Extremist Forums Provide Digital OpSec Training

By Aaron Brantly and Muhammad al-`Ubaydi

THE AVERAGE NETIZEN has terrible digital hygiene. We click on random links, open emails from unknown individuals, use public WiFi hotspots, leave computers and devices unsecured, and often do not even use basic anti-virus packages. Most Chief Information Systems Officers' largest problem is not a talented nation state, but rather lazy or ignorant employees, oblivious to the risk they are exposing themselves, their networks, and their systems to through simple careless acts.

"Instead of calling help desk support, jihadists have formed online technical support communities."

The majority of individuals, whether using personal or corporate devices, do not have much need for high levels of digital operational security (often shortened to Digital OpSec) beyond the basic ability to protect personal information from malicious actors. When they have trouble with their computers they take them to their local help desk support staff, call remote help hotlines, or ask their children. However, many of the concerns the average person avoids on a daily basis become increasingly important when individuals are engaged in illegal or potentially illegal behavior.

Numerous news stories show how engagement with the Internet or mobile phones can generate a significant leakage of digital breadcrumbs.[1] These clues make it possible (although still quite time-consuming and difficult) for law enforcement and intelligence agencies to follow nefarious actors. The average potential foreign fighter or terrorist cannot pick up the phone to call the Geek Squad for help hiding their digital communications. Even as a well trained cybersecurity professional, it remains remarkably difficult to maintain highly robust digital operational security.

Instead of calling help desk support, jihadists have formed online technical support communities. The authors examined a variety of open source data comprising more than 40 forum conversations over the past year in which terrorists and potential terrorists examine, discuss, and ask for assistance in establishing robust digital operational security. We have leveraged forums including al-Minbar al-I`lami al-Jihadi, an open network that does not require registration unless posting content or engaging in personal communications via the platform; Shmukh al-Islam, a password-protected network with limited user access; and Al-Fida', a network similar to Shmukh al-Islam. Each of these networks also suffers from its own issues including hacking, but each contains content related to digital operations security.[2]

This study illustrates a skill gap between those who are capable of hiding their digital tracks and those who are not. The material also highlights the regularity of these conversations, sometimes in response to illegally obtained and disseminated classified documents, including those released by Edward Snowden. These discussions illustrate the role that information leaks can play in the digital environment for terrorist organizations. This analysis of more than 40 forum conversations, each with multiple threads and participants over the past year, presents a robust representative sample of the dynamics and issues facing terrorists in their efforts to achieve digital operational security.

The Jihadi Help Desk

This analysis indicates that jihadist forum and chat room participants are turning to one another with increasing frequency to learn best practices for digital operational security. Many of the questions are mundane and the answers are easily found either by consulting NGO sites dedicated to providing information about online privacy and security or popular commercial sites dedicated to information security.[3] Yet, despite multiple other avenues of information, questions of security regarding popular platforms such as Skype, Google, Gmail, WhatsApp, Tor Mail, are being posed in jihadi forums. Individuals with higher levels of technical acumen regularly warn those inquiring about commonly used products, indicating both their fundamental lack of security and the prevalence of surveillance by nation states on these platforms. These low-level questions are quickly and effectively answered. This illustrates a fundamental change in Tactics, Techniques, and Procedures (TTPs) associated with online behavior.

"The level of technical sophistication...indicates a mid-level understanding of digital operational security."

These low-level questions are the tip of an iceberg and demonstrate that even inexperienced users are beginning to recognize the fundamental constraints associated with using digital tools to communicate for jihadist purposes.

1 For a discussion on some aspects of digital tracking see: Aaron Brantly, "You Were Identified as a Participant in a Mass Disturbance," National Democratic Institute for International Affairs-Tech blog, January 24, 2014

2 Muhammad al-`Ubaydi collected dozens of conversations from these forums on issues related to digital operations security.

3 We will not focus on the NGOs that fund the development of these projects. The development process works in such a way as to include multiple government and privately funded NGOs as well as software development groups who receive government grants and funds. Various aspects of different software packages can be developed independently of one another through multiple funding streams. Often software development requests are in response to perceived and actual threats posed to democracy and human rights activists as well as to civil liberties and privacy.

The level of technical sophistication associated with the average user's question indicates a mid-level understanding of digital operational security often only secured through consistent study or training.

