Routledge
Taylor & Francis Group

Survival

Global Politics and Strategy

ISSN: 0039-6338 (Print) 1468-2699 (Online) Journal homepage: http://www.tandfonline.com/loi/tsur20

Innovation and Adaptation in Jihadist Digital Security

Aaron Brantly

To cite this article: Aaron Brantly (2017) Innovation and Adaptation in Jihadist Digital Security, Survival, 59:1, 79-102, DOI: 10.1080/00396338.2017.1282678

To link to this article: http://dx.doi.org/10.1080/00396338.2017.1282678

Innovation and Adaptation in Jihadist Digital Security

Aaron Brantly

The importance of the internet to contemporary jihadists as a tool for recruitment, propaganda and operational planning is well established.[1] Less thoroughly studied are the ways in which jihadists work to keep this activity secure from monitoring and disruption, and in particular the ways in which they innovate and adapt to changes in the technological environment.[2]

Online forums, training manuals, tweets, blogs, Facebook posts and other forms of communication point towards a jihadist community that is alert to changes in both the technology and the laws and policies of its adversaries. Supporters of the Islamic State, also known as ISIS or ISIL, and resurgent elements of al-Qaeda make use of increasingly decentralised online networks to learn and spread technical knowledge. These communities operate outside of the groups' zones of physical control, exploit emerging technologies and develop novel technical solutions when their communications and organisational infrastructure is challenged. This cycle of innovation and adaptation, informed by community learning and external information sources, is a challenge to intelligence and law-enforcement efforts to stop potential terrorist attacks.

It should not come as a surprise that terrorist groups are able to learn, innovate and adapt. Groups under sustained external threat from various foreign and domestic actors are forced to face the realities of the world in which they

Aaron Brantly is Assistant Professor of International Relations and Cyber in the Department of Social Sciences, Cyber Policy Fellow at the Army Cyber Institute, and Cyber Fellow at the Combating Terrorism Center, West Point. The views expressed are those of the author and do not reflect the official policy or position of West Point, the Department of the Army, the Department of Defense or the US government.

Survival | vol. 59 no. 1 | February–March 2017 | pp. 79–102 DOI 10.1080/00396338.2017.1282678

exist. Intelligence and law-enforcement agencies are trying to prevent terrorist attacks; terrorist organisations are trying to avoid being caught.

Organisations such as ISIS and al-Qaeda develop the organisational capacity to enhance their operational security (OPSEC) by learning from experience. This includes both their own experience and that of groups facing similar constraints, from criminals such as the Russian Business Network (RBN) to hacker groups such as Anonymous, and human-rights activists trying to foster women's rights, free press and democracy in the face of oppressive governments. In the latter case, terrorists are often evading exactly the same governments' attempts to capture them and prevent their attacks. And states' efforts to censor, surveil and arrest their citizens in an effort to stifle internal dissent have induced more liberal governments to fund low-cost technologies that circumvent surveillance.[3] In turn, the causal link between civil-society repression and terrorist use of encryption and obfuscation technologies is remarkably straightforward.

Terrorist organisations are attuned to changes in the digital environment. As states increase the pressure, these groups must either adapt or, in all likelihood, they will perish. This applies equally to all actors that experience significant state pressure. Non-jihadist actors also use tools and technologies designed for benign purposes for illegal ends. As recently as summer 2016, for example, the FBI was in the process of prosecuting more than 100 individuals engaged in the trafficking of child pornography through the dark web.[4]

Terrorist groups must contend with multiple types of surveillance,[5] comprising various forms of signals, imagery, human and cyber intelligence.[6] Surveillance and censorship are pitted against a wide array of actors and generate a wide range of responses. Some states engage in carte-blanche surveillance; others help provide the means to circumvent it. The surveillance actions of one state and the remediation efforts of another are intrinsically linked. Moreover, the linkage is not only state-to-state, but also state-to-corporate, state-to-NGO (non-governmental organisation), and so on down the chain of capable actors. What results is a technological race in terms of both capability development and capability mitigation.[7]

As information about states' capabilities to surveil and censor has become public, jihadists have moved towards robust, decentralised approaches to

learning and practising digital OPSEC. And as the life cycle of open-source and freeware products facilitating digital security evolves, the task of monitoring and disrupting jihadist organisations will become increasingly difficult, particularly at the core of the networks of concern.

