Vol.6 • No.1 • Spring & Fall 2014 ISSN. 1307 - 9190

Defence Against Terrorism Review

DATR

Cryptocurrencies: The Next Generation of Terrorist Financing?
Alan BRILL & Lonnie KEENE

Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States
Uchenna Jerome ORJI

Improvements Required for Operational and Tactical Intelligence Sharing in NATO
Stewart WEBB

Youth Extremism in Pakistan – Magnitude, Channels, Resident Spheres and Response
Muhammad FEYYAZ

COE-DAT
Centre of Excellence - Defence Against Terrorism

Defence Against Terrorism Review - DATR

DATR is an international peer-reviewed journal that is abstracted and indexed in EBSCO Publishing.

The Defence Against Terrorism Review (DATR) is calling for papers for coming issues. The DATR focuses on terrorism and counterterrorism. All of the articles sent to DATR undergo a peer-review process before publication.

For further information please contact datr@coedat.nato.int

Defence Against Terrorism Review
DATR

Vol. 6 No. 1, Spring&Fall 2014

ISSN. 1307-9190

CONTENT

Editor's Note

Dear Defence Against Terrorism Review (DATR) readers,

Six years have passed since the first issue of DATR was published and now we are happy to introduce you to the Fall 2014 issue (9th issue). In this issue we present four articles on various topics for your appreciation and constructive criticism. We hope you will enjoy these articles and their contents. We also hope that these articles will spark discussion in the necessary fora and will lead to action to address the issues raised.

The first article was written by Alan Brill and Lonnie Keene. Alan Brill is an expert on cybersecurity issues and senior managing director for Kroll Cybersecurity & Investigations. He has been an instructor for the FBI, Secret Service, Federal Law Enforcement Training Center, AICPA, ABA, John F. Kennedy School of Government at Harvard and the NATO Center of Excellence-Defense Against Terrorism. Lonnie Keene is the managing director for Kroll Cybersecurity & Investigations and is a leading authority in the areas of market entry and compliance matters, including anti-money laundering, OFAC, and the Foreign Corrupt Practices Act. Their article is about virtual currencies, which have become an important factor in global funds transfers. Virtual currencies are not legal tender in any country and are not issued or backed by any government. In their article they examine what these financial vehicles are, how they work and why they facilitate terrorist funding. They then offer suggestions to members of the antiterrorism community for investigating cases involving virtual currencies and bringing perpetrators to justice. Their experience in analyzing many aspects of financial irregularities is invaluable in highlighting this issue of growing importance to the counterterrorism community.

The second article is written by Uchenna Jerome Orji, an expert on cybersecurity issues and legal regulation, who is currently a research associate at the African Centre for Cyber Law and Cybercrime Prevention (ACCP) at Kampala, Uganda. In his article he explores enhancing the collective responsibility of states to deter cyberterrorism. In particular, he suggests the need for a state to be held accountable where its failure to establish regulatory measures to deter or prosecute cybercrimes or cyberterrorism within its territory has allowed the perpetration of such acts to cause transboundary effects in other states. This is a very timely article based on the cyberthreat that members of the Alliance have dealt in the past and will most certainly face in the future.

The third article is written by Stewart Webb, who is an expert on security issues and political science. He is currently a research associate at the Canadian Center for Policy Alternatives and the editor for Defence Report.com. In his article he deals with the improvements required for operational and tactical intelligence sharing in NATO. While NATO may be drawing down in Afghanistan, globalized terrorism will be a continuing issue for NATO and fighting globalized terrorism requires coordination among nations. He states that under the Connected Forces Initiative, NATO is moving from operational engagement to operational readiness through an increase in exercises and measures that aim to improve interoperability. He points out that if there is anything to be learned from the Afghan and Libyan deployments, it is that intelligence sharing in NATO could potentially be the proverbial Achilles Heel of the Alliance. This article is an excellent contribution to NATO interoperability.

The fourth article is written by Muhammad Feyyaz, who is a former military officer and an academician at the University of Management and Technology, Lahore, Pakistan. In his article he attempts to address religious extremism and the factors confounding its conceptual and definitional understanding within the existing reality of Pakistan. He particularly highlights and analyzes the demographic magnitude of extremists' potential, inspirations, channels and geographical location of extremism in the country; these areas have been ignored in the extant literature on extremism in Pakistan. In his article a few broad policy suggestions are also offered including a generalizable framework to measure the holistic spread of extremism in Pakistan in order to be able respond meaningfully to the situation. Although his analysis focuses on Pakistan, we may draw many lessons from this article for the terrorist threat that faces many NATO member nations.

We would like to express our gratitude to all of the scientists, academicians and practitioners who have sent their deserving articles to our journal. We also would like to thank the referees who accepted our offer and reviewed the articles by spending their valuable time for DATR. We offer these articles to the NATO Alliance as well as our partners in order to better our capabilities to fight against terrorism.

We are hoping to meet again in the 10th issue of DATR, and we present our most heartfelt best wishes to all of you.

Atasay ÖZDEMİR
Editor-in-Chief

Defence Against Terrorism Review
Vol. 6, No. 1, Spring&Fall 2014, pp. 7- 30

ISSN: 1307-9190

Cryptocurrencies: The Next Generation of Terrorist Financing?

Alan Brill
Senior Managing Director, Kroll Cybersecurity & Investigations New York, NY.
abrill@kroll.com

Lonnie Keene
Managing Director, Kroll Cybersecurity & Investigations New York, NY.
lkeene@kroll.com

Abstract: *Virtual currencies — which are not legal tender in any country and are not issued or backed by any government — have become an important factor in global funds transfers. But features associated with these so-called "cryptocurrencies," such as transaction anonymity and irreversibility of payments, have made them extremely attractive to cybercriminals, drug dealers, money launderers and those involved in global terrorist funding. In this paper, we examine what these financial vehicles are, how they work and why they facilitate terrorist funding and offer suggestions to members of the antiterrorism community for investigating cases involving virtual currencies and bringing perpetrators to justice.*

Keywords: *Virtual currency, Cryptocurrency, Bitcoin, Non-sovereign currency, Terrorist financing*

Introduction

Let's assume you own a food store. A customer comes in, selects a basket of food items and comes to you to pay for it. Rather than offering you money or, perhaps, a debit or credit card, the person hands you an obviously photocopied piece of paper which says it is worth "25 Cyber-Beans." It also has on it a long set of numbers and letters on a computer-printed sticker placed in a box marked "Unique ID".

"What is this," you ask?

"It's a new kind of money," the customer says. "You go to the web address shown on the certificate. Then you set up an account. Then you enter the Unique ID Code, and the Cyber-Beans transfer to you instantly. Isn't that great?"

You tell the customer that you do not know what they're talking about. What are Cyber-Beans?

The customer tells you, "Cyber-Beans are a new currency that I developed. Each Cyber-Bean is worth five units of the local currency — but that could change and be worth more or less as time goes on. And you can change them for local currency once you have an account. You just have to find another user who wants to make the exchange, and agree on a price."

You ask whether the currency is backed by the government. "No," says your customer. "We do not trust governments. This is a private non-governmental currency that I helped to create. We keep the government completely out of it for everyone's privacy. In fact, the transactions are virtually untraceable, and they are anonymous." When you ask the customer for identification, they are highly insulted. "Don't you understand — this is all anonymous. You don't need to know who I am. Why would you care? You will have the Cyber-Beans!" You throw the customer out, without any purchase.

This sounds like a strange phenomenon. Money with no government backing? Certainly you understand that you can make an arrangement with a customer to take an 'IOU' that acknowledges that the individual owes you a certain amount of money, and you have always done this for good customers. But made-up money where everything is anonymous, and all done on computers? Sounds crazy!

But it is very real. These new forms of currency — with names like 'Bitcoins' and 'Ripples' — are very real. They are not backed by any government agency. And they have characteristics that make them attractive to those who might use them for money laundering, for narcotics or human trafficking or even as a vehicle for global terrorist funding. In fact, in the United States, the U.S. Treasury Department's Financial Crimes Enforcement Network (known as "FinCEN") has gone so far as to issue guidance on the applicability of FinCEN regulations and registration requirements for those who serve as money services businesses for crypto-currencies.[1] Speaking at a recent conference, FinCEN Director Jennifer Shasky Calvery said that "the guidance responds to questions raised by financial institutions, law enforcement, and regulators concerning the regulatory treatment of persons who use virtual currencies or make a business of exchanging, accepting, and transmitting them."[2] She also pointed out that while many in the financial community understood these emerging payments systems, "many line analysts, investigators, and prosecutors in law enforcement may not."[3]

---

[1] U.S. Department of the Treasury, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," (Financial Crimes Enforcement Network, Publication FIN-2013-G001, March 18, 2013), available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html (accessed 4 December 2014).

[2] Jennifer Shasky Calvery, "Remarks to the National Cyber-Forensics Training Alliance" (CyFin 2013 Conference, Pittsburgh, PA, April 16, 2013), p. 4, available at http://www.fincen.gov/news_room/speech/html/20130416.html (accessed 4 December 2014). Ms. Calvery is the Director of the Financial Crimes Enforcement Network, U.S. Treasury.

[3] Ibid, p. 3.

Government reactions to virtual currencies are varied. Some countries have announced regulatory rules surrounding them. Some have recognized them in various ways and sometimes tax them. Other countries have effectively banned them.

In this article, it is our objective to provide a briefing to the defense against terrorism community on what these new payment systems are (and are not), why they can facilitate terrorist and other forms of criminal activities, and actions that governments around the world have taken or may take to reduce the risk factors associated with these artificial currencies.

What is Cryptocurrency?

Cryptocurrency goes by many generic names. It is often referred to as 'virtual currency' or as 'non-fiat currency.'

Perhaps the simplest definition comes from FinCEN: "'virtual' currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction."[4]

Artificial currencies are not new. In fact, we have probably all encountered them.

- As noted in the introduction, I can accept an IOU from you, which is certainly a form of payment, assuming I trust you to redeem it with "real" money). In fact, I could probably sell your IOU to a friend, and you would then owe them the money. This works because you trust the friend. But when you sell it, the friend who buys the IOU either has to also trust the person who issued the IOU, or you have to guarantee payment, or the buyer builds in a discount that covers the risk. (For example, they might pay you $80 for a $100 IOU, with the other $20 covering their profit and risk acceptance.)
- Many games use virtual currencies. One of the most famous board games in the world, Monopoly, published by Parker Brothers, uses its own currency within the game, called "Monopoly Money." It is useful within the game, but it is universally recognized as having no real-world exchange value.[5] But some games played by multiple participants in an online environment also use currency that is only useful within the game itself, but which has enough value to the players that they will exchange real money for game money. For example, in the game "Second Life" essentially everything in the game (from houses and cars to your clothing, hair or skin) can be bought and sold using their in-game currency called "Linden Dollars" or, in the virtual currency community, Second Life Lindens ("SLL"). Real money can be converted into Linden Dollars through the game-maker's site or through other sites that essentially trade in this virtual currency.[6] Many sites have been set up to trade goods

[4] U.S. Department of the Treasury, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," p. 1.

[5] Craig M. Boise, "Playing with 'Monopoly Money': Phony Profits, Fraud Penalties and Equity," *Minnesota Law Review* 90 (1) (2005), p. 144, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=688586 (accessed 4 December 2014).

[6] See, e.g. Jeremy and Eli Linden, "Buying and Selling Linden Dollars," *Second Life* (06 August 2012), at http://community.secondlife.com/t5/English-Knowledge-Base/Buying-and-selling-Linden-dollars/ta-p/700107#Section_.1(accessed 16 October 2014)

and in-game money for real money.[7] As will be noted later in this report, the Bitcoin exchange known as Mt. Gox, which filed for bankruptcy in Japan and admitted that hundreds of millions of U.S. dollar value in the form of Bitcoin virtual currency were missing, started its corporate life as a platform for the buying and selling of trading cards that were part of the game named "Magic: The Gathering." The trading of these cards (which provided the holders with certain capabilities within the play of the game) was a real business, and the move to Bitcoin transactions came somewhat later.

- Store coupons — issued by manufacturers or stores themselves — are essentially a form of currency. For example, you can use a coupon good for US $5 off of a US $20 purchase in place of a real U.S. five-dollar bill. These work because a community of vendors (who issue the coupons) and stores (that accept the coupons) have agreed on trust issues and procedures to assure that the store gets the value represented by the coupons (plus a small fee for accepting and handling the coupon transactions). It is estimated that in 2012, considering only the U.S. market, consumers redeemed 2.9 billion coupons with a face value of approximately US $800 million.[8]

In fact, according to a recent report,[9] eBay's online commerce site PayPal has filed a patent application that would provide for "secure tokens that would let people buy products without creating a payment provider account." The report points out that such tokens could potentially be "used for purchases outside of eBay and PayPal."

On some dates last year, it was reported that the amount of value transferred in the form of the virtual currency called 'Bitcoins' exceeded the amount of value transferred by eBay's PayPal service.

Another example of transactions that do not depend on currency is bartering. I offer to sell you a cow in exchange for a number of goats. You offer four, I ask for six, we settle for five. This transaction occurs because each party believes that what they are receiving has a value that makes the transaction worthwhile for them. Of course, even barter carries with it a degree of risk. Are the goats healthy? Does the cow produce milk, and does the seller actually own it? Transactions involving virtual currencies fall into the category where the parties' assessment of the risks of virtual currencies lead them to a decision to go ahead with the deal, or not. If one party feels that the virtual currency offered does not offer an acceptable combination of risk and value, the deal does not happen.

In the next sections of this paper, we will discuss how these cryptocurrencies are created; converted from and to regular currencies; how they are transferred; and how the characteristics of anonymity, speed, low transaction cost and difficulty in tracking transactions has led to problems — some of which have resulted in law enforcement action, and others which have resulted in regulatory actions by a number of nation-states.

---

7 Ryan M. Pierson, "How Gamers Make Real Money from Video Games," *Locker Gnome* (20 April 2012), at http://www.lockergnome.com/news/2012/04/20/how-gamers-make-real-money-from-video-games/ (accessed 01 June 2014).

8 The face value does not include the fee paid to retailers for handling the coupons. I [Love] Coupon Month, "Statistics," at http://www.ilovecouponmonth.com/statistics/ (accessed 13 October 2014).

9 Asian News International, "eBay Likely to Launch Own Virtual Currency," DNAIndia (3 January 2014), available at http://www.dnaindia.com/money/report-ebay-likely-to-launch-own-virtual-currency-1944662 (accessed 10 February 2014).

How Does Cryptocurrency Work?

Because cryptocurrencies do not exist in the form of banknotes or coins (the physical coins that are often pictured in connection with Bitcoin articles are not Bitcoins; they are more in the form of a souvenir), you cannot just pull them out of your purse or wallet and use them to buy a cup of coffee. They only exist as strings of digital characters.

To buy, sell or use them, you must have a way of storing them (known as a digital 'wallet') and you have to find a way to acquire them. You also at some point may want to convert them into a national currency.

There are many organizations on the Internet that will provide you with a digital wallet for your virtual currencies. There are also offline wallets that enable you to store them on your personal computer, tablet or phone. Essentially, a virtual wallet is a program that can receive, send and store the codes that represent the currency. Of course, if you use a wallet stored on your device and your device's storage mechanism fails and your wallet is not backed up, your virtual money may simply (and permanently) disappear. You can also establish a wallet at a virtual currency exchange. There are now listings of these organizations that can be accessed on the Internet.[10]

Of course, the dangers to those using virtual currencies are pointed out, even in the instructions to new users. The clear warning says:

> Warning: Please be careful with your money. When sending money to an exchange or seller you trust that the operator will not abscond with your funds and that the operator maintains secure systems that protect against theft — internal or external. It is recommended that you obtain the real-world identity of the operator and ensure that sufficient recourse is available. Because Bitcoin services are not highly regulated a service can continue operating even when it is widely believed that it is insecure or dishonest and webpages recommending them (including these) may not be regularly updated. Exchanging or storing significant amounts of funds with third-parties is not recommended.[11]

But let us assume you've decided to use virtual currencies. You establish an account with one or more exchanges. For many, the authentication of who you are consists of having a verifiable email address (which can, of course, be with any number of virtually anonymous email services) and in some cases a phone which can send and receive messages (which can be an anonymous prepaid phone). Once you have an account, you determine how many units of the virtual currency you want, and what that will cost you in a real-world currency (or equivalent like a prepaid gift card or prepaid credit card) that the exchange accepts. You make your payment (perhaps by making a cash deposit to a designated account at a designated bank) and you get your virtual currency. You can then send payments to anyone else with a wallet and presumably, at some point, you can exchange it back to a government-backed currency.

---

[10] For example, the Bitcoin Wiki maintains a page on buying Bitcoins for newcomers to virtual currency dealings. BitCoin, "Buying BitCoin (the newbiw version), at http://en.bitcoin.it/wiki/Buying_Bitcoins_%28the_newbie_version %29 (accessed 4 December 2014).

[11] Ibid. Note that these risks are as real for those using wallets for criminal or terrorist financing as they are for anyone else.

Cryptocurrencies also have to be created. There are two major methods that various cryptocurrency creators have used.

In the first, the creator decides on the number of units of the currency that will ever be needed, and creates the currency all at once, then releases it according to a schedule.

The other method — the one used by Bitcoin — is to have a process for people to create the currency over time, but with a maximum number of Bitcoins that will ever exist fixed in advance.

Bitcoins are created, or 'mined,' "by solving extremely difficult mathematical problems. The problems are automatically made harder over time to ensure that the overall supply of Bitcoins cannot grow too fast."[12] An industry has grown around the creation of specialized computers and custom-designed chips (called Application-Specific Integrated Circuits, or "ASICs" which are optimized to conduct the mathematical calculations needed for mining Bitcoins. In recent years, criminals have made use of 'botnets' (networks of thousands of compromised computers) to carry out mining calculations.[13] There have also been instances of software applications for mobile devices which, in addition to their normal function, used the mobile device's processor to contribute to Bitcoin mining.[14] However, with the advent of specialized machines using vast arrays of ASIC chips, virtually all mining profits now go to the organizations that have built and operate these Biticoin mining powerhouses.

Bitcoins are not issued by a central bank or government. They may be purchased from a Bitcoin exchanger. Bitcoin exchangers accept conventional currencies and exchange them for Bitcoins based on a fluctuating exchange rate.[15] Once acquired, the Bitcoins are stored in a digital wallet associated with "the user's Bitcoin 'address,' analogous to a bank account number, which is designated by a complex string of letters and numbers."[16]

Only the Bitcoin address of the user is necessary to conduct a transaction, "which by themselves do not reflect any identifying information."[17] A Bitcoin transaction, which takes the form of a transfer of value between Bitcoin wallets, is recorded in a public ledger called the 'blockchain.'[18] "To

[12] "Bitcoin: Monetarists Anonymous," *The Economist* (Sep. 29, 2012), available at http://www.economist.com/node/21563752 (accessed 10 February 2014).

[13] Brian Krebs, "Botcoin: Bitcoin Mining by Botnet," *Krebs on Security* (July 13, 2013), at http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet/ (accessed13 October 2014); Danny Yuxing Huang, et al., "Botcoin: Monetizing Stolen Cycles," (Network and Distributed System Security *(*NDSS*)* Symposium, 23-26 February 2014), available at http://sysnet.ucsd.edu/~dhuang/static/ndss14-cr.pdf (accessed 13 October 2014).

[14] Chris Brook, "Google Removes Bitcoin Mining Android Malware From Play," *ThreatPost* (April 28, 2014), at http://threatpost.com/google-removes-bitcoin-mining-android-malware-from-play/105740 (accessed 13 October 2014); Samantha Murphy Kelly, "Report: Android Malware is Mining Bitcoin While You Recharge," *Mashable* (Mar. 27, 2014), available at http://mashable.com/2014/03/27/android-app-bitcoin-malware/ (accessed 13 October 2014).

[15] Emily Flitter, "Prominent Bitcoin Entrepreneur Charged with Money Laundering," *Reuters* (Jan. 27, 2014), available at http://www.reuters.com/article/2014/01/28/us-usa-bitcoin-arrests-idUSBREA0Q15N20140128 (accessed 13 October 2014).

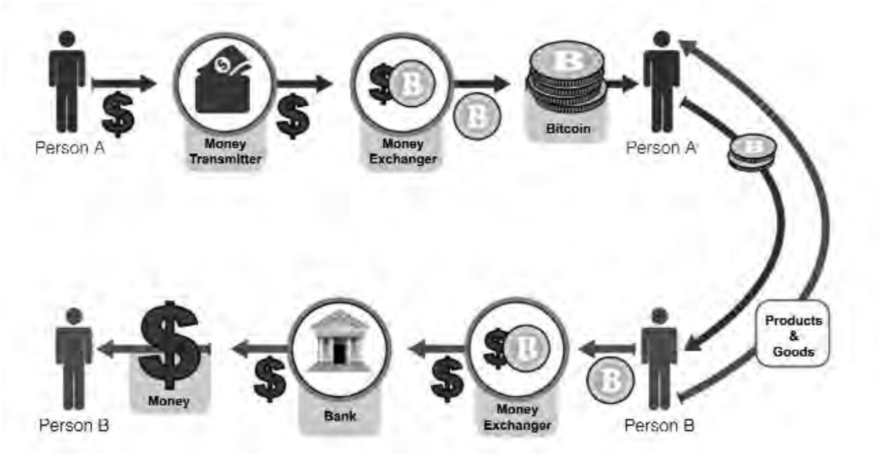
[16] Sealed Complaint, United States of America v. Robert M. Faiella, a/k/a 'BTCKing,' and Charlie Shrem," (Southern District of New York, January 24, 2013), §14.c.

[17] Ibid., at §14.d.

[18] Bitcoin, "How does Bitcoin work?" at https://bitcoin.org/en/how-it-works (accessed 07 February 2014).

be confirmed, transactions must be packed in a *block* that fits very strict cryptographic rules which center around a very long random number that Bitcoin miners must guess, and which will be verified by the network."[19]

The following chart provides a simple overview of a transaction using a virtual currency (a Bitcoin for purposes of example). [20]



Person A wants to pay Person B for some product or service. Person A may be able to go directly to a money exchanger (who will exchange a sovereign currency for Bitcoins) or may have to go through a money transmitter to get it to the exchanger. The Bitcoins go into Person A's virtual currency wallet. Person A transfers them to Person B. Person B then can go through a money exchanger to get currency which can be deposited in a bank.

Why is Cryptocurrency Attractive to the Terrorist, Money Laundering and Criminal Underground?

If you were a terrorist, a money launderer or a criminal who wished to use the Internet to move funds globally to support your drug dealing or human trafficking operations, what characteristics would you want in a value-transfer tool?

- Anonymity — You would certainly want a system that did not require you to prove your identity and to have that validated identity tied to all of your transactions. In fact, you would like a system that did not require you to identify yourself at all, or to provide any information about yourself. Of course, anonymity, while highly desirable for terrorists, money launderers and others carrying out illegal schemes, is not in and of itself an indication of criminal behavior. Recent world events such as those seen in the Ukraine where both pro- and

[19] Ibid, at p. 3.

[20] Jennifer Shasky Calvery, "Statement Before the United States Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy" (November 19, 2013), available at http://www.fincen.gov/news_room/testimony/pdf/ 20131119.pdf (accessed 13 October 2014).

anti-government supporters have used Internet anonymity to protect themselves from identification and potential retaliation for their views, have clearly demonstrated that there are many cases in which online anonymity is important. For those speaking against what they feel are repressive regimes, anonymity may be literally a matter of life and death for those communicating.

- Global Reach — The system should permit money to be transferred from anywhere to anywhere, and in any amount. You also want the ability to carry out transactions through third countries that you have little or no connection with to confound those trying to identify you or at least identify the country from which you are operating. You may physically be in Country A, initiate a transaction through the Internet to convert the national currency of Country B through a virtual currency exchange in Country C, and transfer the virtual currency to a wallet in Country D. The virtual currency could be transferred (possibly through intermediary steps) to the ultimate receiver's wallet in Country E. They might go through an exchange in Country F and convert to the currency of Country G. You might also choose to deal with virtual currency companies located in countries that are politically hostile to countries which you fear may be seeking your arrest.
- Speed — The system should carry out the transfers quickly, preferably within seconds. The faster the transaction, the less chance that it can be intercepted and blocked.
- Non-Repudiation — Transactions should be immediately final. No additional verification or validation should be necessary to execute any transaction. The person sending the money should not be able to 'unsend' it or reverse the transfer.
- Low Cost to Use — While this is less important to the criminal user, it would be desirable if the system operated with minimal overhead allowing large and small transactions to occur without eating up the value of small transactions in fees. Of course, intermediaries who cater to illegal uses of cybercurrency can charge premium fees for their services. For example, a service which knowingly fails to file required reports of suspicious transactions to regulatory authorities might well expect a greater fee in exchange for their complicit silence.
- Relative Ease of Use — Whatever system you use, it should be easy for non-technical people to use. Preferably it should have a computer interface that makes setting up a transaction fast and easy and should be able to be used on a computer, tablet or smartphone that is connected to the Internet.
- Difficult for Authorities to Track Transactions — Obviously, you want a system that is not going to be an open book for the authorities to use to track your transactions or the actions of your group.
- Potential Upgrades to Security and Anonymity — You would like the system to have the ability to apply additional means of security. Using additional layers of anonymity (through anonymizing networks that currently exist or could be created) would make the job of law enforcement and anti-terrorism agencies much harder.

- Venue Changes to Make Cooperation with Governments Difficult — While some venues have taken regulatory action (for example the U.S. FinCEN regulations cited earlier which have the effect of bringing many virtual currency companies under the definition of "money transmitting businesses"), other countries have taken no action at all.
- Another level of complexity will face government regulators, law enforcement personnel and terrorism-funding analysts resulting from the frequent movement of these loose networks of servers from venue to venue over time.

Why is Cryptocurrency Not Attractive to the Terrorist, Money Laundering and Criminal Underground?

It is fair to ask if there are aspects of cryptocurrency that might be unattractive to the criminal/terrorist community. Certainly, criminals and terrorists face some of the same risks that legitimate users face:

- Values of virtual currency that can change rapidly and unpredictably.
- Holding virtual currencies in wallets that are subject to theft, either by insiders or hackers.
- Failure to identify methods of converting sovereign currencies to virtual currencies, or virtual currencies to sovereign currencies, or to goods and services through organizations that the criminals can 'trust.'
- The potential inability to transfer sovereign currencies to or from virtual currencies because of supply, demand or cost issues. At a moment when you want to make an exchange, it is possible that no one would be willing to undertake the transaction at a cost that you could accept.
- The growing interest in virtual currencies and increasing expertise in tracking virtual currency use by government regulators and law enforcement authorities worldwide.

As with any legitimate organization, criminal and terrorist users of virtual currencies have to move toward a continuous process of risk assessment to determine when (and whether) virtual currencies are appropriate for their use and whether the risks that they face are acceptable to them. At any given time, criminals or terrorist users of virtual currencies have the problem of converting the virtual currency into something they can use, be it a national currency, drugs, weapons or anything else. How they do this will involve a range of considerations, including the presence in the system of money transmitters and exchangers that they can trust, or whom they feel will not notice/care who they are; potential significant changes in virtual currency values; and the ability to structure the transaction into multiple parts, each of which is smaller and may make it suitable for a larger number of smaller exchangers/transmitters. It may also be possible to structure a transaction through the use of multiple currencies that a counterparty (for example an arms dealer) might accept in total.

Cryptocurrency and Unlawful Transactions: The Current State of Affairs

When you look at cryptocurrencies today, an initial review would suggest that they meet a lot of the needs of terrorists, money launderers and other criminals who depend on the ability to move funds globally. The very characteristics of cryptocurrencies described above that make them attractive to terrorists, money launderers and criminals pose challenges for law enforcement and regulators. Law enforcement and regulators are increasingly concerned about the threat posed by virtual currencies to move monetary value outside of traditional and highly regulated banking and money transfer services.[21] Governments are coming to understand that virtual currencies — the ones that exist today like Bitcoins, and those which will be developed in the future — cannot simply be ignored. While some governments have reacted by essentially trying to outlaw the currencies, others have moved in the direction of regulation.

In describing the current security environment, the U.S. Department of Homeland Security reports that "[t]ransnational crime and trafficking facilitate the movement of narcotics, people, funds, arms, and other support to hostile actors, including terrorist networks."[22] An underlying assumption of the U.S. Department of Homeland Security in assessing the current security environment is that "[t]errorists, proliferators, and other criminal elements will seek to take advantage of the increasingly globalized financial system and its legitimate and beneficial functions to move money in support of their dangerous conduct."[23] Cryptocurrencies transcend traditional nation-state-based financial systems and continue the trend toward globalization of financial systems. Making the development of cryptocurrency even more worrisome, however, for the ability of the international security community to deter and detect terrorist financing, is the inherent ability of cryptocurrencies to operate beyond the monitoring and surveillance capabilities of many — perhaps most — national financial regulatory systems.

Regulators Move to Assert Oversight

In the United States, FinCEN is charged with enforcing compliance with the Bank Secrecy Act ("BSA"), the nation's anti-money laundering and counterterrorism statute.[24] FinCEN is a bureau of the U.S. Treasury Department and reports to the Treasury Undersecretary for Terrorism and Financial Intelligence.[25] FinCEN's Director, Jennifer Shasky Calvery, told an international antimoney-laundering ("AML") and financial crime conference in March 19, 2013, that

[21] Reed Albergotti and Jeffrey Sparshott, "U.S. Alleges $6 Billion Money-Laundering Operation at Liberty Reserve," *Wall Street Journal* (May 28, 2013), available at http://online.wsj.com/articles/SB10001424127887323855804578511121238052256 (accessed 4 December 2014).

[22] U.S. Department of Homeland Security, "Quadrennial Homeland Security Review Report: A Strategic framework for a Secure Homeland" (1 February 2010), p. 7, available at https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (accessed 4 December 2014).

[23] Ibid, p. 9.

[24] U.S. Department of the Treasury Financial Crimes Enforcement Network, "What We Do," at http://www.fincen.gov/about_fincen/wwd/ (accessed 10 February 2014).

[25] Ibid.

"FinCEN's analysts are continually working to understand the schemes and methods used to exploit emerging payment methods for money laundering and terrorist financing, and to develop related guidance for law enforcement."[26]

Director Shasky Calvery was speaking the day after her agency had issued "guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies."[27] The new interpretive guidance provides that any administrators and exchangers of virtual currencies "that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person."[28] As a result, "FinCEN's guidance explains that administrators or exchangers of virtual currencies have registration requirements and a broad range of AML program, recordkeeping, and reporting responsibilities. Those offering virtual currencies must comply with these regulatory requirements, and if they do so, they have nothing to fear from Treasury."[29]

In the United States, money services business rules require administrators and exchangers of virtual currencies that are subject to the BSA and its AML program obligations, among other things, to register with FinCEN, verify customer identification, file various reports (including suspicious activity reports) with the U.S. government, create and maintain specified records, and respond to law enforcement requests.[30]

In addition, on March 21, 2014, the U.S. Internal Revenue Service ("IRS") issued IRS Notice 2014-21,[31] which defines virtual currencies, not as money, but as property. What this means is that the same recordkeeping requirements that exist for other forms of property will exist for virtual currencies. Under these rules, for example, every time you paid a bill using virtual currency, you would have to calculate your gain or loss on the virtual currency you used, and potentially pay taxes on any gain. Some payments (for example to an independent contractor who helps you to run your website) might require a U.S. entity to issue a Form 1099 (Misc.). For a firm subject to U.S. tax laws, failure to maintain the correct records or to file the correct reports may subject the organization or individuals to both civil and criminal penalties.

---

[26] Jennifer Shasky Calvery, "Remarks to the Association of Certified Anti-Money Laundering Specialists" (18th Annual International AML and Financial Crime Conference, Hollywood, Florida, March 19, 2013), available at http://www.fin-cen.gov/ news_room/speech/pdf/20130319.pdf (accessed 10 February 2014).