More experienced users providing advice in our sample pointed to other tools, among them were some that are often used to safeguard human and democracy rights activists around the world. Many of these programs or tools were developed with the expressed intent of safeguarding individuals working under the threat of states to provide added security for their operations. These same tools, often funded in part by the U.S. Government, NGOs, corporations, and others, are now expressly being used for illicit purposes. Programs such as Tor (an anonymous routing network, also referred to as the Onion Network), Tails, DuckDuckGo, StartPage, PhotoMe Beta, ExifTool, MetaNull, Jitsi, JustPasteIt, Silent Circle, and several others from the Guardian Project are being openly discussed on jihadi forums.[4] They are often accompanied by well-written Arabic documents explaining their implementation and use.[5] There are also numerous discussions on how to bypass security mechanisms such as registered emails and phone numbers so that individuals can take advantage of more popular platforms such as Twitter and Facebook for propaganda purposes.

"More experienced users providing advice in our sample pointed to other tools, among them were some that are often used to safeguard human and democracy rights activists."

Each of these tools provide ways to establish or enhance anonymity when communicating online. Combined use of these tools does not fully safeguard the anonymity of individuals online, yet it can significantly enhance the probability of remaining anonymous. Tools such as Tor and Tails facilitate anonymous browsing behavior. Tails can also alter the MAC address of a system, which serves as the computer's identification number while browsing, much like a postal address in the physical world. DuckDuckGo and StartPage enable anonymous or quasi anonymous searches.[6] JustPasteIt enables the quick and largely anonymous sharing of information via HTML links and has become increasingly popular with organizations such as the Islamic State.[7] Silent Circle is an encrypted email platform that has recently worked on the Black Phone project to enable stronger privacy.[8] The Guardian Project applications are designed to enhance privacy and secure communications on mobile devices.[9]

None of the democracy, human rights, or civil liberties organizations want to facilitate terrorist activities. Each of the developers or communities behind these products seeks to encourage privacy and human rights protection.[10] These products serve valuable legitimate purposes when civil liberties are under sustained threat. Many of these tools can help protect personal information when traveling, particularly when accessing insecure WiFi networks or when visiting countries that spy on foreign nationals.[11]

Digital security tools ostensibly developed to advance human rights are, however, now being used for terrorist activities. It is important to realize that despite a popular focus on the battlefields of Iraq, Syria, Libya, and other zones of contention, the infrastructure that goes into supporting the frontline fighters is deep and diverse.[12]

"Digital security tools ostensibly developed to advance human rights are, however, now being used for terrorist activities."

To communicate, transfer funds, plan and organize operations, train, and travel, groups such as the Islamic State and al Qa`ida rely on integrated communications strategies within a complex information environment that is constrained by state intelligence services.

When organizations are small it is conceivable to engage in direct forms of communication. Previous Combating Terrorism Center reports and occasional papers examined how the Islamic

4 We found mentions and discussions of all of these tools and many more in dozens of posts on jihadist forums.

5 We collected 24 unique digital training manuals in Arabic and saw embedded within various forum posts more than a dozen training videos.

6 See: https://duckduckgo.com/about and https://startpage.com/eng/aboutstartpage/

7 Carmen Fishwick. "How a Polish Student's Website Became an Isis Propaganda Tool." *The Guardian*, August 15, 2014.

8 See: https://silentcircle.com

9 See: https://guardianproject.info.

10 Examples of human rights protection include the Tactical Tech Collective's project "security in a box" found at: https://securityinabox.org/en, Reporters Without Borders "We fight Censorship" project found at: https://www.wefightcensorship.org/article/digital-security-basicshtml.html and the Open Technology Fund, a project that funds projects to help promote human rights and open societies found at: https://www.opentechfund.org/about-otf. These are just a small sample of dozens of similar projects that work on the development of platforms in the digital space.

11 One project that was historically very useful was the "security in a box" project that has now been overtaken by more current variants. Yet the trend remains the same, to provide training and resources to facilitate human rights and free and open societies, http://securityinabox.org.

12 Sarah Elizabeth Parkinson, "Organizing Rebellion: Rethinking High-Risk Mobilization and Social Networks in War," *American Political Science Review*, 107:3, (2013): pp. 418–432.