Online contests

ISIS has developed a sophisticated and wide-ranging recruitment operation via social media, building on earlier efforts by al-Qaeda.[8] The West Point researcher Dan Milton and others have attributed the success of the Islamic State's overall media operations to a long process of trial and error, marked by the possession of largely uncontested territory in which the jihadist groups had time and space to hone their messaging.[9] Just as the quality of media has improved over that period, so too has the Islamic State's technological acumen. Unlike the geographical space provided for the development of media operations, however, the internet remains largely contested. This means ISIS has had to develop novel strategies for engagement that extend beyond the traditional website-development models found in previous iterations of al-Qaeda and its affiliates.[10]

The linking of various online platforms on which potential recruits are attracted casts a broad net that is largely immune to the destruction of any given node. Network theory suggests that the structure used by jihadists, often referred to as a distributed network, is remarkably robust and resilient.[11] Literature on the evolution of terrorist behaviour also highlights the draw of the internet specifically because of its embedded resilience.[12] By using common words, hashtags, usernames and graphics, ISIS and al-Qaeda supporters are able to avoid losing individuals when any given account or website is suspended or shut down.

Current efforts to combat innovative propaganda by the Islamic State are underwhelming. The US Department of State established in December 2013 a countering-violent-extremism presence on social media, titled 'Think Again Turn Away', which had 11,000 followers on Facebook and 23,000 on Twitter as of September 2015. It was unable to compete with either the emotion or the volume of ISIS propaganda. State's Twitter account had posted or retweeted more than 8,390 tweets by September 2015. By comparison, a

single account from the media wing of ISIS posted or was retweeted more than 42,000 times in the same period, despite being shut down by Twitter halfway through the time frame.[13] (This is a limited and relatively gentle assessment of State's effort – others have been blunter.[14]) Gabriel Weimann, the author of numerous works on terrorism in cyberspace, and others have helpfully illustrated the volume of messaging and propaganda that leads individuals from learning about religious life to eventual radicalisation. The now-suspended Twitter account @reyadiraq, for example, belonging to an ISIS supporter with a prolific posting record, accumulated more than 90,000 followers.[15] Thousands more accounts tweet, hashtag, retweet and follow jihadist movements, radical clerics and other jihadist groups.

Yet jihadists' fluency in digital media is not all bad news for counter-terrorism efforts. As potential recruits make the journey from curious beginner to trusted member, they must demonstrate increasingly sophisticated means of safeguarding not only their own security, but also that of the network they wish to join.[16] Recruits who fail to protect their digital security are less likely to make it to the fight in the first place.

The social-media presence and online behaviour of potential recruits is being scrutinised by law enforcement, intelligence agencies, communities, parents, teachers and friends.[17] Many of those radicalised leave breadcrumbs in plain sight. Zachary Chesser, for example, a 21-year-old Virginia man who had made plans to travel to join al-Shabaab in Somalia, practised little digital OPSEC in posting increasingly extreme content to his personal blog, YouTube, Twitter and Facebook accounts, eventually making threats against the writers of *South Park*.[18] Chesser's sloppiness earned him a 25-year sentence for posting radical messages online and attempting to provide material support to a terrorist organisation.[19]

Personal conversations among participants in the online jihadist movement are conducted under conditions in which each participant is explicitly instructed not to make physical contact with fellow participants outside of zones of control in which the identity of both participants is assured.[20] It is fine to meet up online and share values and ideas, but not to release personal information that might identify one's location or other key attributes that might incur unnecessary risks. Simply put, cyberspace is a good place

to learn about Islam and jihad, but not to make personal connections when planning to travel from a third-party country to a conflict zone or when seeking material support for an attack at home. To build true interpersonal connections and to become more than a member of a virtual network, it is necessary to physically locate oneself within that network or become a trusted member through other means.

Most jihadist forums or social-media communications contain cautionary posts advising against trusting relationships. Moreover, they advise the consumers (of information) and participants in forums and online social media to take all necessary precautions through the use of good digital OPSEC. Over the longer term, doing so requires innovation and adaptation.