[27] Department of the Treasury, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies."

[28] Ibid., p. 3 (emphasis in the original, without footnote).

[29] Jennifer Shasky Calvery, "The Virtual Economy: Potential, Perplexities and Promises" (United States Institute of Peace, Washington, June 13, 2013).

[30] See, e.g. "Anti-money Laundering Programs for Money Services Businesses," 31 CFR 1022.210 (as amended July 29, 2011), "Reports by Money Services Businesses of Suspicious Transactions," 31 CFR 1022.320 (as amended July 29, 2011), and "Registration of Money Services Businesses," 31 CFR 1022.380 (as amended July 29, 2011), available at http://www.ecfr.gov (accessed 10 February 2014).

[31] U.S. Internal Revenue Service, "Notice 2014-21," (March 21, 2014), available at http://www.irs.gov/pub/irs-drop/n-14-21.pdf (accessed 28 March 2014).

Internationally, many countries have enacted similar AML regulatory regimes for money transmitters operating in their jurisdictions. The Financial Action Task Force ("FATF"), an independent intergovernmental body, has published "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," known as "the FATF Forty Recommendations."[32] The FATF Forty Recommendations include a recommendation (Recommendation 14) regarding money or value transfer services that states, in part: "Countries should take measures to ensure that natural or legal persons that provide money or value transfer services ("MVTS") are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations."[33] These measures include customer due diligence (Recommendation 10),[34] correspondent banking (Recommendation 13),[35] and reporting on suspicious transactions (Recommendation 20).[36] Additionally, the European Banking Authority has issued an opinion on virtual currencies[37]

One of the problems with any article on a current issue like virtual currencies is the velocity with which governments are evolving their attitudes and responses to these financial instruments. To get too specific guarantees the fact that the data will be out-of-date. Fortunately, the Decentralized Virtual Currency industry practice of a large international law firm, Perkins Coie, has established a webpage titled "Virtual Currencies: International Actions and Regulations," which provides a country-by-country update on the state of affairs in the field.[38]

The Case of Liberty Reserve

In what is described as possibly the largest online money laundering case ever brought by the U.S. government,[39] in May 2013, federal prosecutors charged Liberty Reserve, a Costa Rica-based currency transfer and payment processing company, with allegedly laundering billions of dollars, having conducted 55 million transactions that involved millions of customers around the world.[40]

According to the indictment: "The defendants deliberately attracted and maintained a customer base of criminals by making financial activity on Liberty Reserve anonymous and untraceable."[41]

---

32 Financial Action Task Force, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations" (February 2012), available at http://www.fatf-gafi.org/ media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (accessed 4 December 2014).

33 Ibid, p. 17.

34 Ibid, p. 14.

35 Ibid, p. 16.

36 Ibid, p. 19.

37 European Banking Authority, "EBA Opinion on 'Virtual Currencies,'" (Document EBA/Op/2014/08, 04 July 2014), available at http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies .pdf, (accessed 13 October 2014).

38 Perkins Coie LLP, "Virtual Currencies: International Actions and Regulations," at http://www.perkinscoie.com/en/ news-insights/virtual-currencies-international-actions-and-regulations.html (accessed 13 October 2014).

39 Marc Santora, William K. Rashbaum, and Nicole Perlroth, "Online Currency Exchange Accused of Laundering $6 Billion," *The New York Times*, May 28, 2013), available at http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html (accessed 10 February 2014).

40 Ibid.

41 Sealed Indictment, United States of America v. Liberty Reserve S.A., et al., Case 13 Cr. 368 (United States District Court, Southern District of New York, 20 May 2013), §8.

Liberty Reserve's digital currency was referred to as "LR."[42] To open an account at Liberty Reserve and trade in LRs, a user was required to provide name, address and date of birth.[43] However, unlike banks or legitimate money transmitters, Liberty Reserve did not require registering users to validate their identity by providing copies of official identification.[44] According to the indictment, "[a]ccounts could therefore be opened easily using fictitious or anonymous identities."[45] A user could also pay an extra fee, a 'privacy fee' of 75 U.S cents per transaction, to hide their account number on transactions, "effectively making the transfer completely untraceable."[46]

Indeed, "only a working, even if anonymous, email address," was all that was really required.[47] Liberty Reserve's failure to verify the identity of its users and the resultant anonymity it afforded made "Liberty Reserve a particularly attractive money transfer system for a criminal clientele seeking to launder criminal proceeds, to move funds to or from sanctioned jurisdictions and entities, or to finance terrorism internationally."[48]

The money trail was further obscured by Liberty Reserve's use of exchanges to act as middlemen between the user and Liberty Reserve. Users of Liberty Reserve were not allowed to deposit funds directly into their Liberty Reserve accounts, for example by credit card or cash deposits; nor were they able to make withdrawals directly from their Liberty Reserve accounts, for example through ATMs.[49] "Instead, Liberty Reserve users were required to make any deposits or withdrawals through the use of third-party 'exchangers,' thus enabling Liberty Reserve to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail."[50]

In a typical transaction, a Liberty Reserve account holder would have funds transferred from the account holder's regular bank account to a Liberty Reserve exchanger. The exchanger would convert the funds to Liberty Reserve's virtual currency and deposit the LRs into the account holder's Liberty Reserve account. From there, the account holder could transfer the LRs to another Liberty Reserve account or to another exchanger. The exchanger would convert the LRs into funds for transfer to a payee's bank account.[51] Liberty Reserve exchangers "tended to be unlicensed money transmitting businesses operating without significant governmental oversight or regulation, concentrated in Malaysia, Russia, Nigeria, and Vietnam."[52]

---

42 Ibid, §14.

43 Ibid.

44 Ibid.

45 Ibid.

46 Ibid, §15.

47 Department of the Treasury, "Notice of Finding that Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern," (May 28, 2013), §II.C, available at http://www.fincen.gov/statutes_regs/files/311—LR-Noticeof Finding-Final.pdf, (accessed 10 February 2014).

48 Ibid.

49 Sealed Indictment, United States of America v. Liberty Reserve S.A., et al, §16.

50 Ibid.

51 "How Liberty Reserve's Virtual Currency Works," *The New York Times* (May 28, 2013), at http://www.nytimes.com/interactive/2013/05/29/nyregion/how-liberty-reserves-virtual-currency-works.html (10 February 2014).

52 Sealed Indictment, "United States of America v. Liberty Reserve S.A., et al," §18.

Another key feature of Liberty Reserve transactions was that they could not be repudiated. As FinCEN, in the Liberty Reserve Notice of Finding, observed: "The fact that the transactions are irrevocable, meaning that they cannot be reversed or refunded in the event of fraud, makes it a highly desirable system for criminal use and a highly problematic one for any legitimate payment functions. Revocability protects merchants and users from fraud and is a common feature of legitimate payment systems."[53]

In sum, Liberty Reserve featured many of the characteristics that make virtual currencies attractive to terrorists, money launderers and criminals: anonymity, global reach, speed, non-repudiation, relative ease of use, difficult for authorities to track, potential upgrades to security and anonymity, and was located in a venue to make cooperation with governments difficult. Indeed, this was not just an abstract risk. According to the U.S. government, "a facilitator of a foreign extremist group in 2013 held a Liberty Reserve account, which may have been used to collect funds for the group."[54]

The Case of Bitcoin and Silk Road

For approximately two and a half years, an underground website known as Silk Road "was used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over a hundred thousand buyers, and to launder hundreds of millions of dollars derived from these unlawful transactions."[55] Silk Road sought to operate beyond the reach of law enforcement by:

(1) "[O]perating Silk Road on what is known as 'The Onion Router,' or 'Tor' network, a special network of computers on the Internet, distributed around the world, designed to conceal true IP addresses and therefore the identities of the networks' users. The Tor network is designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network;"[56] and

(2) Requiring "that all transactions on Silk Road be paid with Bitcoins, an electronic currency that is as anonymous as cash."[57]

Silk Road operated from January 2011, when it was established, until October 2, 2013, when the website was seized by law enforcement.[58] Silk Road could only be accessed through the Tor anonymizing network.[59] "Silk Road also used a so-called 'tumbler' which," as the site explained,

---

53 Department of the Treasury, "Notice of Finding that Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern," §II.E.

54 Ibid., at §II.D.

55 United States Attorney for the Southern District of New York, "Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of 'Silk Road' Website," (Press Release, October 25, 2013), available at http://www.justice.gov/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php (accessed 4 December 2014).

56 Ibid.

57 Ibid.

58 Sealed Complaint, United States of America v. Robert M. Faiella, a/k/a 'BTCKing,' and Charlie Shrem", (Southern District of New York, January 24, 2013), at §13.

59 Ibid., at §13b.

'"sen[t] all payments through a complex, semi-random series of dummy transactions... making it nearly impossible to link your payment with any coins leaving the site.'"[60] The tumbler "obscures any link between the buyer's Bitcoin address and the vendor's Bitcoin address where the Bitcoins end up — making it fruitless to use the 'Blockchain' to follow the money trail involved in the transaction, even if the buyer's and vendor's Bitcoin addresses are both known,' the complaint said."[61]

In addition to illegal drugs, Silk Road also offered online buyers access to such services as computer hacking, malicious software, pirated media content and "offers to produce fake driver's licenses, passports, Social Security cards, utility bills, credit card statements, car insurance records, and other forms of false identification documents."[62] In all, Silk Road is alleged to have generated the Bitcoin equivalent of "approximately $1.2 billion in sales and approximately $80 million in commissions."[63]

Like other virtual currencies, one source of vulnerability for Silk Road was its exchangers. In late January 2014, the U.S. Attorney's Office for the Southern District of New York brought charges against the operator of a Bitcoin exchange service, Robert Faiella, for running an exchange service

> directly on Silk Road that enabled Silk Road users to convert cash into Bitcoins anonymously. Faiella's customers could then use those Bitcoins to make illegal purchases on Silk Road. Faiella never registered as a money transmitting business, and he conducted transactions in a manner designed to enable Silk Road users to maintain their anonymity.[64]

A Tokyo-based Bitcoin exchange, Mt. Gox, had a U.S. account seized after a court issued a seizure warrant on May 14, 2013.[65] At the time of the account seizure, Mt. Gox was the world's largest Bitcoin exchange.[66] The seized account was alleged to have been used "to conduct transactions as part of an unlicensed money service business."[67]

---

60 United States Attorney for the Southern District of New York, "Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of 'Silk Road' Website."

61 Samuel Rubenfeld, "Prosecutors Expose 'Silk Road' Bitcoin Laundering Trail," *The Wall Street Journal* (October 2, 2013), available at http://blogs.wsj.com/riskandcompliance/2013/10/02/prosecutors-expose-silk-road-bitcoin-laundering-trail (accessed 10 February 2014).

62 United States Attorney for the Southern District of New York, "Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of 'Silk Road' Website."

63 Sealed Ex Parte Application for a Second Post-Complaint Protective Order, United States v. Ross William Ulbricht, Case No. 1:2013cv0691 (JPO) (Southern District of New York, October 24, 2013), p. 4.

64 Richard B. Zabel, "Prepared Testimony for the New York State Department of Financial Services Hearing on Law Enforcement and Virtual Currencies," (January 29, 2014), available at http://www.justice.gov/usao/nys/press speeches/2014/DFSLawEnforcementandVirtualCurrenciesHearing2014.php (accessed 13 October 2014).

65 Seizure Warrant, The Contents of One Dwolla Account**,** Case Number 13-1162 SKG (United States District Court, District of Maryland, May 14, 2013), available at http://s3.documentcloud.org/documents/701252/mt-gox-dwolla-warrant-5-14-13.pdf (10 February 2014).

66 Ibid, p. 2.

67 Ibid, p. 4.

Current Conundrum

Increasing regulatory oversight and law enforcement scrutiny notwithstanding, Bitcoins and virtual currencies are finding greater acceptance in the commercial world. The Sacramento Kings basketball team announced in January 2014 that they would become the first professional sports franchise to accept Bitcoins, after Overstock.com announced a month earlier that it would accept Bitcoins, becoming the first significant retailer to do so.[68]

A firearms dealer in Texas has started accepting Bitcoins in payment for guns.[69] They have even installed a Bitcoin automatic teller machine ('ATM') in their store for their customers' use. Under U.S. law, firearms dealers are required to do background checks, so the form of payment is somewhat irrelevant. However, sales of firearms between private individuals in Texas are not subject to background checks. The acceptance of Bitcoins in such a situation would make tracing the identity of the purchaser more difficult, as might be the case for a purely cash transaction.

Bitcoins were becoming increasingly popular in China, with BTC China recently becoming the world's largest Bitcoin exchange.[70] According to Bitcoincharts.com, a website that tracks Bitcoin activities, "Bitcoin is being used to pay for everything from cupcakes to electronics on the Internet, with almost 12 million Bitcoins in circulation."[71]

As virtual currencies become more widely accepted and play an ever-expanding role in commerce, governments have increasingly come to recognize that they are an emerging and potentially enduring reality. As the Deputy United States Attorney for the Southern District of New York recently noted, "we recognize first of all that virtual currency systems can be legitimate, innovative global commerce mechanisms that may offer advantages over other forms of payment. Some advantages can be efficiency, cost benefits, and certain desired privacy features."[72]

Yet, these very same features pose challenges to international security and the ability to deter and detect terrorist financing. As Mythili Raman, Acting Assistant Attorney General of the U.S. Department of Justice, testified before the United States Senate Committee on Homeland Security and Governmental Affairs on November 18, 2013:

---

68 Emily Flitter, "Prominent Bitcoin Entrepreneur Charged with Money Laundering."

69 Keith Wagstaff, "Texas Gun Dealers Draw Tech Crowd with Bitcoin," *NBCNews.com* (March 31, 2014), at http://www.nbcnews.com/tech/innovation/texas-gun-dealers-draw-tech-crowd-bitcoin-n65596 (accessed 13 October 2014).

70 Olga Kharif, "Bitcoin Climbs to Record on Wider Acceptance, China Trade," *Bloomberg* (November 7, 2013), available at http://www.bloomberg.com/news/print/2013-11-06/bitcoin-climbs-to-record-on-wider-acceptance-china-trade.html (accessed10 February 2014).

71 As cited in ibid.

72 Richard B. Zabel, "The New York State Department of Financial Services Hearing on Law Enforcement and Virtual Currencies."

> Our experience has shown that some criminals have exploited virtual currency systems because of the ability of those systems to conduct transfers quickly, securely, and often with a perceived higher level of anonymity than that afforded by traditional financial services. The irreversibility of many virtual currency transactions additionally appeals to a variety of individuals seeking to engage in illicit activity, as does their ability to send funds cross-border.[73]

In late 2013 and early 2014, a number of nations took steps to ban or at least strictly limit virtual currencies.

- Thailand was first.
- The Peoples Republic of China prohibited banks in the country from dealing in virtual currency.
- The Danish Financial Supervisory Authority has gone on record warning against the use of these non-governmental instruments.[74]
- On January 29, Russia's central bank published an official warning stating that Bitcoin transactions are illegal in Russia, and that any such transactions would be considered to be potentially suspicious acts.[75]
- On February 13, the central bank of Indonesia took similar steps, commenting that "Bitcoin and other virtual currencies are neither currency nor legal payment tools in Indonesia."[76]

Of course, the degree to which the use of virtual currencies can actually be controlled is questionable. Funds could be transferred to a country nearby the target, converted and moved into the target nation. Or given the difficulty of tracking the transactions, the laws or regulations could simply be ignored.

Investigative Approaches to Tracking Virtual Currency Transactions

In order to understand, analyze and respond to the challenge of virtual currencies and their use as vehicles for financing the activities of terrorist groups, governments must make an investment in training to build a cadre of experts who can approach the problem of tracking virtual currency transactions in a manner similar to forensic accountants separating truth from falsehood in a company's financial systems.

---

[73] Mythili Raman, "Beyond the Silk Road: Potential Risks, Threats and Promises of Virtual Currencies," (Remarks before the United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013), available at http://www.justice.gov/criminal/pr/speeches/2013/crm-speech-131118.html (accessed 10 February 2014).

[74] Dan Pototsky and Anna Kuchma, "Russia Becomes the Second Country to Ban Bitcoin," *Russia Beyond the Headlines* (February 5, 2014), available at http://rbth.ru/business/2014/02/05/russia_becomes_the_second_country_ to_ ban_bitcoin_33871.html (accessed 13 October 2014).

[75] Ibid.

[76] Jonathan Thatcher, "Indonesia Bans Use of Bitcoins, Other Virtual Currencies," *Reuters* (Feb. 6, 2014), available at http://uk.reuters.com/article/2014/02/06/uk-indonesia-bitcoin-idUKBREA150HV20140206, (accessed 13 October 2014).

Virtual currency systems are often designed to operate with great anonymity. They are unlike traditional funds transfer transactions, which "are denominated in existing fiat currencies (*e.g.*, dollars or Euros), explicitly identify the payer in transactions, and are centrally or quasi-centrally administered. In particular, there is a central controlling authority who has the technical and legal capacity to tie a transaction back to a pair of individuals."[77] For the law enforcement professional or antiterrorism analyst, this is certainly not good news. Yet we have seen (and cited documents relating to) recent cases in which purported criminals using the Bitcoin virtual currency have, in fact, been traced and arrested. How can an analyst trace what appears to be an anonymous transaction?

It turns out that many virtual currencies are not completely shrouded in cyberspace mysteries. Researchers have pointed out that as much as the proponents of these systems say that they are completely anonymous, they are not completely right. Cash transactions can be anonymous. I can agree to transfer £10,000 using essentially untraceable means, like throw-away unregistered cell phones. I put the cash in a jar and hide it in a pre-arranged location. At some later time, you retrieve the jar and get the money. Neither of us knows who the other is, and once our means of communication is severed (for example by throwing away the phones) we can't identify each other. That works because the medium of exchange — in this case British currency — is self-authenticating. I do not need anything to verify that it is real money (assuming that one party is not delivering counterfeit money to the other). I do not need to involve a third party.

The same is not true in the world of virtual currency. The authors of a recent paper point out that while virtual currency transactions (they use Bitcoin as an example) do not specifically identify the sender and recipient of funds, they are not the same as cash. Virtual currency transactions require third party mediation: a global peer-to-peer network of participants validates and certifies all transactions; such decentralized accounting requires each network participant to maintain the entire transaction history of the system, currently amounting to over 3 GB of compressed data. Bitcoin identities are thus pseudo-anonymous.

While not explicitly tied to real-world individuals or organizations, all Bitcoin transactions are completely transparent."[78] There is an important exception to this. Transactions between parties on a single private exchange do not use the standard method of transaction accounting, and those transactions would not be part of a globally available transaction directory. The ability of criminal elements to take advantage of this exception cannot be overlooked. The anti-money laundering community may be a powerful ally in identifying these emerging underground private exchanges.

For many interexchange transactions, the nature of the virtual currency process provides the analyst with valuable opportunities. As an example, assume that traditional intelligence techniques had enabled an analyst to learn the virtual currency wallet identifier used by a terrorist group; this is essentially the identification of the location where the terrorist group wants its virtual currency records — effectively, the virtual currency — stored. To send or receive virtual currency, you need

[77] Sarah Meiklejohn, et. al, "A Fistful of Bitcoins: Characterizing Payments among Men with No Names," (IMC 13 Conference of the Association for Computing Machinery (ACM), October 23–25, 2013, Barcelona, Spain), p. 1, available at http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (accessed 10 February 2014).

[78] Ibid.

a wallet. Since all wallets must be unique, they have a unique signature. To send virtual money to you, I have to know the address of your wallet. Let's assume that I deal with one exchange organization, and you deal with another. The transaction results in my getting the money, but there is a trail of a transaction between the recipient's wallet and the sender's exchange. Knowing what exchange was used by a terrorist financer is a useful data point. A subpoena, legal process or other forms of intelligence data collection can provide access to the exchange's records and determine the wallet identification of the sender. Further research may result in identifying the sender. The study cited earlier suggests that criminal users of virtual currencies are coming to understand the limits of anonymity and are seeking ways to make the job of the antiterrorism analyst harder.

Another data point that analysts can use involves the time of the transfer. When sifting through massive online virtual currency transaction records, characteristics like the exact time of the transfer and the exact amount of virtual currency can provide valuable search criteria.

One of the less obvious problems facing investigators in cases involving virtual currencies is the volatility of the companies that could (at least conceptually) be looked to for evidence. A major example of this involved what was one of the largest and unquestionably the most well-known organization that provided conversions between real currency and virtual currency. This exchange, located in Tokyo and called Mt. Gox, suddenly suspended real/virtual exchanges, disappeared from the Internet, and then filed for bankruptcy, claiming that hackers had stolen hundreds of millions of dollars worth of Bitcoins. While this case will play out – probably over the course of several years – in the press and in the courts, the lesson for investigators is that it is dangerous to assume that any organization that might hold evidence will be there when you are ready to act.

For individuals who lost Bitcoins in the Mt. Gox collapse, and for individuals and businesses that trade in virtual currencies more generally, the lesson may be that there is a role for governments in virtual currency consumer protection. Increased consumer protection can have the added ancillary benefit of increasing stabilization of a virtual currency's value. The take-away for governments may be that they do have a responsibility to oversee and regulate the virtual currency marketplace and that the time has arrived to engage the virtual currency community in serious dialogue to this end.

Another lesson that undoubtedly comes out of the Mt. Gox case is that unlike the vast majority of financial services firms across the globe, Mt. Gox was not founded to handle billions of dollars in transactions, nor did it, like long-lived firms, have the time to evolve the controls and security measures appropriate to the amounts of money — and the risk factors — involved. In the case of Mt. Gox, it was, amazingly, established to sell and trade cards that were part of a popular trading-card game called "Magic: The Gathering." In fact, the name "Mt. Gox" is an acronym for "Magic: The Gathering Online eXchange." By 2011, it had begun trading Bitcoins, and by April 2013, it was handling an estimated 70 percent of global Bitcoin trades.[79]

---

[79] Robert McMillan and Cade Metz, "The Rise and Fall of the World's Largest Bitcoin Exchange," *Wired* (November 06, 2013), available at http://www.wired.com/2013/11/mtgox/all/ (accessed 03 March 2014).

Recommendations for Action

Virtual currencies present a real and emerging challenge to the international community in its efforts to deter, detect and prevent terrorist financing. The very characteristics that make virtual currencies attractive to some — anonymity, low cost, speed, non-repudiation, decentralization and global reach — also make them potentially vulnerable to abuse by criminals, money launderers and terrorists. To date, different countries have taken different approaches to this challenge. Some have essentially barred their use. Others have begun to integrate virtual currencies into existing regulatory regimes. Most countries have yet to decide on an approach.

The following recommendations can address this extant challenge:

1. Update the Financial Action Task Force ("FATF") Recommendations to explicitly address virtual currencies - the FATF Recommendations "are universally recognized as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT)."[80] The latest version of the FATF Recommendations, dated February 2012, incorporates FATF's previously issued Nine Special Recommendations on Terrorist Financing.[81] As an intergovernmental body with the "mandate to deal with the issue of the funding of terrorist acts and terrorist organizations,"[82] FATF is well-placed to bring the international community together to harmonize standards on transparency, beneficial ownership, reporting of suspicious transactions and international cooperation, among other areas, for applicability to the new realm of virtual currencies.
2. Encourage the development of national (and international) self-regulatory organizations – one way to balance the commercial opportunity of virtual currencies with their potential for abuse by criminals and terrorists is to create non-governmental, self-regulatory organizations charged with overseeing virtual currency operations within a national jurisdiction. Self-regulatory organizations would provide the independence from governmental control sought by the virtual currency community while providing for consumer protection and transactional integrity through the application of disciplinary enforcement of operating rules agreed to by the virtual currency community in a particular jurisdiction and that jurisdiction's national authorities.
3. Encourage an increased level of cooperation, knowledge sharing and skills sharing between the agencies and organizations responsible for anti-money laundering activities with those responsible for the interdiction of terrorist financing – the commonalities in the need for data collection and analysis and the potential to use common tool sets can lead to more effective use of scarce analytic resources and can result in savings from joint licensing of software, systems and databases. There may be instances where data sharing agreements may be appropriate since many cases of terrorist funding also involve money laundering.

---

[80] Financial Action Task Force, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," p. 7.

[81] Ibid.

[82] Ibid.

4. In the interdiction of terrorist funding, understand the broad range of laws that may be available for the prosecution of offenders – sometimes it is easier to prove an economic crime like money laundering or operating an unlicensed money transmitter under existing laws than to directly prove that the funds were used for terrorism. This is nothing new. During the period of Prohibition in the United States (when the sale or purchase of alcoholic beverages was rendered unlawful as a result of a constitutional amendment), the U.S. Treasury Department recognized that sometimes it was substantially easier to prove crimes like tax evasion than it was to successfully prosecute for violations of the liquor prohibition laws. The gangster Al Capone was famously convicted in 1931 of tax evasion and failing to file tax returns, and served eight years in federal prisons. Where persons violate laws governing the use of virtual currencies, tax or regulatory violations may be an easier case to prove than to determine with certitude what specific funds were eventually used for.

5. Maintain vigilance with regard to the evolution of virtual currencies – you can be certain that those involved in money laundering, drug dealing, cybercrimes and terrorist financing are doing that, and you cannot afford to let them gain an operational or technical edge on your ability to investigate and interdict unlawful funding of terrorism.

Conclusion

In recent years, we have seen the introduction of a new form of money known as virtual (or crypto-) currency. These currencies — Bitcoin is the best known — are non-fiat, *i.e.,* they are neither issued by nor backed by any sovereign government in the world. This currency only exists as entries in online ledgers. For the most part, these virtual currencies can be transferred from person to person (or group to group) anywhere in the world, and essentially instantaneously. And also, in some circumstances, neither the sender nor the recipient need identify themselves.

The global nature of virtual currencies, their anonymity and similar factors have led to growing adoption of virtual currencies like Bitcoin in many environments. For example, you can make purchases from Overstock.com and pay in Bitcoins. You can purchase a season ticket to Sacramento Kings basketball games. And in some places, you can even buy a pizza pie with Bitcoins. But those same characteristics are, perhaps, even more attractive to those involved in terrorist funding, money laundering and other forms of financial crime. They seek the ability to move funds across national borders quickly and quietly, and at low cost. They obviously crave anonymity. They want to be able to collect money in multiple countries and to convert them to a common currency which can be distributed easily to specific destinations and converted to local currencies.

The rapid growth of virtual currencies has become a challenge to governments around the world. Some have chosen to ban these non-sovereign currencies. Others are attempting to regulate them and require both registration of trading firms and imposition of anti-money laundering regulations. But even with such controls, the recent shutdown of the Silk Road website, which provided a marketplace for illegal drugs and other criminal activities, showed that virtual currencies were being used to fund a wide range of unlawful activities. The failure of the Mt. Gox Bitcoin exchange, with the announced loss of hundreds of millions of U.S. dollar equivalents in Bitcoins, also indicates that as of today, dealing in virtual currencies can be a very risky investment.

Virtual currencies represent a challenge for every national government. How they should be exploited to take advantage of their promise to provide fast, safe and low-cost global funds transfers must be viewed relative to the risks associated with these currencies being used to facilitate and obfuscate transactions related to criminal activities, including money laundering, trading in illicit drugs, moving the proceeds of human trafficking, and serving as a vehicle for funding of terrorist groups.

The challenge for governments will be to gain the maximum advantage while minimizing the risks of misuse of these payment systems and payment vehicles. Navigating the fast-evolving waters of virtual currencies will not be easy for any government, but failing to do so is simply unacceptable. Ignoring the issue will facilitate the misuse of these currencies (including for the financing of terrorist activities). Ignoring the problem empowers criminals to launder money, fund drug deals, and support terrorism and a range of undesirable outcomes. Ignoring the problem, or not making the investment in time, training, staffing and technology to meet the problem, gives the criminals a real advantage, one that we cannot afford to give them and certainly, an advantage that they do not deserve.

BIBLIOGRAPHY

Albergotti, Reed, and Jeffrey Sparshott, "U.S. Alleges $6 Billion Money-Laundering Operation at Liberty Reserve", *Wall Street Journal* (May 28, 2013).

Asian News International, "eBay Likely to Launch Own Virtual Currency", DNAIndia (3 January 2014).

"Bitcoin: Monetarists Anonymous", *The Economist* (Sep. 29, 2012).

Boise, Craig M., "Playing with 'Monopoly Money': Phony Profits, Fraud Penalties and Equity", *Minnesota Law Review* 90(1) (2005).

Brook, Chris, "Google Removes Bitcoin Mining Android Malware From Play", *ThreatPost* (April 28, 2014).

Calvery, Jennifer Shasky, "Remarks to the Association of Certified Anti-Money Laundering Specialists" (18th Annual International AML and Financial Crime Conference, Hollywood, Florida, March 19, 2013).

Calvery, Jennifer Shasky, "Remarks to the National Cyber-Forensics Training Alliance" (CyFin 2013 Conference, Pittsburgh, PA, April 16, 2013).

Calvery, Jennifer Shasky, "The Virtual Economy: Potential, Perplexities and Promises" (United States Institute of Peace, Washington, June 13, 2013).

Calvery, Jennifer Shasky, "Statement Before the United States Senate Committee on Banking, Housing, and Urban Affairs, Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy" (November 19, 2013).

European Banking Authority, "EBA Opinion on 'Virtual Currencies'" (Document EBA/Op/2014/08, 04 July 2014).

Financial Action Task Force, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations" (February 2012).

Flitter, Emily, "Prominent Bitcoin Entrepreneur Charged with Money Laundering", *Reuters* (Jan. 27, 2014).

"How Liberty Reserve's Virtual Currency Works", *The New York Times* (May 28, 2013).

Huang, Danny Yuxing, et al., "Botcoin: Monetizing Stolen Cycles" (Network and Distributed System Security *(*NDSS*)* Symposium, 23-26 February 2014).

Kelly, Samantha Murphy, "Report: Android Malware is Mining Bitcoin While You Recharge", *Mashable* (Mar. 27, 2014).

Kharif, Olga, "Bitcoin Climbs to Record on Wider Acceptance, China Trade", *Bloomberg* (November 7, 2013).

Krebs, Brian, "Botcoin: Bitcoin Mining by Botnet", *Krebs on Security* (July 13, 2013).

McMillan, Robert, and Cade Metz, "The Rise and Fall of the World's Largest Bitcoin Exchange", *Wired* (November 06, 2013).

Meiklejohn, Sarah, et. al, "A Fistful of Bitcoins: Characterizing Payments among Men with No Names" (IMC 13 Conference of the Association for Computing Machinery (ACM), October 23–25, 2013, Barcelona, Spain).

Pierson, Ryan M., "How Gamers Make Real Money from Video Games", *Locker Gnome* (20 April 2012).

Pototsky, Dan, and Anna Kuchma, "Russia Becomes the Second Country to Ban Bitcoin", *Russia Beyond the Headlines* (February 5, 2014).

Raman, Mythili, "Beyond the Silk Road: Potential Risks, Threats and Promises of Virtual Currencies" (Remarks before the United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013).

Rubenfeld, Samuel, "Prosecutors Expose 'Silk Road' Bitcoin Laundering Trail", *The Wall Street Journal* (October 2, 2013).

Santora, Marc, William K. Rashbaum, and Nicole Perlroth, "Online Currency Exchange Accused of Laundering $6 Billion", *The New York Times* (May 28, 2013).

Thatcher, Jonathon, "Indonesia Bans Use of Bitcoins, Other Virtual Currencies", *Reuters* (Feb. 6, 2014).

U. S. Attorney for the Southern District of New York, “Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of ‘Silk Road’ Website” (Press Release, October 25, 2013).

U.S. Department of Homeland Security, “Quadrennial Homeland Security Review Report: A Strategic framework for a Secure Homeland” (1 February 2010).