State's administrative processes grew.[13] Everything from reporting structures to finance structure and recruiting processes has to be developed. In constrained geographic areas this process can occur over what can best be described as the "SneakerNet," which describes the ability for complex organizational structures to be built up through direct personal contact facilitated by for example, walking or driving.

As the size and complexity of an insurgency increases so do the challenges of managing a transnational network. The logistical challenges for managing foreign fighters are extensive.

"Individuals are highly attuned to the security status of popular applications including Skype."

The International Center for the Study of Radicalisation and Political Violence estimates that more than 20,000 individuals have traveled to Syria to fight as of January 2015, a number that exceeds foreign fighter estimates for Afghanistan in the 1980s.[14] Once on the ground, these fighters need to be fed, organized, and often paid, an enormous challenge, which in the case of the Islamic State is made more difficult by external intelligence services seeking to halt foreign fighter flows.

The SneakerNet breaks down as logistical challenges increase. Globalized jihad has increasingly gone online to handle communications, monetary transfers, and other supporting and propaganda functions. This movement to global digital communications has increased the urgency associated with what is best described as tech support for jihad.

Jihadi Techies

Users like Tiqani al-Islam, who provides detailed analysis of Virtual Private Networks (VPNs) and their legal obligations regarding data retention, add to already robust discussions on secure communications in response to questions posed by community members. By identifying and highlighting which networks should not be used, they are enhancing the aggregate security of the network. By educating users how to use VPNs or the Tor network they are increasing the costs to intelligence and law enforcement in what Hoffman calls the "Technological Treadmill," in which terrorists seek to stay ahead of counterterrorist practitioners.[15]

We also found clear indications in the forums that individuals are highly attuned to the security status of popular applications including Skype. For instance, in response to a question about how to use Skype through Tor, a jihadi with more knowledge responded, "Skype is insecure, and Americans are recording every single call since 2008." Later, another jihadi specifically indicates that Skype cannot be used through Tor. These types of conversations are repeated in the sampled forum traffic for a number of applications. Discussions on the use of Skype, WhatsApp and many others are not of themselves surprising, but the conversations on the forums shift individuals away from using less secure to more secure communication.

The discussions also deal with facilitating secure mobile communications and browsing. A detailed post by Rakan al-Iraqi analyzes the security of several mobile platforms and a number of available communication applications. He begins by highlighting Wickr Software, a multi-platform messaging application that claims a number of highly secure features. He explains that using Wickr, user ID and device communications undergo multiple rounds of salted cryptographic hashing using SHA256, data at rest and in transit are encrypted with AES256, password and password hashes do not leave the device, and lastly that messages and media are subject to auto-deletion upon expiration. The application functions as a peer-to-peer encryption protocol eliminating the storage of encryption keys by a middleman. The program is designed for secure communications between human rights activists, journalists, friends, and individuals requiring high levels of privacy. Ratan al-'Iraqi explains the software's utility

"With the increasing sophistication of geo-mapping capabilities comes a heightened ability to plan operations."

and offers up Wickr's own $100,000 reward for those able to crack its protocols as a testament to its security.

Rakan al-'Iraqi also discusses Telegram, a Russian-made encrypted communications application. He notes that Telegram does force registration, but provides instructions for how to spoof the process with fake mobile numbers. Al-'Iraqi also demonstrates real technical prowess. A detailed discussion of and instructions on how to Root an Android Device[16] and install Tor shows a high degree of concern for systemic protection of communications. He provides a link to a detailed instruction manual on justpaste.it (in Arabic and with pictures) detailing how to root the device and install Tor. While the technical sophistication is probably too much for the basic user, the simplicity of the instructions opens it up to most moderately skilled users. The relative enhancement of security provided by the rooting of a mobile

13 Danielle F. Jung, Jacob N .Shapiro, Pat Ryan, and Jon Wallance, *Managing a Transnational Insurgency: The Islamic State of Iraq's "Paper Trail,"* 2005-2010, (Combating Terrorism Center at West Point, 2014). Muhammad Al-`Ubaydi, Nelly Lahoud, Daniel Milton, and Bryan Price, *The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State,* (Combating Terrorism Center at West Point, 2014).

