 11 Response—Let Us Step Back and Take a Deep Breath?, 36 INT'L L. 103, 121 (2002) (arguing that Title III of the PATRIOT Act might impose an onerous burden on banks).
113. See generally FED. FIN. INST. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (Oct. 12, 2005), www.ffiec.gov/pdf/authentication_guidance.pdf [hereinafter AUTHENTICATION] (discussing the rise in online banking and the application of the BSA
identification not only during the registration process, but also during each individual transaction.\textsuperscript{114} One immediate solution for companies and clients who want to reduce the amount of personal information needed is to offer two different accounts—one permitting residents to engage in financial transactions and one that does not. Thus, those interested in pursuing their virtual fortune will be required to enter additional information during the registration process.

As with origination of bank accounts online, verifying virtual users' identities is difficult.\textsuperscript{115} Online banking services now verify personal information through the use of: (i) "[p]ositive verification[,] to ensure that material information provided by an applicant matches information available from trusted third party sources"; (ii) "[l]ogical verification[,] to ensure that information provided is logically consistent (e.g., do the telephone area code, ZIP code, and street address match)"; and (iii) "[n]egative verification[,] to ensure that information provided has not previously been associated with fraudulent activity."\textsuperscript{116} Building upon these techniques, virtual worlds should collect as much personal information as practicable and cross-check that information against public records to verify its accuracy.\textsuperscript{117}

V. CONCLUSION

"It is time to take a fresh look at anti-terrorist financing and anti-money laundering regulations as we enter the next administration and next Congress and see what has worked, and what hasn't, how methods have changed and how to change the [PATRIOT] Act, the Bank Secrecy Act and other regulations to go along with that."\textsuperscript{118} As terrorist financiers shift to unregulated

\begin{flushleft}
\footnotesize\textsuperscript{114} AUTHENTICATION, supra note 113, at 1.
\footnotesuperscript{115} \textit{Id.} at 4–5.
\footnotesuperscript{116} \textit{Id.} at 13.
\footnotesuperscript{117} \textit{Id.} at 13–14.
\footnotesuperscript{118} Posting of Andrew Cochran to Counterterrorism Blog, Assessment of International Counter-Financing of Terrorism Efforts Needed for Next Administration & Congress, http://counterterrorismblog.org/2008/05/assessment_of_international_co.php
\end{flushleft}
financial sectors, law enforcement officials and the tools they use must likewise evolve.  

Efforts to disrupt terrorists' ability to fund their operations will not succeed if focused solely on formal banking or the mainstream financial sector. Instead, U.S. government officials must implement a comprehensive counterterrorist financing policy that continues to effectively curtail abuse of the formal financial sector while implementing broader regulations to address developing underground banking systems.

With the increasing virtualization of terrorism and the developing of virtual world economies, law enforcement officials must carefully consider the opportunity virtual worlds present as potential informal value transfer systems. Once the vulnerabilities of these platforms are identified, appropriate patches can be devised to close the loopholes. The quickest way to move towards effective regulation is for the Department of the Treasury to immediately designate virtual worlds as covered institutions subject to the BSA's anti-terrorist financing regulations. Next, the most important step will be verifying user identity during registration and ensuring that each virtual transaction can be traced back to identifiable senders and recipients.

None of these proposals will be easy to implement and, unfortunately, no amount of regulation will completely cut off the financing of terrorist operations. However, to stand idly by and allow the Internet to remain the last place where criminals and terrorist groups can anonymously do as they please is unacceptable.

(May 7, 2008, 10:09 EST).

119.  Id.

120.  See Money Laundering Strategy, supra note 92, at 3 (explaining other ways of tracking terrorist financing).
PART IV: PROFESSIONAL ARTICLES

The following section contains professional articles. The first argues that national security advice and advocacy should expressly consider institutional culture’s impact. The second discusses the dichotomy that is often debated when there is a threat to national security and suggests that such a dichotomy is false. The third, among other things, proposes ways that our Nation’s national security can best be protected.