Studying jihadi OPSEC

To analyse that process, the author, with assistance from Muhammad al-'Ubaydi at the Combating Terrorism Center at West Point, examined a variety of open-source data comprising hundreds of forum conversations over 18 months from October 2014 to April 2016, in which jihadists and potential jihadists examined, discussed and asked for assistance in establishing robust digital OPSEC. We used forums such as 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, and Shumukh al-Islam and al-Fida, password-protected networks with restricted user access. These networks, it should be noted, suffer from their own cyber-security issues. Reports surfaced in autumn 2015 of vigilante hackers, including @th3j35t3r (the most prominent such individual), hacking multiple ISIS websites and blogs.[21]

We also made use of ForSight by Crimson Hexagon, a big-data analytics platform developed by Harvard University's Institute for Quantitative Social Science, to search public Facebook and Twitter posts, YouTube comments, Tumblr, Google Plus, and many blogs, news sites, reader comments and forums to search for references to various types of training related to digital OPSEC. This amounted to approximately seven years of historical data. In addition, we analysed the content of al-Qaeda's *Inspire* magazine, volumes 1–14, as well as ISIS's *Dabiq* and *Kybernetiq* for tips (both implicit

and explicit) on maintaining good digital OPSEC. The resultant data pool, while not comprehensive, is representative of the jihadist state of the art. Through consistent monitoring, we generated a sample of dozens of conversations from these forums on issues related to digital OPSEC, and hundreds of thousands of tweets, posts, blogs, articles, JustPaste.it and Dump.to documents,[22] videos and more.[23] I have made available online several hundred pages of original source materials (excluding those containing personally identifiable information of US and foreign nationals, or other sensitive information). These materials were generated by printing these websites to PDF files without alteration.

We found a capability and skill gap, and indications that these and other conversations are occurring with regularity in response to classified documents illegally obtained by Edward Snowden and disseminated by various outlets,[24] rumours, news stories and what tend to be misconceptions about how the internet functions, plus the outright co-option of materials designed for other audiences. Information leaks, vulnerability releases of known bugs or back doors within software and communications platforms, and acknowledgements and hearsay play a role in the changing digital OPSEC environment for terrorists and their supporters.[25]

So, too, do the approaches taken by those who run online platforms used by jihadists. On 9 April 2015, the *New York Times* reported that Twitter had suspended more than 10,000 ISIS-linked accounts in a single day.[26] Based on a cursory sample of both active and suspended accounts within our own and others' data, however, we are confident this is a drop in the ocean of ISIS and other terrorist-related Twitter accounts. Moreover, once a particular account is taken offline, its owner and followers can use multiple methods to quickly reconstruct the account. To do this, they use a combination of fake telephone numbers and email addresses, other online platforms such as Telegram and Signal, and iterative usernames and relevant hashtags to re-establish followers within a given network.[27] The ISIS developer community has also generated automated Twitter-regeneration programs with the ability to reconstruct suspended accounts with minimal effort. Jihadists are adept at disseminating information on how to spoof phone numbers and email addresses to reinstate or closely approximate

their original account and follower base, both manually and using home-grown developer solutions such as an Android application, 'Twitterbk', replete with ISIS branding.

There are strong indications that many of these individuals are using anonymous communications networks including Tor, I2P and other services to hide their point of origin.[28] By examining geographically identifiable tweets within our population, we found that, of those with identifiable locations, nearly 48% came from two cities that are not known to be radical jihadist hotbeds, Minsk (25.87%) and Belgrade (21.32%). What both these cities do have in common are Tor exit nodes. While largely anecdotal, observational data provide reasonable evidence to suggest that highly influential Twitter users engaged in propaganda are taking precautions with their digital security.

The users of these accounts are conscious of the fact that they are violating both the terms of service of Twitter and potentially the laws of multiple nations. This awareness is evident in forum posts. For example, in a Shumukh thread debating the virtues of Twitter direct messages versus Shumukh private messages, and the use of Tor, Ala al-Ahad (user number 12726) warns that sending private messages via Shumukh is safer. He notes that both Twitter and Shumukh are under surveillance, but concludes: 'Shumukh is more prepared for hacking, and knows how to deal with the "NSA". Shumukh knows who is watching it, fears being hacked, and tries its best to protect its servers.'[29]

Teaching and learning

Most of the tools and techniques needed to maintain digital security are not widely known to the average user. To become more secure requires a reasonable amount of training. Intelligence agencies now have established organisations whose sole job is to provide training and tools to hide intelligence officers and the spies they run,[30] a resource that jihadists cannot match. Instead, they turn to a collection of resources online which amount to the equivalent of a digital OPSEC help desk.