14 Peter Neumann, "Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s." (ICSR, 2015).

15 Bruce Hoffman, *Inside Terrorism*, (New York: Columbia University Press: 2006), pp. 252-253.

16 Rooting a device allows for base level access to the device outside of the normal phone operating system.

phone and the installation of Tor can be significant, it does not provide fool-proof protection. Its consideration, however, demonstrates a level of awareness among the jihadists of the intense level of surveillance that is brought to bear on them.

Cyber Tools for Terrorists

Terrorists are able to leverage digital tools in other ways. User Abu 'Umbar al-Filistini, writing with the Twitter handle Usayyid al-Madani, provided detailed explanations on how to download and use online mapping programs to plan and coordinate "military operations." This discussion harkens back to the use of Google Earth by Lashkar-i-Tayyiba operatives to conduct the 2008 Mumbai attacks that resulted in approximately 160 civilian fatalities. Al-Filistini provides links to three different mapping services including the Universal Maps Downloader, Global Mapper, and Google Earth. He also included videos explaining how to use the mapping software and how to download maps for on-the-go operations. He closes his post with: "This work is dedicated to mujahideen everywhere, on top of them, the mujahideen of the Islamic State and Ansar Bayt al-Maqdis," illustrating the direct linkage of the online and offline communities.

The use of online mapping services demonstrates an increasing organizational capacity facilitated by the tools many use for normal activities. With the increasing sophistication of geo-mapping capabilities comes a heightened ability to plan operations with a better understanding of local terrain and its tactical advantages and disadvantages. A final case illustrating jihadis' increasing technical acumen comes in a detailed post by one Abu `Umar al-Misri. In it, he includes links to documentation as well as video tutorials on how to hack into WiFi networks.

The tutorials explain how to manipulate a vulnerability in WiFi Protected Setup (WPS), a feature that is enabled by default runs on most WiFi routers using WPA2 protection. This feature is still enabled on many WiFi routers and poses a security threat because the password can be broken quickly using brute force (trying a different password over and over until access is granted). Although the absolute technical skill required to exploit this vulnerability is relatively low, the discussion again serves to highlight the use and discussion of technology vulnerabilities.

This article cannot examine all instances where advice and instructions are being disseminated, but the information is both deep and broad. What is frustrating for the privacy and security community is the realization that the government position on so-called backdoors might have some merit. The burden clearly does not fall entirely on well-intentioned developers.

"Jihadist tech support through online communities is likely to grow in importance in the coming years."

Many tools are being developed by jihadis. We found conversations indicating jihadis are in the early stages of developing secure communications and browsing programs independent of the efforts by Western privacy advocates. The effectiveness of these tools is likely to be limited in most cases, yet will likely increase the concerns of intelligence and law enforcement individuals as they represent a small first step down the road to developing potential cyber weapons. Requests among the sampled forum traffic for targeted low-level attacks against websites in other countries and information about strategies and techniques to facilitate such attacks also add to concerns about digital security.

Insights into Jihadist Behavior Online

Our sample provides intriguing insights into an evolving area of operations. The low level of Internet penetration in some Middle Eastern and North African nations (Iraq, Syria, and Yemen having 9.2%, 26.2%, and 20% respectively as of 2014)[17] contrasts with the high levels in Europe and other Western countries. It indicates that the role of jihadist tech support through online communities is likely to grow in importance in the coming years.

Understanding how jihadists establish digital security will become more important. By enhancing their digital hygiene, jihadists are augmenting costs both in time and money for intelligence services and law enforcement.

These jihadist tech support posts were in many ways inevitable and their level of sophistication is likely to grow as does the percentage of the population who qualify as digital natives. As the membership of terrorist/jihadist organizations evolve from technically weaker older generations to younger generations with a far greater comfort and respect for the uses and limits of technology, it is likely that the threat environment will become increasingly complicated. Jihadist tech support for the application of digital tools is quite literally in its infancy and the future offers both opportunities and threats.

Muhammad al-`Ubaydi is a research associate at the Combating Terrorism Center and monitors Arabic jihadist websites.

Aaron F. Brantly is Assistant Professor of International Relations and Cyber in the Department of Social Sciences at the United States Military Academy, Cyber Policy Fellow for the Army Cyber Institute and Cyber Fellow at the Combating Terrorism Center.

The views expressed here are those of the authors and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

17 "Middle East Internet Users, Population and Facebook Statistics." Internet World Stats, 2015.