U.S. Department of the Treasury, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (Financial Crimes Enforcement Network, Publication FIN-2013-G001, March 18, 2013).

U.S. Department of the Treasury, “Notice of Finding that Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern” (May 28, 2013).

Wagstaff, Keith, “Texas Gun Dealers Draw Tech Crowd with Bitcoin”, *NBCNews.com* (March 31, 2014).

Zabel, Richard B., “Prepared Testimony for the New York State Department of Financial Services Hearing on Law Enforcement and Virtual Currencies” (January 29, 2014).

Defence Against Terrorism Review
Vol. 6, No. 1, Spring&Fall 2014, pp. 31-46

ISSN: 1307-9190

Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States

Uchenna Jerome Orji
Research Associate at the African Centre for Cyber Law and Cybercrime Prevention (ACCP), Kampala, Uganda.
jeromuch@yahoo.com

Abstract: *The increasing interconnectivity of countries and national critical infrastructures in today's global network society have ushered the world into what has been aptly described as "an age of interdependence where each nation's security is also dependent on the actions of the other nations of the world." This state of affairs clearly underscores the need for the collective responsibility of states for global cybersecurity. This article explores some prospects towards enhancing the collective responsibility of states to deter cyberterrorism. It particularly suggests the need for a state to be held accountable where its failure to establish regulatory measures to deter or prosecute cybercrimes or cyberterrorism within its territory has allowed the perpetration of such acts and the causation of transboundary effects in other states.*

Keywords: *Cyberterrorism, information society, collective responsibility, legal framework, transboundary effects, attribution, critical information infrastructure*

Introduction

The emergence of the information society following the integration of computer and digital communications technologies into all aspects of life has redefined traditional notions of security. Malicious conduct against computer systems and networks now has the potential to affect individuals, countries and the global economy in ways previously unimagined. Consequently, one of the most critical challenges of the information society has been the need to deter cyberterrorism. For the purposes of this article, cyberterrorism refers to terrorist attacks against computers and networked infrastructure which aim to hinder the operation of critical infrastructures and further terrorist objectives by causing the loss of lives, panic, widespread economic failure or intimidation in order to affect political conduct. This article examines the concept of cyberterrorism and suggests that the increasing interconnectivity of countries and national critical infrastructures in the global network society underscores the need for the collective responsibility of states for global cybersecurity, including the deterrence of cyberterrorism. Accordingly, this article proposes several strategies towards enhancing the collective responsibility of states to respond to cyberterrorism. This includes *inter alia* the need for every state to establish appropriate deterrent legal measures that would ensure that activities in cyberspace that are conducted within its jurisdiction do not cause transboundary harm in other states. It particularly suggests the need for a state to be held accountable where its failure to establish regulatory measures to deter or prosecute cybercrimes or cyberterrorism within its territory has allowed the perpetration of such acts and the causation of transboundary effects in other states.

Defining Cyberterrorism

'Cyberterrorism' is a term that is used to classify malicious activities that embody the twin elements of cybercrime and terrorism. According to Judge Stein Schjølberg,[2] "terrorism in cyberspace consists of both cybercrime and terrorism. Terrorist attacks in cyberspace are a category of cybercrime and a criminal misuse of information technologies. The term 'cyberterrorism' is often used to describe this phenomenon."[3] In a constricted sense, the term 'cyberterrorism' refers to the unlawful use of computers and networked communications infrastructure to carry out disruptive acts or attacks with the aim of hindering the operation of critical infrastructures[4] such as transport, energy and communications sectors or "threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in

---

1 *See* Lt. Gen. Harry D. Raduege *(Ret.)* "Fighting Weapons of Mass Disruption: Why America Needs a 'Cyber Triad', in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed., East West Institute, 2010), p. 13.

2 Judge Stein Schjølberg (Justice of the Court of Appeal, Norway) is the Chairman of the EastWest Institute Cybercrime Legal Working Group and also the Chairman of the International Telecommunication Union (ITU), High Level Expert Group (HLEG) on Cybersecurity that produced the ITU Global Security Agenda in 2008. Cybercrime Law, Biography of Stein Schjolberg, at http://www.cybercrimelaw.net/biography.html (accessed 14 October 2014).

3 See Stein Schjølberg, *Terrorism in Cyberspace – Myth or reality?* (NATO Advanced Research Workshop on Cyberterrorism, Sofia, Bulgaria, October 2007), p. 3, available at http://www.cybercrimelaw.net/ documents/Cyberterroism.pdf (accessed 14 October 2014).

4 "Critical infrastructures" refer to key infrastructures or sectors that are vital to the functioning of modern societies. What constitutes critical infrastructure varies in different countries, however, where the prolonged disruption of a sector or infrastructure would affect the well being of a nation by causing severe military and economic dislocation then such sector or infrastructure would qualify to be classified a "critical infrastructure." Sectors that are classified as critical infrastructure include (but are not limited to the following): banking and finance: government services: telecommunication/ information and communication technologies (ICTs); emergency/rescue services; energy/electricity; health services; transportation, logistics, distribution, and water (supply). *See* Uchenna J. Orji, *Cybersecurity Law and Regulation* (Wolf Legal Publishers, 2012), pp. 24-30.

furtherance of political or social objectives"[5] or other terrorist objectives. Thus, in this regard, the term cyberterrorism is used to define any act of terrorism that uses information systems or computer technology either as a weapon or as a target.

However, in a more generic sense 'cyberterrorism' may be used to broadly classify unlawful activities relating the terrorist use of the Internet, or threats or actual malicious acts carried out either by physical or virtual means against computers, networks, or critical infrastructures with the intention to cause harm or to coerce a government or its people in furtherance of social, ideological, religious, or political objectives. Here the term is used more broadly to refer to physical or virtual acts of terrorism that use computer information systems and also includes the terrorist use of networked information communications technologies to carry out activities such as spreading terrorist propaganda, propagating terrorist ideology, mobilizing recruits and supporters, gathering information, preparing for real world attacks and financing terrorist activities. While the above definitions are not comprehensive, there is currently no internationally accepted definition of 'cyberterrorism.' However, there has been an attempt to forge a legal definition of the term in the Draft Proposal for an International Convention on Cybercrime and Terrorism which was developed in 1999 as a proposal to globally address cybercrime following the conference on "International Cooperation to Combat Cybercrime and Terrorism" at the Stanford University in the United States.[6] The Draft Convention defines 'cyberterrorism' as the "intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cybersystems,[7] when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm."[8] However, other definitions of cyberterrorism appear not limit the target to only cybersystems but also includes any terrorist attack carried out through the Internet or against cyberinfrastructure.

Another legal definition of 'cyberterrorism' is found in the Black's Law Dictionary where it was defined as "terrorism committed by using a computer to make unlawful attacks and threats of attacks against computers, networks, and electronically stored information, and actually causing the target to fear or experience harm."[9] Although the above definitions may not be comprehensive, however, they maybe used to establish a minimum standard of what can be regarded as cyberterrorism.

---

5 *See* Dorothy Denning, "Cyber Terrorism" (Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000). Regarding the definitions of cyberterrorism, see generally, Sarah Gordon and Richard Ford, *Cyberterrorism?* (Symantec Security Response, 2003).

6 *See* Abraham D. Sofaer, et al, *A Proposal for an International Convention on Cyber Crime and Terrorism,* unpublished, August 2000, available at http://www.iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf (accessed 14 October 2014); *see* Abraham D. Sofaer, "Towards an International Convention on Cyber Crime" in *The Transnational Dimension of Cyber Crime and Terrorism* (Seymour E. Goodman, and Abraham D. Sofaer, eds., Hoover Institution Press, 2001), p. 225.

7 A "cyber system" is defined as "any computer or network of computers used to relay, transmit, coordinate or control communications of data or programs.". *See* Article 1(3), Draft International Convention on Cyber Crime and Terrorism in Sofaer,, *A Proposal for an International Convention on Cyber Crime and Terrorism,*

8 *See* Article 1(2) Draft International Convention on Cyber Crime and Terrorism. Ibid.

9 *Blacks Law Dictionary* (8th Edition, West Group, 2004), p. 1513.

The effect of a malicious act in cyberspace or the intent of a malicious actor in cyberspace may also be used to determine situations where an act of cyberterrorism has occurred. For example, the effect of a malicious act may be classified as cyberterrorism when such causes disruptive effects that are enough to generate fear comparable to a traditional act of terrorism, even if such acts were done by mere criminals.[10] In determining whether the effects of an attack qualify as cyberterrorism, Professor Denning notes that:

> To qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[11]

On the other hand, the intent of a malicious actor may be used to classify an act as cyberterrorism where for example unlawful attacks are carried out against computer systems with the aim of hindering the operation of critical infrastructures to achieve objectives such as intimidating or coercing a government or people or to further a social, political or religious objective, or to cause grave harm or severe economic damage in a society.[12] For example, if a criminal hacks into a bank customer's account and steals credit card information, such activity may be referred to as mere cybercrime, because the intent of the criminal actor is neither political nor social. However, if similar attacks are directed to a substantial number of bank accounts and the responsible criminal actor declares that he/she is going to continue attacks until the government accepts his demands then such conduct is labeled as cyberterrorism.[13] As such, once there is a terrorist intent common acts of cybercrime may constitute cyberterrorism. Such acts include hacking, virus dissemination, website defacing, denial-of-service (DoS) attacks, disrupting critical information infrastructures, and issuing threats to disrupt computer-based infrastructure either by virtual or physical means.

Exploring Prospects to Enhance the Collective Responsibility of States to Deter Cyberterrorism

Responding to cyberterrorism has been a challenging issue. Due to the universal nature of information networks, virtual terrorist attacks can be launched from anywhere in the world. Tracing the origin of such terrorist attacks in cyberspace is usually a huge challenge, assuming the attacks are even detected at all. This is because of the ability of terrorists to use anonymous communication

---

10 John Rollins and Clay Wilson, "Terrorist Capabilities for Cyber Attack: Overview and Policy Issues," (RK 33123, CRS Report for Congress, January 22, 2007), p. 3, available at http://fas.org/sgp/crs/terror/ RL33123.pdf (accessed 8 December 2014).

11 *See* Denning, *Cyber Terrorism.*

12 *See* Rollins and Wilson, "Terrorist Capabilities for Cyber Attack: Overview and Policy Issues."

13 *See* Murat Dogrul, Adil Aslan, and Eyyup Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in *Proceedings of the 3rd International Conference on Cyber Conflict* (NATO/CCD COE Publications, 2011, pp. 31-32, available at http://www.ccdcoe.org/publications/2011proceedings/Developing AnInternationalCooperation...-M.%20Dogrul-Aslan-Celik.pdf (accessed 14 October 2014).

facilities and encryption technology to hide their identity, as well as loop attacks through computer systems in various countries that may not have cybercrime laws[14] and other deterrence mechanisms. Thus, terrorist actors may originate or transmit cyberattacks from jurisdictions where legal mechanisms and other cybersecurity measures are either weak, not yet in existence or from permissive jurisdictions that appear to provide safe havens for such conduct by not prosecuting such actors or permitting their extradition. Hence, countries that do not have cybercrime laws apparently create safe havens for cyberterrorist activities. This is because in countries where malicious cyberactivities have not been criminalized, any related conduct by malicious actors may not be successfully prosecuted on the basis of the principle of *nullum crimen nulla poena sine lege*.[15] This principle implies that a person shall not be convicted of a criminal offence unless that offence is defined and the penalty is prescribed in a written law.[16]

However, with the growing application of information technologies in all aspects of life and the increasing interconnectivity of national critical infrastructures and global information networks, all states are now exposed to the threats and vulnerabilities, such as cyberterrorism, that affect an information society. Consequently, effective solutions to address these threats and vulnerabilities will require the active cooperation of all state actors in the global information society. A major step towards addressing this challenge is for all states to establish cybercrime laws that prohibit terrorist conduct in the information society. Every state is a stakeholder in the global information society; hence, it follows that every state has a duty to take reasonable and appropriate measures towards securing this society by ensuring that cyberactivities within its jurisdiction do not cause transboundary harm in other states. This underscores the collective responsibility of states for global cybersecurity. This concept is already entrenched in Article 5A of the International Telecommunication Regulations which provides that:

> Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public.[17]

Member states of the International Telecommunication Union (ITU) are also under an obligation to implement its regulations in a manner that respects and upholds their human rights obligations.[18] One way of implementing the regulations is through the establishment of legal measures to ensure the security and robustness of international telecommunication networks. Thus, within this concept of collective responsibility, there is an implied primary duty on every state to establish regulatory

---

[14] *See* Marco Gercke, *Understanding Cybercrime: A Guide for Developing Countries* (ITU, 2009), pp. 51-57.

[15] Latin for 'no crime or punishment without a law,' a basic principle of criminal law

[16] *Blacks Law Dictionary*, p. 1098.

[17] *See* Final Acts of the World Conference on International Telecommunications, *International Telecommunication Regulations*, (International Telecommunication Union, 2012); *see also* Article 45(1) of the Constitution of the International Telecommunication Union, available at http://www.itu.int/ en/history/Pages/ConstitutionAndConvention.aspx (accessed 25 November 2014).

[18] *See* Article 1, Constitution of the International Telecommunication Union. Ibid.

frameworks designed to provide an effective deterrent system and crossborder cooperation against cyberterrorist conduct that may affect the security and robustness of international telecommunication networks or cause transboundary harm. A state's failure to fulfill such duty should give rise to liability, since states have been held responsible where activities within their territories produced harmful transboundary effects in other countries. For example, in the *Trail Smelter Arbitration* that arose from a transboundary air pollution dispute between the United States and Canada, where damage had been caused to property in the United States due to air pollution which had originated in Canada, the arbitral tribunal held that "no State has a right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence."[19]

The decision of the arbitral tribunal laid the foundation in establishing the principle that a state shall not "permit the use of its territory in such a manner as to cause injury in or to the territory of another."[20] This principle has now been enshrined in some aspects of international environmental and human rights law. Thus, "international law already requires states to control activities that may cause transboundary harm."[21] Consequently, states can be held responsible where activities within their territories produce harmful transboundary effects in other countries. In *Cyprus v. Turkey*,[22] the European Courts of Human Rights held that the responsibility of states can arise as a result of acts and omissions of their authorities which produce effects outside their own territory.[23] Accordingly, Professor Alan Boyle has also argued that:

> …human rights law could in appropriate circumstances have extra-territorial application if a state's failure to control activities within its territory affects life, health, private life or property in neighboring countries. If states are responsible for their failure to control soldiers and judges abroad, *a fortiori* they should likewise be held responsible for a failure to control transboundary pollution and environmental harm emanating from industrial activities inside their own territory.[24]

---

19 *See* "The Trail Smelter Arbitral Decision", *American Journal of International Law* 35 (1941), p. 684.

20 *See* Cesare P.R. Romano, *The Peaceful Settlement of International Environmental Disputes: A Pragmatic Approach* (Kluwer Law International, 2000), p. 261.

21 *See* Principle 2, Rio Declaration on the Environment and Development, U.N.Doc.A/CONF.151/ 5/REV.1,31.I.L.M.874 (1992); Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports (1996) 226, at para 29; Articles on Trans-boundary Harm, ILC Report (2001) GAOR A/56/10, 366; *Tatar v. Romania* [2009] ECHR, para 111; *Osman v. the United Kingdom*, judgment of 28 October 1998, Reports 1998-VIII, p. 3164; *Calvelli and Ciglio v. Italy* [GC], no. 32967/96, ECHR 2002-IX, and *August v. the United Kingdom*, no. 36505/02, 21 January 2003; Alan Boyle, "Human Rights and the Environment: A Reassessment" (UNEP Paper Revised, 2010), p. 27; Thomas Gehring and Markus Jachtenfuchs, "Liability for Trans-boundary Environmental Damage Towards a General Liability Regime?" *European Journal of International Law* 4 (1993), pp. 92-106.

22 [2001] ECHR No.25781/94; Alan Boyle, "Human Rights and the Environment: A Reassessment," *Fordham Environmental Law Review* 18 (2008), pp. 471-511; Boyle, "Human Rights and the Environment: A Reassessment," p. 26.

23 *Ibid.*

24 Ibid, p. 27.

To some extent, the norm that states may be held responsible for acts and omissions within their territories which produce transboundary harm in other countries may be applied for the purpose of promoting the concept of the collective responsibility of states for global cybersecurity.[25] Thus, where a state's failure to promote cybersecurity by establishing appropriate regulatory mechanisms to deter malicious cyberconduct has given rise to the existence of a safe haven for cybercriminality, that state should be held responsible for any transboundary harm that arises from the perpetration of cybercrimes in that safe haven. This implies that a state should be held responsible where its failure to establish adequate cybercrime laws and other deterrent regulatory measures within its territory has encouraged the perpetration and non-prosecution of cybercrimes that affected other states or individuals or organizations located in other states. The case of the "I LOVE YOU" Virus provides an example in this regard. The virus was created in 2000 by Onel de Guzman (a Filipino computing student at the AMA Computer University in Manila, Philippines) and spread worldwide through the Internet - infecting over 45 million computers and causing businesses billions of dollars in losses. Many of the affected businesses were located in the United States which had already established laws prohibiting cybercrime. When FBI agents succeeded in identifying the creator of the virus in Philippines, it was also found that the country did not have cybercrime laws under which he could be prosecuted. Philippines had an extradition treaty with the United States. However, there was no basis to apply for Onel de Guzman's extradition under the treaty, since Philippines had not criminalized the creation and spreading of computer viruses at that time.[26] Consequently, he was able to escape criminal liability for the enormous damage caused by the spread of the "I LOVE YOU" virus.[27] However, within the concept of the international norm that states may be held responsible for acts and omissions within their territories which produce transboundary harm in other countries, there are prospects that Philippines could have been held responsible for the transboundary effects of the "I LOVE YOU" virus, since the country failed to establish regulatory measures that might deter such cybercrimes or enable its prosecution. Thus, if a state can be held responsible for failure to control territorial activities that may cause transboundary harm, then there is a prospect that a state may also be held accountable where the failure to establish regulatory measures to deter or prosecute cybercrimes within it territories has allowed the perpetration of cybercrimes or acts of cyberterrorism that caused transboundary effects in other states.

Another step that would enhance the collective responsibility of states to deter cyberterrorism is the establishment of a single international treaty of all nations on cybersecurity. Thus, considering the ubiquitous nature of the information society and the transnational nature of cyberterrorism, a safe haven for cyberterrorism can only be eliminated if all states have access to one enforceable

[25] *See generally*, "*A Conceptual Approach for Setting a Standard of Care for cCross-border Internet* (Discussion paper of the Council of Europe Ad Hoc Advisory Group on Cross-border Internet for Workshop 6: Sovereignty of States and the Role and Obligations of Governments in the Global Multi-stakeholder Internet Environment, European Dialogue on Internet Governance (EuroDIG), Madrid, 28-29 April 2010),

[26] Following the incident, Government of the Philippines introduced the Electronic Commerce Act of 2000 (RA 8792) to criminalize the dissemination of computer viruses and other cybercrimes. Gilbert C. Sosa, "Country Report on Cybercrime: The Philippines" (UNAFEI, 140th International Training Course Participants' Papers, undated), p. 80.

[27] See Shannon C. Sprinkel, "Global Internet Regulation: The Residual Effects of the 'I LOVEYOU' Computer Virus and the Draft Convention on Cyber-Crime", *Suffolk Transnational Law Review* 25, (2002), pp. 492-493.

global cybersecurity treaty that defines and prohibits cybercrimes, including cyberterrorism, also creates a framework for mutual assistance amongst state parties. The adoption and ratification of such a global treaty by states will technically eliminate safe havens for perpetrators, since every state will have an obligation to deter, prosecute or assist other states in tackling cybercrimes and cyberterrorism. Thus, in order to ensure effective collective responsibility of states to deter cyberterrorism, it is imperative that such global treaty imposes obligations on states to establish legal measures to deter cyberterrorist activities and also enhance effective cross-border cooperation for the prevention or investigation and prosecution of such activities. Consequently, if potential perpetrators of cyberterrorism are aware that they cannot hide in any country in the world, they may to some extent be discouraged from committing such acts. However, the absence of such an international treaty has been an obstacle to the global harmonization of cybersecurity laws. This has also hindered the effective promotion of the concept of the collective responsibility states for global cybersecurity. Thus, the establishment of a global treaty on cybersecurity is imperative to secure the harmonization of cybersecurity laws amongst all sovereign states. Accordingly, a global treaty on cybersecurity would enhance a better understanding of cyberterrorism and other aspects of cybersecurity, and facilitate the development and deployment of measures that can help to increase resilience to the impacts of cyber threats.[28] Such a treaty would provide the minimum standards for the criminalization of cyberterrorism and serve as the basis for the global harmonization of related national laws. This has a great prospect of encouraging international cooperation to the widest extent possible amongst state parties for the purposes of investigations or legal proceedings concerning cyberterrorism.

The concept of a harmonized legal environment where all sovereign states can have access to one global treaty calls for the negotiation of an international cybersecurity treaty under the aegis of the United Nations General Assembly. Accordingly, Judge Stein Schjølberg argues that:

> Cyberdeterrence may best be achieved within a global framework of a United Nations Cyberspace Treaty on cybersecurity and cybercrime. Regional and bilateral conventions or treaties will not be sufficient. International law should provide the framework for peace and security in cyberspace.[29]

The United Nations has been working toward developing initiatives for an international treaty on cybersecurity;[30] however; there has also been a lack of consensus amongst states on what the focus of a cybersecurity treaty should be. For example, while Russia highly favors a cybersecurity treaty to regulate cyberwar or information warfare,[31] on the other hand the United States highly

---

[28] *See* Solange Ghernaouti-Hélie, "Need for a United Nations Cyberspace Treaty," (*WISIS Forum 2010-High-Level Debate on Cybersecurity and Cyberspace* (ITU, Geneva, 10-14 May, 2010), p. 1.

[29] Ibid, p. 13. *See also* Solange Ghernaouti-Hélie, "Need for a United Nations Cyberspace Treaty," p. 2. (where Professor Ghernaouti-Hélie made similar arguments).

[30] Orji, *Cybersecurity Law and Regulation*, pp. 96-112.

[31] Ibid, pp. 204-207; Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity", in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway*, pp. 6-8; Dorothy Denning, "Obstacles and Options for Cyber Arms Controls," *Arms Control in Cyberspace* (Heinrich Böll Foundation, Berlin, Germany, June 29-30, 2001), pp. 4-5.

favors the criminalization of malicious conducts against computer systems by individual actors[32] as well as international cooperation to improve mutual legal assistance and extradition.[33] Also while states like China filter and prohibit certain information that may harm or damage the stability of state power as a part of their cybersecurity program,[34] other states like the United States see such activities as an impediment to free speech.[35] However, the United Nations has also been working toward developing initiatives to improve consensus on cybersecurity. In July 2010, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (a group of cybersecurity specialists and diplomats representing 15 countries which was established in 2009 pursuant to the United Nations General Assembly Resolution 60/45)[36] agreed on a set of recommendations for negotiations on an international computer security treaty which were transmitted to the United Nations Secretary General.[37] The Group of Experts Report noted *inter alia* the need for further dialogue amongst states to discuss norms pertaining to state use of ICTs to reduce collective risk and protect critical national and international infrastructure; the need for information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices; and the need for states to find possibilities to develop common terms and definitions relating to cybersecurity.[38]

Aside from the United Nations, some other international organizations have also developed initiatives to improve consensus on cybersecurity. An example is the Council of Europe, which developed the Council of Europe Convention on Cybercrime.[39] The Convention which currently has about forty-three state parties[40] is recognized as the only international treaty on cybercrime. It criminalizes four different categories of substantive offences in its Articles 2-10:

(1) offences against the confidentiality, integrity and availability of computer data and systems;

(2) computer-related offences;

(3) content-related offences and;

(4) offences related to infringements of copyright and related rights.

---

[32] Office of the President of the United States of America, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (The White House, Washington D.C., May 2011), p. 10; Paul Cornish, et al, *On Cyber Warfare* (The Royal Institute of International Affairs, Chatham House, 2010), p. 23.

[33] Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (U.S. Department of Defense, May 1999), p. 47.

[34] Uchenna J. Orji, "An Analysis of China's Regulatory Response to Cybersecurity", *Computer and Telecommunications Law Review* 7 (2012), pp. 212-226.

[35] Office of the President of the United States of America, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, pp. 5 and 10; Tang Lan and Zhang Xin, "Can Cyber Deterrence Work?" in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway*, p. 2.

[36] *See* United Nations General Assembly Resolution 60/45, para 4.

[37] See United Nations General Assembly, *Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Document A/65/201 (30 July 2010).

[38] Pauline C. Reich, et al, "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity," *European Journal of Law and Technology* 1(2) (2010), pp. 9-11.

[39] *See* the Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

[40] A list of state parties to the Convention is available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (accessed 14 October 2014).

The above offences have been used by the Convention's state parties and several other states to establish a minimum standard of what can be regarded as cybercrime or computer crime.[41] As such the above offences can be regarded as establishing the consensus of the Convention's state parties on what constitutes a cybercrime since state parties have an obligation to ensure the criminalization of those offences in their municipal laws.[42]

Another example of consensus building on cybersecurity is the bilateral cooperation of experts from Russia and the United States under the auspices of the EastWest Institute[43] which produced twenty consensus terms on cybersecurity and information security. The terms are meant to serve as a conceptual framework to facilitate the challenging process of creating definitions for a common international lexicon on cybersecurity and information security. The effort is also intended to establish a foundation for international agreements or "rules of the road" on cyberspace and information security.[44] There has also been a similar bilateral cybersecurity initiative between experts from the United States and China under the auspices of the EastWest Institute.[45] Apparently, these developments indicate that there are prospects that the negotiation process for the development of a global cybersecurity treaty will enhance the development of a common standard for the criminalization of malicious cyberconduct, such as cyberterrorism and also facilitate the development of effective platforms for cross-border legal cooperation in that regard.

It is also imperative to enhance global research efforts towards the creation of an international system for the accurate attribution of any cyberattack or hostile action in cyberspace.[46] Accordingly, the Center for Strategic and International Studies (CSIS) report on cybersecurity aptly emphasizes that, "creating the ability to know reliably what person or device is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy."[47] Presently, the challenges of accurately attributing cyberattacks to a particular entity affects the categorization of cyberattacks as acts of terrorism or acts of war. For example, various incidents of cyberattacks in several countries such as Estonia and the United States have been categorized as acts of cyberwarfare and cyberterrorism in the media and speculatively linked to Russia[48] and China,[49] however given

---

41 *See* Stein Schjølberg, "The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva" (unpublished, 2008), pp. 8-9, available at http://www.cybercrimelaw.net/documents/cybercrime _history.pdf (accessed 14 October 2014).

42 *See* ITU High Level Experts Group (HLEG), "ITU Global Cyber-Security Agenda (GCA)," *High Level Experts Group [HLEG] Global Strategic Report* (ITU, 2008), p. 16; Orji, *Cybersecurity Law and Regulation*, p. 119.

43 Further information about the activities of the EastWest Institute with respect to the development cybersecurity initiatives is available at EastWest Institute, "Cyberspace," at http://www.ewi.info/issues/cyberspace (accessed 14 October 2014).

44 *See generally*, Karl Frederick Rauscher and Valery Yaschenko, *Russia-U.S. Bilateral on Cybersecurity- Critical Terminology Foundations* (EastWest Institute and the Information Security Institute of Moscow State University, 2011).

45 *See* Karl Frederick Rauscher and Zhou Yonglin, *China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust* (EastWest Institute, 2011).

46 *See* Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity," in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway*, p. 6.

47 *See* James A. Lewis, et al., *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th* Presidency (Center for Strategic and International Studies, December 2008), p. 62.

48 *See* Paul Meller, "Cyberwar: Russia vs Estonia", *Networkworld.com* (May 24, 2007) available at http://www.network-world.com/news/2007/052207-ec-urges-coordinated-effort-against.html (accessed 14 January 2012).

49 *See* Susan Landau, "National Security on the Line," *Journal of Telecommunications and High Technology Law* (2006), p. 429; *see generally* Micah Schwalb, "Exploit Derivatives and National Security," *Yale Journal of Law and Technology* 9 (2007), p. 162.

that these attacks were not traced with certainty to state or terrorist organizations, it becomes difficult to clearly categorize those incidents as cyberwarfare or acts of cyberterrorism. This has given rise to a state of mutual distrust which has been detrimental to international relations and prompting several accusations, denials and counteraccusations of state-sponsored cyberattacks between countries such as United States and China,[50] as well as Estonia and Russia. Thus, the problem of attribution presents the advantage of anonymity to terrorists since they can loop through different computer systems in the process of perpetrating cyberattacks or even orchestrate attacks to appear to originate from government computers in another country. Consequently, terrorists can employ cyberattacks to strike at the heart of society or infrastructure from a remote location or an unidentifiable address.[51] However, it has been shown that the establishment of trusted identification systems in Public Key Infrastructure (PKI) can help address the problem of attribution. For example, it is noted that the frequency of unauthorized intrusions into the United States Department of Defense (DOD) network decreased by 50 percent following the DOD's introduction of a new identification system (Common Access Card) to address authentication in 2008.[52] While this solution may not be possible on a global scale, it underscores the fact that the development of authentication mechanisms for digital identities will enhance attribution in cyberspace.

To address the challenge of attribution, it has also been aptly suggested that states such as Russia and the United States should champion the idea of establishing a binding multilateral agreement on Public Key Infrastructure (PKI) to promote internationally an "ecosystem" of trusted identities under the auspices of the International Telecommunication Union (ITU).[53] However, while such an arrangement is yet to come to life, there are prospects that the development of common ITU standards for the verification of networked digital devices would enhance attribution in cyberspace. Apparently, such mechanisms may raise concerns over anonymity in cyberspace, as well as fears of censorship and the infringement of the human rights to the freedom of expression and privacy by governments. This however underscores the need for an appropriate balance between Internet freedom/human rights and cybersecurity measures.

There is also need to enhance the capabilities of multilateral systems for early warning and cyberincident management. This will entail the strengthening of information sharing capacities of multilateral institutions such as the International Multilateral Partnership against Cyber Threats (IMPACT),[54] the NATO Cooperative Cyber Defense Centre of

---

[50] *See* Elizabeth M. Lynch, "Adam Segal Discusses U.S.-China Relations in a Cyber World," *China Law & Policy*, (April 14, 2010), available at http://chinalawandpolicy.com/2010/04/14/adam-segal-discusses-u-s-china-relations-in-a-cyber-world/. (accessed 14 January 2012).

[51] Paul Cornish, et al, *On Cyber Warfare* (The Royal Institute of International Affairs, Chatham House: London, 2010) p. 11.

[52] *See* Lewis, *Securing Cyberspace for the 44th Presidency.*

[53] Franz-Stefan Gady and Greg Austin, *Russia, The United States, and Cyber Diplomacy: Opening the Doors* (EastWest Institute, 2010), p. ii.

[54] The IMPACT operates a comprehensive Global Response Centre (GRC) which is designed to be the foremost cyber threat resource centre in the world. It aims to provide the global community with a real-time aggregated early warning system and assist member countries in the early identification of cyber-threats and also provides guidance on the necessary remedial measures. Through is way, the IMPACT plays a pivotal role in the realization of the ITU's Global Cybersecurity Agenda (GCA) objective of establishing technical measures to combat new and evolving cyber threats. *See* The International Multilateral Partnership Against Cyber Threats (IMPACT), at http://www.impact-alliance.org/ (accessed 14 October 2014).

Excellence[55] and the 24/7 Network of Contacts under the Council of Europe Convention on Cybercrime.[56] Apparently, many countries find it difficult to share critical cybersecurity information due to domestic sensitivities associated with national security. However, strengthening the capacities of these institutions on the basis of common interests or collective security in order to enhance the ability of their member states to share information, resources, and best practices on cybersecurity will go a long way towards facilitating timely warnings and responses to transnational cyberincidents such as cyberterrorism. This approach will require states to harmonize their cybersecurity and countercyberterrorism interests within the framework of multilateral institutions such as the IMPACT, the NATO Cooperative Cyber Defense Centre of Excellence and the 24/7 Network of Contacts and also share resources and best practices to facilitate their collective interests.

