Terror Group and Terrorist Operations Security: Assessing the Impact of the Snowden Revelations

by

Christopher Joseph Benka

Advisor: Dr. David Alan Grier

A Thesis
Submitted to the Department of International Affairs, Computer Science
George Washington University
In Partial Fulfillment of the Requirements
for the Degree of Bachelor of Arts
December 2017

Table of Contents

Introduction

In June 2013, the United Kingdom newspaper outlet, the Guardian, published, in what would be one of many reports, a detailed analysis on classified documents about the National Security Agency's (NSA) Signals Intelligence (SIGINT) programs. The Guardian's source, Edward Snowden, an intelligence contractor for Booze Allen Hamilton assigned to the NSA's Hawaii headquarters. Since the Guardian's initial report, newspaper outlets have published over 7,000 top-secret documents detailing many classified programs.[1] For many heads of intelligence, including Director of National Intelligence James Clapper and General Michael Hayden, former head of the NSA and CIA, the disclosures of classified information mark the most damaging theft of intelligence information in U.S. history.[2]

In the years following the reports of classified information, intelligence agencies, intelligence officials, and newspaper outlets have claimed to bear witness to the advent of the secure terrorist and terror group as a direct result of the disclosures. Recent literature has primarily focused on the 'new application' of technologies designed to secure terror groups and terrorist communications. Few works open to the public have qualified the new technology applications through a simple contextualization of terror groups and terrorist technology applications before the disclosures. This study performs the necessary contextualization to assess the validity of the word 'new' to describe strategies and tools used by terror groups and terrorists following the disclosures. This study finds that terrorist organizations responded hastily to the information relating to the reach of NSA SIGINT programs. The organizations sought to operate

[1] Szoldra, Paul, 'This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks,' *Business Insider,* 16 September 2016, available at: http://www.businessinsider.com/snowden-leaks-timeline-2016-9, last visited: 17 December 2017.
[2] Simcox, Robin, 'Surveillance After Snowden: Effective Espionage in an Age of Transparency,' *Henry Jackson Society*, 2015, available at: http://henryjacksonsociety.org/wp-content/uploads/2015/06/Surveillance-After-Snowden-16.6.15.pdf, last visited: 17 December 2017, p. 19.

securely and privately. It shows how terrorist organizations altered their strategies by examining different terror organizations before and after the disclosures. However, the study argues that those strategies have inconsistently been implemented by organizational members and thereby do not challenge NSA SIGINT counterterrorism efforts.

Statement of Problem

The study will be assessing two claims issued following the disclosures of classified information pertaining to NSA SIGINT programs. First, the disclosures resulted in terror groups and terrorists using *new* strategies to secure operational communication. Second, the new strategies and implementations present challenges to NSA SIGINT programs' abilities to collect information vital to counterterrorism efforts. This paper does not assume the recommendation and implementation of operational strategies to be one of the same. As such, the claims are assessed through a comparison of strategies *recommended* by terror groups and *implemented* by the groups' devotees both before and after the disclosures. In each stage of the comparison, the study assesses the efficacy of strategic implementations against NSA SIGINT programs.

Methodology

This study compares operations security strategies advocated for at the organizational level and implemented amongst terrorists across telecommunication networks. Operations security is an appropriate lens of guidance because its goal lies directly opposite the goals of NSA SIGINT programs. That is, while the NSA SIGINT programs seek to collect as much information about terror groups and terrorists as possible, operations security attempts to protect information sensitive to the organization from an outside entity.[3] Therefore, any emergent shifts

[3] U.S. Department of Defense Education Activity, *Operations Security (OPSEC)*, available at: http://www.dodea.edu/offices/safety/opsec.cfm, last visited: 17 December 2017.

in behavior can be assessed through how an organization changes its operations security strategies considering the latest information regarding adversarial capabilities.

Since operations security is concerned with information security, this study assesses changes in operations security based on information security's fundamental principles, commonly referred to as the CIA triad: confidentiality, integrity, and availability. As terror groups and terrorists are also inherently concerned with impunity, the study also assesses anonymity as critical to terror operations security. In identifying essential components in operations security, the study can categorically identify shifts in actions and thus assess cumulative behavioral changes and respective efficacy.

Terror groups require that information deemed sensitive remain private, only readable to authorized entities. Therefore, terror groups are concerned with the *confidentiality* of information. Methods undertaken to achieve confidentiality are those that prevent unauthorized entities from reading sensitive information. The encryption of information is a common method used to attain confidentiality.

Terror groups also require that information shared maintain accuracy and trustworthiness, otherwise referred to as *integrity.* Terror groups require information shared not be modified in the process of being shared and require that information can be trusted with regards to with whom the information originated. Methods undertaken to achieve informational integrity, include any mechanism that seeks to guarantee the validity of the source of the information and the data itself.

Terror groups are also concerned with the ability for authorized, fellow organizational members to access an information asset. Thus, terror groups are concerned with *availability.*

Mechanisms put in place to ensure the availability of information, include added redundancy of information in case a particular source of information fell unavailable.

Finally, terror groups due to the illicit nature of their activities are concerned with *anonymity.* That is, in the case of informational discovery by an external entity, the entity should not be able to trace the information back to a particular individual. Methods undertaken to attain anonymity, include the use of anonymizing browsers, proxy servers, or any other mechanism that prevents an external entity from identifying the source of the communication or information shared.

This study uses qualitative research to examine the state of operations security techniques before and after disclosing 7,000 classified documents. A review of NSA SIGINT programs obtained through secondary sources allows the researcher to understand the efficacy of terror groups and terrorist operations security strategies. This study was limited by time and access to open-source information, which inherently prevents an incomplete understanding of the topic at hand. Further work is needed to solidify and expand upon the arguments presented here.

Current Literature: Selected Views on Shifts in Terror Group and Terrorist Strategies

In the years following the disclosures, various public and private organizations have published studies to measure the impact of the disclosures on the adoption of new technologies by terror groups and terrorists. Prevalent studies include a report produced by the neoconservative think tank, the Henry Jackson Society, the nonprofit monitoring and analysis organization, the Middle East Research Institute, and the United States Military Academy's Combating Terrorism Center. These studies have focused mainly on the recommendation by terror organizations of new technologies designed to secure the confidentiality of information. Significant findings produced by the studies include an expansion of encryption tools released by

terror organizations, a decrease in the use of content service providers (CSP) cooperative with selectors issued by the NSA, and increased adoption of mobile applications that provide end-to-end encryption. The findings, however, are predicated on evidence related to terror group recommendations without proper contextualization.