The @Software_ENG Telegram account, for example, operating under the name 'Tiqani al-Dawlah al-Islamiyyah' or 'Islamic State Tech', has

posted hundreds of pages of training materials to forums and websites. Some are co-opted directly from other organisations, and some are original. Each training document starts with an affirmation of God and the fight against non-believers, and many of the documents include watermarks of the Islamic State Tech logo. Many of the training documents are interrelated, and link to other manuals. The combined volume of documents across the forums is immense, covering hundreds of topics and case studies.

Not surprisingly, many of the questions on cyber security posed by jihadists are mundane; the answers could be easily found by examining the headlines of major news outlets or NGOs dedicated to providing information on privacy and security online. Despite multiple other avenues of information, questions pertaining to the security of popular platforms such as Skype, Google, Gmail, WhatsApp and others are being posted to jihadist forums. In response to a question by Allahumma 'Ighfirli on the Minbar forum on how to use Skype through Tor, for example, Mula'ib al-Assina responded: 'Skype is insecure, and Americans are recording every single call since 2008.' Abbas al-Qatari specifically indicates that Skype cannot be used through Tor, as the platform itself is inherently unencrypted. Such discussions shift individuals away from insecure means of communication to more secure alternatives, spreading the word about problems with well-known platforms and their monitoring by nation-states, and directing posters to Telegram channels that provide daily updates on OPSEC.

The questions and posts in both the forums and on Telegram are not exclusively high-level technical discussions. Often, conversations revolve around mundane application usage for maintaining contact with family members and loved ones. Yet technically simple questions constitute only the tip of a very large iceberg of questions associated with digital security, and indicate that even the most inexperienced users are beginning to recognise the fundamental constraints associated with using digital tools to communicate for jihad. Most questions indicate a mid-level understanding of digital OPSEC often only achieved through consistent study or training. The training documents, however, illustrate a broad understanding of the difference between technical understanding and implementation, and are often step-by-step guides with easy-to-follow directions.

Choosing tools

Jihadist OPSEC discussions cover a variety of tools designed in some way to reduce the digital breadcrumbs left by individuals online, such as Tor, Tails, DuckDuckGo, StartPage, PhotoMe Beta, ExifTool, MetaNull, Jitsi, JustPaste.it, Silent Circle, Telegram and others. These same tools are often accompanied by well-written Arabic, English and other multilingual training documents explaining their implementation and use, written by jihadists or co-opted from other organisations. There are numerous discussions on how to take advantage of more popular platforms such as Twitter and Facebook for propaganda and communication purposes, by bypassing security mechanisms such as the requirement for registered emails and phone numbers.

Proper implementation of secure tools, used in combination, enhances the probability of remaining anonymous online (though even minor lapses in OPSEC can provide valuable information to state intelligence agencies; as the American cryptographer Bruce Schneier has highlighted, the power of big data in the hands of a determined state can break apart attempts at digital security).[31] Nevertheless, these tools make the use of state-based intelligence and law-enforcement systems more difficult.

Table 1 provides a list of some of the tools identified or discussed in forums or online. The list is by no means exhaustive, but does provide the reader with a sense of the scale and scope of the conversation currently occurring on the topic of digital OPSEC. It presents a sample drawn from hundreds of forum conversations and linked training documents. The security of each tool is not independently verified by known technical experts before being recommended within the jihadist cyber community. On the whole, however, the movement is towards enhanced OPSEC with a recognition of the online threat environment. Some notable categories of tools are discussed below.

Browsing

Tools such as Tor and Tails facilitate anonymous browsing behaviour. In addition, Tails can alter the MAC address of a system.[32] Tor, originally a project of the United States Naval Research Laboratory, is a network of

Table 1: **Software Tools Discussed by Individuals with Identifiable Jihadist Sympathies**