To further enhance the concept of the collective responsibility of states to promote global cybersecurity and deter cyberterrorism, it may also be necessary to develop international mechanisms for blacklisting states that do not develop standard regulatory measures to deter cybercrimes. A similar approach has been applied by the Financial Action Task Force (FATF) in fighting global money laundering.[57] Also, despite the absence of efficient attribution mechanisms, the development of a multilateral platform that is similar to the FATF may to some extent facilitate the prevention of some forms of cyberterrorism such as DoS attacks. This will require member states to agree to impose obligations on Internet Service Providers to scan the data traffic going to and from computers attached to their networks for unusual patterns of traffic that indicate botnet (zombie)[58] activity, and disconnect the associated computers.[59]

---

[55] The NATO Cooperative Cyber Defense Centre of Excellence is responsible for conducting research and training in cyber defense. In accordance with NATO collective security agenda, the major objective of the cyber defense centre is to help member states achieve collective self defense in the cyberspace by defying and countering threats of cyber warfare.

[56] *See* Article 35, Council of Europe Convention on Cybercrime. The establishment of the 24/7 network is hinged on the need to ensure a "round the clock" efficiency of mutual assistance requests and also to enhance the efficiency and speed of international cybercrime investigations. The Convention provides that each State party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence regarding a criminal offence under the Convention. Presently, countries that have not signed or ratified the Convention can join in the 24/7 network of contacts. *See* Report of the Second Meeting of the Cybercrime Committee T-CY (2007) 03 p. 3, cited in Gercke, *Understanding Cybercrime: A Guide for Developing Countries*, p. 215.

[57] *See* Financial Action Task Force (FATF), "High Risk and Non-Cooperative Jurisdictions," available at http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236992_1_1_1_1_1,00.html (accessed 14 October 2014).

[58] "Botnet" is a short term for a group of compromised computers running programmes that are under external control (also known as "zombie armies" or "drone armies"). Botnets may comprise networks of coordinated groups of several tens, hundreds or even thousands of computing devices such as PCs, laptops and even the new generation of mobile devices such as "smart phones" all infected with the same virus or other malware and compromised to turn them into "zombies" or "robots." Such computers can be controlled without the owner's knowledge. Criminals use the collective computing power and connected bandwidth of these externally-controlled networks for malicious purposes and criminal activities such as launching of Distributed Denial of Service (DDoS) attacks. *See* ITU (ICT Applications and Cybersecurity Division Policies and Strategies Department-ITU Telecommunications Development Sector) *Botnet Mitigation Toolkit* (ITU, 2008, pp. 1 and 5; *see also* Alana Maurushat, "Zombie Botnets", *SCRIPTed,* 7(2) (August 2010), pp. 371-383.

[59] *See* Lillian Edwards, "The Internet and Security: Do We Need a Man with a Red Flag Walking in Front of Every Computer," *SCRIPT-ed* 4(1) (March 2007), p. 1.

Conclusion

With the increasing interconnectivity of countries and national critical infrastructures in the global network society, the world has leaped into an age that has been aptly described as "an age of interdependence where each nation's security and prosperity is increasingly dependent on the actions of the other nations of the world."[60] This state of affairs underscores the need for the collective responsibility of states for global cybersecurity including the deterrence of cyberterrorism. States that fail to establish appropriate cybercrime laws would create safe havens for cybercrimes that would include cyberterrorism. Under international law, states are already under an obligation to "prevent and suppress in their territories through all lawful means the preparation and financing of any acts of terrorism."[61] Lawful measures to prevent and suppress the preparation and financing of terrorism include the establishment and harmonization of legal mechanisms to deter cyberterrorism and also enhance effective cross-border cooperation for the prevention or investigation and prosecution of such conduct. Thus, despite varying levels of digital development and economic disparity amongst states, a major step toward realizing the concept of the collective responsibility of all states to deter cyberterrorism should commence with the establishment of national regulatory mechanisms that eliminate safe havens for cybercrime as well as well as the facilitation of international cooperation to the widest possible extent.

BIBLIOGRAPHY

Boyle, Alan, "Human Rights and the Environment: A Reassessment" (UNEP Paper Revised, 2010).

Boyle, Alan, "Human Rights and the Environment: A Reassessment", *Fordham Environmental Law Review* 18 (2008).

Cornish, Paul, et al, *On Cyber Warfare* (The Royal Institute of International Affairs, Chatham House, 2010).

Denning, Dorothy, "Cyber Terrorism" (Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000).

Denning, Dorothy, "Obstacles and Options for Cyber Arms Controls", *Arms Control in Cyberspace* (Heinrich Böll Foundation, Berlin, Germany, June 29-30, 2001).

Dogrul, Murat, Aslan, Adil, and Celik, Eyyup, "Developing an International Cooperation on Cyber

[60] Harry D. Raduege, "Fighting Weapons of Mass Disruption: Why America Needs a 'Cyber Triad', in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway*, p.13.

[61] *See United Nations Security Council Resolution 1373* (September 28, 2001); the *United Nations Security Council Resolution 1269* (October 19, 1999); the *International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations in Resolution 54/109 (9 December 1999); Article 4 of the African Union Convention on The Prevention and Combating of Terrorism (1994); and the United Nations Global Counter-Terrorism Strategy (2006).

Defense and Deterrence against Cyber Terrorism", in *Proceedings of the 3rd International Conference on Cyber Conflict* (NATO/CCD COE Publications, 2011).

Edwards, Lillian, "The Internet and Security: Do We Need a Man with a Red Flag Walking in Front of Every Computer", *SCRIPT-ed* 4(1) (March 2007).

Gady, Franz-Stefan and Austin, Greg, "Russia, The United States, And Cyber Diplomacy: Opening the Doors" (EastWest Institute, 2010).

Gehring, Thomas and Jachtenfuchs, Markus, "Liability for Trans-boundary Environmental Damage Towards a General Liability Regime?" *European Journal of International Law* 4 (1993).

Gercke, Marco, *Understanding Cybercrime: A Guide for Developing Countries* (ITU: Geneva, 2009).

Gordon, Sarah, and Ford, Richard, "Cyberterrorism?" (Symantec Security Response, 2003).

Grigoriev, Dmitry I., "Russian Priorities and Steps Towards Cybersecurity" in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed., East West Institute, 2010).

Ghernaouti-Hélie, Solange, "Need for a United Nations Cyberspace Treaty", *WISIS Forum 2010-High-Level Debate on Cybersecurity and Cyberspace* (ITU, Geneva, 10-14 May 2010).

ITU High Level Experts Group (HLEG), "ITU Global Cyber-Security Agenda (GCA)", *High Level Experts Group [HLEG] Global Strategic Report* (ITU, 2008).

ITU, *Botnet Mitigation Toolkit* (ITU, 2008).

Lan, Tang and Xin, Zhang, "Can Cyber Deterrence Work?" in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed., East West Institute, 2010).

Landau, Susan, "National Security on the Line" *Journal of Telecommunications and High Technology Law* 4 (2006).

Lewis, James A., et al., "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" (Center for Strategic and International Studies, December 2008).

Lt. Gen. Raduege, Harry D. *(Ret.)* "Fighting Weapons of Mass Disruption: Why America Needs a "Cyber Triad", in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed.i East West Institute, 2010).

Lynch, Elizabeth M. "Adam Segal Discusses U.S.-China Relations in a Cyber World", *China Law & Policy* (April 14, 2010).

Maurushat, Alana, "Zombie Botnets", *SCRIPTed* 7(2) (2010).

Meller, Paul, "Cyberwar: Russia vs Estonia", *Networkworld.com* (May 24, 2007).

Office of the President of the United States of America, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (The White House, May 2011).

Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (U.S. Department of Defense, May 1999).

Orji, Uchenna J., “An Analysis of China’s Regulatory Response to Cybersecurity”, *Computer and Telecommunications Law Review* 7 (2012).

Orji, Uchenna J., *Cybersecurity Law and Regulation* (Wolf Legal Publishers, 2012).

Rauscher, Karl Frederick and Yaschenko, Valery, *Russia-U.S. Bilateral on Cybersecurity- Critical Terminology Foundations* (EastWest Institute and the Information Security Institute of Moscow State University, 2011).

Rauscher, Karl Frederick and Yonglin, Zhou, *China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust* (EastWest Institute, 2011).

Reich Pauline C., et al, “Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity”, *European Journal of Law and Technology*, 1(2)(2010).

Rollins, John and Wilson, Clay “Terrorist Capabilities for Cyber attack: Overview and Policy Issues” (RL 33123, CRS Report for Congress, January 22, 2007).

Romano, Cesare P.R., *The Peaceful Settlement of International Environmental Disputes: A Pragmatic Approach* (Kluwer Law International, 2000).

Schjølberg Stein, “The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva” (unpublished, December 2008).

Schjølberg, Stein, “Terrorism in Cyberspace – Myth or reality?” (NATO Advanced Research Workshop on Cyberterrorism, Sofia, Bulgaria (October 2007).

Schjølberg, Stein, “Wanted: A United Nations Cyberspace Treaty” in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed., East West Institute, 2010).

Schwalb, Micah, “Exploit Derivatives and National Security”, *Yale Journal of Law and Technology* 9 (2007).

Sofaer, Abraham D., et al**,** “A Proposal for an International Convention on Cyber Crime and Terrorism” (unpublished, August 2000).

Sofaer, Abraham D. “Towards an International Convention on Cyber Crime” in *The Transnational Dimension of Cyber Crime and Terrorism* (Goodman, Seymour E. and Sofaer, Abraham D., eds., Hoover Institution Press, 2001).

Sosa, Gilbert C., “Country Report on Cybercrime: The Philippines” (UNAFEI, 140th International Training Course Participants’ Papers, undated).

Sprinkel, Shannon C., “Global Internet Regulation: The Residual Effects of the ‘I LOVEYOU’ Computer Virus and the Draft Convention on Cyber-Crime”, *Suffolk Transnational Law Review* 25 (2002).

The Blacks Law Dictionary (8th Edition: West Group, 2004).

“The Trail Smelter Arbitral Decision”, *American Journal of International Law* 35 (1941).

The Council of Europe, “Convention on Cybercrime” 41 I.L.M. 282 (Budapest, 23.XI, 2001).

Defence Against Terrorism Review
Vol. 6, No. 1, Spring&Fall 2014, pp. 47-62

ISSN: 1307-9190

Improvements Required for Operational and Tactical Intelligence Sharing in NATO

Stewart Webb
Editor for DefenceReport.com
swebb@defencereport.com

Abstract: *Intelligence sharing within the ISAF structure was an issue in the Afghan Theatre of Operations (ATO). It has been accepted that improvements are needed within the American intelligence structures, however contributing state caveats played a role in creating this situation. The International Security Assistance Force (ISAF) consisted of 46 contributing countries, with 28 of them being NATO members. It is evident that counterinsurgency operations are here to stay even with the ISAF drawdown in Afghanistan. Globalized terrorism still remains one of the key threats in NATO strategic planning. In January 2013, French forces intervened in the Malian conflict to support regional African troops by reversing the gains of the Tuareg rebellion that was hijacked by militant Islamist insurgent groups. Although it was not a NATO-sanctioned mission, French forces were supported by European Union members, Canada and the United States. EU members continued to assist in the training of Malian government forces, while the United States provided intelligence support and Canada provided strategic airlift capabilities. NATO, under the Connected Forces Initiative, is moving from operational engagement to operational readiness through an increase in exercises and measures that aim to improve interoperability. If there is anything to be learned from the Afghan and Libyan deployments, it is that NATO intelligence sharing potentially could be the proverbial Achilles Heel of the Alliance.*

Keywords: *Smart Defence Initiative, Connected Forces Initiative, Libya Air Campaign, Mali, Intelligence Sharing, Joint Operations Planning Process*

Introduction

The International Security Assistance Force (ISAF) is currently drawing down its deployment in Afghanistan. This was the first major international multinational deployment for NATO since the breakup of Yugoslavia and it was the first time the alliance has conducted a prolonged counterinsurgency (COIN) operation. The age of the interstate conflict seemed to dissipate into a new reality of sustained COIN operations after the 11 September 2001 attacks.

After twelve years of sustained operations, NATO has been able to identify various interoperability issues and come up with solutions. One issue that has yet to be resolved fully is the sharing of tactical intelligence in coalition operations. Lieutenant General Marc Lessard, commander of Canada's Expeditionary Force Command, believes that intelligence sharing and other enablers within NATO have proved to be difficult.[1] It has also been recognised that it took too long to develop a counterinsurgency strategy and to understand the cultural, political and tribal sensitivities in Afghanistan.[2] The nuances of ethnic and tribal traditions that have developed over centuries would be difficult to grasp in the first few years. However, there was little shift into developing a COIN strategy because of the American and British involvement in Iraq.

With the popular uprising in Libya and the United Nations Security Council's consent, NATO coordinated fourteen members and four non-members of the alliance to impose the 'no-fly' zone and maritime blockade. The Libyan Air Campaign also proved to be problematic for sharing intelligence. French fighter jets did not use American surveillance performed by Unmanned Aerial Vehicles (UAVs) or satellites. This is because it was taking too long for French pilots to be cleared for access American imagery intelligence (IMINT).[3] The US Department of Defense Inspector General found that improvements were needed in dissemination of tactical intelligence to ISAF coalition partners.[4]

The 2012-2013 Malian conflict erupted out of consequence of the Libyan Air Campaign. A historical and socio-economic assessment of the greater region would have demonstrated the need to strengthen regional borders to stem the migration of trained and armed ethnic fighters. It is not just a matter of how NATO members share their information, but also a question of an expanded assessment before conducting operations.

In 2007, the NATO Intelligence Fusion Center (NIFC) became fully operational and able to provide "intelligence to warn of potential crisis and to support the planning and execution of NATO operations; to include direct intelligence support to NATO Special Operations Forces."[5] The NIFC was created under a US-sponsored Memorandum of Understanding.[6]

---

1 Chicago Council on Global Affairs, "Smart Defense and the Future of NATO: Can the Alliance Meet the Challenges of the Twenty-First Century?," (Chicago, Illinois, 28-20 March 2012), p. 6.

2 Ibid.

3 Robert Densmore. "French Pilots Over Libya Decline US Intel; Clearance Just Too Slow," *Breaking Defense* (21 September 2011), at http://breakingdefense.com/2011/09/french-pilots-over-libya-decline-us-intel-clearance-just-too-sl/ (accessed 15 May 2014).

4 Department of Defense Inspector General, "Results in Brief: Improvements Needed in Sharing Tactical Intelligence with International Security Assistance Force-Afghanistan" (Report 11-INTEL-13, 18 July 2011), available at http://www.dodig.mil/Ir/reports/ISAFRIB002.pdf (accessed 15 May 2014).

5 NATO Intelligence Fusion Center, "What is the NIFC?" at http://web.ifc.bices.org/about.htm (accessed 15 May 2014); for a list of operations supported, see NATO Intelligence Fusion Center, "Support to Operations," at http://web.ifc.bices.org/ops.htm (accessed 15 May 2014).

6 NATO Intelligence Fusion Center. "What is the NIFC?"

There have to be improvements to NATO members' intelligence sharing in order to make the alliance's campaigns more effective and efficient. Intelligence is one of the major pillars for special operations. Special operations forces (SOF) rely on actionable intelligence to conduct their missions. It is also the cornerstone of an effective COIN operation. More importantly, intelligence sharing is the ultimate demonstration of trust and interoperability. After the prolonged COIN operation in Afghanistan and the difficulties that in Libya, NATO's intelligence-sharing capabilities need to be improved to show the utility of the Alliance.

Intelligence and Intelligence Sharing

Military intelligence can be divided into different categories: strategic, operational and tactical. Strategic intelligence concentrates on the larger picture of political intelligence, and the highest level of the military, which involves force posturing by hostile governments and their capabilities.[7] Operational intelligence is current intelligence on the enemy that includes, "leadership, force organization, dislocations, readiness, mobilization, foreign suppliers and possible technical capabilities."[8] Tactical intelligence combines operational intelligence, but includes data and developments on combat, enemy tactical misjudgements, indigenous political and ethnic developments, indigenous attitudes and terrorism and counterinsurgency.[9] Operational and tactical intelligence has the greatest impact on theatre operations.

Much of NATO's intelligence in Afghanistan has been concentrated on the enemy combatants (i.e, the Taliban and other insurgent groups), and not on the political, economic or cultural environment.[10] This has led to the ethos of an anti-insurgency campaign bent on the elimination of the insurgent threat, rather than a counterinsurgency campaign which advocated a holistic approach and focuses not only on the combatant but the indigenous population or human environment in which the insurgent operates.[11] Actionable COIN intelligence was stymied in the Afghan Theatre of Operations (ATO) with this mentality. Without discerning the powerholders and their concerns, according to David Kilcullen, local populations had set up ambushes and stalled reconstruction projects violently in protest.[12]

---

7 Friedrich W. Korkisch, "NATO Gets Better Intelligence: New Challenges Require New Answers to Satisfy Intelligence Needs for Headquarters and Deployed/Employed Forces" (Institut für Aussen- und Sicherheitpolitik Strategy Paper 1-2010, April 2010), p. 14, available at http://www.natowatch.org/sites/default/files/ NATO_Gets_ Better _Intell_April_PDP_0.pdf (accessed 15 May 2014).

8 Ibid.

9 Ibid.

10 Major General Michael T. Flynn, Captain Matt Pottinger, and Paul D. Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan" (Center for New American Security, January 2010), p. 7, available at http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf (accessed 15 May 2014).

11 Ibid., p. 23.

12 David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (Oxford University Press, 2013), pp. 3-17.

Pre-Operational Concerns

Before Afghanistan, NATO had not dealt with a high-level insurgency operation. NATO has provided peacekeeping and peacemaking operations in the Balkans and for decades has prepared for a conventional war with the Soviet Union. NATO must conduct historical and regional impact assessments to ensure that measures are undertaken to reduce the probability of violent fallout.

The initial operation supporting the Afghan Northern Alliance against the Taliban was heralded as a success. It is known that the Taliban and al-Qaeda leadership sought refuge in the Federally-Administered Tribal Areas (FATA) in Pakistan, a tactic that the Afghan *mujahideen* utilised during the Soviet invasion of Afghanistan as displaced Afghans sought refuge in Pakistan.

The Soviet Union was unable to sever these mountainous links between Afghanistan and Pakistan along the Durrand line. This proved to be the downfall for the Soviet occupation of Afghanistan. The Pakistani links with the Afghan Taliban, Haqqani Network, al-Qaeda, and other insurgent groups proved to be difficult to handle. In fact, during the Soviet occupation the Haqqani majahideen cell was integral to the smuggling of fighters and vital supplies. The Haqqani Network was permitted to evolve from small hit-and-run tactics and propaganda activities in 2004 to one of the most prominent insurgent groups in the region. It begun after an insult to the Haqqani family as Jalaluddin Haqqani, the former notable mujahideen commander, was not invited to the Bonn Conference in 2001 because he was a Taliban minister. His archrival and American supporter, Pacha Khan Zadran, was invited to the conference in his place.[13] However, given unaddressed grievances with the local population, the Haqqani family was able to build its support base and realign its efforts. An ideal historical assessment would include regional actors and integrate them within the overall COIN strategy.

Lessons have been learnt on how missions should be planned and carried out since the initial deployment in the ATO. The Joint Operations Planning Process (JOPP) was created in 2006 and assists commanders with their day-to-day operations while offering a strategic overview with an environmental framing that consists of political, military, economic, social, information, and infrastructure (PMESII) constructs.[14] Utilising a JOPP approach provides a clearer image on how an operation will affect the theatre and the indigenous population. NATO should utilise the JOPP approach to maintain of the indigenous political and social-political nuances that affect (or feed) insurgencies. NATO can improve upon the JOPP approach by carrying out regional historical assessments and by creating an awareness of regional characteristics that could pose an impediment to NATO's efforts and spread violence into surrounding regions.

NATO's air campaign over Libya provides an example of why a historical assessment of the surrounding regions is necessary. The instability caused by the Libyan Air Campaign was a major catalyst for the 2012-2013 Malian Conflict. To date Mali has experienced four ethnic Tuareg rebellions

[13] Thomas Ruttig, "Loya Paktia's Insurgency: The Haqqani Network as an Autonomous Entity," in *Decoding the New Taliban: Insights from the Afghan Field* (Antonio Giustozzi, ed., Columbia University Press, 2009), p. 66.

[14] Dan McCauley, "Design and Joint Operation Planning," *Canadian Military Journal* 12(1) (2011), p. 32, available at http://www.journal.forces.gc.ca/vol12/no1/doc/CMJ%20Vol12%20No1%20Page30-40%20McCauley%20 Eng.pdf (accessed 1 December 2014).

as consequences of ethnic strife between the Arab-descended Tuaregs in Northern Mali and the ethnic Africans in the south. Since Mali's independence and subsequent conflicts, droughts and rampant poverty, many ethnic Tuaregs have migrated. For decades, ethnic Tuaregs found refuge in Colonel Gaddafi's regular army and in the Libyan-sponsored Islamic Legion.[15]

The last rebellion was started by a coalition between the secular, secessionist Tuareg group, *le Mouvement National de Libération de l'Azawad* (MNLA) and a partnership of militant Islamist groups. This was the first instance where the ethnic Tuareg cause involved militant Islamist groups - Ansar al-Dine, Movement for Unity and Jihad in West Africa (MUJAO), and al-Qaeda in the Islamic Mahgreb (AQIM). However, the seeds for insurgency were already apparent years before NATO's air campaign.

USAID figures in 2004 illustrated the rampant poor socio-economic conditions; the three largest towns in Northern Mali have these average poverty rates: Timbuktu, 77 percent; Gao, 78.7 percent and Kidal, 92 percent.[16] Poor socio-economic conditions, a history of multiple rebellions and severe droughts have caused a substantial migration of ethnic Tuaregs. Colonel Gadaffi's regime welcomed them openly into the Libyan Armed Forces and portrayed them as 'Lords of the Desert.'[17]

France's colonial history with the region provides France with a unique picture of the region that many countries do not have. Intelligence ties in former French colonial territories continue to exist. American SOF relations with the region were established with the Pan Sahel Initiative after 9/11.[18] American Special Forces were training Malian government forces on border security. It is true that the fourth Tuareg rebellion occurred after the Libyan Air Campaign, but the campaign was a catalyst for the rebellion. The United Nations cites that regional countries reported that "…rocket propelled grenades, machine guns with anti-aircraft visors, automatic rifles, ammunition, grenades, explosives (Semtex), and light anti-aircraft artillery (light calibre bi-tubes) mounted on vehicles" were being smuggled out of Libya.[19] This coincided with an estimated 420,000 displaced people of which approximately 30,000 returned to Mali.[20] A historical assessment of the region would have illustrated that a migration of trained and well-armed ethnic Tuaregs would spark another insurgency in Mali given the desperate socio-economic conditions at the time. Measures, such as strengthening the Pan Sahel Initiative or training Malian government forces, could have been thusly taken to reduce the impact.

---

15 Yehudit Rohen, "Libya, the Tuareg and Mali on the Eve of the 'Arab Spring' and in its Aftermath: An Anatomy of Change Relations," *Journal of North African Studies* 18(4) (2013), p. 545, available at http://www.tandfonline.com/doi/abs/10.1080/13629387.2013.809660#preview (accessed 1 December 2014); Scott Shaw, "Fallout in the Sahel: The Geographical Spread of Conflict from Libya to Mali," *Canadian Foreign Policy Journal* 19(2) (2013), p. 203, available at http://www.tandfonline.com/doi/abs/10.1080/ 11926422.2013.805153#preview (accessed 1 December 2014).

16 Hussein Soloman. "Mali: West Africa's Afghanistan," *RUSI Journal* 158(1) (2013), p. 13, available at http://www.cerium.ca/IMG/pdf/Mali_-_West_Africa_s_Afghanistan.pdf (1 December 1, 2014).

17 Rohen, "Libya, the Tuareg and Mali on the eve of the 'Arab Spring," p. 546.

18 Phillip Ulmer, "Special Forces Support Pan Sahel Initiative in Africa" (American Forces Press Service, 8 March 2004), available at http://www.defense.gov/News/NewsArticle.aspx?ID=27112 (accessed 15 May 2014).

19 United Nations Security Council. "Report of the Assessment Mission on the Impact of the Libyan Crisis on the Sahel Region" (UN Doc S/2012/42, 18 January 2012), p. 10, available at http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Libya%20S% 202012%2042.pdf (accessed 15 May 2014).

20 Ibid., p. 6.

For future NATO interventions, it is imperative that NATO undertakes measures to ensure that violent spillover does not transcend borders, or at least mitigate the impact with preventative measures – including enhancing the capabilities of neighbouring countries. If not, this may lead to: safe havens for insurgent networks, new insurgencies taking root in surrounding regions or both scenarios. It is also imperative that NATO coalition partners disseminate tactical and operational intelligence within the coalition more freely.

Afghanistan Lessons

Major General Flynn's report for the Center of New American Security: *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* can provide a benchmark to improve military intelligence collection, analysis and dissemination for tactical intelligence for COIN operations.[21] Major General Flynn argues that intelligence in the Afghan COIN operation should be demarcated by territorial lines rather than functional lines and collect data from a myriad of on-the-ground sources, including but not limited to: "civil affairs officers, PRTs, atmospherics teams, Afghan liaison officers, female engagement teams, willing non-governmental organizations and development organizations, United Nations officials, psychological operations teams, human terrain teams, and infantry battalions."[22] This does not solve the issue that tactical and operational intelligence needs be to disseminated throughout the coalition more freely. In Afghanistan, coalition partners were given different regions and provinces to operate in; however the intelligence cannot stop at these demarcations as the insurgency does not respect those borders.

Gaining trust and leverage with indigenous power holders is pivotal to winning a COIN operation. Major General Flynn asserts that "guerrilla warfare as a tactical-level information operation is laden with strategic significance far more than in conventional conflicts."[23] Tactical information is to be collected by those on the ground. COIN operations are not a science; there is no formulaic equation that solves an insurgency.

Organizational structures were created within the Allied Operation Command during the prolonged Afghan mission. ISAF did create the Afghan Mission Network to boost intelligence-sharing capability. It was only possible after the United States announced that it would share sensitive technology that would counter the Improvised Explosive Device (IED) threat, which accounted for the majority of ISAF casualties.[24] The Afghan Mission Network is comprised of a high-speed broadband link between 63 locations to improve the access of operational information and databases to coalition members.[25]

---

[21] See Flynn, Pottinger, and Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan."

[22] Ibid., p. 4.

[23] Ibid., p. 11.

[24] David Brunnstrom. "NATO Launches Afghan Intelligence-sharing Drive," *Reuters* (15 July 2010), at http://www.reuters.com/article/2010/07/15/us-nato-afghan-intelligence-idUSTRE66E5YL20100715 (accessed 15 May 2014)

[25] Ibid.

The Afghan Mission Network had caveats though, "NATO officials conceded there would be different levels of access depending on the sensitivity of information, and it would remain the prerogative of countries to decide whether to share intelligence."[26] A greater need to proliferate operational and tactical intelligence across the coalition is needed. In a COIN operation, there is the notion of 'competitive control' where the COIN contingent, whether military or civilian, attempts to gain the population's support by demonstrating their ability to govern the region.

There have also been allegations that NATO members were paying off Afghan insurgents not to attack the ISAF contingent. In 2009, ten French soldiers were killed, and twenty-one wounded, in the Surobi District of Kabul. It was alleged that the Italian intelligence services were paying the local insurgents off,[27] an occurrence that the French were unaware of when they took over the district. These allegations were firmly denied by the Italian government.[28]

Regardless of whether the allegations are true or not, this is a lesson that should be heeded. When members transfer an operational role then the nuance of the role and the approach needs to be disclosed. If the Italians were conducting different practices than the French, albeit adhering to, or showing respect to, local customs the French contingent should have been made aware of these practices. Ignazio La Russa, then Italian Defence Minister, rebutted the French allegations by saying that Italian soldiers created a connection with the local population and were very different than other contingents.[29] The actionable intelligence of how the Italians were interacting with the local population was not shared with the French. This may have led to attack as local Afghans felt that the French were not paying the respect due to them.

This is the danger that lurks in not sharing actionable intelligence within the coalition while deployed. Not only did this instance create a moment where the French and Italian governments were at loggerheads, but the French population also mourned the bloodiest day for French forces in twenty-five years and French public opinion on the war and Italy as a coalition partner also suffered. The environment for intelligence sharing within the coalition needs to be a naturally fostered event and not an enforced action. NATO is creating the organizational structures to foster intelligence sharing within the Alliance, but innovative methods of encouraging that relationship need to be nurtured.

Intelligence Sharing within the Coalition

Intelligence sharing in coalitions is difficult. The very point of intelligence is to collect material, and analyse it for one's own interests and internalise the information. It is against the sociological nature of the intelligence services to share their sensitive information with others, in case it later

---

26 Ibid.

27 Lizzy Davies and John Hooper, "French Outcry over Claim Italian Payments Masked Taliban Threat," *The Guardian* (16 October 2009), at http://www.theguardian.com/world/2009/oct/16/france-italy-taliban-afghanistan (accessed 15 May 2014).

28 Ben Farmer, "Italy Denies Report It Paid Off Taliban in Afghanistan," *The Telegraph* (15 October 2009), available at http://www.telegraph.co.uk/news/worldnews/europe/italy/6337019/Italy-denies-report-it-paid-off-Taliban-in-Afghanistan.html (accessed 15 May 2014).

29 Ibid.

becomes a threat to the home country. However, intelligence co-operation in Western countries does exist and has been institutionalised. The UKUSA, or “Five Eyes” agreement, which was established in 1946, has been expanded to involve Australia, Canada and New Zealand.[30] The Five Eyes arrangement was able to provide actionable intelligence for the members through the All-Source Intelligence Centre (ASIC), which was beneficial for Canadian military operations in Kandahar province.[31] The ASIC was able to provide “innovative and actionable intelligence products by integrating SIGINT, geospatial intelligence, human intelligence (HUMINT) and other analyzed information.”[32] Five Eyes intelligence was a great resource for the membership, however actionable intelligence was not disseminated to other ISAF members even those who were conducting Special Operations.

Actionable intelligence for Special Operation Forces (SOF) is vital and SOF are “voracious consumers of intelligence.”[33] NATO SOF Headquarters (NSHQ) is working to increase trust among members and streamline intelligence.[34] The *NATO 2020: Assured Security; Dynamic Engagement* report, which provided a framework for a new strategic concept, stated that the Alliance can provide a supporting role for sharing intelligence and providing assistance against unconventional threats.[35]

Two benefits to intelligence cooperation are its allowance for review through comparative processes and the potential to divide the intelligence demands across a larger support network.[36] During the Cold War, many NATO members routinely kept intelligence from other members and believed that NATO headquarters was not secure and was infiltrated by Soviet agents.[37]

Intelligence sharing is not unproblematic and the benefits and negatives have to be considered. In terms of strategic intelligence, intelligence sharing can present several problems. One of these is how the material will impact the supplier-recipient relationship. Information that is contrary to the recipient’s viewpoint could be hazardous to the relationship and this challenge could produce a negative effect.[38]

---

30 James Cox, “Canada and the Five Eyes Intelligence Community” (*Canadian Defence and Foreign Affairs Institute),* December 2012, available at http://2glspd2t2a9zr20ie1z7bx8zbb.wpengine.netdna-cdn.com/wp-content/uploads/2012/12/SSWG-Paper-James-Cox-December-2012.pdf.pdf (1 December 2014), p. 5.