This study seeks to advance current literature measuring the impact of the disclosures in two regards. First, in decomposing 'new developments' into applicable categories inherent to terror group operations security previously described, the study provides a more precise and new analysis regarding the responses of terror groups and terrorists. Second, in distinguishing between recommendation and implementation of operations security strategies before and after the disclosures, the study examines the complexity encompassing the descriptors 'new' and 'secure' used in depicting terror group strategies and efficacy following the revelations, respectively.

Disclosures related to U.S. Signals Intelligence Programs

The disclosures released thousands of documents about the National Security Agency's (NSA) signals intelligence (SIGINT) programs. The tools and methods used by the NSA to perform SIGINT collection fall under three broad categories: the interception of data in transit, access to stored data, and the use of active attacks conducted through network exploits.[4] This section explores the SIGINT tools and methodologies used by the NSA discussed in the disclosures to formulate a basis for the future discussion of terror group and terrorist decisional efficacy.

UPSTREAM programs

[4] Lyon, David, *Surveillance after Snowden*, Polity Press (2015), p. 19.

UPSTREAM data collection refers to the bulk collection of in-transit internet communications from foreign and domestic communication networks. UPSTREAM data collection is obtained through tapping into fiber cables and other infrastructure used for communication.[5] According to the NSA, internet data acquired by the NSA under UPSTREAM programs includes communications to, from, or about a selector.[6] An example of a communication captured through an 'about' selector is an email that includes a targeted email address in the body of an email between two individuals who are not target themselves.[7]

Programs conducted under the UPSTREAM umbrella include, FAIRVIEW and BLARNEY. FAIRVIEW collects messages and phone calls at major junctions in the international communications systems.[8] The NSA conducts FAIRVIEW operations through collaboration with U.S. telecommunication companies that then make agreements with international telecommunications companies for their data.[9] BLARNEY performs collection of metadata at core junction points on international fiber optic cables.[10] Metadata is information not related to the contents of a message, and often includes the source and destination of messages. The collection of metadata through BLARNEY is in large a result of partnerships with German and British intelligence agencies. The partnerships have the NSA access to metadata moving through international telecoms like the British telecom company BT and German telecom company Vodafone.[11]

---

[5] Ibid, p. 18.
[6] 'NSA Stops Certain Section 702 "Upstream" Activities – Statement issued by NSA,' *National Security Agency*, 28 April 2017, available at: https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml, last visited: 17 December 2017.
[7] Ibid.
[8] Kloc, Joe, 'The definitive guide to NSA spy programs,' *The Daily Dot*, 14 August 2013, available at: https://www.dailydot.com/layer8/nsa-spy-prgrams-prism-fairview-blarney/#fairview, last visited: 17 December 2017.
[9] Ibid.
[10] Ibid.
[11] Ibid.

In practice, the UPSTREAM programs work as follows. Upon discovering a foreign national's intent to conduct a terrorist attack, the NSA provides a series of selectors, which might include the target's phone number, email address, as well as name, to an Internet Service Provider (ISP). The ISP is then compelled to provide all results containing the pre-identified selectors. It is estimated that 9% of all emails the NSA collects is via the aforementioned UPSTREAM programs.[12]

Access to Stored Data

Another critical component to US SIGINT collection programs is querying or accessing previously stored information. The NSA programs PRISM and XKeyscore are among the most popular tools used to perform querying of stored information.

PPRISM collects information from data stored by popular content service providers (CSP) through issuing a selector to the CSP.[13] Identical to the selectors issued in UPSTREAM programs, the selector may include a keyword pertaining to metadata or the content of the message sent. Upon receiving the selector, the CSP is compelled to provide all available records involving the selector to the NSA.[14] Popular CSPs often compelled by a selector include, Google, Yahoo, Microsoft, and Facebook. [15]

XKeyscore allows NSA intelligence analysts to search through the vast databases of information previously collected through PRISM and UPSTREAM programs.[16] Through the program, analysts are quickly able to search through the scores of metadata and content of all

[12] Simcox, 'Surveillance After Snowden: Effective Espionage in an Age of Transparency,' p. 23.
[13] Ibid, p. 11.
[14] Ibid, p. 21.
[15] Ibid.
[16] Greenwald, Glen, 'Xkeyscore: NSA tool collects nearly everything a user does on the internet,' *The Guardian,* 31 July 2013, available at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, last visited: 17 December 2017.

data. Potential search terms include, a telephone number, an IP address[17], the browser used, or the encryption method used.[18] XKeyscore also allows searching of data beyond simple emails. Through the program, analysts can search across an unlimited array of internet activities, including social media activates and any activity conducted over HTTP.[19] The ability to search HTTP activity grants analysts access to "nearly everything a typical user does on the internet".[20]

Active Attacks

The National Security Agency (NSA) also conducts 'active attacks' to expand the agency's domain over obtainable, readable information transmitted via telecommunications networks. Active attacks refer to attempts to manipulate data on a targeted computer or as the data is transmitted. BULLRUN and QUANTUM INSERT are among the many programs that enable the NSA to perform active attacks.

BULLRUN is the highly classified program used by the agency to crack encryption of online communications and data.[21] According to reports, the program has cracked protocols designed to encrypt internet communications, including HTTPS, voice-over-IP, and SSL.[22] The agency has used the program, for example, to decrypt data that had been securely encrypted between Google and its users as the data traveled between each Google data center.[23]

Quantum Insert executes a man in the middle attack to infiltrate the user's computer with malware. Man in the middle refers to an attack conducted in which an attacker secretly alters the

[17] Defined as a unique set of numbers that identifies a computer using the internet (Oxford Dictionary).
[18] Greenwald, 'Xkeyscore: NSA tool collects nearly everything a user does on the internet,' *The Guardian.*
[19] Ibid.
[20] Ibid.
[21] Ball, James, Borger, Julian, Greenwald, Glenn, 'Revealed: how US and UK spy Agencies defeat internet privacy and security,' *The* Guardian, 6 September 2013, available at: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, last visited: 17 December 2017.
[22] Ibid.
[23] Edwards, Jim, 'Google Engineers Speak Out Against NSA Surveillance, And Drops The F-Bomb While Doing So,' November 6, 2013, available at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, last visited: 17 December 2017.

communication between two parties. The program enables the NSA access to to the infected computer, allowing the agency to perform data collection and manipulation. In 2011, the agency utilized the program to gain access to the Belgacom's networks.[24] Belgacom is a Belgian communications company, responsible for routing a substantial number of calls and internet traffic throughout Europe. Through Quantum Insert, the agency gained access to many of the routers used to route traffic throughout Europe. As a result, the agency gathered information and data transmitted from foreign nationals through new sources of information.