Tool Name	Sentiment Towards Tool	Tool Name	Sentiment Towards Tool
Encryption		**General Web**	
Tor	Positive	JustPaste.it	Positive
Avast SecureLine	Positive	Facebook	Positive
F-Secure	Positive	Twitter	Positive
Onion Browser	Positive	Instagram	Positive
Hola VPN	Negative	Java	Negative
Hotspot Shield	Negative	Archive.org	Negative
TorGuard	Positive	Stashbox	Positive
UltraVPN	Negative	Rapidlash	Negative
Orweb	Positive	Adblock	Positive
AES Crypt	Positive	Disconnect	Positive
Tails	Positive	Self-Destructing	Positive
obfs2	NA	Yahoo	Negative
obfs3	NA	Bing	Negative
ScrambleSuit	NA	Google Search	Negative
CyberGhost	Positive	DuckDuckGo	Positive
TrueCrypt	Positive	Ixquick	Positive
CcLeaner	Positive	StartPage	Positive
VeraCrypt	Positive	Earth Moon Earth	NA
Windows BitLocker	Positive	Google Earth	Negative
Hardskat	Positive	Global Mapper	Positive
Cryptocat	Positive	VPNbrowser.org	Positive
Surespot	Positive	Google Photos	Negative
		Viber	Positive
		YouTube	Positive
		WOT	Positive
		UniversalMapDownloader	Positive

computers that routes traffic anonymously through a volunteer network consisting of thousands of encrypted relays. The network also contains hidden web servers and other services within a '.onion' domain – known as the dark web – that are only accessible within the anonymous and encrypted network. (The extent to which these hidden services are being used by jihadists, however, appears limited.[33])

Many media reports on documents leaked by Edward Snowden indicate that the NSA attempted unsuccessfully to penetrate the Tor network.[34] However, new evidence from the British Government Communications Headquarters (GCHQ) indicates that the security of Tor is being significantly challenged.[35] Jihadist trainings and online conversations are replete with references to Tor.[36] Discussions on Twitter and other services include comparisons of Tor's protection of online behaviour in comparison to virtual

Tool Name	Sentiment Towards Tool	Tool Name	Sentiment Towards Tool
General Software		Communication	
PhotoME Beta	Positive	Tutanota	Positive
ExifTool	Positive	iCloud	Negative
Metanull	Positive	RedPhone	Positive
Format Factory	Positive	Signal	Positive
Adobe Media Encoder	Positive	YOPmail.com	Positive
Adobe Premiere Pro	Positive	Gmail	Positive
Technitium	Positive	K7.net	Positive
MiniTool Drive Wipe	Positive	Skype	Negative
Photo GPS Editor	Positive	Linphone	Positive
Mappr	Positive	Jitsi	Positive
		Telegram	Positive
		Threema	Positive
		Truecaller	Negative
		WhozCalling	Negative
		NumberBook	Negative
		Paltalk	Positive
		Tor Mail	Negative
		Safe-mail.net	Positive
		TextNow	Positive
		Wickr	Positive
		Vimeo	Positive
		RCS spying app	Negative
		FireChat	Positive
		TinCan	Positive
		Hushmail	Positive
		ProtonMail	Positive

private networks (VPNs).[37] Jihadists are discussing the Snowden leaks in regard to the NSA's attempts to successfully penetrate Tor, and cite activists' continued use of Tor as an indication that the software is still secure.[38]

On Twitter, Tumblr, blogs, forums and comments over a period of roughly a year from September 2014, we were able to identify 1,601 posts directly referencing the use of the Tor network in Arabic, of which we estimate approximately 20% were focused on enhancing digital OPSEC with the intent to participate in jihadist activities, based on auto-categorisation using assisted machine learning; the rest were benign. OPSEC in and of itself, of course, does not imply criminality, though its use in criminal or terroristic enterprises violates the laws of most sovereign nations. We found substantial evidence of linkages to the Islamic State, some through shared documents offering the purchase or sale of illicit goods and services, others

derived from forum discussions on groups being tracked or prosecuted by intelligence and law-enforcement agencies. Local dialects and linguistic obfuscation complicate textual analysis in Arabic, however, making pure data-mining on this topic largely unreliable at present.

In contrast to public social media, a sampling of jihadist forums revealed dozens of references to Tor, frequently including training materials on the Tor browser bundle. The information was shared without any pretence of relating to privacy or civil liberties. Content in the private forums is typically more detailed and explicit in intent than similar materials posted in more public venues.