31 Ibid., p. 9.

32 Ibid.

33 Lawrence E. Cline, “Special Operations and the Intelligence System,” *International Journal of Intelligence and Counterintelligence* 18(4) (2005), p. 576, http://www.tandfonline.com/doi/abs/10.1080/08850600500177077 #preview (accessed 1 December 2014).

34 Martin J. Ara and Brage A. Larsse, “Help a Brother Out: A Case Study in Multinational Intelligence Sharing, NATO SOF (Master’s Thesis, Naval Postgraduate School, Monterey, 2011), p. v, available at https://calhoun.nps.edu/bitstream/handle/10945/10727/11Dec_Ara.pdf?sequence=1 (accessed 1 December 2014).

35 NATO, “NATO 2020: Assured Security; Dynamic Engagement,” (17 May 2010), at http://www.nato.int/cps/en/ natolive/official_texts_63654.htm?selectedLocale=en (accessed 15 May 2014).

36 Don Munton and Karima Fredj. “Sharing Secrets: A Game Theoretic Analysis of International Intelligence Cooperation,” *International Journal of Intelligence and Counterintelligence* 26(4) (2013), p. 672, available at http://www.tandfonline.com/doi/abs/10.1080/08850607.2013.807189#.VH3tZ2cRTXQ (accessed 1 December 2014).

37 Ibid., p. 673.

38 Ibid, p. 674.

Consider the example of the lead-up to the Second Gulf War in 2003. Munton and Fredj suggested that sharing intelligence on Iraq's Weapons of Mass Destruction program with the United States might have had the potential to avert the war and would have established a cohesive intelligence sharing structure, where the Western intelligence community would have been able to enrich the debate. The US State Department's Intelligence and Research (INR) unit had a contrary view to that of the Pentagon.[39] Providing contrary intelligence could have created the effect that Munton and Fredi suggested, but it is also likely that it could have created a more hostile relationship between the US and the suppler countries.

When it comes to providing operational and tactical intelligence and data to coalition partners in theatre, sharing in a timely manner is a different matter entirely. Consider the examples of American intelligence and their interaction with French forces of late. The first example concerns the French experience with US IMINT sharing in the Libyan Operational Theatre. The IMINT data was available for use, but given the red tape needed to clear French pilots, they had to innovate to provide their own data in a shorter window. French pilots were using their own reconnaissance pods rather than the IMINT provided by American UAV and satellite surveillance.[40] Tactical imagery was delayed at the Combined Air Operations Center (CAOC). Instead, the French would typically launch a reconnaissance mission, identify targets and then launch a strike mission within five hours.[41]

The frustration of not being given timely intelligence created a wedge between American and French units. The aim of the Libyan Air Campaign was not only to create a 'no-fly' zone but also to counter pro-Gaddafi forces. The lack of actionable and timely intelligence was a limitation on French air assets, but also a further drain on resources. The window before French reconnaissance and strike missions was five hours on average. French pilots expressed their constant concern on identifying targets without ground controllers and avoiding air strikes on civilians.[42] In the Kosovo intervention, Serbian anti-air units were intuitive with repositioning their assets regularly.[43]

If the pro-Gaddafi forces had been better organised, they could have potentially led to missing the strike target, thus not only causing a further waste on resources, but potentially putting the anti-Gaddafi movement, or worse civilians, in jeopardy. British Royal Air Force Marshal Andy Pulford stated "In Libya we got away with it. We made do, we had work-arounds, [but] we were not fighting a sophisticated enemy."[44] This five hour gap could have potentially created the opportunity for NATO coalition casualties if the pro-Gaddafi forces were more sophisticated.

---

39 Ibid., p. 672.

40 Densmore, "French Pilots Over Libya Decline US Intel; Clearance Just Too Slow."

41 Ibid.

42 Ibid.

43 Martin Van Crevald, *The Age of Air Power* (Public Affairs, 2011), p. 328.

44 Sydney J. Freedberg, Jr, "US Allies Wrestle with Intel Sharing Problems Exposed in Libya," Breaking Defense (20 September 2012), at http://breakingdefense.com/2012/09/us-allies-wrestle-with-intel-sharing-problems-exposed-in-libya (accessed 15 May 2014).

The intelligence-sharing problem within NATO may be caused by its multinational structure. In the case of Mali, American satellites, the US Air Force UAVs and the US Army's HUMINT and SIGINT provided intelligence for the French intervention that proved to be crucial for the first air strikes.[45] Unlike in Libya, the integration and shortening of the 'observation-decision-action loop' was unprecedented.[46] Bilateral cooperation would be easier given the established relationship between the American and French governments.

Reducing the intelligence lag is key for operational and tactical coalition partners. After the lessons learned in Libya, US Air Force Lieutenant General Frank Gorenc suggested that instead of officers deciding on whether information should be disseminated to coalition pilots, a capacity for direct machine-to-machine coordination should be created.[47]

The US Department of Defense Inspector General stated that improvements for sharing tactical intelligence with coalition partners are needed.[48] The Inspector General found that the US has an outdated approach with foreign disclosure policies and procedures. He also called for the implementation of a "single, theatre-wide, computerized source registry to be utilised by the coalition for de-confliction of counterintelligence and human intelligence source data."[49]

Sharing intelligence can be seen as a *faux pas* within the intelligence community. However, a study examining the sharing of intelligence in the realist-centric Game Theory has proven that sharing intelligence with allies is a positive activity.[50] Game Theory, in the context of intelligence cooperation, demonstrates that players will continue to cooperate with one another. This is in contrast with other scenarios where after a finite period of time the players revert to their 'dominant strategy' of non-cooperation.[51] This coincides with the nature of intelligence cooperation and liaisons where finite relationships are almost irrelevant because of the matter of trust. When Munton and Fredj added in the factors of 'reputation and retaliation' their Game Theory model further proved that cooperation would continue.

Operational Caveats meet Intelligence Caveats

It has been well established that countries that participate in multilateral military operations can impose 'caveats' that limit the total involvement of the country's forces. These caveats can be that the country's forces will not participate in the use of cluster munitions or even that the forces will not operate at night. This practice for NATO commanders dates back to at least Bosnia where

[45] Maj. Gen. Oliver Tramond and Lt. Col. Philippe Seigneur. "Early Lessons from France's Operational Serval in Mali," *Army* (June 2013), p. 43, available at http://www.ausa.org/publications/armymagazine/archive/2013/06/Documents/Tramond_June2013.pdf (accessed 1 December 2014).

[46] Francois Heisbourg, "A Surprising Little War: First Lessons of Mali," *Survival: Global Politics and Strategy* 55(2) (2013), pg. 12, available at http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival—global-politics-and-strategy-april-may-2013-b2cc/55-2-02-heisbourg-2805 (accessed 1 December 2014).

[47] Freedberg, "US Allies Wrestle with Intel Sharing Problems Exposed in Libya."

[48] US DoD Inspector General. "Results in Brief: Improvements Needed in Sharing Tactical Intelligence with International Security Assistance Force-Afghanistan."

[49] Ibid.

[50] Munton and Fredj. "Sharing Secrets: A Game Theoretic Analysis of International Intelligence Cooperation."

[51] Ibid., p. 680.

NATO commanders created spreadsheets that specified each contributing contingent's restrictions.[52] Unfortunately, caveats can also be non-written. For both Lieutenant General Marc Lessard and Pakistani author and journalist Ahmed Rashid, these caveats proved to be a serious obstacle for NATO to overcome in Afghanistan.[53] The majority of the caveats were imposed in order to reduce the risk of casualties or for domestic political reasons.

One caveat that potentially affected the ISAF mission concerned German reconnaissance missions and the German caveat of not being part of counterterrorism operations. Specifically, the mandate for German participation in ISAF prohibited involvement in Operation Enduring Freedom (OEF). As a result, the pictures taken by German reconnaissance planes could not be distributed if there was a risk that they might be used as part of counterterrorism efforts. The parallel operational structures of OEF and ISAF increased the likelihood of operational confusion.[54] The distribution of IMINT gathered by German reconnaissance planes in Afghanistan was limited because of this operational caveat.[55] There were only select countries that participated in both ISAF and in OEF, so the dissemination of intelligence was limited.

This German example may prove to offer part of the solution to mitigating the impact of NATO members not willing to share intelligence. The NIFC could potentially require the statement of intelligence caveats from the participating NATO members in future operations. German reconnaissance may not be available for counterterrorism operations, but the ACO would know that American IMINT is also unavailable for NATO pilots for X amount of hours until proper clearance or at least knowledge of the conditions of why clearance requires that length of time. This would allow for ACO, NSHQ and the NIFC to have a clearer vision of what intelligence assets can be deployed. This also have minimal impact on the NATO intelligence structure as well.

Smart Defence Initiative and Connected Forces Initiative

The economic crisis that began in 2008 has had a severe impact on NATO member states. Many NATO members took measures to mitigate the impact the budgetary cuts would have on their respective ministries of defence. This led to the creation of the SDI and the Connected Forces Initiative. Innovative ways have been found to increase efficiency, interoperability and to reduce costs, such as pooling chemical, biological, radiation and nuclear (CBRN) protection equipment, the NATO Universal Armaments Interface and Multinational Military Flight Crew Training.[56]

---

52 David P. Auerswald and Steven M. Saideman. "NATO at War: Understanding the Challenges of Caveats in Afghanistan" (Paper presented at the Annual Meeting of the American Political Science Association, Toronto, 2-5 September 2009), p. 7, available at http://www.aco.nato.int/resources/1/documents/nato% 20at%20war.pdf (accessed 1 December 2014).

53 Chicago Council on Global Affairs, "Smart Defense and the Future of NATO: Can the Alliance Meet the Challenges of the Twenty-First Century?," p. 7.

54 Timo Noetze and Sibylle Scheipers. "Coalition Warfare in Afghanistan Burden-sharing or Disunity?"(ASP/ISP BP 07/01, Chatham House, October 2007), p. 3, available at http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/bp1007afghanistan.pdf (accessed 15 May 2014).

55 Auerswald and Saideman. "NATO at War: Understanding the Challenges of Caveats in Afghanistan," p. 8.

56 NATO, "The Secretary General's Annual Report 2013" (23 January 2014), pp. 14-15, at http://www.nato.int/ nato_static/assets/pdf/stock_publications/20140123_SG_AnnualReport_2013_en.pdf (accessed 15 May 2014).

These initiatives may also provide a framework for intelligence sharing in future coalition operations. The economic crisis has forced NATO members to find innovative ways to cut costs while maintaining operational capability during a prolonged COIN operation.

This multinational approach showed a glimpse of what NATO's Smart Defence Initiative (SDI) would look like in future NATO-led COIN operations. SDI was envisioned to maintain NATO's military capabilities, but also to respect the reality that no member-state could fulfill all roles needed. The economic crisis that began in 2008 forced many Western countries to cut or adjust their proposed defence budgets, while also finding the funds to continue operations in the Afghan theatre, and procure vital equipment for operations. SDI promotes the "prioritisation, specialisation and multinational approaches to acquisition."[57] It proposes that member-states should specialise in various roles, such as strategic airlift, anti-armour capabilities and so forth. Canada, for example, has already divested from its thirty-four Air Defence Anti-Tank Systems (ADATS) in a bid to save money.[58] NATO suggests that any savings that are produced using the SDI approach should be diverted to increasing the overall capability of the country's regular forces.

Although not a NATO-sanctioned mission, the French intervention in Mali demonstrated the potential need for alliance members to complement each other with support operations. While the French supported local African troops in Operational SERVAL against the militant Islamist insurgency, the European Union provided a training mission for Malian government forces, and the Canadians provided strategic airlift – a capability that the French Air Force lacked. The United States was able to provide significant intelligence to French forces for the initial air strikes of the campaign.

The Connected Forces Initiative (CFI) proposes to maintain "NATO's readiness and combat effectiveness through expanded education and training, increased exercises and better use of technology." This is part of the shift of operational engagement in the Afghan theatre and operational readiness for the next theatre of operations. CFI is dedicated to improving communication and interoperability within NATO with additional exercises, and improvements to the NATO Response Force and SOF. The NSHQ is making efforts to improve intelligence sharing and it is likely that the CFI will attempt to improve intelligence sharing and trust among the Alliance.

Both the SDI and CFI provide a unique opportunity for NATO. The SDI proposes that NATO members should provide a level of specialisation within its military capabilities. Major General Flynn wrote in his report that intelligence operatives should not be confined by their functionality but by territorial lines.[59] Should NATO troops be deployed in prolonged COIN operations, Flynn's model of increased connectivity with intelligence operatives and all personnel on the ground needs to be upheld.

---

[57] Ibid., p. 13.

[58] David Pugliese, "ADATS Heading to Museums and Concrete Pads outside Bases," *DefenceWatch* (16 May 2012).

[59] Flynn, Pottinger, and Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," p. 46.

The SDI model can provide an alternative model to foster a tradition of cooperation if applied to intelligence operations. In future COIN operations, NATO members could provide specialised intelligence. France has a significant intelligence capability in terms of HUMINT in the Middle East, North and West Africa because of its colonial ties.[60] Within the Alliance, the United States dominates IMINT with its UAV and satellite capabilities, but French capabilities in the aforementioned regions could provide the United States, and NATO, with actionable intelligence that the US or other members would lack.

This Smart Intelligence Initiative would provide not only specialisation with NATO intelligence structures, but also foster an environment of collaboration. The NIFC could potentially oversee this initiative encouraging its theoretical use in the CFI exercises.

Low Impact Solutions

Intelligence sharing within NATO has been problematic. Intelligence sharing is built on trust and although NATO has been in existence since 1949, the Alliance has found itself in unfamiliar territory with sustained COIN operations in Afghanistan and an air campaign in Libya with no ground-control assets in place.

Intelligence sharing is becoming a thorn in NATO's side. NATO has created new structures within the organization to combat the difficulties with intelligence sharing, but new innovative methods are needed to nurture the intelligence sharing ethos and not impose it on its members.

This report aimed to outline the difficulties of NATO intelligence sharing by providing case studies and providing low impact solutions on the current NATO structure that would require no or little reorganization to foster such a cooperative relationship.

To be succinct, the recommendations within this report are as follows:

- A comprehensive study of potential regional impacts should be conducted. It is apparent that some conflicts cannot be internalised within a single country and may transcend borders. Actions should be undertaken, by the Alliance or individual members, to reduce the impact of violent spill over to the region as a whole.
- Intelligence caveats should be provided before operations to permit Allied Command Operations to assess what NATO member assets can be deployed to provide optimal intelligence coverage.
- Intelligence specialisation within theatre should be considered. Depending on the next NATO intervention, certain member states may have specialised intelligence assets, eg. IMINT, HUMINT, SIGINT, for the region. By creating an environment where NATO intelligence has to complement one another and not compete would create a stronger bond within the Alliance.

---

[60] Kennan Mahoney, *et al*, "NATO Intelligence Sharing in the 21st Century" (Capstone Research Project, Columbia School of International and Public Affairs, 2013), p. 12, available at https://sipa.columbia.edu/sites/default/files/AY13_USDI_FinalReport.pdf (accessed 1 December 2014).

Terrorism continues to be a major threat for the Alliance. To counter terrorism and future insurgencies, NATO has to continue the innovation that the economic crisis sparked. NATO is a security alliance that was born in the age of nuclear war with the Soviet Union. The Cold War is over and the security threat paradigm of the 21st Century has changed from the traditional, conventional interstate conflict to the unconventional battlefields of terrorism, counterinsurgency and cyberincursion. In order to survive, NATO has to evolve and find nuances within the Alliance to compete in a changing world. NATO has taken part in two major operations since 9/11 – Afghanistan and Libya – and yet the Alliance is just beginning to find ways to improve connectivity in a globalised world. Former Warsaw Pact members are not contributing members of NATO and although the Ukrainian Crisis has given a glimpse of a traditional threat in Russia, NATO needs to continue to meet the challenges of the 21st Century.

Conclusion

Intelligence sharing has been an issue that NATO has taken steps to address. During the Cold War, intelligence sharing was not high on the priority list. It was even joked in NATO headquarters, and satirized in the public mainstream, that the Soviet Union was more aware what the Alliance was doing than some allies were. The Cold War is over and the events on 11 September 2001 demonstrated that intelligence sharing is key to averting further terrorist attacks and that cooperation with agencies will be key to this. Globalized terrorism still remains one of the key threats in NATO strategic planning.

NATO's prolonged counterinsurgency (COIN) operation in Afghanistan showed the Alliance the difficulties of conducting large-scale operations with operational caveats. The International Security Assistance Force (ISAF) was more concerned with conducting an anti-insurgency operation where targeting insurgents was the objective. For years, ISAF did not have a clear understanding of the political, economic and cultural aspects of the Afghan situation. This was detrimental to the successfulness of the COIN operation. It was only recently that a COIN doctrine was imposed on that theatre of operations. Intelligence sharing within the coalition of 46 contributing countries, with 28 of them being NATO members, showed weaknesses in their inability to do so.

NATO's air campaign in Libya illustrated the Alliance's problematic intelligence-sharing apparatus. American imagery intelligence was provided, but clearance for pilots took too long. The French contingent, on the hand, adapted by sending its own reconnaissance missions, analysing the data and then launching a strike mission – something that would take five hours. Although the contributing members of the coalition had the same objectives, intelligence enablers were not readily available. This would have proved to be catastrophic is NATO was facing a more sophisticated adversary.

Again, an understanding of the region's political, economic and cultural aspects was not taken into account. The Libyan Air Campaign displaced an estimated 420,000 people, with 30,000 of them returning to Mali. In January 2012, the fourth ethnic Tuareg rebellion began. Malian government forces were ill-prepared and a hostile takeover of the country was almost assured. French intervention was necessary because of the new insurgent alliance with militant Islamists and the secular ethnic Tuareg group, the MNLA.

Because of the economic crisis and the drawdown of forces in Afghanistan, NATO is looking at innovative ways to move from operational engagement to operational readiness and increase interoperability. If there is anything to be learned from the Afghan and Libyan deployments, it is that NATO intelligence sharing potentially could be the proverbial Achilles Heel of the Alliance. This report aims to illustrate these issues, but also to provide low-impact solutions that will be able to foster an intelligence-sharing relationship for the Alliance and not impose such a relationship forcibly.

BIBLIOGRAPHY

Ara, Martin J.and Larssen, Brage A., "Help a Brother Out: A Case Study in Multinational Intelligence Sharing, NATO SOF" (Master's Thesis, Naval Postgraduate School, Monterey, 2011).

Auerswald, David P. and Saideman, Steven M., "NATO at War: Understanding the Challenges of Caveats in Afghanistan" (Paper presented at the Annual Meeting of the American Political Science Association, Toronto, 2-5 September 2009).

Brennen, Kate, "NATO Signs $1.7 billion Global Hawk Contract", *Defense News* (21 May 2012).

Brunnstrom, David, "NATO Launches Afghan Intelligence-sharing Drive", *Reuters* (15 July 2010).

Chicago Council on Global Affairs, "Smart Defense and the Future of NATO: Can the Alliance Meet the Challenges of the Twenty-First Century?", (Chicago, Illinois, 28-20 March 2012).

Cline, Lawrence E., "Special Operations and the Intelligence System" *International Journal of Intelligence and Counterintelligenc*e 18(4) (2005).

Cox, James, "Canada and the Five Eyes Intelligence Community" (Canadian Defence and Foreign Affairs Institute, December 2012).

Davies, Lizzy and Hooper, John, "French Outcry over Claim Italian Payments Masked Taliban Threat", *The Guardian* (16 October 2009).

Densmore, Robert, "French Pilots over Libya Decline US Intel; Clearance Just Too Slow", *Breaking Defense* (21 September 2011).

Farmer, Ben, "Italy Denies Report It Paid off Taliban in Afghanistan", *The Telegraph*, (15 October 2009).

Freedman Jr., Sydney J. "US Allies Wrestle with Intel Sharing Problems Exposed in Libya", *Breaking Defense*, 20 September 2012).

Flynn, Major General Michael T, Pottinger, Captain Matt, and Batchelor, Paul D., "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan" (*Center for New American Security,* 2010).

Heisbourg, Francois, “A Surprising Little War: First Lessons of Mali”, *Survival* 55(2), April-(May 2013).

Kilcullen, David, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (Oxford University, 2013).

Korkisch, Friedrich W., “NATO Gets Better Intelligence: New Challenges Require New Answers to Satisfy Intelligence Needs for Headquarters and Deployed/Employed Forces” (Institut für Aussen- und Sicherheitpolitik Strategy Paper 1-2010, April 2010).

Mahoney, Kennan; Mladenovic, Nemanja; Molina, Salvador; Scher, Adam; Stern, Selma and Zoia, Christopher. NATO Intelligence Sharing in the 21st Century” (Published Capstone Research Project, Columbia School of International and Public Affairs, 2013)

McCauley, Dan, “Design and Joint Operation Planning”, *Canadian Military Journal* 12(1) (2011)

Munton, Don and Fedj, Karima, “Sharing Secrets: A Game Theoretic Analysis of International Intelligence Cooperation”, *International Journal of Intelligence and Counterintelligence* 26(4) (2013).

NATO, “The Secretary General’s Annual Report 2013” (23 January 2014).

Noetzel, Timo and Scheipers, Sibylle, “Coalition Warfare in Afghanistan Burden-sharing or Disunity?”(*Chatham House*, October 2007),

Pugliese, David. “ADATS Heading to Museums and Concrete Pads outside Bases”, *DefenceWatch* (16 May 2012).

Rohen, Yehudit. “Libya, the Tuareg and Mali on the Eve of the ‘Arab Spring’ and in its Aftermath: An Anatomy of Change Relations”, *Journal of North African Studies* 18(4) (2013)

Ruttig, Thomas, “Loya Paktia’s Insurgency: The Haqqani Network as an Autonomous Entity” in *Decoding the New Taliban: Insights from the Afghan Field* (Antonio Giustozzi, ed., Columbia University Press, 2009).

Shaw, Scott, “Fallout in the Sahel: The Geographical Spread of Conflict from Libya to Mali,” *Canadian Foreign Policy Journal* 19(2) (2013).

Tramond, Maj. Gen. Oliver and Siegneur, Lt. Col. Phillipe, “Early Lessons from France’s Operational Serval in Mali,” *Army* (June 2013).

Soloman, Hussein, “Mali: West Africa’s Afghanistan”, *RUSI Journal* 158(1)(2013).

United Nations Security Council, “Report of the Assessment Mission on the Impact of the Libyan Crisis on the Sahel Region” (18 January 2012).

US DoD Inspector General, “Results in Brief: Improvements Needed in Sharing Tactical Intelligence with International Security Assistance Force-Afghanistan” (18 July 2011).

Van Crevald, Martin, *The Age of Air Power* (Public Affairs, 2011).

Defence Against Terrorism Review
Vol. 6, No. 1, Spring&Fall 2014, pp. 63-92

ISSN: 1307-9190

Youth Extremism in Pakistan – Magnitude, Channels, Resident Spheres and Response

Muhammad Feyyaz
Assistant Professor, School of Governance and Society, University of Management and Technology, Lahore, Pakistan.
faizy68@googlemail.com

Abstract: *This paper attempts to address religious extremism and the factors confounding its conceptual and definitional understanding within the existing reality of Pakistan. It particularly highlights and analyzes the demographic magnitude of extremists' potential, inspirations, channels and geographical location of extremism in the country. These areas have been ignored in the extant literature on extremism in Pakistan. The conclusions respond to the reviewed issues besides proposing a contextualized definition of religious extremism. A few broad policy suggestions are also offered, including a generalizable framework to measure holistic spread of extremism in Pakistan to meaningfully respond to the situation.*

Keywords: *Pakistan, religious extremism, youth, definition, inspirations, channels, processes*

Introduction

Youth attitudes are rarely studied in Pakistan as a conscious policy measure to be able to address needs of this segment of the society. The discourse on militancy exclusively examined from the perspective of youth has received even lesser attention.[1] On the contrary, the most widely discussed risk associated with Pakistan's demographic profile is the threat of millions of young,

[1] For list of some relevant youth studies, see Ayesha Siddiqa, "Red Hot Chili Peppers Islam – Is the Youth in Elite Universities in Pakistan Radical?" (Heinrich Bölle Stiftung, 2011), p. 6, available at http://www.pk.boell.org/ downloads/Red_Hot_Chilli_Peppers_Islam_-_Complete_Study_Report.pdf (accessed 8 December 2014).

impoverished, and unemployed people succumbing to the blandishments of extremism.[2] A worrisome dimension of the evolving character of violence is the fast expanding scope of traditional ages of terrorists from between 15-24 years previously to 10-30 years currently.[3] By implication it has created a surge in numbers of youth, rising to alarming proportions from 52.66 million / 29 % to 75 million/ 41 % of a total citizenry estimated to be around 184.35 million.[4] About one-half of this population comprises females. Such a bloated youth presence suggests that the direction this critical mass of the demographic segment chooses to take the country will inevitably become Pakistan's destiny,[5] which not only underscores the need to study all challenges confronting the country with the youth duly factored in but also the urgency for their sustained engagement.

Furthermore, an added problem generated by the literature dealing with extremism is the proliferation of a plethora of expressions, like fundamentalism, fanaticism, salafism, radicalism, latent radicalism, violent takfirism, and obscurantism, to mention a few. The impact has been an intellectual haze, evident from interchangeable use of these terms that in many ways is factually incorrect.[6] Some analysts hence argue that "lack of consensus on definitions makes it difficult to arrive at a comprehensive understanding of the phenomenon, complicating efforts aimed at countering extremism".[7] Besides, other than an odd effort there is no attempt made in any of the available studies on youth to estimate the magnitude of extremism in Pakistan. The geographical references of extremism have been identified (e.g., by Moeed as well as Winthrop and Graff), but these are too broad (i.e., province or nationwide), to be of any empirical value.[8] Moreover, while Ayesha Siddiqa, a leading Pakistani scholar, has alleged the existence of latent radicalism among the country's youth as a consequence of the dominant religious narrative,[9] this view is not believed to be wholly true. Instead, there are multiple lenses and sources that play a defining role in building a worldview of the Pakistani youth who are amenable to violent extremism that the referred study clearly fails to highlight. This paper is an attempt to address all of these issues.

It first proceeds with a conceptual discussion of extremism and its various dimensions to establish a theoretical frame of reference. Section II outlines the demographic profile of Pakistan and attempts to identify the youth population that is vulnerable to extremism. The next section details

---

2 Moeed Yusuf, "A Society on the Precipice? Examining the Prospects of Youth Radicalization in Pakistan," in *Reaping the Dividend: Overcoming Pakistan's Demographic challenges,* (Michael Kugelman and Robert M. Hathaway , eds, Woodrow Wilson International Center for Scholars, 2011), p. 13.

3 'Youth' in this paper is based on the ages (10-30 years) of apprehended militants and suicide bombers in Pakistan.

4 Nargis Mazhar, "Population, Labour Force and Employment," *Pakistan Economic Survey 2012-13* (Pakistan Ministry of Finance, 2013), p. 157, available at http://finance.gov.pk/survey_1213.html (accessed 8 December 2014).

5 Yusuf, "A Society on the Precipice? Examining the Prospects of Youth Radicalization in Pakistan." p. 77.

6 See, e.g. Manzar Zaidi, "The Radicalisation Process," *The Dawn* (Feb 2011).

7 Abdul Basit and Mujtaba Muhammad Rathore, "Trends and Patterns of Radicalization in Pakistan," *PIPS Research Journal Conflict and Peace Studies* 3(2)(2010).

8 Moeed Yusuf, "Prospects of Youth Radicalization in Pakistan: Implications for US Policy" (Brookings Institution – October 2008), available at http://www.brookings.edu/research/papers/2008/10/pakistan-yusuf (accessed 8 December 2014); Corrinne Graf and Rebecca Winthrop, "Beyond Madrassas: Assessing the Links between Education and Militancy in Pakistan" (Brookings Institution, 2010), available at http://www.brookings.edu/research/papers/2010/06/pakistan-education-winthrop (accessed 8 December 2014).

9 Siddiqa, "Red Hot Chili Peppers Islam – Is the Youth in Elite Universities in Pakistan Radical?"

multiple lenses and sources that build the worldview of Pakistanis who are generating enclaves of violent extremism. Its key feature is an explanation of the pathways to counter extremism. While the discourse here implicitly touches drivers of extremism in Pakistan, it does not by design dwell upon these due to existence of extensive scholarship on this issue. In Section VI, an effort is made to locate prevailing coverage of extremism. The conclusions among other respond to the reviewed issues. Foremost is the attempted definition of religious extremism followed by a suggested methodical framework to measure its holistic spread and a few policy recommendations to address the situation.

Religious Extremism – Theoretical Discourse

Mubarak Haider in his book *Tahzeebi Nargissiat (Narcissism from Civilization)* ascribes the notion of extremism within Islam to the thought of the 'chosen ones' and the 'perfect people'. He notes "[t]his is a diseased thought that lends bias, prejudice and a sense of narcissism … and these feelings always lead to intolerance and gender violence."[10] In a sociological framework, extremism refers to political ideologies that oppose a society's core values and principles. For example, exploring the cultural-extremism nexus, Elaine Pressman finds 'extremism' to be a culturally relative term in that extremist beliefs are dependent on the cultural perspective since the person who holds views which are considered to be 'extreme' within one cultural context or time may not be considered to hold 'extremist' beliefs within another cultural context or time. He therefore suggests that "[n]orms and values are intricately bound up in the definition of 'extremism.'"[11] However, other than emphasizing culture and temporal differentials as the context changers, his discourse falls short in defining extremism. In liberal democracies, extremism is applied to any ideology that advocates racial or religious supremacy and/or opposes the core principles of democracy and human rights,[12] such as the multiform political extremism in Florida.[13]

Extremism is often mixed up with radicalism, which indicates the extent of its being misunderstood as a distinct approach or attitude. Hasan Askari views radicalization as the mindset and orientation of people and groups advocating and supporting drastic changes in society and the political system based on their interpretation of Islamic religious scripture and traditions.[14] This definition is akin to one described above in the political domain. Manzar Zaidi on the other hand, connotes extremism

[10] Xari Jalil, "Giving Context to Religious Extremism," *Pakistan Today* (19 Jun 2011), available at http://www.pakistantoday.com.pk/2011/06/giving-context-to-religious-extremism/ (accessed 8 December 2014).

[11] D. Elaine Pressman, "Risk Assessment Decisions for Violent Political Extremism 2009-02," (Canadian Centre for Security and Intelligence Studies, 2009), available at http://www.publicsafety.gc.ca/cnt/rsrcs/ pblctns/2009-02-rdv/2009-02-rdv-eng.pdf (accessed 13 Nov 2014).

[12] Peter Neumann, "Prisons and Terrorism Radicalisation and De-radicalisation in 15 Countries," (International Centre for the Study of Radicalisation and Political Violence (ICSR), 2010), available at http://icsr.info/publications/papers/1277699166 PrisonsandTerrorismRadicalisationandDeradicalisationin15Countries.pdf (accessed 8 December 2014).

[13] "Extremism in Florida: The Dark Side of the Sunshine State," (Anti-Defamation League, 3rd Edition, 2011), available at http://www.adl.org/assets/pdf/combating-hate/ExtremismFloridaINSIDE.pdf (accessed 8 December 2014).

[14] Hasan Askari Rizvi, "Radicalization and Political System of Pakistan," in De-radicalization and Engagement of Youth in Pakistan (M. H. Nuri, et al, eds., Islamabad Policy Research Institute), p. 12.

as radicalization, which he defines "as a process whereby originally moderate individuals or groups of individuals become progressively more extreme in their thinking — and possibly their behaviour — over time."[15] Robert Mandel refers to radicalization as an increase in and/or reinforcement of extremism in the thinking, sentiments, and/or behaviour of individuals and/or groups of individuals.[16] Ayesha's definition of 'latent radicalism' as a "tendency to be exclusive instead of inclusive vis-à-vis other communities on the basis of religious belief, departs from others. She nevertheless excessively employs extremism and radicalism interchangeably."[17] Carefully viewed, Zaidi, Mandel and Ayesha are only synthesizing the contours of extremism. The defining lines between extremism and radicalism are subtle and are overlapping, yet the two represent distinct zones, with extremism generally, but not necessarily, occurring earlier than radicalism or any one of them happening at a time.