Approaches to Operational Security & Efficacy, Pre-Snowden

Prior to the disclosures, terror groups and terrorists applied non-technical tradecraft to ensure the confidentiality, integrity, and availability of information. Terror groups and terrorists also applied non-technical tradecraft to ensure the anonymity of communicators. This trend largely continued despite growing organizational awareness and recommendations pertaining to the use of technical tradecraft. This section explores terror group and terrorist operations security strategies from the late 90s until the months leading to the disclosures.

Confidentiality & Integrity

Terrorists have long been aware of the importance of ensuring the confidentiality of information. Their focus on securing the confidentiality of information, however, rarely extended beyond securing information stored in files. As early as the 1990s, terror groups and terrorists used modern encryption to ensure the confidentiality of information stored in files. Investigation into the Japanese terror group Aum Shinrikyo revealed the use of the RSA encryption algorithm

[24] Zetter, Kim, 'How to Detect Sneaky NSA 'Quantum Insert' Attacks,' *Wired*, 22 April 2015, available at https://www.wired.com/2015/04/researchers-uncover-method-detect-nsa-quantum-insert-hacks/, last visited: 17 December 2017.

to secure the confidentiality of files.[25] The public key[26] cryptosystem provides guarantees to both the integrity and confidentiality of Aum Shinrikyo's data. Similarly, investigators discovered Ramzi Yousef used encryption to secure files on his computer, prior to his participation in the World Trade Center in 1994 and Malina Air liner in 1995.[27] In 1998 FBI director, Louis J. Freeh, highlighted the adoption of encryption by terror groups in testimony given to the Senate Select Committee on Intelligence. His testimony, however, only contained evidence of terrorists applying encryption to secure files. The testimony does not include evidence of terrorists using encryption to secure the confidentiality of communications.

In attempts to secure the confidentiality of communiques, terrorists, applied non-technical methodologies. In the 1998 embassy bombings, perpetrated by Al Qaeda and the Egyptian Islamic Front, terror operatives relied on open coded messages to communicate. Open coded messages refer to the use of secret keywords to transmit hidden information. Trial transcripts indicate the messages were sent through standard email services. Thus, terror groups relied on non-technical encryption in the form of open-coded messages to secure information sent through unencrypted standard email services. As a result, terrorists provided weak guarantees to the confidentiality and integrity of their communiques.

By 2000, more technical means of encryption had been encouraged to secure the confidentiality and integrity of communiques. By 2000 PGP had been encouraged to secure the confidentiality and integrity of information sent over email. However, the use of PGP was

[25] Koops, Bert-Jaap, *The Crypto Controversy: A Key Conflict in the Information Society,* Kluwer Law International (1998), p. 65.
[26] In this report, Public key cryptography is defined as a cryptographic system that uses two pairs of keys: public keys which can be known by anyone, and private keys which can be known only to the owner. An individual encrypts a message using that individual's public key, who then uses his private key to decrypt the message. Public key cryptography ensures message integrity and non-repudiation through digital signatures. Otherwise referred to as asymmetric encryption.
[27] Suro, Roberto and Corcoran, Elizabeth, 'U.S. Law Enforcement Wants Keys to High-Tech Cover,' *Washington Post*, March 30, 1998, available at: https://media.washingtonpost.com/wp-srv/politics/special/encryption/stories/cr033098.htm, last visited: 17 December 2017.

encouraged solely in a non-operational context. PGP, or Pretty Good Encryption, is an encryption software built on public key cryptography. The first mention of PGP occurred in the "Mujahedeen Poisons Handbook," promulgating as an appendix to the popular "Encyclopedia of Jihad." As the authors of the handbook close, they encourage the contribution of books or information, which would further add value to the Encyclopedia of Jihad. The authors instruct those interested in contributing to share information through use of PGP, a system that provides guarantees to the integrity and confidentiality of information sent. The subsequent third and fourth editions of the Encyclopedia of Jihad, now an Al Qaeda project, also did not advocate for the extension of PGP to secure operational communications.[28] Thus, up to the year 2000 operations security strategies to secure the confidentiality and integrity of operational information included the application of non-technical tradecraft, particularly with regards to operational communiques.

After the 9/11 terror attacks, reports focused on the advent of the 'encrypted terrorist'. Deeper inspection of the use of encryption methodologies, however, reveals that terror organizations and their operatives continued to rely on non-technical methodologies to secure their communications. USA Today first suggested the use of steganography, or use of images to embed secret messages, as a method to 'encrypt' messages shared between terrorists. Newspaper outlets and briefings have continued to recycle the claim since the 9/11 attacks. [29] There is little evidence, however, to support the claim regarding the use of steganography. Nor is there evidence to support the claim that the 9/11 hijackers had used any form of technical encryption

[28] Campbell, Duncan, 'How Terrorists Encrypt 3: Communication Tools,' *Privacy PC*, 11 August 2012, available at: http://privacy-pc.com/articles/how-terrorists-encrypt-3-communication-tools.html, last visited: 17 December 2017.
[29] Don, Bruce W., Frelinger, David R., Gerwehr, Scott, Landree, Eric, Jackson, Brian A., 'Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations – Briefing Produced for the Department of Homeland Security,' *Rand Corporation* (2007), p. 31.

to secure their communications. In fact, according to an FBI briefing, the hijackers continued to use non-technical tradecraft, particularly open coded messages, to communicate over Hotmail.[30] Once more, terrorists did not undertake any additional steps to ensure the integrity of information.