The definition of extremism by Tomas Precht "as immoderate uncompromising views and measures beyond the norm" appears plausible but is equally subjective. His observation that "for the most part, extremist groups pose a threat to public order, but not to national security" is also intriguing.[18] Empirical evidence, such as the Mumbai attacks, the militant raid on Pakistan Army Headquarters in October 2009, suicidal strikes at air bases or other sensitive installations do not validate this assertion. A particular feature of religious extremism that is generally ignored is its persistence and virulence which provokes 'reactive' religious violence, terrorism, and even terrorist movements.[19] Evolving Barelvi militant assertiveness in Pakistan and behavioural transformation among scores of Muslims to reciprocate in kind or emulate heroism of perceived martyrs in response to the kinetic killing of Abu Musab al-Zarqawi in Iraq in June 2006, the mysterious death of Osama Bin Laden consequent to US special forces raid on 2 May 2011 and the burning of Quran by Terry Jones in Florida during 2011 exemplify reactivity nuances of religious extremism.

Uniquely, 'extreme' and 'extremism' have been expounded by Uwe Backes to mean something which is the 'farthest out.' He opines that there is "nothing beyond the extreme; extremes cannot be increased, they embody something which cannot be surpassed or exceeded."[20] In effect, Backes is merely conflating extremism with a measurement instrument without providing a precise definition as well as the determining attribute of extremism. Likewise, the term extremism is used to describe methods through which political actors attempt to attain their aims, that is, by using means that "show disregard for the life, liberty, and human rights of others" i.e., by resorting to violence. Many

---

[15] Zaidi, "The Radicalisation Process."

[16] David R. Mandel, "Radicalization: What does it mean?" in *Indigenous Terrorism: Understanding and Addressing the Root Causes of Radicalization among Groups with an Immigrant Heritage in Europe* (Thomas M. Pick, Anne Speckhard, Beatrice Jacuch, eds., IOS Press, 2010).

17 Siddiqa, "Red Hot Chili Peppers Islam – Is the Youth in Elite Universities in Pakistan Radical?" pp. 12, 25.

[18] See Tomas Precht, "Home Grown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism (Danish Ministry of Justice, Dec 2007).

[19] Arshi Saleem Hashmi, "Pakistan: Politics, Religion & Extremism," (Institute of Peace and Conflict Studies (IPCS) Research Papers, May 2009), available at http://www.ipcs.org/pdf_file/issue/RP20-Arshi-Pakistan.pdf (accessed 8 December 2014).

[20] See Uwe Backes, "Meaning and Forms of Political Extremism in Past and Present," *Central European Political Studies Review* 4 (2007).

governments therefore refer to terrorists as "violent extremists."[21] The imposition of *shari'a* in neighborhood and armed confrontation with the state by clergy and students of Lal Masjid (Red Mosque) and Jamia Hafsa Madrassa in Islamabad during July 2007 was violent extremism in the operational sense, and religious vigilantism in terms of an intent "to enforce the *sharia* apart from the hand of the state."[22]

Religious extremism vastly differs from its ideological equivalents. For example, fundamentalism for religiously imbued minds means belief and loyalty to the fundamental sources and a value framework of a faith.[23] While in political Islam, it refers to resistance to modernity and strict adherence to a literal interpretation of sacred texts.[24] Some connote it as an orientation to the world that is anti-intellectual, bigoted, and intolerant, [25] which "rejects all forms of ijtihad (simply reasoning), opposes all forms of hierarchy within the Muslim community, including tribalism or royalty, favour, excluding Shia from participation in the polity, and takes a very restrictive view of the social role of women." [26] Professor Khurshid Ahmad, a known Muslim scholar, calls these definitions a "reductionism that emphasizes, out of all proportion, the 'pathological' or 'economic' situations", hence "is flawed, deceptive and unhelpful."[27] He considers extremism a product, not of the mainstream historical tradition of Islam, but of modern politics and the modern state that the West itself has produced.[28]

In the sub-continent, the term fanatic was used by W.W. Hunter during the early 19th Century for Sayyid Ahmad to characterize his Tauheed (oneness of Allah), war waging upon all infidels, spirit of revolt against the British Rule and declaring India as '*dar-ul-harb*' ('house of war'). [29] In the 20th Century, the backdrop furnishing the contemporary setting was the Deoband-Tribal nexus against the British, rooted in the new and exciting politics of anticolonialism and pan-Islamism, galvanized by the start of First World War.[30] Fanaticism is hence different from extremism and fundamentalism, in terms of its contextualized drive directed at political adversaries while the other two are generally understood to be religiously motivated.

---

21 See Neumann, "Prisons and Terrorism Radicalisation and De-radicalisation in 15 Countries."

22 Joshua T. White, "Vigilante Islamism in Pakistan: Religious Party Responses to the Lal Masjid Crisis", *Current Trends in Islamist Ideology* 7 (2008), available at http://www.hudson.org/content/researchattachments/ attachment/1319/ white_vol7.pdf (accessed 8 December 2014).

23 As'ad Abukhalil and Farid Esack, "The US, the Muslim World and an Islamic Response," *Policy Perspectives* 5(1) (2008), available at http://www.ips.org.pk/the-muslim-world/1003-the-us-the-muslim-world-and-an-islamic-response (accessed 8 December 2014).

24 Mustafa Aydin, "De-legitimizing Religion as a Source of Identity-Based Security Threats in a Global World," *Connections-The Quarterly Journal* (Winter 2006), p. 11, available at http://procon.bg/article/de-legitimizing-religion-source-identity-based-security-threats-global-world (accessed 8 December 2014).

25 Malise Ruthven, *Fundamentalism: The Search for Meaning* (Oxford University Press USA, 2004), p. 7.

26 Hashmi, "The Arabist Shift from Indo-Persian Civilization & Genesis of Radicalization in Pakistan."

27 Khurshid Ahmad, "Terrorism and War against Terrorism: Some Fundamental Issues," *Policy Perspectives* 3(2) (2006), available at http://www.ips.org.pk/global-issues-and-politics/1125-terrorism-and-war-against-terrorism-some-fundamental-issues (accessed 8 December 2014).

28 Ga Pervaiz, "Political Islam and the Media," *Policy Perspectives* 4(2)(2007), available at http://www.ips.org.pk/pakistan-and-its-neighbours/1005-political-islam-and-the-media (accessed 8 December 2014).

29 W. W. Hunter, *The Indian Musalmans* (Sang-e-Meel Publications, 1999), pp. 52-53, 58-60, 63.

30 Sana Haroon, *Frontier of Faith: Islam in the Indo-Afghan Borderland* (Hurst & Company, 2007), pp. 93-98.

Apart from exposing the confusion prevailing in existing scholarship on the theoretical aspects of extremism, the above discourse clearly establishes differentiation among synonyms of religious extremism. Besides, it reveals a propensity to define extremism with a bias and partiality. That reiterates the need for an original construction of the term to help pragmatic analyses and meaningful response formulation.

Demographic Profile of Pakistan

Because Pakistan has not conducted a census since 1998, estimating the country's total population size is an inexact science.[31] The Pakistan National Institute of Population Studies assessed the population to be 184.35 million in May 2014 (which is used here as the standard measure), locating 71.07 million in urban and 113.28 million in rural areas.[32] Excluding the 0-14 age group, 40% of the population falls in the category of youth, using the criteria set out at the beginning of the article.[33] In terms of aging, with a median age of 21.0 years old, Pakistan stood in 139th place out of 196 countries in 2009.[34] In 1988, the proportion of people in the age range of 15-65 was 53% while it will be 67% in 2030, with the majority being those between 15 and 30 years of age. The economic surveys therefore project that Pakistan is becoming younger.[35] This longevity in youth will be significant in consequentially shaping youth attitudes, *inter alia*, due to the continuously rising age at marriage over the last several decades and the accompanying increase in the gap between generations.[36] Besides being populous, Pakistan is also the most urbanized nation in South Asia with city dwellers making up 38% of its population, which increased from 58.74 million in 2008 to 69.87 million in 2013.[37] The year 2030 is expected to be a major landmark in Pakistan's demographics wherein for the first time in its history, the urban and rural population in Pakistan are projected to be evenly constituted, 50% each.[38]

In 2005, more than half of the total urban population of Pakistan lived in eight urban areas: Karachi, Lahore, Faisalabad, Rawalpindi, Multan, Hyderabad, Gujranwala and Peshawar.[39] This trend, which continued well into 2014 at a rate of 3 percent per annum, means that a youth population of 25 million and 50.22 million is currently located in urban and rural areas, respectively; most are

---

[31] Michael Kugelman, "Pakistan's Demographics: Possibilities, Perils, and Prescriptions," in *Reaping the Dividend: Overcoming Pakistan's Demographic Challenges* (Wilson Center, 2011), p. 6, available at http://www.wilsoncenter.org/sites/default/files/ReapingtheDividendFINAL.pdf (accessed 8 December 2014).

[32] National institute of Population Studies," Introduction to NIPS," at http://www.nips.org.pk/ (accessed 11 May 2014).

[33] See note 3 above.

[34] UN DESA, "Country Ranking by Median Age," at http://www.un.org/esa/population/publications/WPA2009/WPA2009_WorkingPaper.pdf (accessed 9 December 2014).

[35] Norina Bibi, "Population, Labour Force and Employment," *Pakistan Economic Survey 2010-11* (2011), pp. 153-4, available at http://www.finance.gov.pk/survey/chapter_11/12-Population.pdf (accessed 8 December 2014).

[36] The singulate mean age at marriage of females rose from 16 to 22.8, and of males from 18 to 26.4, between 1961 and 2007. For details, see Zeba A. Sathar, "Demographic Doom or Demographic Dreams: Pakistan at the Crossroads," *Reaping the Dividend: Overcoming Pakistan's Demographic Challenges,* p. 33.

[37] Mazhar, "Population, Labour Force and Employment," p. 160.

[38] Ibid.

[39] Nausheen Saba Nizami, "Population, Labour Force and Employment," *Pakistan Economic Survey 2009-10 (2010).*

unemployed.[40] Within this grouping, up to 10 million are estimated to be child laborers,[41] six million are unemployed youth (15-25 ages) and 3.40 million come from the unemployed labor force.[42] In general, the unemployment phenomenon is believed to be more of urban and male issue in Sindh and KP (Khyber Pakhtunkhwa) while rural in Punjab, with Balochistan experiencing no significant change.[43]

An important aspect within this calculus is the considerable surge of the unemployment rates during 2010-2011 of three age groups between 15 and 29 including females. This may impact internal migratory patterns, especially in Punjab; other provinces are least likely to experience net change in in-outflows in the short term. Cumulatively out of 25 million in the major urban centres of four provinces, and some 10 million in rural Punjab, approximately ten million youth including child labourers as well as those unemployed and underemployed emerge as relatively more susceptible to extremism.[44] In case trust in the present system is analyzed from the perspective of the youth, rampant disillusionment exists across the board among today's youth, which believe the government has failed to deliver on countless occasions due to inept policies and politicians.[45] All these cohorts can be considered to be in grave peril in that they are starved of education and productive opportunities, and are vulnerable to manipulation by those who do not have their best interests at heart.[46] These numbers constitute a menacing dimension if also viewed from the prism of 'latent radicalism' wherein radicalism [or extremism] may not necessarily be confined to the poor and less educated but found with equal intensity among affluent classes.[47]

Pathways of Youth Extremism

Pathways to extremism are not simple to define nor are they presumed to be linear in terms of occurrence. Conceptually, however a possible construct that welds together the whole process of extremisation in Pakistan comprises four fundamental elements - societal mindset, inspiration, channels and resident spheres (Figure 1).

---

40 UNICEF, "Pakistan Statistics," at http://www.unicef.org/infobycountry/pakistan_pakistan_statistics.html (accessed 9 December 2014).

41 Reuters, "Millions Pushed into Child Labour in Pakistan," *The Express Tribune* (7 February 2012), available at http://tribune.com.pk/story/332927/millions-pushed-into-child-labour-in-pakistan/ (accessed 8 December 2014).

42 United Nations, "Youth Unemployment Rate, Aged 15-24, at http://unstats.un.org/unsd/mdg/ SeriesDetail.aspx?srid=630 (accessed 9 December 2014).

43 Pakistan Bureau of Statistics, "Labour Force Participation Rates and Unemployment Rates by Age, Sex and Areas, 2012-2013," at http://www.pbs.gov.pk/sites/default/files/Labour%20Force/publications/lfs_Annual_2012_13/t14-pak.pdf (accessed 9 December 2014).

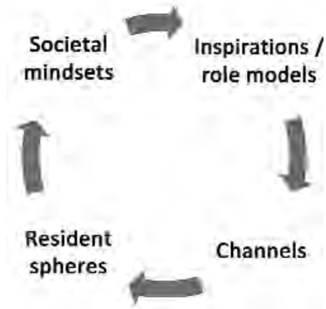
44 Zubair Chaudhry, "Unemployment and the PM's Youth Programme," *Express Tribune* (15 December 2013), available at http://tribune.com.pk/story/645852/unemployment-and-the-pms-youth-programme/ (accessed 8 December 2014).

45 Husham Ahmed, "Identity Crisis Haunts Pakistani Youth!" *The Statesmen* (2 Feb 2010), available at http://www.thestatesmen.net/news/identity-crisis-haunts-pakistani-youth/ (accessed 9 December 2014); Sadaf Basharat, "Craving for Change: Educated Youth, Perception Survey Report" (Peace Education and Development Foundation, 12 August 2012), available at http://pead.org.pk/Craving-for-Chang.pdf (accessed 9 December 2014).

46 "Pakistan: The Next Generation Report," (British Council, November 2009), p. 2, available at http://www.britishcouncil.pk/ programmes/society/next-generation (accessed 9 December 2014).

47 Siddiqa, "Red Hot Chili Peppers Islam – Is the Youth in Elite Universities in Pakistan Radical?" p. 26.

Figure 1 - Pillars of extremism in Pakistan



Source: Author's construction

Societal mindsets

As a nation-state, some have described Pakistan as a collection of mere images, and hence a distortion of reality; few have labeled it an unimagined nation, yet others have termed Pakistan an unachieved nation.[48] Manzoor Ahmed constructs Pakistan as a contradiction, arguing that the country has been either anti-intellectual or non-rational for ages. The people have a proclivity for sentimentalism, can be quickly provoked and have a mindset that cannot sustain a long and involved rational argument.[49] In part this popular mindset is inspired by a thinking mode that feeds on the conceptualization of social issues, including religious one, through a domain of binaries bordering on contradictory behaviors. Binary-framing schema are found among almost all societies; however while among Pakistanis it is an ingrained element of their organic traits, elsewhere or in Western popular discourse attitudinal distinction is confined to stereotyping certain issues.[50]

Consequently, the framework for understanding religious practice is generally seen through the binaries of informal–formal, common–elite, authentic–superstition, and orthodox–heterodox, amongst others. For example, it is a fact that poorer Pakistanis were actually less likely to support extremist groups than more affluent, better educated people.[51] Yet it is equally true of Pakistanis that alongside militants they favor some of the severest sentences for socioreligious crimes. A poll conducted in 2009 found broad support for harsh punishments: 78% favored death for those who

---

[48] Muhammad Feyyaz, "Ethnic Conflict in Sindh" (PILDAT Background Paper, October 2011), available at http://www.pil-dat.org/ publications/publication/Conflict_management/EthnicConflictinSindhOctober2011.pdf (accessed 8 December 2014) .

[49] Manzoor Ahmed, "Pakistan : Aporia of its Kind," in *Pakistan: The Contours of State and Society* (Soofia Mumtaz, Jean-Lucm, Imran Anwar Ali, eds., Oxford University Press, 2002), p. 61.

[50] For dominant narratives on Islamism and Islam, see David Belt, "Islamism in Popular Western Discourse," *Policy Perspectives* 6(2)(2009), available at http://www.ips.org.pk/islam-and-the-west/1084-islamism-in-popular-western-discourse (accessed 8 December 2014).

[51] Rob Crilly, "Poverty Does Not Breed Extremism in Pakistan, Study Finds," *The Telegraph* (20 May 2011), available at http://www.telegraph.co.uk/news/worldnews/asia/pakistan/8526473/Poverty-does-not-breed-extremism-in-Pakistan -study-finds.html (accessed 8 December 2014).

leave Islam; 80% favored whippings and cutting off hands for crimes like theft and robbery; 83% supported stoning adulterers and 71% favoured institutionalization of religious judges.[52] Even the youth from upper-middle class backgrounds tends to view the world from a black and white lens, amply demonstrated in a large youth sampling from leading universities of the country. The respondents clearly subscribed to a 'clash of civilizations' paradigm and, in spite of their privileged position, were unable to rise above their bias towards regional or global competitors.[53] It will be recalled that while the high-profile assassination of Governor Salmaan Taseer shocked many in Pakistan, not all condemned the murder. Indeed, thousands rallied to the assassin's (Mumtaz Qadri) defense lionizing him for his "religious honor and integrity, especially the so called moderate barelvi clergy.[54] *The Washington Post* reporting of the incident is instructive:[55]

> While many factions have lauded the slaying [of Governor Taseer], the peace-promoting Barelvi sect has spearheaded mass rallies to demand the release of the assassin, a policeman. Because most Pakistanis are Barelvis, their stance is challenging the belief long held among liberals here – and hoped for by nervous U.S. officials – that the Muslim majority in this nuclear-armed nation is more moderate than militant.

Inspiration and Extremist Role Models

Given the dominant role of religion in social narratives and Pakistan's status as an ideological state, inspirations generating religious extremism have ensued either directly from the proponents of a particular doctrine (some of which have transformed into larger movement(s)) or the ideologies propagated by external actors to further local interests. The leading examples of the former category are Mawlana Syed Abul Ala Mawdoodi, Haq Nawaz Jhangvi and Hafiz Saeed; all have radically shaped religious discourse in Pakistan.[56] Other than these people, the active jihadi ideologue collectivity in Pakistan spans an array of figures. Few have attained more fame than Fazalullah, Mawlana Aziz, Abdul Rashid Ghazi and Mawlana Samiulhaq. Dr Farhat Hashmi is likewise perceived as a religious bigot with increasing access to female space both in and outside Pakistan.[57]

---

52 The Pew Global Attitudes Project, "Pakistani Public Opinion: Growing Concerns about Extremism, Continuing Discontent With U.S.," (Pew Research Center, 13 Aug 2009 Pew Research Center, available at http://pewglobal.org/files/pdf/265.pdf (accessed 9 December 2014).

53 See Siddiqa, "Red Hot Chili Peppers Islam – Is the Youth in Elite Universities in Pakistan Radical?"

54 "The Flip Side of the Coin – Sunni Tehreek Plans to Provide Killer Legal Assistance," *Pakistan Today* (10 Jan 2011), available at http://www.pakistantoday.com.pk/2011/01/10/city/lahore/the-flip-side-of-the-coin-sunni-tehreek-plans-to-provide-killer-legal-assistance/ (accessed 9 December 2014); " Sunni Tehreek's Protest against Qadri Verdict Turns Violent," *The Express Tribute* (3 Oct 2011), available at http://tribune.com.pk/story/265857/sunni-tehreeks-protest-against-qadri-verdict-turns-violent/ (accessed 9 December 2014).

55 Karin Brulliard, "In Pakistan, Even Anti-violence Islamic Sect Lauds Assassination of Liberal Governor," *Washington Post* (29 Jan 2011), available at http://www.washingtonpost.com/wp-dyn/content/article/2011/01/29/AR2011012904706.html (accessed 9 December 2014).

56 See, e.g., Joy Aoun, et al, "Religous Movements, Militancy, and Conflict in South Asia" (Center for Strategic and International Studies, July 2012), available at http://csis.org/files/publication/120713_Aoun_Religious Militancy_Web.pdf (accessed 9 December 2014).

57 See Khalid Ahmed, "Daughters of Al Huda," *The Express Tribune* (August 21, 2010), available at http://tribune.com.pk/story/41523/daughters-of-al-huda/ (accessed 9 December 2014).

Jamaat-e-Islami (JI), an Islamist party similar to the Arab Muslim Brotherhood that Mawdoodi founded in 1941 at Lahore, possesses perhaps the most powerful and organized youth force in the form of the Islami Jamiat Talaba (IJT) in all higher educational institutions of the country. Over time, the source of its inspiration has transcended from the charisma of its erstwhile leader to the organizational appeal that it injects among vulnerable sections of freshmen and women joining colleges and universities. The IJT is widespread, authoritative, and violent, and knows nothing but to preach their radical version of Islam and build the JI's strength.[58] The Thunder Squad, the IJT armed wing designed to neutralize opponents, and the Allah's Tigers - a vigilante group of hooligans raised in early 1990s whose task was to attack cultural events it deemed 'un-Islamic' – outside campuses (disbanded by the JI in the mid-1990s), exemplify a level of violence that the IJT can pursue.[59] It draws its organizing philosophy from the JI's platform which "has built a coherent ideological case for global Islamic revivalism – a revivalism that includes the defense of violent jihad, but without identifying [itself] clearly with militant struggle."[60] Like IJT, Jamiat Talaba Arabia (JTA) is another youth arm of JI that is composed of students from a vibrant madrassa network operating under the banner of Rabitaul Madaris Al-Islamia. Other experiments by JI to mobilize youth through Shabab-e-Milli – its youth wing, and earlier through the somewhat controversial and later disowned 'Pasban' remained far from becoming as effective. Two of the four militant groups created by the JI i.e., Hizbul Mujahideen and al-Badar Mujahideen, are still active in Indian-held Kashmir, which facilitated the participation of IJT and JTA members in fighting in Kashmir and Afghanistan.[61]

The real spirit to vitalize JI youth lay in the person of Qazi Hussain Ahmed, Ameer-e-Jamaat for four terms in a row and Professor Khurshid Ahmad.[62] While the inspirational leadership of Qazi Hussain was characterized by a passion for jihad and a gift of gab, Professor Ahmad provided intellectual input to sustain the spiritual skeleton of the organization, including IJT. He has founded two institutions, namely, the Institute of Policy Studies Islamabad and the Islamic Foundation Leister, UK and edits Jamaat's monthly, Tarjuman-ul-Quran. Qazi Hussain Ahmed, who was described the patriarch of the transnational jihadists and held responsible for stoking the fire of civil wars in Afghanistan and beyond which eventually spilled over into Pakistan, played a pivotal role

---

58 Zahid Shahab Ahmed and Rajeshwari Balasubramanian, "Extremism in Pakistan and India: The Case of the Jamaat-e-Islami and Shiv Sena," (Policy Studies 50, Regional Centre for Strategic Studies, Colombo, 2010), available at http://www.rcss.org/publication/policy_paper/Policy50.pdf (accessd 9 December 2014).

59 Nadeem F. Parachi, "Bleeding Green: The Rise and Fall of the IJT," *Dawn.com* (16 August 2012), at http://www.dawn.com/news/742642/bleeding-green-the-rise-and-fall-of-the-ijt (accessed 9 December 2014).

60 Husain Haqqani, "The Ideologies of South Asian Jihadi Groups," *Current Trends in Islamic Ideology* (2005), available at http://www.carnegieendowment.org/2005/04/13/ideologies-of-south-asian-jihadi-groups/5uc (accessed 9 December 2014).

61 The other two groups are Hizb-e-Islami and Jamiatul Mujahideen. Hizbul Mujahideen primarily operates in Kashmir but also has a network in Pakistan. Muhammad Amir Rana, "Evolution of Militant Groups in Pakistan," Conflict and Peace Studies 4(2) (Apr-June 2011).

62 Jamaat-e-Islami Pakistan, "Prof Khurshid Ahmed," at http://jamaat.org/beta/site/page/44 (accessed 9 December 2014). Qazi Hussain Ahmed was active member of IJT during his student life, and remained patron of Shabab-e-Milli as well as Pasban before it finally parted ways with JI. S. Athar H. Rizvi, "Seminar Recalls Contributions of Three Subcontinental Luminaries," Saudi Gazette (March 22, 2013), available at http://www.saudigazette.com.sa/index.cfm?method=home.PrintContent&fa=regcon&action= Print&contentid=20130323158071&simplelayout=1 (accessed 9 December 2014).

in ideologising[63] the religious youth during his command tenures of the JI, which also saw a large participation of IJT and JTA members in Afghanistan and later in Kashmir Jihad. It would be remiss however not to highlight his change of heart in later years that was clearly visible from his affirmative recognition of societal radicalisation as a national threat, during an interview in late November 2010, by declaring extremists (mainly the Taliban) to be "inflexible in pursuing a fixated agenda of Islam."[64] How much his legacy persists in motivating the present generation of youth cadres of JI to participate in violent jihad is difficult to ascertain. There is nevertheless a nigh incarnation of Qazi Hussain - Siraj al-Haq the present head of JI, who shows a similar zeal, reflected in part by his public statements to wage jihad against US in case of an invasion of FATA and in part by his stern resentment against the textbook revision project by the KP government.[65] He is assessed to be a formidable surrogate to keep youth engaged in violent undertones.[66]

Punjabi Sunni hardliners follow the teachings of Mawlana Haq Nawaz Jhangvi, which arose out of the perceived cultural discrimination against the working Sunni class by local Shia landlords in the Jhang district of Punjab province. The primarily economic move against the Shias assumed sectarian and cultural dimensions when the entrepreneurs of this Sunni movement like Haq Nawaz Jhangvi (1952-1990) emphasized the cultural differences between the Sunnis and Shias to attribute the poverty of rural Sunni serfs to the cleverly manipulated sociocultural order that the Shi'ite landlords had imposed on the poor Sunnis for their own benefit.[67] Jhangvi and his affiliates who had "inherited the legacy of Deobandi Seminary went to the extent of reiterating the Deobandi position of 1940 that Shias should be declared non-Muslims and Kafirs."[68] Commencing with the founding of Anjuman Sipah-e-Sahaba (ASS) in 1970s which became Sipah-e-Sahaba Pakistan (SSP) in September 1985 to finally emerge as Ahl-e-Sunnat Wal Jamat (ASWJ) during 2002, the entire spiritual odyssey of the deeply religious Jhangvi was built on hatred of the Shias who he thought indulged in disrespect of or calling out names of sahaba (companions) of the Prophet Muhammad.[69] In particular, he detested the eclectic influence of Shi'i Sufi philosophy on Sunni Islam at local levels and avowed to challenge Shias culturally at all levels. [70] The underlying philosophy of the SSP was to purify Islam from heretical Sufi practices and defend Sahaba from its opponents, which was originally aimed at Shias but later also placed Barelvis, in the category of adversaries.[71] Glimpses of his sectarian philosophy have become part of the enduring appeal of

---

63 Dr Mohammad Taqi, "COMMENT: Qazi Hussain Ahmad: The Jihadist Patriarch," *Daily Times* (January 10, 2013), available at http://archives.dailytimes.com.pk/editorial/10-Jan-2013/comment-qazi-hussain-ahmad-the-jihadist-patriarch-dr-mohammad-taqi (accessed 8 December 2014).

64 Qazi Hussain Ahmed, "Maududi's Conception of Jihad and Radicalisation (Interview by the Author in Mansoora, Lahore 18 November 2010).

65 Qaiser Butt, "Shrinking Space: K-P Govt Shelves Plans for Textbook Reforms: JUI, JI Protested against Revised, Secular Syllabus," *The Express Tribune* (6 April 2012), available at http://tribune.com.pk/author/965/qaiser-butt/page/21/ (accessed 8 December 2014).

66 Comments by a key member of JI youth network (name is withheld on request), Lahore (7 February 2013).

67 Ashok K. Behuria, "Sunni-Shia relations in Pakistan: The Widening Divide," *Strategic Analysis* 28(1)(2004), pp. 157 – 176.

68 Ibid.

69 Ibid.

70 Ibid.

71 South Asia Terrorism Portal, "Sipah-e-Sahaba Pakistan," at http://www.satp.org/satporgtp/countries/pakistan/terroristoutfits/Ssp.htm (accessed 9 December 2014).

SSP, including its violent body Lashkar-e-Jhangvi (LeJ), which labels the SSP (or now ASWJ) putatively as non-violent and non-aggressive towards its opponents. The unyielding strength of the SSP and the LeJ can be judged from the resolve of its present leadership, as indicated in their firm commitment to constantly seek out and persuade their opponent "that he is mistaken."[72] Deobandi madrassa students in particular and Deobandi youth in general are the centre of their inter/intra sectarian appeal. For Shia youth, spiritual sources are personified by the theology of the Najfi and Qum schools.

Within the Salafi stream of thought, Hafiz Saeed is the foremost name and founder of the Markaz al-Dawa-wal-Irshad (Centre for Preaching and Guidance - MDI) which he along with Dr. Yousuf Abdullah Azzam and Professor Zafar Iqbal established to propagate an ideology integrating missionary work and jihad during the mid-1980s.[73] It participated in the Afghan jihad under the same name, but in 1993, MDI divided its activities into two related but separate organisations: MDI proper continued the mission of proselytization and education.[74] In December 2001, Hafiz Saeed renamed MDI to be Jamaatud-Dawa (JuD), a larger umbrella organization to sustain missionary pursuits, and created a military component, Lashkar-e-Taiba (LeT), which henceforth focused on jihad in Kashmir. Saeed's son Talha Saeed and son-in-law Hafiz Khalid Waleed are the emerging faces of JuD, who along with six higher echelons in leadership hierarchy have recently been targeted under an expanded sanctions regime by the US for continuing terrorist activities in Pakistan, Afghanistan, India, Nepal, Bangladesh and other regions.[75] Hafiz Saeed and his group primarily hail from the Ahle Hadit confession, "a sub continental movement vaguely beginning in the 8th Century that grounds its tradition in a belief of the advent of the Hadit (sayings of the Prophet Muhammad) into this region directly through various sahabas during the life time of Prophet, hence are called 'Ahle Hadit' (bearer of sayings of the Prophet)'.[76] Hafiz Saeed was educated in Saudi Arabia, therefore he had no financial constraints when he launched MDI.[77] What particularly distinguishes the ideological leanings of Hafiz Saeed from contemporaries is his organizational commitment to the integrity of Pakistan and his opposition to Deobandis' militancy against Barelvis; JuD and LeT instead insist that Pakistani Muslims are all brothers, irrespective of their sectarian dispositions. In sociopolitical terms, such resolve has translated into some key impacts on ground. First, it has maintained discernable support for Hafiz Saeed, both from Islamabad and from ordinary Pakistanis, evident also from his custodial releases by superior courts.

---

72 Ibid.

73 Dr. Thomas K. Gugler, "Jihadism in Pakistan: Going Global" (unpublished paper), available at http://www.academia.edu/ 2122078/ Jihadism_in_Pakistan_Going_Global (accessed 8 December 2014).

74 C. Christine Fair, "Lashkar-e-Tayiba and the Pakistani State," *Survival,* 53:4 (2011), pp. 29-52, available at http://www.iiss.org/en/publications/survival/sections/2011-2760/survival—global-politics-and-strategy-august-september-2011-66cf/53-4-06-fair-2-578e (accessed 8 December 2014).

75 Arif Qoreshi, "Hafiz Saeed's 'Son' and 'Son in Law' Included into the FTO," *The Fortress* (10 September 2012), available at http://www.thefortress.com.pk/hafiz-saeeds-son-and-son-in-law-included-into-the-fto-2/ (accessed 8 December 2014).

76 Muhammad Feyyaz, "Facets of Religious Violence in Pakistan," *Counter Terrorist Trends and Analysis*, 5(2) (2013), pp. 9-13.