Despite the expansion of surveillance powers granted to US intelligence agencies through the Patriot Act of 2001, terror groups continued to rely on non-technical methodologies to maintain informational confidentiality and integrity. In December 2001, Richard Reid attempted to detonate an explosive in his shoe while aboard a flight to Miami.[31] The individual used web drops to communicate with another individual. Web drops is a process in which an individual writes a message to the drafts folder of an email service for another individual with access to the account to access later. Web drops were used as a strategy to avoid sending information over a telecommunication network in attempts to provide operational confidentiality. Similarly, web drops were used to provide guarantees to operational integrity, as only those who trusted with the password and username to the email service could read or write to the draft folder. The application of open-coded messages and web drops continues throughout 2004, 2005 and 2006, with a noticeable exception, Operation Mazhar.[32]

The 2005 Scottish yard operation, Operation Mazhar contains convincing evidence of a terrorist applying technical tradecraft to attain operational confidentiality and integrity. In 2005, authorities arrested Younis Tsouli for ties to Al-Qaeda after developing numerous websites on

[30] FBI Briefing
[31] Campbell, Duncan, 'How Terrorists Encrypt 4: "Mujahideen Secrets" Software,' *Privacy PC*, 12 August 2012, available at: http://privacy-pc.com/articles/how-terrorists-encrypt-4-mujahideen-secrets-software.html, last visited: 17 December 2017.
[32] For more information, see: Operation Theseus, Operation Niche, Operation Praline and Operation Overt.

behalf of the terror organization, and later distributing video-content.[33] According to reports, Younis Tsouli used both a combination of PGP over email services, and the encrypted messenger GAIM to communicate with those in his network.[34] In using PGP, Tsouli applied technical tools to secure the confidentiality and integrity of information sent. His use of the off the record (OTR) encrypted messenger app, GAIM also provided confidentiality and anonymity. OTR uses a new secret key to encrypt messages sent per session, providing confidentiality of messages. Similarly, OTR practices deniable authentication, preventing any eavesdropper from identifying communicators.

Despite, the use of tools by a terrorist and terror group to achieve confidentiality, integrity of information, and anonymity of communicators, Tsouli's case is a clear outlier. From evidence presented, he possessed a strong technical background, prior to his exposure to Jihadism. Tsouli worked as both a hacker and data manager.[35] Therefore, the case is an outlier, not reflective of broader trends regarding the application of tradecraft to secure confidentiality, integrity, and anonymity.

In 2007, terror groups began organizational efforts designed to secure the confidentiality and integrity of information shared amongst members. In July 2007, the Global Islamic Media Front (GIMF), the propaganda wing of Al Qaeda, released Mujahedeen Secrets. Mujahedeen Secrets is an encryption software built on PGP to ensure the confidentiality and integrity of information shared. The release of the software represents among the first organizational efforts to secure the confidentiality and integrity of information shared through modern technological methods.

---

[33] Campbell, Duncan, 'How Terrorists Encrypt 5: International Anti-Terror Operations,' *Privacy PC*, 14 August 2012, available at: http://privacy-pc.com/articles/how-terrorists-encrypt-5-international-anti-terror-operations.html, last visited: 17 December 2017.
[34] Ibid.
[35] Ibid.

In the first issue of *Inspire,* an online publication by Al Qaeda, the authors stress the need to secure the confidentiality and integrity of messages. The authors argue that spies are actively attempting to read emails, and to remain secure members must use encryption software, like Muhajdeen Secrets. In attempts to ensure the program's usage, the authors provide illustrative, systematic instructions detailing public and private key creation, the importation of the recipient's public key, encrypting the message, decrypting the message, verifying the integrity of the message, and simple troubleshooting tips. The magazine continues campaigning for the use of the Mujahedeen Secrets program in subsequent issues published from 2010 to 2013.

Despite organizational campaigns, terrorists inconsistently utilized the Mujahedeen Secrets program to secure the confidentiality and integrity of messages. In his book entitled Agent Storm, Martin Storm, a former terrorist turned double agent for the CIA, recalls receiving a briefing from Anwar Al-Awalaki, then head of Al Qaeda. According to Storm, during the briefing he received training on how to use the program to communicate with senior Al Qaeda leadership in late 2009. [36] In addition, Storm notes that Al-Awalaki had been using the program to communicate with his contacts in the west.[37]

At the same time, terrorists also continued to rely on the application of non-technical tradecraft, including web drops and open coded messages. In 2009, two years after GIMF released the Mujahedeen Secrets program, British police arrested twelve men under suspicion for being a bombing cell.[38] An independent review of the sting operation leading to the group's

[36] Storm, Martin, *Agent Storm: My Life Inside al Qaeda and the CIA*, Penguin Group (2014).
[37] Ibid.
[38] Campbell, Duncan, 'How Terrorists Encrypt 6: Traces Cleanup with TrueCrypt,' *Privacy* PC, 14 August 2012, available at: http://privacy-pc.com/articles/how-terrorists-encrypt-6-traces-cleanup-with-truecrypt-software.html, last visited: 17 December 2017.

arrest indicated no use of Mujahedeen Secrets, or encryption for that matter. Instead, the report found that the group's members had relied on the use of open coded messages.[39]

Terrorist inconsistent use of the encryption software continued due to a growing distrust in the authenticity of the software released on a variety of terrorist forums. As a result, terrorists also relied on rudimentary encryption techniques. In 2010, Anwar Al Awalaki began communicating with Rajib Karim, an IT Engineer at British Airways living in the United Kingdom. Al-Awalaki urged the use of Mujahedeen Secrets, but Karim paranoid about the authenticity of the program, resorted to the use of a rudimentary encryption process developed and used by senior leadership of the terror organization Jamaat-ul-Mujahedeen Bangladesh known as Tadpole.[40] Tadpole used a single-column, fixed monoalphabetic substitution cipher, similar to that used by Julius Caesar in 44 BC.[41] Thus, both Al Qaeda and JMB senior leadership relied on a rudimentary encryption process to 'secure' communications.

Availability

Terror groups and terrorists relied on popular CSPs for availability guarantees. Yahoo is one content service provider (CSP) identified to have been regularly used by Al Qaeda to communicate information.[42] As a popular CSP, Yahoo provides strong availability guarantees for the communication of operational information. To provide additional availability guarantees, Al Qaeda used a variety of Yahoo services, including chat, email, and Yahoo Groups to add redundancy for informational assets.[43]

---

[39] Ibid.
[40] Campbell, Duncan, 'How Terrorists Encrypt 7: Peculiarities of Encryption using Tadpole,' *Privacy PC,* 18 August 2012, available at: http://privacy-pc.com/articles/how-terrorists-encrypt-7-peculiarities-of-encryption-using-tadpole.html, last visited: 17 December 2017.
[41] Ibid.
[42] Forest, James K. F, *Teaching terror: strategic and tactical learning in the terrorist world,* Rowman & Littlefield Publishers (2006), p. 112.
[43] Ibid.

In addition, terrorists and terror groups also relied on Gmail and Hotmail to ensure availability of operational information. In many of the operations previously discussed, Hotmail and Gmail were among the email services often used. Similarly, in many publications released by the Global Islamic Media Front (GIMF), terror organizations often listed Hotmail and Gmail email addresses as a means for possible communication with the organization. Hotmail and Gmail, owned by Microsoft and Google, respectively, provided a reliable medium for the availability of operational information transmitted through web drops and open coded messages.

To provide added redundancy, terror groups and terrorists also relied on non-indexed webpages, commonly referred to as the Darknet, to share information. In 2010, cybersecurity and intelligence firm Procysive estimated that the Darknet is home to more than 50,000 extremist websites and more than 300 terrorist forums.[44] As non-indexed webpages, forums and websites hosted on the Darknet are unlikely to be censored unlike electronic groups or forums hosted on popular CSPs like Yahoo. As a result, terrorist and terror group use of the Darknet provides added availability guarantees. It should be noted, however, that the report produced by Procysive does not differentiate between forums used for the sharing of propaganda and forums used for the sharing of operational information. Nonetheless, the use of non-indexed webpages is a noteworthy development with regards to terror group and terrorist availability strategies.

Anonymity

Coinciding with the release of the Mujahedeen Secrets program, many terrorists began exploring new operations security strategies related to anonymity. Archives indicate that in May 2007, terrorists began evaluating secure browsers on jihadi forums for disseminating propaganda

[44] McCormick, TY, 'The Darknet: A Short History,' *Foreign Policy*, 9 December 2013, available at: http://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/, last visited: 17 December 2017.

and communicating via email.[45] Thus, at the individual level, fellow terrorists began recommending tools to ensure the anonymity of fellow terrorists communicating details via the web.

As previously noted Procysive estimated that, the Darknet is home to more than 50,000 extremist websites and more than 300 terrorist forums. Since anonymous browsers like Tor are among the only ways to access the Darknet, it is safe to assume terrorists began to use Tor to communicate. Again, no information is given to distinguish the use of the technology to share propaganda anonymously and the use of the technology to share operational information anonymously. Regardless, terrorists often used the anonymizing technology inconsistently. According to counterterrorism analysts, terrorists largely did not use any anonymizing tools when accessing email and group chat services on popular American CSPs.

Efficacy of Operations Security Techniques

Thus far, there exist several emergent trends regarding terror group and terrorist operations security. Despite organizational recommendation and instruction, to ensure the confidentiality and integrity of information, terrorists inconsistently utilized provided encryption software. Instead, terrorists consistently relied on open coded messages and web drops. The efficacy of open coded messages likely varied. Certainly, the NSA could read the contents of the messages likely collected through UPSTREAM and PRISM data collection programs. However, the NSA's ability to 'crack' the coding system would depend on the coding system itself. That is, a confidentially secure coding system would require the messages maintain proper grammar, be consistent, and fit a plausible conversation.[46] The system, however, does have serious flaws.

[45] Alkhouri, Laith, Kassirer, Alex, 'Tech for Jihad: Dissecting Jihadists' Digital Toolbox,' *Flashpoint*, July 2016, available at: https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf, last visited: 17 December 2017, p. 2.
[46] Grugq, 'Secure Communications,' *Tumblr,* 29 November 2013, available at: https://grugq.tumblr.com/post/68453478391/secure-communications, last visited: 17 December 2017.

Once a word is de-obfuscated, the rest of the system can begin to unravel. Similarly, terror groups and terrorists are known to repeatedly use the same words. As a result, intelligence officials may begin to formulate a database of words of potential selectors for UPSTREAM and PRISM data collection. The system also limits the availability of information for newly authorized entities, as code words need be pre-arranged. Therefore, potentially limiting the ability of terrorists to conduct operational business. The system also simply provides no guarantees to the integrity of information nor to the anonymity of communicators.

Web drops also likely provided limited guarantees of confidentiality. While the messages may not have been sent over the network, the NSA retained access to the electronic dead drops through the agency's PRISM and XKeyScore programs. Yahoo and Hotmail, two of the most popular CSPs used by terror groups, were compliant to NSA selectors issued via a FISA 702 court order. As a result, information shared via web drop could be readily read by the NSA, and corresponding parties could be consequently identified. Such claims are borne not only by simple logic, but also by congressional testimony that has reported PRISM's role in disrupting more than fifty potential terrorist events in more than twenty different countries.[47]

The Mujahedeen Secrets software proved an effective tool to secure the confidentiality and integrity of operational information. The NSA's supercomputers, operating under the SIGINT programs previously discussed, could not decrypt messages sent using PGP. The difficulty in 'cracking' the PGP encryption results from the program's use of keys of 512 to 4096 bits in length, making the brute-force decryption of the files largely impossible.[48] However PGP

[47] Young, Mark D., 'National Insecurity: The Impacts of Illegal Disclosures of Classified Information', *A Journal of Law and Policy for the Information Society*, vol. 10, no. 2 (2014), p. 378.
[48] 'Chapter 4. Keys', *PGP,* available at: http://www.pgp.net/pgpnet/pgp-faq/pgp-faq-keys.html, last visited: 17 December 2017.

offers a significant amount of metadata for programs like PRISM and UPSTREAM to begin to formulate a network of communicators.

Information protected via the software, however, proved rather damaging to the anonymity of communicators. Each message encrypted with the software, began with the string, 'Asrar al-Mujahedeen V.2.0'. As a result, the NSA through UPSREAM programs, PRISM, XKeyscore could each issue a selector across the broad domain of accessible data, allowing the NSA the ability to identify terrorist communiques and communicators. Through doing so, the NSA could identify suspected terrorists email accounts, their respective IP addresses, and therefore begin to formulate a network of suspected terrorists, largely compromising the operations security of the terrorists communicating.

Each of the implemented methodologies presents serious challenges to the operations security strategies of terror groups and terrorists. NSA SIGINT programs could identify the IP addresses of the communicators, and thereby begin to formulate a network of suspected terrorists. Web drops, in cases where messages were written non-obscurely, allowed for easy readable access for the NSA via PRISM and XKeyscore. In cases where open-coded messages were utilized, the NSA likely had access to the messages, the IP addresses of the messengers, and often the meaning of the message. Thus, operations security strategies implemented by terrorists were ineffective against NSA SIGINT programs.