77 Aoun Sahi, "Dawa, Jihad, Charity or All?" *The Jang-News Weekly* (16 April 2012), available at http://jang.com.pk/thenews/apr2012-weekly/nos-15-04-2012/spr.htm#6 (accessed 8 December 2014).

Secondly, his message of jihad in Kashmir has nationwide appeal, not only among Ahle Hadit student movements such as Talaba Jamaatud Daawa and Ahle Hadith Student Federation (ASF), as well as lay youth like theAhle-Hadith Youth Force and Jamaat-ul / Tehreekul Mujahideen, but also among Deobandis and Barelvis youth who form the overwhelming segment of its recruitment. [78]

The Daawa school system has grown in strength with the current number of schools as high as 500 throughout Pakistan.[79] It is difficult to estimate the present number of students in Dawa schools; it was around 35,000 during 2007.[80] Engagement in social work and participation in natural calamities during the earthquake of 2005 and floods in Pakistan during 2010 allowed the organisation to permeate into the lower strata of the society. [81] Besides, JuD has instituted training camps for its members with sight and hearing impairment, most of them young. Presently, the number of these members runs into thousands. There are 1,500 in Lahore alone that regularly attend JuD resource persons lectures in which they are taught about society and religion. JuD also teaches these disabled youth the affairs of the world to foster awareness in "what is happening in Kashmir, Palestine and what is the role of India, America and Israel in these issues," [82] Umm-Talha, wife of Hafiz Saeed, is also giving *dars* (lesson) for women at JuD's main mosque, the Masjid Qadsia in the Chauburji neighborhood of Lahore.[83] Unlike several identical organisations, JuD has never experienced a leadership split of any consequence since its founding; Hafiz Saeed has continued as the ideological head of JuD.

The TTS (Tehrik-e-Taliban Swat) under Fazalullah which has its origin in the TNSM (Tehrik Nifaz Shariat-e-Muhammadi), was the principal showpiece of the TTP (Tehrik-e-Taliban Pakistan) at its peak during 2007-2009. Considerably waned in the wake of military operations, Fazalullah, now leading the TTP, commands strong influence among a extremist constituency of the sectarian and *jihadi* zealots.[84] In the same way Mawlana Aziz and his late brother Ghazi from Lal Masjid remained on *jihadi* epics as the much revered religious symbols but subsequent to military operations have become history.

Nicknamed the father of the Taliban for his role in educating many of the Afghan students who rose up to capture Kabul in the 1990s,[85] Samiul Haq, leading his faction of Jamiat Ulmae-e-Islam (JUI), is noteworthy in terms of his outreach to violent extremists. He has mentored thousands of jihadi youth who are part of the ranks of the Afghan and Pakistan Taliban. As a political leader but most significantly as the chancellor of the Darul Uloom Jamia Haqqania (DUJH) Akora Khattak, which houses up to 4000 students and is ranked among the leading Deobandi seminaries in the

---

78 See Fair, "Lashkar-e-Tayiba and the Pakistani State."

79 Gugler, "Jihadism in Pakistan: Going Global."

80 Ibid.

81 Ibid.

82 Waqar Gillani, "Able Partners: JuD's Deaf Wing Camps Are Quite Productive," *The Jang-News Weekly* (16 April 2012), available at http://jang.com.pk/thenews/apr2012-weekly/nos-15-04-2012/spr.htm#6 (accessed 8 December 2014).

83 Gugler, "Jihadism in Pakistan: Going Global."

84 For a detailed account of Fazul-ul-llah, see Muhammad Feyyaz, "Political Economy of Tehrik-e-Taliban Swat," *Peace and Conflict Studies* 4(3) (2011), pp. 37-60.

85 "Samiul Haq Renounces Support for Polio Immunization," Pakistan Today (22 Jul 2012), http://www.pakistantoday.com.pk/2012/07/22/national/samiul-haq-renounces-support-for-polio-immunisation/ (accessed 8 December 2014).

country,[86] Samiulhaq influences youth mindsets markedly as evinced by his methods and content of instruction (DUJH is dubbed the 'University of Jihad'). Pakistan's FIA has claimed that the plan to assassinate Benezir Bhutto was hatched at this seminary.[87] Another somewhat less discussed but still prominent religious scholar is Farhat Hashmi, whose controversial theology has earned her censure from a large body of ulema (religious scholars) for allegedly cultivating narratives of al-Qaeda in Muslim women.[88] Her interpretations are marked by the doctrinal stance of Ahl-i Hadith, which rejects most customary practices and intermediaries to privilege foundational texts and individual religious responsibility.[89] Some observers therefore worry whether the conservative Islamic activism of al-Huda's (Hashmi's Institute) could lead to endorsement of, or participation in, radical forms of Islamic extremism. A few fear that a generation of South Asian girls will follow Dr Hashmi's extremist teachings.[90]

In addition to the aforementioned, two key sources in the public arena engendering extremists are madrassas and public schools. Apart from being dubbed as recruitment centres for militancy, madrassas are increasingly becoming a source of a new social order. Its commissioning religious leadership is "not necessarily well-versed in religious scholarship but is enthusiastic in instrumentalising Islam by increasingly becoming assertive and uncompromising in projecting their own form of *Shari'a*."[91] It is not uncommon hence to find turf wars among competing ideologues and their young followers in urban locales to gain control of the mosques of rival sects through land acquisition[92] and coercively eliciting political clientele in universities by armed youth wings of student organisations.

The discussion here should not obscure the fact that madrassas alone are responsible for producing youth power elites. Some experts (such as Christine Fair, Pervez Hoodbhoy, Asim Ijaz Khwaja, Tahir Andrabi, Jishnu Das and Tristan Zajonc) have challenged assumptions of these schools as major militant hubs.[93] According to Anatol Lieven, a majority of known Pakistani

---

86 For details, visit Darul Uloom Jamia Haqqania, "Akora Khattak," at http://www.jamiahaqqania.edu.pk/ (accessed 8 December 2014).

87 "View: Blackguards of Fanaticism Silenced Bashir Bilour," *Daily Times* (December 29, 2012), available at http://alisalmanalvi.wordpress.com/tag/sami-ul-haq/ (accessed 8 December 2014).

89 Faiza Mushtaq, "A Controversial Role Model for Pakistani Women," *South Asia Multidisciplinary Academic Journal* (4) (2010), available at http://samaj.revues.org/3030 (accessed 8 December 2014).

90 Khalid Hasan, "Quake God's Punishment for 'Immoral Activities': Farhat Hashmi," *Friday Times (*1 November 2005), available at http://archives.dailytimes.com.pk/national/01-Nov-2005/quake-god-s-punishment-for-immoral-activities-farhat-hashmi (accessed 8 December 2005).

91 Saeed Shafqat, "Praetorians and the People," in *Pakistan: Beyond the Crisis State* (Maleeha Lodhi, ed, Columbia University Press, 2011), p. 101; Huma Yusuf, "Sectarian Violence: Pakistan's Greatest Security Threat?" (NOREF Report, 9 August 2012), available at http://www.peacebuilding.no/Regions/Asia/Pakistan/ Publications/Sectarian-violence-Pakistan-s-greatest-security-threat/%28language%29/eng-US (accessed 8 December 2014).

92 "One Killed as Jamaat-ud-Dawa and Sunni Tehreek Fight over Mosque," *The Express Tribune* (2 July 2011), available at http://tribune.com.pk/story/200553/one-killed-as-jamaat-ud-dawa-and-sunni-tehreek-fight-over-mosque/ (accessed 8 December 2014).

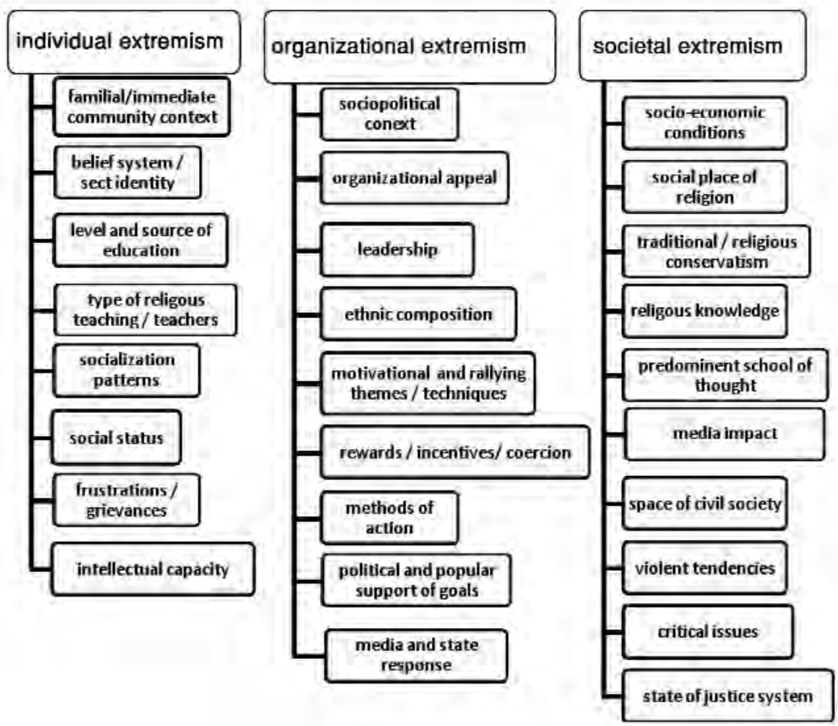
93 See Tahir Andrabi, et al, "Religious School Enrolment in Pakistan: A Look at the Data" (unpublished paper, 2005), available at http://www.hks.harvard.edu/fs/akhwaja/papers/MadrassaCERNov05.pdf (accessed 8 December 2014; Tahir Andrabi, et al, "The Madrasa Myth," *Foreign Policy* (June 2009), available at http://foreignpolicy.com/2009/06/ 01/ the-madrasa-myth/m (accessed 8 December 2014); Robert O'Neill, "Learning from Pakistan," *Harvard Kennedy School Magazine* (Winter 2010), available at http://www.hks.harvard.edu/news-events/publications/hks-magazine/archives/winter-2010/learning-from-pakistan/ (accessed 8 December 2014); Jayshree Bajoria, "Pakistan's Education System and Links to Extremism" (Council of Foreign Relations Backgrounder, 7 Oct 2009), available at http://www.cfr.org/pakistan/pakistans-education-system-links-extremism/p20364 *accessed 9 December 2014(; "Ideas on democracy, free and peace" (Future Youth Group, 2009), available at https://fygpakistan.wordpress.com/; K. K. Aziz, *The Murder of History* (Vanguard Books Pvt Ltd, 1993); Husham Ahmed, "Identity crisis haunts Pakistani youth," *The Statesman* (Feb. 2nd, 2010), available at http://www.thestatesmen.net/news/identity-crisis-haunts-pakistani-youth/ (accessed 8 December 2014); "History taught in Pakistan challenged," *Times of India* (3 Feb 1999), available at https://groups.google.com/forum/#!topic/alt.india.progressive/bJaInlTyO_Q (accessed 8 December 2014).

terrorists have in fact attended government schools and quite often have a degree of higher education. He pins the basis for Islamism on the urban lower middle classes rather than the impoverished masses, [94] for in Pakistan, the rural masses can occasionally be stirred up to the furious panic by the cry of 'Islam in danger.'[95] For instance, LeT draws its recruits not from madrasas but from universities, colleges and among unemployed youths.[96]

Channels and Resident Spheres

Individual, organizational and societal extremism in Pakistan can be understood to comprise the elements shown in Figure 2. The frames in the figure reveal sources cultivating extremism in individuals, groups or the society at large. The process to become violent extremist may be direct (or instant), graduated or forced, and is determined by the perspective (opportunity or motive) being espoused by those adapting to extremism. Among others, mainly the family, madrassas, mosques, individual ideologues and society feed the human resource to violent organizations (Figure 3).

Figure 2 – Determinants / Elements of Religious Extremism



Source: Author's compilation

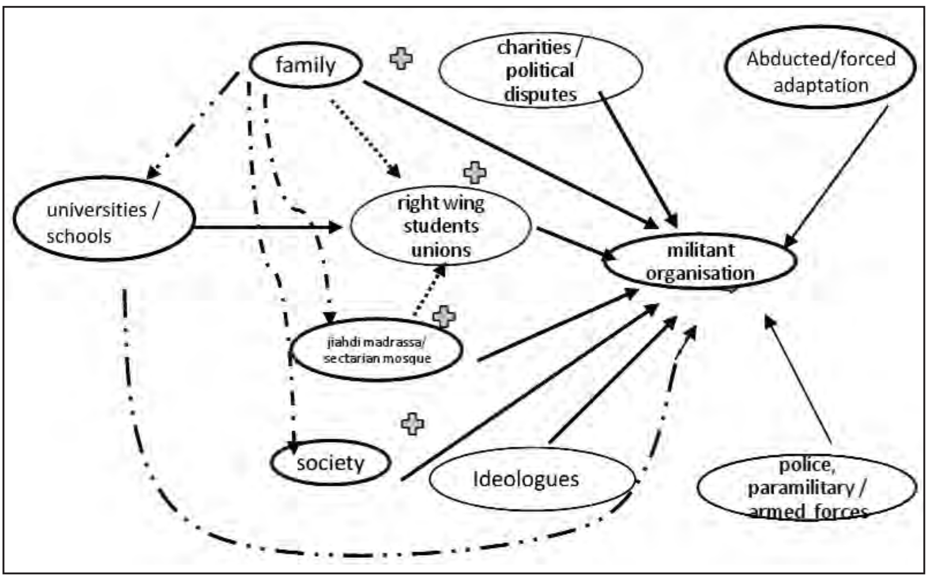
[94] Anatol Lieven, *Pakistan – A Hard Country* (Public Affairs, 2011), p. 160.

[95] Ibid, pp. 127-28.

[96] See Fair, "Lashkar-e-Tayiba and the Pakistani State."

The opportunity incentives i.e., prospective gains steered by economic and ideological factors or motives paradigm informed by grievance(s), constitute the dominant motivational frameworks in micro-macro decisionmaking to join rebel organizations.[97] More fertile constituencies that readily fall for militant organizations are madrassa students and local (tribal) youths followed by college students or those unemployed motivated by the appeal of glamour, feelings of revenge, financial incentives, and religious beliefs. The local cell of the organization acts as the recruiting hub. Recruitment exploits family and clan loyalties, tribal lineage, personal friendships, social networks, madrassa alumni circles, and shared interests.[98] For instance, almost all religious seminaries, fugitives and youth section of religious movements were the first to join the ranks of the Taliban during 2003. After entrenching itself firmly in the FATA during 2003, the reach of terrorist groups gradually expanded to adjacent settled areas (the southern districts of KP) into its hinterland; later they engulfed all major and medium-sized urban centres of the country. [99]

Figure 3 - Sources and channels for extremis



Source: Author's compilation

It is difficult to classify with precision which of the channels are most common; madrassas known for jihadi products, armed religious student unions and militant organisations can be described generally as the more frequented routes to violent extremism. In most cases, however,

[97] For an explanation, see Henrik Urdal, "A Clash of Generations? Youth Bulges and Political Violence," (UN Doc. UN/POP/EGM-AYD/2011/10 (2011), p. 1, available at http://www.un.org/esa/population/meetings/egm-adolescents/p10_urdal.pdf (accessed 8 December 2014).

[98] Major Shahid Afsar, Pakistan Army; Major Chris Samples and Major Thomas Wood, U.S. Army, "The Taliban: An Organizational Analysis," *Military Review* (May-June 2008), available at http://usacac.army.mil/cac2/AIWFC/COIN/repository/Understanding_Taliban_Organization_Mil_Review%28May-Jun08%29.pdf (accessed 9 December 2014).

[99] Muhammad Feyyaz, "Conceptualising Terrorism Trend Patterns in Pakistan – an Empirical Perspective," *Perspectives on Terrorism* 7(1) (2013), available at http://www.terrorismanalysts.com/pt/ index.php/pot/article/ view/ 243/html (accessed 9 December 2014).

family alone accounts for the grooming of siblings into jihadi mindsets. Practically, this dimension of channeling has not received as much attention for policy and reform agendas by the state and non-state development institutions. The state's responses to extremism are at best limited to easily available cosmetic solutions rather than addressing the deep-rooted problem – the social environment for violence and radicalization.[100]

Physical Spread of Youth Extremism

Lieven pointedly indicates urban areas as potential breeding spots of extremism with selective encroachments in the rural regions, such as in central and southern Punjab, in KP and the FATA.[101] He mainly identifies two radical forces that, according to him, have established a long-running presence in parts of the countryside i.e., Sunni sectarian extremists of the central and southern Punjab, as well as other Islamist Taliban groups in KP and the FATA.[102] Amir Rana claims that over 100 militant and Taliban groups and foreign terrorist networks are operating in and from the tribal areas of Pakistan, having grown from 26 during 2009.[103] Besides the Taliban, other non-state actors involved include a spectrum of militant organizations – some operating under control of the TTP, others loosely affiliated with it. The TTP now boasts having franchises in all four provinces of the country. Each province has a regional commander (located mostly in provincial capitals) who coordinates the planning, organization and execution of contemplated acts independently or in cooperation with other militant groupings. At the local level, provincial chapters of the TTP give primacy to their particular tribal or ethnic identity, even though they cooperate with other provincial chapters in terms of operations when required.[104] Foreign fighters of Afro-Asian origins comprising financers, logisticians and technical tentacles belonging to 'al-Qaeda and Associated Movements' (AQAM) such as *Qaeda al-Jihad* etc. and elements of the Eastern Turkestan Islamic Movement are also reported present in the FATA.[105] Further, there are numerous cell-centric outfits, almost amorphous and unknown to each other, operating on individualistic impulses and theological interpretations that have nominal associations with major terrorist organizations and accept no central authority.[106]

---

[100] Akbar Nasir Khan, "Radicalisation and State Response," The *Friday Times* (21-27 Jan 2011), available at http://www.thefridaytimes.com/21012011/page7.shtml (accessed 8 December 2014).

[101] Lieven, *Pakistan – A Hard Country,* pp. 127-28.

[102] Ibid.

[103] Amir Rana, "What is Young Pakistan Thinking?" *The Express Tribune Blogs* (2 Sep 2010), http://blogs.tribune.com.pk/story/1342/what-is-young-pakistan-thinking/; Muhammad Amir Rana, "Taliban Insurgency in Pakistan: A Counterinsurgency Perspective," *Conflict and Peace Studies* 2(2)(2009), pp. 9-31.

[104] Feyyaz, "Facets of Religious Violence in Pakistan."

[105] Muhammad Rana, Safdar Sial and Abdul Basit, *Dynamics of Taliban Insurgency in FATA*, (PIPS Publications, 2010), pp. 57-58; Mansur Khan Mahsud, "The Battle for Pakistan: South Waziristan - Militancy and Conflict in South Waziristan" (Counterterrorism Strategy Initiative Policy Paper, New America Foundation, 2010), available at http://newamerica.net/publications/policy/the_battle_for_pakistan_south_waziristan (accessed 9 December 2014);

Wajahat Ali, "China Says Terrorists from Xinjiang Hiding in Pakistan," *Daily Times* (29 May 2004); South Asian Terrorism Portal, "FATA Timeline 2003," at http://www.satp.org/ (accessed 9 December 2014).

[106] Feyyaz M. Pasha, "Osama's departure and its aftermath for Pakistan," *pkarticleshub.com* (6 May 2011), http://www.pkarticleshub.com/2011/05/06/osama%E2%80%99s-departure-and-its-aftermath-for-pakistan/ (accessed 9 December 2014).

Outside the FATA, the government was able to register around 24,000 madrassas during December 2011,[107] leaving countless more seminaries as unregistered. There are 83 illegally constructed mosques and seminaries in Islamabad alone.[108] In Balochistan, its provincial capital Quetta leads the figures with 573 religious schools, Khuzdar has 206, Pishin 117, Chaghai 105 and Loralai 109.[109] The figures are believed to be staggering in other Pakhtun districts of northern Balochistan. Quetta is the operational centre of scores of Baloch armed groups, Afghan Taliban, LeJ Balochistan and Iran-based Jundullah. In KP, in addition to its southern districts which are considered religiously dogmatic, the influx of more than 2.5 million Afghan refugees, perhaps a million of them now naturalised as citizens of Pakistan (carrying Pakistani identity cards), served to change the socio-demographic fabric of the frontier regions.[110] The ethnic Pakistanis, if not all, those residing in KP and Balochistan bordering Afghanistan, having common lineage, therefore cannot remain indifferent to the sufferings and tribulations besetting their ethnic brethren. The resultant pain and anguish is shared and manifested in varying degrees, including religious extremism. Darul Aloom Haqqania is the largest seminary located in KP, which has churned out a major part of the Afghan Taliban leadership in addition to those from the FATA. Only 3,343 seminaries are registered with the government, but the actual number is not known.[111] The schools and madrassas run in Afghan refugee camps by Deobandi clergy are yet to be recorded, but are estimated to be at least 100. It may be noted that the JUI (F) and JUI-Sami, (two factions of the Deobandi political parties) ran over 65 per cent of all madrassas in Pakistan (in KP and northern Balochistan) until 2007.[112] One of the largest, Darul Aloom madrassa in Balochistan, was annually enrolling 1,500 boarders and another 1,000 day-students a few years ago.[113] At present, more than half are controlled by the Deobandi JUI-F and are evenly scattered throughout the province, including Baloch-dominated areas. While in government earlier as well as now, the Deobandis have poured resources into their madrassa network to consolidate and expand their political hold over the province.[114] It is important to note that since the collapse of Taliban rule in Afghanistan, Balochistan province became a major centre of anti-Shi'a militants.[115]

---

[107] "Madaris Not Registered to be Considered Illegal after Jan 1: Rehman Malik," *Associated Press of Pakistan* (19 December 2011), available at http://app.com.pk/en_/index.php?option=com_content&task=view&id=171165&Itemid=2 (accessed 13 November 2014).

[108] "The Trouble with: Madrassas in Pakistan," *The Express Tribune* (January 25, 2012), http://tribune.com.pk/story/326941/the-trouble-with-madrassas-in-pakistan/ (accessed 9 December 2014).

[109] "18,352 Registered Madressahs in Country, NA Told," *Dawn* (12 Sep 2011), available at http://www.dawn.com/news/658520/18352-registered-madressahs-in-country-na-told (accessed 9 December 2014).

[110] Are Knudsen, "Political Islam in South Asia" (Chr. Michelsen Institute, 2002), available at http://www.cmi.no/publications/file/796-political-islam-in-south-asia.pdf (accessed 9 December 2014).

[111] "18,352 Registered Madressahs in Country, NA Told."

[112] "Pakistan: Karachi's Madrasas and Violent Extremism" (Asia Report N°130, International Crisis Group, 29 Mar 2007), available at http://www.crisisgroup.org/en/regions/asia/south-asia/pakistan/130-pakistan-karachis-madrasas-and-violent-extremism.aspx (accessed 9 December 2014).

[113] William Dalrymple, "Inside Islam's "Terror Schools," *New Statesman* (28 March 2005), available at http://www.newstatesman.com/politics/international-politics/2014/04/inside-islams-terror-schools (accessed 9 Decem-ber 2014).

[114] "The State of Sectarianism in Pakistan," (Asia Report N°95, International Crisis Group, 18 Apr 2005), available at http://www.crisisgroup.org/en/regions/asia/south-asia/pakistan/095-the-state-of-sectarianism-in-pakistan.aspx (accessed 9 December 2014).

[115] Husain Haqqani, "'Weeding out the Heretics': Sectarianism in Pakistan," (01 Nov 2006), at http://www.friendskorner.com/forum/f137/sectarianism-pakistan-must-read-article-59650/ (accessed 9 December 2014).

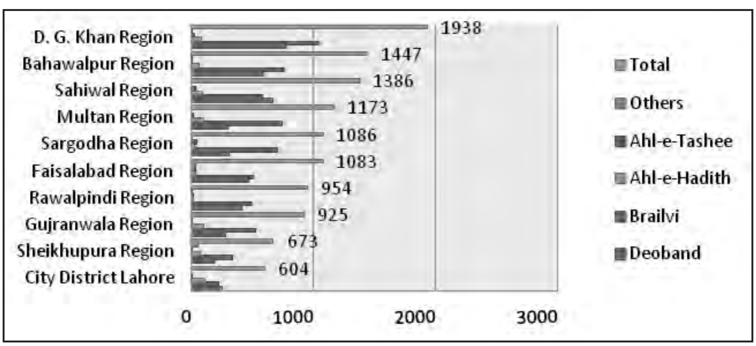
Punjab is the largest province of Pakistan. All major sectarian terrorist groups (ASWJ, LeJ, SeM), Salafist-Wahibi-Deobandi militants (JuD, LeT, TTP Punjab) and Kashmiri fighters, are present there. The highest concentration of religious organizations is in this province, where 107 organizations have their headquarters. The provincial capital Lahore, described as the capital of religious organizations, is the only city in South Asia where at least 71 religious organizations operate. Multan is the second major hub in the province where 18 religious organizations have their headquarters.[116] Besides, in Punjab, areas of religious extremism can be determined from the rapid growth of seminaries between 1975 and 2001 in major districts (see Table 1 below). From a total of 2715 in 2001, these grew to a total 11269 in the next decade, more than 400 percent, including proliferation to new areas and regions belonging to all the sects most notably Deobandi, Barelvi and Shia (Figure 4). With some variations, at present Punjab has the largest number of madrassas — 12,903. Except for Lahore which has 1,110 madrassas, the heavy concentration is situated in the southern districts of the province.[117] A worrisome aspect is that 90 per cent of foreigners studying in religious seminaries across Punjab have expired visas. [118]

Table 1 – Growth of Seminaries in Punjab 1975-2001

Division	1975	1980	1985	1990	1994	2001
Bahawalpur	278	417	598	795	883	971
D. G. Khan	153	217	297	363	411	397
Multan	45	102	179	212	325	363
Lahore	75	120	170	219	323	356
Rawalpindi	58	85	119	157	169	186
Sargodha	75	98	130	148	149	164
Gujranwala	52	66	96	131	140	154
Faisalabad	?	?	?	?	112	124
Total	**736**	**1105**	**1589**	**2025**	**2512**	**2715**

Sources: Zaman (1998: p. 710), Herald (2001d)

Figure 4 - Sect Wise Breakup - Deeni Madrassas in Punjab 2010



Source: Punjab Police 2010

[116] Rana, "Evolution of Militant Groups in Pakistan."

[117] Ibid.

[118] Ibid.

In Sindh, Karachi is the centre of extremist ideologues and operatives. It is also Pakistan's crime capital with a seamy underbelly of arms, drugs, land mafia, contract killers, extortionists and kidnappers, involved in a business estimated around Pakistani Rs 4,000 and Rs 5,000 crore annually.[119] The city has bled persistently for about two decades on account of ethnic, political, sectarian and other reasons.[120] By contrast the Taliban and other religious extremists kill tiny numbers in Karachi.[121] But infiltration by ideologues inimical to the interests of the state and violent jihadis has added complexity into the already fluid and explosive environment of the urban areas of Sindh.[122] Other than a handful of JI and Ahle Hadith seminaries, the vast majority of Karachi's sectarian and jihadi madrasas follow the Deobandi confession and are associated with the Wafaq al-Madaris al-Arbiya, the Deobandi madrassa union.[123] Many Karachi leaders state that over 60 percent of the seminarians in the city are Pakhtun and Afghan (Deobandi) madrassas. Recently a madrassa was shown on TV training troubled youths as suicide-bombers for al-Qaeda and the Taliban.[124] It is also the regional seat of TTP Sindh, Pakistani Jundullah, Pakistan Sunni Tehrik, and Afghan cartels, among others.

Ironically most of the nation's universities have also seen widespread intimidation, threats of mass violence, and interference with examinations, faculty hiring, and admission of new students, by heavily-armed radical religious organizations.[125] During March 2010, the death of a student for playing music inside his dormitory room at the hands of a student wing of the Jamaat-i-Islami sparked riots and clashes between rival student factions, prompting the authorities to close down all educational institutions on the campus of the University of Engineering and Technology, Peshawar.[126] In another instance, IJT's hooliganism at Punjab University following the assassination of one of their former activists in May 2012 created a big commotion. [127] In June of the same year, intimidation and harassment of students and teachers in the Philosophy Department of Punjab University by activists allegedly belonging to IJT caught the attention of national media, which was termed as alarming by the Human Rights Commission of Pakistan.[128] Experiencing similar practices

---

119 Qaswar Abbas, "Karachi: World's Most Dangerous City," *India Today* (27 Aug 2011), available at http://indiatoday.intoday.in/story/worlds-most-dangerous-country/1/149333.html (accessed 8 December 2014).

120 Ibid.

121 "Violence in Karachi, Into the Abyss," *The Economist* (27 Aug 2011), available at http://www.economist.com/node/21526919 (accessed 8 December 2014).

122 Feyyaz,,"Ethnic Conflict in Sindh."

123 "Pakistan: Karachi's Madrasas and Violent Extremism."

124 Khaled Ahmed, "Too Weak to Attack North Waziristan", *Friday Times* XXIV(37) (October 26 - November 01, 2012), available at http://www.thefridaytimes.com/beta3/tft/article.php?issue=20121026&page=2 (accessed 9 December 2014).

125 Patrick Belton, "Democracy In Pakistan: A Legacy Of Democratic Failure (2/3)," *WindsofChange.com* (Oxford Democracy Forum, 6 May 2004), at http://www.windsofchange.net/archives/democracy_in_pakistan_a_legacy_of_democratic_failure_23.html (accessed 12 November 2014).

126 Ali Hazrat Bacha, "UoP Closed after Student`s Death Sparks Riots," *Dawn* (Mar. 20, 2012), available at http://archives.dawn.com/archives/74451 (accessed 9 December 2014).

127 Xari Jalil, Campus Politics Turns Bloody, *Dawn* (May 23, 2012), available at http://www.dawn.com/news/720717/campus-politics-turns-bloody (accessed 9 December 2014).

128 Zohra Yusuf, "Armed Jamiat Fanatics Attack Students & Teachers at PU," *Viewpoint* (30 June 2011), available at http://www.viewpointonline.net/2014/06/armed-jamiat-fanatics-attack-studentsteachers-at-pu/887-armed-jamiat-fanatics-attack-students-teachers-at-pu (accessed 9 December 2014).

in the past, the University of Karachi was forced to issue a code of ethics for the students on the commencement of the new academic session in January 2013, which among other things specifically addressed the use of force, intimidation or interference in the university's administrative affairs.[129] Finally, in ascertaining the physical spread of extremism, household women should not be ignored as they constitute a major target audience amenable to manipulation by the media, as well as dictated socio-religious ethos transmitted by male family heads. [130]

Conclusion and Policy Suggestions

The paper has reviewed youth religious extremism in Pakistan delineating the contexts, demographics, inspirations and resident spheres of its occurrences. It finds that the phenomenon has firm roots in the society; however, no given definition fully captures its manifest character due to conflicting social nuances and the absence of bipartisanism in defining it. The literature views extremists as diseased, immoderate, inflexible or irrational actors, at times mixing conservatism as well as sentimental attributes of society with religious narratives. To the contrary, the stakes involved e.g., esteem, reputation, ambitions, money, power and life, plainly defy these assertions warranting a revisit to the fundamentals of definitional aspects. Also, this skewed approach towards youth extremism limits the spectrum of policy responses. Likewise, the narratives, inspirations and motivational themes employed by extremist organizations and their ideologues are so skillfully harmonized with topical grievances and frustrations of the society that these have become deeply ingrained as a regular feature of social life in Pakistan. Only a reasoned, articulate and structurally coherent policy response can meaningfully address these. It should, it is suggested, envisage youth religious extremism in Pakistan as a rational belief position underpinned by an internalized worldview that seeks clout, revenge and deliverance. It is expected that interventions predicated on this suggestion will help craft policy options which will be consistent with realities, hence are expected to be resulted oriented.