Approaches to Operational Security & Efficacy, Post-Snowden

Awareness of the Disclosures

Any argument discussing the resultant behavioral shifts of terror groups and terrorists following the disclosures requires an examination of two assumptions. First, terror groups and

terrorists observed the disclosures. Second, both terror groups and terrorists understood the significance of the disclosures as they pertained to their respective operations security.

At the organizational level, terror groups became quickly aware of the disclosures and their corresponding significance to operations security. Soon after the disclosures, Global Islamic Media Front (GIMF) posted words of warning on the organization's mobile encryption for Android page, "Take your precautions, especially in the midst of the rapidly developing news about the cooperation of global companies with the international intelligence agencies, in the detection of data exchanged over smartphones".[49] The words of warning published by GIMF prove that an organizational level terror groups were aware of the NSA's bulk data collection programs. In addition, the warning published by GIMF serves as evidence of an organizational need and intent to improve operations security.

At the individual level, terrorists also proved to be both aware of the disclosures and their corresponding significance pertaining to operations security. In the months that followed the disclosures, terrorists published blog posts that relayed the significance of the information released in the disclosures. In a post entitled "Remaining Anonymous Online", an ISIS sympathizer discussed the reach of intelligence agencies bulk data collection programs, the power of metadata collection, and the corresponding need to remain anonymous online. Thus, the blog post is evidence of individual terrorists identifying a need for improving operational security in light of the Snowden Disclosures, and an intent to do so.

Given both awareness of the disclosures and an intent to devise new operations security strategies at both the individual and terror group level, one might assume a subsequent adoption of strategies that would challenge NSA SIGINT programs. Thus far, however, terror groups are

[49] 'Al-Qaeda and Snowden: Correlation, Causation, and Temporal Analysis,' *Recorded Future,* 6 August 2014, available at: https://www.recordedfuture.com/al-qaeda-encryption-technology-reaction/, last visited: 17 December 2017.

the only entities that have proven consistently respondent to the disclosures in the form of recommendations. At the operational level, individual members inconsistently and inefficiently implemented organization recommendations to secure their operations strategy. As a result, the disclosures have not yet caused the advent of the advent of the operationally secure terrorist and terror group, despite reports to the contrary.

Confidentiality & Integrity

At the organizational level, terror groups quickly adapted their operations security in response to the disclosures. Terror groups advocated for the adoption of technologies that would strengthen the organization's ability to confidentially transmit information. Within a year of the disclosures, GIMF released four new encryption technologies.[50] GIMF designed each of the technologies to confidentially secure a new mode of communication. On September 4, 2013, GIMF released Tashfeer al-Jawwal, a mobile encryption program designed to secure SMS texts sent via android.[51] In doing so, GIMF confidentially secured an increasingly popular mode of communication for members. Releases prior to the disclosures only secured communications sent via Windows computers. The release of encryption software designed to secure new modes of communication is a clear response to limiting UPSTREAM and PRISM's access to readable information shared between members.

The new encryption software released by GIMF neglected to provide guarantees pertaining to the integrity of information shared. As noted previously, Mujahedeen Secrets provided guarantees of integrity through use of public key crypto. Recent releases of encryption software relied on symmetric key encryption, which does not provide any guarantees to integrity.

---

[50] 'How Al-Qaeda Uses Encryption Post-Snowden [Part 2] – New Analysis in Collaboration with Reversing Labs,' *Recorded Future,* 1 August 2014, available at: https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/, last visited: 17 December 2017.
[51] Ibid.

The decision is an attempt to limit the potential leaks of metadata through use of PGP to mass surveillance programs like UPSTREAM and PRISM.

Like Al Qaeda, ISIS also attempted to increase the adoption of tools that would further aid in ensuring the confidential transmission of information. In a 34-page manual on operations security distributed amongst the organization, ISIS expands the list of terrorist approved full device encryption software beyond the popular TrueCrypt software to include VeraCrypt, Windows Bitlocker, and encrypted stand-alone disks to secure the confidentially and integrity of information transmitted. ISIS also advocated for the adoption of end-end encrypted messengers, including Telegram, Whisper, Threema, and Wickr. While some applications offer stronger guarantees to the confidential and integrity of information shared than others, the recommendations by ISIS nonetheless indicate an attempt to counter UPSTREAM and PRISM.

Considering the disclosures, terror groups also urged members to avoid use of content service providers (CSP) that fall under FISA's domain. In the 34-opeations security manual previously referenced, ISIS warns against the use of Facebook, WhatsApp, and other programs that are compliant to NSA's requests for data. Similarly, ISIS warns against the use of any US based email provider. ISIS argues that the US government may utilize any information sent or stored in these services. The organization instead advocates for the use of Hushmail, ProtonMail, and Tutanota because each operate outside of FISA's domain. Thus, terror groups recommended the use of new, non-American CSPs to confidentially secure information against PRISM and UPSTREAM.

The organizational strategies recommended by terror groups has continued to be recycled across a wide range of media. Terror organizations like ISIS, Al Qaeda, and other affiliated terror groups have taken to Telegram public channels and Twitter to disseminate organizational

strategies. However, the organizational recommendations disseminated have produced decidedly mixed results.

On the surface, a statistical analysis indicates that terrorists adopted many of the resources recommended to secure the confidentiality and integrity of information transmitted. In over 2,301 accounts identified as openly supporting terror groups, when listing an email address, 34% listed a Gmail account, 21% listed a Mail2Tor account, and the rest a combination of Sigaint, RuggedInobx, and Yahoo mail.[52] When listing an instant messenger account, 34% listed a Telegram account, 15% listed a Signal Account, 15% listed a WhatsApp account, and the rest listed either Wickr Surespot, Threema, or other. [53] Thus, on some level terrorists have adopted many of the encrypted services advocated for at the organizational level to secure the confidentiality and integrity of information. The report, however, makes no distinction between accounts managed by a terror organization or their affiliated media outlet, which often only produce propaganda, and accounts managed by those interested in planning and executing a terror attack.

Upon examining recent terror operations, successful or unsuccessful, an inspection of technologies used to plan and execute terrorist operations shows an inconsistent implementation of technologies advocated for at the organizational level. As Figure 1 indicates, over the course of 2014 to 2016, terrorists haphazardly used encryption to secure the integrity and confidentiality of operational information shared in communications between fellow operational members, as well as stored on their respective computers. In addition, there is no evolutionary trend to indicate the future consistent adoption of technical tradecraft to secure the confidentiality and

[52] 'Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations,' *Trend Micro*, 3 May 2016, available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/overlapping-technologies-cybercriminals-and-terrorist-organizations, last visited: 17 December 2017.
[53] Ibid.

integrity of operational communications and information. The Center for Strategic & International Studies in their report *The Effect of Encryption on Lawful Access to Communications and Data* examining many of the cases above also finds that most terrorists do not rely on encryption for their operational communications.[54]

Terror Attack	Date	Encryption Used	Type
Brussels, Jewish Museum	May 2014	Unknown	-
Paris, Charlie Hebdo Attack	Jan 2015	Yes and No	Mix of encrypted and unencrypted emails
Attack at Verviers	Jan 2015	No	-
Paris cell operating	Aug 2015 – January 2016	Yes	Telegram
Attack on Thalys Train	August 2015	Unknown	-
Reda Hame Cell	August 2015	Yes	TrueCrypt
Bataclan attacks	November 2015	No	-
Brussels Airport	March 2016	No	-
Dhaka Café	June 2016	Yes	Threema
Hyderabad (foiled attack)	July 2016	Yes	Tutanota
Salah Abdeslam	May 2016	No	-
Westminster	March 2017	Yes	WhatsApp

Figure 1[55]

Availability

Terrorists and terror organizations continued to rely on popular American content service providers (CSP), despite recommendations made to avoid their usage. In the survey of 2,301 accounts previously mentioned, 34% of terrorists maintained a Gmail account and 12% maintained a yahoo mail account. Thus, nearly half of identified terrorist and terror group

[54] Lewis, James A., Zheng, Denise E., Carter, William A., 'The Effect of Encryption on Lawful Access to Communications and Data,' *Center for Strategic & International Studies*, February 2017, available at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE, last visited: 17 December 2017.

[55] Grugq, 'Just the Facts: ISIS Encryption,' *Medium*, 24 April, 2016,available at: https://medium.com/@thegrugq/just-the-facts-isis-encryption-c70f258c0f7, last visited: 17 December 2017.

accounts continue to use popular American CSPs. As the world's most popular CSPs Yahoo and Google provide strong availability guarantees. For instance, according to a Google representative, Gmail suffers only about 10 to 15 minutes of downtime per month, giving the service provider an average uptime rate of 99.99 percent.[56]

Terror groups and terrorists have also increasingly adopted the end-end encryption mobile app, Telegram to provide availability guarantees. Aside from motivations related to confidentiality, the popularity of the app has been fueled by the crackdown on terrorist-related accounts on Twitter. Although Telegram has begun to ban accounts that transmit terrorist related materials, the app has not been as successful as Twitter and other popular CSPs. Thus, attacks on the terror group and terrorist informational availability are less likely to occur through using the app. The app provides the ability to disseminate information through public channels, allowing those interested to securely participate in the sharing of information. However, as noted, the increased adoption of Telegram by terrorists and terror groups is not driven solely by the disclosures. In fact, from an availability perspective, the phenomenon is likely, driven by social media's crackdown on terrorist and terror group affiliated accounts.

Anonymity

Anonymity also became of greater concern following the disclosures. The discussion and instruction of anonymizing browsers and anonymizing VPNs migrated from decentralized jihadi forums to online official literature released by terror organizations. ISIS advocates for the use of Tor and other anonymizing mechanisms in their French online publication, Dar al Islam, in several different editions following the disclosures. ISIS also recommends several anonymizing browsers for a variety of platforms. Platforms that include, iPhone, android, windows, and macs.

[56] Perez, Juan Carlos, 'Google Apps' Gmail Faces Downtime Problems,' *PCWorld: IDG News Service*, available at: https://www.pcworld.com/article/130187/article.html, last visited: 17 December 2017.

In addition, Al Risalah, an Al Qaeda affiliate, encourages the use of Tor, arguing that the tool is one of the most important in an organization's defensive weapons arsenal. The article additionally provides advice on mitigating some of Tor's weaknesses to ensure the users anonymity. Thus, after the disclosures, anonymity became a focal point for operations security, migrating from forums to official literature released by the organizations.

To aid in anonymization, ISIS recommended that its members download and use Tails. Tails is an operating system, typically stored on a USB, which runs an encrypted version of Linux and provides encryption and anonymizing tools. The OS comes loaded with a myriad of tools, including metadata cleaners and the browser Tor.[57] Since Tor is Tails's default browser, recommendations for Tails is an attempt to secure the anonymity of terror group members.

Despite clear recommendations, terrorists often neglected to use technologies to secure their anonymity online. Both counterterrorism and fellow terror group members have acknowledged the refusal. According to a counterterrorism official, ISIS supporters have experimented with anonymous browsers including Tor, but often their experimentation is short-lived.[58] ISIS supporter Samata Ullah also noted a refusal to use Tails as well as Tor to remain anonymous online.[59]

Efficacy of Operations Security Techniques

At an organizational level, terror groups proved respondent to the disclosures. Individuals, however, inconsistently, and haphazardly utilized respondent recommendations to secure their operations security. Certainly, a statistical increase in the number of terrorists utilizing technical methodologies occurred following the disclosures. However, once more, those

[57] Ibid.
[58] Goodwin, Bill, 'Islamic State supporters shun Tails and Tor encryption for Telegram,' *Computer Weekly*, 8 June 2017, available at: http://www.computerweekly.com/news/450419581/Islamic-State-supporters-shun-Tails-and-Tor-encryption-for-Telegram, last visited: 17 December 2017.
[59] Ibid.

strategies have been inconsistently applied, particularly to terror operations. The inconsistently largely arises due to the remote-agent structure of ISIS and other globalized terror operations. Thus, both statistically and foundationally operation strategies *implemented* present *manageable* threats to NSA SIGINT programs.

Statistically, terror groups occasionally utilized end-end encrypted messengers to secure operational communications. Telegram, often citied to be favored among ISIS 'fanboys' and other terror operatives, and thus at the center of the debate involving the operationally secure terrorist and terror group, provides several potential attack surfaces for the NSA SIGINT programs to utilize.