The number of violent extremists is an insignificant fraction given the demographics of the country. However, those vulnerable to extremism including women are assessed to be sizeable due to a burgeoning youth population deprived of opportunities, and the urban areas is their primary abode. The type of extremism they may espouse will depend upon the religious or sectarian community they belong to in addition to the prevailing degree of religiosity and cultural conservatism at home. The state and family units are unlikely to insulate such large youth population, more specifically the males, from developing intimate interactions with groups and organizations who can meet their psychosocial, spiritual and material needs, as no coherent anti-extremism policy exists at any level, barring efforts by a handful of civil society organizations. Due to longer exposure periods, social trends of late marriages have also implications for attitude formation and warrant matching attention. A national policy and action plan is required by integrating relevant ministries,

---

129 Associated Press of Pakistan, "KU Issues Code of Ethics for Students," *The Nation* (19 January 2013), available at http://nation.com.pk/karachi/19-Jan-2013/ku-issues-code-of-ethics-for-students (accessed 9 December 2014).

130 "Pakistan: The Next Generation Report," p. 14.

constitutional bodies, religious forums, think tanks, and academic institutions to decisively transform extremist mindsets and practices consistent with popular beliefs, values and norms. The Ministry of the Interior and the Council of Islamic Ideology, are considered appropriate forums to initiate a national youth anti-extremism policy having inbuilt structural linkages with education and domestic security policies. A few short and long term measures are suggested to materialize a moderate, conflict free and progressive youth in Pakistan.

Short-term Measures

The family, public schools, colleges, public universities, mosques and madrassas have emerged as the key channels to spawn extremism among youth. In the reformation drive, both by the government and non-state agencies - local as well as foreign, the family which is the building block of society, should become the prime focus of attention. The NGOs and development organizations should strategize family as the agent of societal change. For this purpose, pilot projects can be initiated in selected districts of southern Punjab and KP, as well as the restive suburbs of Karachi, later enfolding affluent families. The corrective discourse should comprise an assessment of existing tendencies, frustrations and aspirations which should be translated into short-term development programmes aimed at ensuring their stable social security and access to an informed source of knowledge, both secular as well as religious. Within the target communities, families housing the age groups between 10 and 19 years should be viewed with priority.

Students in colleges and universities unions are adults, and therefore should be allowed their political rights which in many ways provide an effective forum to vent frustrations and sustained engagement. Consequently, ban on student unions should be lifted. Nevertheless there is a need to revisit and redraw a charter for ethical conduct of students as has been recently initiated by Karachi University. Deprivation of opportunity for just expression is antithetical to the democratic norms and values for which this country is struggling so hard.

The state's intervention in mosques is tantamount to interference in individual faith. Yet this is inevitable to regulate malpractices, including spread of hate and violent ideologies by these otherwise peaceful abodes. However a minimalist approach is suggested that desires the governing committees of the mosques and their imams (religious leaders) to evoke ways to harmonize an objective message of Islam with emerging challenges faced by society to make religious practices simple and more practicable, rather than ritualistic, besides creating space to forge solidarity among diverse schools of thought for the collective good. The Ministry of Religious Affairs and the Ministry of the Interior, should become the lead agencies to undertake this initiative after careful planning and formulation of implementation strategies. Here too the context of a specific approach is proposed which can be subsequently expanded to the entire country.

The use of force against extremist criminals should be resorted to where required only as a last resort. Theoretical constructs like religious intelligence – the branch of cultural intelligence responsible for obtaining and analyzing information about the sacred beliefs and its impact on security operations, should be frequently dovetailed into planning by experts at the interior ministry, intelligence agencies and law enforcement agencies for operational efficiency. An organizational framework comprising multidisciplinary sources is proposed to help identify empirical swell of extremism for analysis, targeting and policy formulation:

i) Government higher secondary schools in all four provinces – Islamabad, Gilgit-Baltistan, the FATA, and Azad Jammu and Kashmir, especially in the provincial capitals as well as major cities;

ii) Selected jihadi madrassas and mosques in the country;[131]

iii) Militant organisations, groups and networks from all confessions;

iv) Publishers and readership of jihadi (religious and sectarian) publications, literature, dailies, monthlies, quarterly journals etc.

v) Mainstream as well as right-wing political parties having sectarian and jihadi agenda and their membership;

vi) Student armed wings of politico-religious parties in major universities;

vii) Armed as well as frustrated citizenry from sectarian conflicted areas;

viii) Training camps operated by militant organizations in FATA and border regions of Afghanistan;

ix) Sympathetic constituencies of militant groups, especially unemployed youth in less as well as least developed areas of the country, especially those adjoining FATA in KP and Balochistan;

x) B areas of Balochistan;

xi) Peace-enforcing lashkars/armed groups and armed peace committees ;

xii) Selected girl schools in the conservative areas of Punjab, KP and northern Balochistan.

xiii) Madrassas and schools run in Afghan refugee camps.

Long-term Measures

Cultural pluralism should be attained by rediscovering and assimilating narratives of forgotten folk history, moderating '*Either*' and 'O*r*' impulses, but most essentially defining 'Pakistaniat' based on citizenship. The basic spirit being proposed, which might appear radical to Pakistani nationalists, should be achieved by prioritizing Pakistanis first rather than Pakistan first. It is contended that the real centre of gravity of a nation is its people which provide vibrancy to national ideals. Territory, governments and sovereignty all owe their inspiration to the aspirations of citizenry which these bodies of the State stand for.

[131] Jihadi madaris are those seminaries that have a history of producing students to fight in Afghanistan and Kashmir; for example, among many others, Jamia Haqqania Akora Khattak and Jamia Binoria in Karachi are two prominently referred to organizations. Qaiser Butt, "Mortal Threat: Reforming Education to Check Extremism," *The Express Tribune* (January 15, 2011), available at http://tribune.com.pk/story/104066/mortal-threat-reforming-education-to-check-extremism/ (accessed 9 December 2014).

Second, the narratives predicated on counterarguments to those espoused by extremists have not yielded any results. In the light of the definition proposed at the outset, there is a need to radically alter this mindset by replacing it with a concordance approach. This necessitates thorough understanding of the ideologies propagated by militants and later harmonizing those into countering strategies in order to the pave way for engagement. The key difference in this approach vis-à-vis customary counterextremism responses is that it does not dismiss an opponent's claim as implausible but instead approaches it in a rational fashion. There can be several variations of operational methodologies to handle such a discourse; however all of these should be based fundamentally in a spirit of concordance. The Good Friday agreement in Northern Ireland is an apt example of such an approach.

In order to assimilate religious monitories into mainstream life, rhetoric of interfaith harmony may not work anymore. The best available model for this purpose are the contents of a letter written by Prophet Muhammad to the monks of St. Catherine Monastery in Mt. Sinai (630 CE), reproduced hereunder. In its expanded interpretation this framework of interfaith harmony may also be used to provide safeguard to other non-Muslim minorities e.g.,Qadianis, Hindus etc.

> This is a message from Muhammad ibn Abdullah, as a covenant to those who adopt Christianity, near and far, we are with them. Verily I, the servants, the helpers, and my followers defend them, because Christians are my citizens; and by Allah! I hold out against anything that displeases them. No compulsion is to be on them. Neither are their judges to be removed from their jobs nor their monks from their monasteries. No one is to destroy a house of their religion, to damage it, or to carry anything from it to the Muslims' houses. Should anyone take any of these, he would spoil God's covenant and disobey His Prophet. Verily, they are my allies and have my secure charter against all that they hate. No one is to force them to travel or to oblige them to fight. The Muslims are to fight for them. If a female Christian is married to a Muslim, it is not to take place without her approval. She is not to be prevented from visiting her church to pray. Their churches are to be respected. They are neither to be prevented from repairing them nor the sacredness of their covenants. No one of the nation (Muslims) is to disobey the covenant till the Last Day (end of the world).

In the same vein, there is a need to reintroduce Deeniat (the study of other religions), in addition to Islamiat (Islamic studies) in schools and university education managed through consensual processes among the higher education commission and provincial text books boards coupled with representation from civil society through a phased programme. The Planning Commission of Pakistan, the Islamic Council of Ideology or the Islamic University Islamabad could coordinate national efforts and institutionalize the whole process by providing necessary mechanisms and procedural pathways to secure this end.

The process of dialogue against extremism has so far been confined to speeches by public figures, clergy and intellectuals on key national days. The situation demands novelty in strategic thinking by initiating revolutionary steps. It is proposed that ideologues representing violent movements, such as Hafiz Saeed, sectarian clergy and leadership of banned organizations should be allowed and urged to express their viewpoints publically on the version, sources and rationale of sharia'h, religious or sectarian thought they propagate. Since sectarianism is rampant in the country with Shias being the principal victims, Shia clerics and intellectuals should take the lead to create awareness about their religious beliefs through structured and highly advertised media programmes, encompassing also historical, legal and theological areas of real or perceived friction and confrontations with those of the Sunni majority. For this purpose, it is essential that an environment be created to allow for safe debate.

To contain the formation of youth 'bulges' in urban centres, a two-prong strategy – selective rural urbanisation of Punjab and manipulative approach i.e., discretely controlled nationwide internal migration – can prove effective. This will reduce if not prevent risks of collusion of rural adults with urban-based religious extremists.

Finally, it is recommended that out of the 25 million people in the major urban centres of the four provinces, and some 10 million people in rural Punjab, the youth segment of the unemployed and underemployed – six million – should receive first priority for rehabilitation. These elements can cause social unrest and violence which, if mistaken for religious violence can compound response strategies with higher risks of societal disturbances. Child labour should be declared to be a social evil, warranting coordinated efforts for its complete elimination. The government cannot do it alone, but must be complemented by support from local and international donor and development agencies.

At this juncture Pakistan is on its way to democracy. Despite some critical inadequacies, it boasts the existence of a free and vibrant media that explains why an Arab spring-type social typology does not manifest here. Besides, political participation is on the rise due to gradually sustaining political processes and the emergence of accountability mechanisms. Further, the country presents its surprising underlying stability, rooted in kinship, patronage, and the power of entrenched local elites.[132] While these indicators bode well for the future, it must be emphasized that Pakistan is also a highly complex and diverse country of competing religious traditions, varied social landscapes, deep political tensions, and historical patterns of violence.[133] Consequently, interventions to deal with the menace of religious extremism ought to be informed by local conditions assimilating all its symmetries and contradictions. The scenario presented is menacing, but it is not insurmountable.

---

[132] See Lieven, *Pakistan: A Hard Country.*

[133] Ibid.

BIBLIOGRAPHY

"18,352 Registered Madressahs in Country, NA Told", *Dawn* (12 Sep 2011).

Abbas, Qaswar, "Karachi: World's Most Dangerous City", *India Today* (27 Aug 2011).

Abukhalil, As'ad, and Farid Esack, "The US, the Muslim World and an Islamic Response", *Policy Perspectives* 5(1) (2008).

Afsar, Major Shahid Afsar, Pakistan Army; Major Chris Samples and Major Thomas Wood, U.S. Army, "The Taliban: An Organizational Analysis", *Military Review* (May-June 2008).

Ahmed, Husham, "Identity Crisis Haunts Pakistani Youth", *The Statesman* (Feb. 2nd, 2010).

Ahmed, Khaled, "Too Weak to Attack North Waziristan", *Friday Times* XXIV(37) (October 26 - November 01, 2012).

Ahmed, Khalid, "Daughters of Al Huda", *The Express Tribune* (August 21, 2010).

Ahmad, Khurshid, "Terrorism and War against Terrorism: Some Fundamental Issues", *Policy Perspectives* 3(2) (2006).

Ahmed, Manzoor, "Pakistan : Aporia of its Kind" in *Pakistan: The Contours of State and Society* (Soofia Mumtaz, Jean-Lucm, Imran Anwar Ali, eds., Oxford University Press, 2002).

Ahmed, Zahid Shahab, and Rajeshwari Balasubramanian, "Extremism in Pakistan and India: The Case of the Jamaat-e-Islami and Shiv Sena" (Policy Studies 50, Regional Centre for Strategic Studies, Colombo, 2010).

Ali, Wajahat, "China Says Terrorists from Xinjiang Hiding in Pakistan", *Daily Times* (29 May 2004).

Andrabi, Tahir, et al, "Religious School Enrolment in Pakistan: A Look at the Data" (unpublished paper, 2005).

Andrabi, Tahir, et al, "The Madrasa Myth", *Foreign Policy* (June 2009), available at http://foreignpolicy.com/2009/06/ 01/ the-madrasa-myth/m (accessed 8 December 2014).

Aoun, Joy, et al, "Religous Movements, Militancy, and Conflict in South Asia" (Center for Strategic and International Studies, July 2012).

Associated Press of Pakistan, "KU Issues Code of Ethics for Students", *The Nation* (19 January 2013).

Aydin, Mustafa, "De-legitimizing Religion as a Source of Identity-Based Security Threats in a Global World", *Connections-The Quarterly Journal* (Winter 2006).

Bacha, Ali Hazrat, "UoP Closed after Student`s Death Sparks Riots", *Dawn* (Mar. 20, 2012).

Backes, Uwe, "Meaning and Forms of Political Extremism in Past and Present", *Central European Political Studies Review* 4 (2007).

Bajoria, Jayshre, "Pakistan's Education System and Links to Extremism" (Council of Foreign Relations Backgrounder, 7 Oct 2009).

Basharat, Sadaf, "Craving for Change: Educated Youth, Perception Survey Report" (Peace Education and Development Foundation, 12 August 2012).

Basit, Abdul, and Mujtaba Muhammad Rathore, “Trends and Patterns of Radicalization in Pakistan”, *PIPS Research Journal Conflict and Peace Studies* 3(2)(2010).

Behuria, Ashok K., “Sunni-Shia relations in Pakistan: The Widening Divide”, *Strategic Analysis* 28(1)(2004).

Belt, David, “Islamism in Popular Western Discourse”, *Policy Perspectives* 6(2)(2009).

Belton, Patrick, “Democracy In Pakistan: A Legacy Of Democratic Failure (2/3)”, *WindsofChange.com* (Oxford Democracy Forum, 6 May 2004).

Bibi, Norina, “Population, Labour Force and Employment”, *Pakistan Economic Survey 2010-11* (2011).

Brulliard, Karin, “In Pakistan, Even Anti-violence Islamic Sect Lauds Assassination of Liberal Governor”, *Washington Post* (29 Jan 2011).

Butt, Qaiser, “Mortal Threat: Reforming Education to Check Extremism”, *The Express Tribune* (January 15, 2011).

Butt, Qaiser, “Shrinking Space: K-P Govt Shelves Plans for Textbook Reforms: JUI, JI Protested against Revised, Secular Syllabus”, *The Express Tribune* (6 April 2012).

Chaudhry, Zubair, “Unemployment and the PM’s Youth Programme”, *Express Tribune* (15 December 2013).

Crilly, Rob, “Poverty Does Not Breed Extremism in Pakistan, Study Finds”, *The Telegraph* (20 May 2011).

Dalrymple, William, “Inside Islam’s “Terror Schools”, *New Statesman* (28 March 2005).

“Extremism in Florida: The Dark Side of the Sunshine State” (Anti-Defamation League, 3rd Edition, 2011).

Fair, C. Christine, “Lashkar-e-Tayiba and the Pakistani State”, *Survival,* 53 (4) (2011).

Feyyaz, Muhammad, “Ethnic Conflict in Sindh” (PILDAT Background Paper, October 2011).

Feyyaz, Muhammad, “Political Economy of Tehrik-e-Taliban Swat”, *Peace and Conflict Studies* 4(3) (2011).

Feyyaz, Muhammad, “Multiform Youth Extremism in Pakistan” (PILDAT Discussion Paper, July 2013).

Feyyaz, Muhammad, “Facets of Religious Violence in Pakistan”, *Counter Terrorist Trends and Analysis* 5(2) (2013).

Feyyaz, Muhammad, “Conceptualising Terrorism Trend Patterns in Pakistan – an Empirical Perspective”, *Perspectives on Terrorism* 7(1) (2013).

Gillani, Waqar, “Able Partners: JuD’s Deaf Wing Camps Are Quite Productive”, *The Jang-News Weekly* (16 April 2012).

Graf, Corinne, and Rebecca Winthrop, “Beyond Madrassas: Assessing the Links between Education and Militancy in Pakistan” (Brookings Institution, 2010).

Haqqani, Husain, "The Ideologies of South Asian Jihadi Groups", *Current Trends in Islamic Ideology* (2005).

Haqqani, Husain, "'Weeding out the Heretics': Sectarianism in Pakistan" (01 Nov 2006).

Haroon, Sana, *Frontier of Faith: Islam in the Indo-Afghan Borderland* (Hurst & Company, 2007).

Hashmi, Arshi Saleem, "Pakistan: Politics, Religion & Extremism", (Institute of Peace and Conflict Studies (IPCS) Research Papers, May 2009).

"History Taught in Pakistan Challenge", *Times of India* (3 Feb 1999).

Hunter, W. W., *The Indian Musalmans* (Sang-e-Meel Publications, 1999).

"Ideas on Democracy, Free and Peace" (Future Youth Group, 2009).

Jalil, Xari, "Giving Context to Religious Extremism", *Pakistan Today* (19 Jun 2011).

Jalil, Xari, "Campus Politics Turns Bloody", *Dawn* (May 23, 2012).

Khan, Akbar Nasir, "Radicalisation and State Response", The *Friday Times* (21-27 Jan 2011).

Knudsen, Are, "Political Islam in South Asia" (Chr. Michelsen Institute, 2002).

Kugelman, Michael, "Pakistan's Demographics: Possibilities, Perils, and Prescriptions" in *Reaping the Dividend: Overcoming Pakistan's Demographic Challenges* (Wilson Center, 2011).

Lieven, Anatol, *Pakistan – A Hard Country* (Public Affairs, 2011).

"Madaris Not Registered to be Considered Illegal after Jan 1: Rehman Malik", *Associated Press of Pakistan* (19 December 2011).

Mahsud, Mansur Khan, "The Battle for Pakistan: South Waziristan - Militancy and Conflict in South Waziristan" (Counterterrorism Strategy Initiative Policy Paper, New America Foundation, 2010).

Mandel, David R., "Radicalization: What does it mean?" in *Indigenous Terrorism: Understanding and Addressing the Root Causes of Radicalization among Groups with an Immigrant Heritage in Europe* (Thomas M. Pick, Anne Speckhard, Beatrice Jacuch, eds., IOS Press, 2010).

Mazhar, Nargis, "Population, Labour Force and Employment", *Pakistan Economic Survey 2012-13* (Pakistan Ministry of Finance, 2013).

Mushatq, Faiza, "A Controversial Role Model for Pakistani Women", *South Asia Multidisciplinary Academic Journal* 4 (2010).

Neumann, Peter, "Prisons and Terrorism Radicalisation and De-radicalisation in 15 Countries", (International Centre for the Study of Radicalisation and Political Violence (ICSR), 2010).

Nizami, Nausheen Saba, "Population, Labour Force and Employment", *Pakistan Economic Survey 2009-10* (2010).

O'Neill, Robert, "Learning from Pakistan", *Harvard Kennedy School Magazine* (Winter 2010).

"One Killed as Jamaat-ud-Dawa and Sunni Tehreek Fight over Mosque", *The Express Tribune* (2 July 2011).

"Pakistan: Karachi's Madrasas and Violent Extremism" (Asia Report N°130, International Crisis Group, 29 Mar 2007).

"Pakistan: The Next Generation Report" (British Council, November 2009).

Parachi, Nadeem F., "Bleeding Green: The Rise and Fall of the IJT", *Dawn.com* (16 August 2012).

Pasha, Feyyaz M., "Osama's departure and its aftermath for Pakistan", *pkarticleshub.com* (6 May 2011).

Pervaiz, Ga, "Political Islam and the Media", *Policy Perspectives* 4(2)(2007).

Precht, Tomas, "Home Grown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism" (Danish Ministry of Justice, Dec 2007).

Pressman, D. Elaine, "Risk Assessment Decisions for Violent Political Extremism 2009-02" (Canadian Centre for Security and Intelligence Studies, 2009).

Qoreshi, Arif, "Hafiz Saeed's 'Son' and 'Son in Law' Included into the FTO", *The Fortress* (10 September 2012).

Rana, Muhammad Amir, "Taliban Insurgency in Pakistan: A Counterinsurgency Perspective", *Conflict and Peace Studies* 2(2)(2009).

Rana, Muhammad, Safdar Sial and Abdul Basit, *Dynamics of Taliban Insurgency in FATA*, (PIPS Publications, 2010).

Rana, Amir, "What is Young Pakistan Thinking?" *The Express Tribune Blogs* (2 Sep 2010).

Rana, Muhammad Amir, "Evolution of Militant Groups in Pakistan", *Conflict and Peace Studies* 4(2) (Apr-June 2011).

Reuters, "Millions Pushed into Child Labour in Pakistan", *The Express Tribune* (7 February 2012).

Rizvi, Hasan Askari, "Radicalization and Political System of Pakistan" in De-radicalization and Engagement of Youth in Pakistan (M. H. Nuri, et al, eds., Islamabad Policy Research Institute).

Rizvi, S. Athar H., "Seminar Recalls Contributions of Three Subcontinental Luminaries", *Saudi Gazette* (March 22, 2013).

Ruthven, Malise, *Fundamentalism: The Search for Meaning* (Oxford University Press USA, 2004).

"Samiul Haq Renounces Support for Polio Immunization", *Pakistan Today* (22 Jul 2012).

Sahi, Aoun, "Dawa, Jihad, Charity or All?", *The Jang-News Weekly* (16 April 2012).

Sathar, Zeba A., "Demographic Doom or Demographic Dreams: Pakistan at the Crossroads", *Reaping the Dividend: Overcoming Pakistan's Demographic Challenges* (Wilson Center, 2011).

Shafqat, Saeed, "Praetorians and the People" in *Pakistan: Beyond the Crisis State* (Maleeha Lodhi, ed, Columbia University Press, 2011).

Siddiqa, Ayesha, "Red Hot Chili Peppers Islam – Is the Youth in Elite Universities in Pakistan Radical?" (Heinrich Bölle Stiftung, 2011).

"Sunni Tehreek's Protest against Qadri Verdict Turns Violent", *The Express Tribute* (3 Oct 2011).

Taqi, Dr. Mohammad, "COMMENT: Qazi Hussain Ahmad: The Jihadist Patriarch", *Daily Times* (January 10, 2013).

"The Flip Side of the Coin – Sunni Tehreek Plans to Provide Killer Legal Assistance", *Pakistan Today* (10 Jan 2011).

The Pew Global Attitudes Project, "Pakistani Public Opinion: Growing Concerns about Extremism, Continuing Discontent with U.S." (Pew Research Center, 13 Aug 2009).

"The State of Sectarianism in Pakistan" (Asia Report N°95, International Crisis Group, 18 Apr 2005).

"The Trouble with: Madrassas in Pakistan", *The Express Tribune* (January 25, 2012).

Urdal, Henrik, "A Clash of Generations? Youth Bulges and Political Violence" (UN Doc. UN/POP/EGM-AYD/2011/10 (2011).

"View: Blackguards of Fanaticism Silenced Bashir Bilour", *Daily Times* (December 29, 2012).

"Violence in Karachi, Into the Abyss", *The Economist* (27 Aug 2011).

White, Joshua T., "Vigilante Islamism in Pakistan: Religious Party Responses to the Lal Masjid Crisis", *Current Trends in Islamist Ideology* 7 (2008).

Yusuf, Huma, "Sectarian Violence: Pakistan's Greatest Security Threat?" (NOREF Report, 9 August 2012).

Yusuf, Moeed, "Prospects of Youth Radicalization in Pakistan: Implications for US Policy" (Brookings Institution – October 2008).

Yusuf, Moeed, "A Society on the Precipice? Examining the Prospects of Youth Radicalization in Pakistan," in *Reaping the Dividend: Overcoming Pakistan's Demographic challenges* (Michael Kugelman and Robert M. Hathaway , eds, Woodrow Wilson International Center for Scholars, 2011).

Yusuf, Zohra, "Armed Jamiat Fanatics Attack Students & Teachers at PU", *Viewpoint* (30 June 2011).

Zaidi, Mansar, "The Radicalisation Process", *The Dawn* (Feb 2011).

PUBLISHING PRINCIPLES

Articles sent to the ***Defence Against Terrorism Review*** must not be published elsewhere or must not have been sent to another publication in order to be published.

The authors who try to submit their already published (even electronically) articles to DATR will not be accepted to submit their articles again and will be forbidden to participate any future activity conducted by COE-DAT.

A. GENERAL PRINCIPLES

1. Language of publication is English. The texts submitted must be clear and understandable, and be in line with scientific/academic criteria in terms of language, expression and citation.

2. The texts submitted to be published should be 15-30 pages, including the abstract and bibliography.

3. The texts must be submitted together with an abstract no longer than 250 words at the beginning of the paper and with five keywords after the abstract.

4. The name of the author must be placed in the first footnote, with his/her title, place of duty and e-mail address. Footnotes for other explanations must be provided both in the text and down the page in numbers.

5. The type character must be Arial, "11 type size", line spacing "1,5 nk", footnotes in "9 type size" and with "single" line spacing.

General Contents

The following are general stylistic conventions used by COE-DAT:

1. Writing should be scholarly in nature and not overly conversational. Do not use "I" or "we" but "the author" or the "authors".

2. Do not use contractions except in quotes.

3. Except in quotes, do not underline or bold text to emphasize it but instead use word order for emphasis. To highlight a term, show the key words in single mark ('aerospace').

4. Use italic font for foreign phrases and names of court cases.

5. For dates, use – date month year format (10 March 2011) – not numbers (10/03/11). In footnotes, dates of the sources may follow the format used in the source.

6. There should be only one space between the period at the end of a sentence and the beginning of the next sentence.

7. Acronyms should be defined when first used with the full name in parentheses after the acronym; acronyms in foreign languages should have the name in the foreign first in parentheses, followed by the English translation. If an acronym has been defined once in the text of the article, it is unnecessary to spell it out again either in text or footnotes.

8. Numbers less than twenty or less should be spelled out; numbers 21 and above should be left in numbers.

9. Values in currency should be quoted in the actual currency followed by the amount in dollars (USD) or euros (€) in parentheses.

10. While making quotations;

a. If the part taken from the source is 4 lines and less than 4 lines, quotation marks ("...sentence...") can be used.

b. If the part taken from the source is more than 4 lines, it must be given with extra indentations.

- In addition, the writer of the article must avoid excessive use of each source, in particular from their own previous writings.

B. PRINCIPLES AS TO PAGE LAYOUT

Formatting: Double-spaced with standard page margins. The text and all headings should be left justified. Set language as American English. The publisher employed by COE-DAT uses a particular document formatting that will be applied by the editors.

C. PRINCIPLES AS TO REFERENCES AND CITATIONS

Citations shall be given down the pages in numbers in ***Defence Against Terrorism Review*** and references shall not be presented in the text (e.g. Waltz, 2009: 101.).

Full identity of the resources cited shall be given; any resource not actually cite shall not be presented in the bibliography.

Format for footnote citations;

1. For Books

a. Books with Single Author:

Name and surname of the author, *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s).

Joseph Needham, *Science and Civilization in China* (Vol. 5, Cambridge Univ. Pres, 1954), p. 7.

Joseph Needham, *Science in Traditional China* (Harvard Univ. Pres, 1981), p. 37.

b. Books with Two or Three Authors:

Name and surname of the first author, name and surname of the second author, name and surname of the third author, *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s).

Joseph S. Nye Jr. and David A. Welch, *Understanding Global Conflict and Cooperation* (Pearson Publication, 2011), p. 280.

c. Books with More Than Three Authors:

Name and surname of the first author et. al., *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s).

Luis Benton et. al., *Informal Economy* (The John Hopkins University Press, 1989), pp. 47-59.

d. Books with Name of Author or Editor Non-Specified:

Redefining Security (Praeger Publication, 1998), p. 81.

2. For Articles

Name and surname of the author (for all authors if two or three, if more than three authors just for the first author and et. al.), "name of the article" (translator if any), *name of periodical in which it is published,* volume number (issue) (publication year), pages in journal, cited page number.

a. Articles with One Author:

Barry Buzan, "New Patterns of Global Security in the Twenty-First Century", *International Affairs* 67(3) (1991), pp. 431-451, p. 442.

b. Articles in Compilation Books:

Barry Buzan, “Is International Security Possible?”, in *New Thinking About Strategy and International Security* (Ken Botth and Don Kaufman, eds, Harper Collins, 1991), pp. 31-55, p. 42.

c. Articles from Daily Newspapers:

Yossi Melman, “Computer Virus in Iran Actually Targeted Larger Nuclear Facility”, *Haaretz* (22 September 2011), p. 7.

“Tehran’s nuclear ambitions”, *The Washington Post* (26 September 2009), p. 5.

3. For Theses

No italics shall be used for the titles of non-published theses. Name and surname of the author, “title of the thesis” (whether it has been published and academic degree of the thesis, institution and institute of the thesis, date of the thesis), page number.

Atasay Özdemir, “Approaches of the Effective Actors of the International System to Iran’s Nuclear Programme” (Unpublished Doctoral Thesis, War College Strategic Researchs Institute, Istanbul, 2013), p. 22.

4. For Reports

a. Report with Author Specified

Tariq Khaitous, “Arab Reactions to a Nuclear Armed Iran” (Washington Institute for Near East Policy, Policy Focus 94, June 2009), p. 14.

b. Report with Author Non-Specified

Albania Country Report (TİKA Publishing, 1995), p. 7.

c. Report prepared by an Institution, Firm or Institute

American Petroleum Institute, “Drilling and Production Practice Proceedings of the Spring Meeting” (Shell Development Company, 1956), p. 42.

d. For Internet Resources

If any of the above resources are available on the Internet, follow the citation above with “available at” with the full http address and the date accessed in paratheses

e. Web Pages

“The World Factbook-Turkey”, Central Intelligence Agency, at https://www.cia.gov/library/publications/ the-world-factbook/geos/tr.htm (accessed 25 February 2013).

“Dimona: Negev Nuclear Research Center”, *Global Security*, at http://www.globalsecurity.org/wmd/world/israel/dimona.htm (accessed 11 January 2010).

“Russia’s National Security Strategy to 2020” (12 May 2009), *Rustrans*, at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (accessed 02 May 2011).

5. Subsequent citations of the same source:

a. If the citation is to the footnote directly before, use “Ibid” – if the page or paragraph changes, you can add the new informatıın, as in “Ibid, p. 48” or Ibid, para. 68).

b. If the source is earlier than the previous one, use the author’s last name (if there is one), followed by the name of the article, followed by the new page or paragraphe number.

Buzan, “Is International Security Possible?”, p. 48.

D. PRINCIPLES TO ABIDE BY IN USING OF DOCUMENTS, TABLES, FIGURES AND GRAPHICS

1. Attachments (documents), shall be presented at the end of the text and down below shall be a brief information as to the content of the document and proper citation in line with the relevant criteria.

2. Other attachments (Table, Figure and Graphics) shall be presented as Additional Table: 1, Additional Graphic: 3 and Additional Figure: 7. If indicators other than the text are too many in number; attachments shall be presented after the References.

   a. References to these attachments in the text shall absolutely be made as Additional Table: 1, Additional Graphic: 3 or Additional Figure: 7.

   b. If citation has been made for table, figure, graphic or picture, the source shall absolutely be indicated.

3. The names of the tables within the text shall be written on the top of the table and these tables shall be cited in the footnote according the publication type from which it was citied.

4. The names of the figures, graphics and maps within the text shall be written at the bottom of the figures, graphics and maps and these figures, graphics and maps shall be citied in the footnote according the publication type from which it was cited.

E. PRINCIPLES TO ABIDE BY IN BIBLIOGRAPHY

1. Just like giving citations but this time surname of the fauthor shall be at the beginning.
2. Resources shall be sorted alphabetically from A to Z.
3. Page numbers shall not be indicated.

COE-DAT