Telegram requires a working phone number to register, which the application then uses as a unique identifier for the account. Users of the application, new to operations security, are likely to register with their personal phone number.[60] Thus, immediately terrorists lose all claim to anonymity. Telegram then verifies the individual has access to the account through use of verification codes sent to the telephone number provided. For an attacker with access to a telecom network, the attacker could hijack the verification code through redirecting the code to a phone that is under control.[61] Given that the NSA has previously accessed control of a telecom network through the agency's Quantum Insert program, the attack is well within the capabilities of the agency.

Surprisingly, Telegram also does not automatically provide end-end encryption of messages sent.[62] Through UPSTREAM, the NSA can read the contents of messages. The app

[60] Grugq, 'Operational Telegram,' *Medium*, 18 November 2015, available at: https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a, last visited: 17 December 2017.
[61] Grugq, 'Operational Telegram,' *Medium*, 18 November 2015, available at: https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a, last visited: 17 December 2017.
[62] Grugq, 'Operational Telegram,' *Medium*, 18 November 2015, available at: https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a, last visited: 17 December 2017.

also leaks a good deal of metadata. The leaking of metadata allows the NSA access to information regarding who talked with whom, at what time, and where they were located. Thus, through the attacks briefly highlighted the NSA has the capability to undermine every facet of terror group and terrorist operations security: confidentiality, integrity, availability, and anonymity. Therefore, the app presents a manageable threat to NSA SIGINT programs.

Notably, Telegram is among the many of tools *inconsistently* utilized by terrorists to transmit information. Terrorist also rely on WhatsApp, Threema, online dead drops through TrueCrypt, and Signal. Each of the applications, however, also contain vulnerabilities for NSA SIGINT programs to exploit. The efficacy of the tools used or not used will continue to be undermined as terror groups continue to devolve into a remote-control agent structure.

The Root of Inefficacy

As state sponsored counter-terrorism operations continue to be successful, terror organizations have devolved into a remote-agent existence to recruit and later launch attacks. ISIS and its lone-wolf attacks serve as an example of the remote-agent architecture terror organizations utilize. ISIS conducts recruitment operations over the web to identify potential operatives.[63] Upon their identification, ISIS recruiters stay in constant contact with the recruits, providing instructions delivered via the web pertaining to securely receiving delivered weapons and other essential information pertaining to the execution of a terror attack. Many counter-terrorism officials refer to the operations strategy as remote-controlled attacks, or violence guided by operatives in areas controlled by ISIS whose only connection to the attack is the internet.[64]

[63] Callimachi, Rukmini, 'Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar,' *New York Times*, 4 February 2017, available at: https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html, last visited: 17 December 2017.
[64] Ibid.

The remote-controlled attacks present two critical vulnerabilities that undermine terrorist and terror group operations security, regardless of tool used or not used. The first vulnerability is that a remote-agent architecture requires an easy to find entry node.[65] Terror groups that seek international recruits require an easy to find entry node or a point of contact for an aspiring recruit to use to join the organization. As a result, terror groups like ISIS are forced to have an extremely visible presence, often in the form of a Telegram channel.[66] This is particularly problematic, as any potential terror operative would have been tainted through reaching out to the organization via the public access node. The IP address associated with the phone would now be linked to a known terror group. As a result, the NSA SIGNT programs now have the capability to identify the individual.

Converting a potential recruit into a terror operative involves constant communication between the remote control agent and the recruit. The more traffic that exists, the more data points the NSA SIGINT can obtain. As internet traffic persists between parties, the NSA SIGINT programs can formulate a pattern of terror operatives. To successfully convert a potential recruit on the web, remote agents often resort to synchronous communications, often in the form of real-time chat.[67] The real-time chat protocol allows for easy correlation for UPSTREAM's bulk data collection program. As a result, NSA SIGINT can identify potential terror operatives.

Conclusion

In an interview conducted in February 2015, NSA Director Admiral Rogers discussed the damage done by Snowden Disclosures. When asked whether the disclosures by Snowden have

[65] Grugq, 'ISIS Remote Control Agent OPSEC,' *Medium*, 9 August 2017, available at: https://medium.com/@thegrugq/isis-remote-control-agent-opsec-3d0e02b35fbf, last visited: 17 December 2017.
[66] Ibid.
[67] Ibid.

reduced the NSA's counterterrorism capabilities, he responded, "Have I lost capability that we had prior to the revelations? Yes."[68] Certainly, the disclosures have presented new challenges related to counterterrorism efforts. Statistically, terror groups and terrorists have increasingly adopted technologies designed to secure the confidentiality, integrity, and availability of information. However, the application of technologies is haphazard and present manageable threats to NSA SIGINT programs.

A simple comparison of operations security strategies recommended by terror groups and implemented by terrorists serve as case studies to show the influence of the disclosures on terrorist behaviors. Al Qaeda and now its child, emerging from al Qaeda in Iraq, ISIS continue to be at the forefront of the debate involving the 'rise' of operationally secure terrorist and terror group. In analyzing ISIS respondent behaviors, contextualized in pre-Snowden al Qaeda behaviors, terror group operations security strategies advanced. Their strategies incorporated new tools designed to secure new modes of communication regarding the confidentiality, integrity, and availability of information shared. With regards to priority given to anonymity following the disclosures, the discussion of popular CSPs and anonymizing browsers entered mainstream organizational publications.

Despite each of the developments that would seek to compromise the efficacy of NSA SIGINT programs, terrorists haphazardly used technology to secure communication over the years following the Snowden Disclosures. In half the cases previously identified, terrorists did not use any form of encryption to secure the confidentiality and integrity of their communiques. Similarly, in those instances that a secure form of messaging was used, there exist many potential leaks of operational security information for NSA SIGINT programs to exploit. Thus,

[68] Epstein, Edward Jay, *How America Lost Its Secrets: Edward Snowden, the Man and the Theft,* E.J.E. Publications Ltd (2017), p. 298.

despite the statistical increase in challenges to NSA SIGINT programs' capacity, as mentioned in Admiral Roger's interview, the statistical increase does not present *unmanageable* threats to NSA SIGINT programs for the time being. However, as technology advances, terror groups continue to remain respondent and the barrier to entry for many of the technologies lowers, the scale could begin to shift in favor of terrorist and terror group operations security.