Searching

One of the more popular recommendations concerns a common internet activity: searching. As Abu Wiqar al-Gharib, user number 12848 on Shumukh, writes: 'never use the following browsers [*sic*]: Yahoo, Bing or Google, instead use DuckDuckGo, Ixquick or StartPage'.[39] These privacy-focused search engines enable anonymous or quasi-anonymous searches, baked into the service. DuckDuckGo states on its privacy-policy page that it 'does not collect or share personal information'.[40] Likewise, StartPage also proclaims: 'StartPage does not collect or share any personal information! Nada. Zilch. Nothing.'[41] In practice, this means that the search engines do not participate in the collection or storage of IP addresses or cookies.[42] This inability to collect data on users is important because it means they are unable to respond with IP information in the event of the issuance of national-security letter under the USA PATRIOT Act.[43]

Storage

Conveying information also requires the storage of documents online somewhere immune from US Immigration and Customs Enforcement (ICE), Europol and similar governmental agencies' efforts to remove websites with illegal content from the internet.[44] To do so, terrorists use services such as JustPaste.it, which enables the quick and largely anonymous sharing of information via HTML links and has become increasingly popular with organisations such as ISIS to disseminate propaganda materials.[45]

Placing documents with information on operations, propaganda, extremist fatwas and training in quasi-anonymous repositories increases their life expectancy.

Highlighting the pervasive use of these repositories is a document that was shared in one of many tweets discussing Tor, containing a link to JustPaste.it. The linked document contained the equivalent of 32 pages' worth of training information on 30 different open-source encryption platforms, obfuscation tools, dark-network access use cases, and hardware and software advice.[46] The Twitter account in question was suspended weeks prior to our selection, yet the link itself was still active and easily accessible. Further investigation determined the origin of the document to have been a Kuwaiti cyber-security firm that developed the document for work with Palestinian human-rights activists. While the document's original intent was largely benign, it was co-opted by ISIS supporters.

Talking

Silent Circle, the privacy-focused company most recently responsible for the Blackphone project, is widely cited as offering secure solutions for voice, browsing and messages. Silent Circle was identified as 'the best software to be used for mobile phone calls, as an alternative for Skype' by Rakan al-Iraqi, a strong Twitter supporter of the Islamic State.[47] The Blackphone and its upcoming replacement, Blackphone 2, are built to be extremely secure mobile environments and come highly recommended within the jihadist forum and Twitter communities.

Advanced discussions

The concern with digital OPSEC goes beyond the simple recommendation of tools. User Tiqani al-Islam on Shumukh, for example, comments on posts by providing detailed analysis of the terms and conditions associated with VPN providers' data-retention policies and legal requirements. This level of analysis adds to already robust discussions on which channels of communication are secure and which are not, adding to the aggregate security of the network and raising the relative costs to intelligence and law-enforcement agencies in disrupting them.

A detailed post by Rakan al-Iraqi to Shumukh in January 2015 explains the security of several mobile platforms as well as various communication applications.[48] He highlights Wickr, a multi-platform encrypted messaging application that claims to be unbreakable.[49] The program is designed for secure communications between human-rights activists, journalists, friends and individuals who require high levels of privacy. Rakan al-Iraqi testifies to the utility of the software and notes Wickr's own $100,000 reward for individuals able to crack its encryption protocols as a show of confidence. Al-Iraqi goes on to discuss Telegram, a Russian-made encrypted-communications application. He notes that Telegram has the downside of forcing registration, but provides instructions for how to spoof the registration with fake mobile numbers.

Al-Iraqi provides detailed discussion and subsequent instructions on how to root an Android device (allow base-level access to the device outside of the normal phone operating system) and subsequently install Tor, showing a level of concern for systemic protection of communications beyond the protection of specific communications channels. Such discussions frequently include links to detailed instruction manuals on JustPaste.it and similar services with pictures and text in Arabic detailing how to establish more secure communications. Although the technical sophistication of rooting a device is likely beyond the basic-user level, the simplicity of the instructions makes digital OPSEC accessible for most moderately skilled users.

To test the reliability of the advice available to jihadists, we purchased a Samsung Galaxy S4 and a Moto G to test out various instructions. We found that in under an hour we could route all the traffic on both mobile devices through the Tor network and could more securely access Telegram accounts. We followed simple directions to unlock Verizon and AT&T bootloaders (the base programs that run the operating system). From there we gained root access to the devices and could implement a diverse array of modifications.

The human-rights nexus

Among the OPSEC modifications being recommended by jihadists are applications and methods often used to safeguard human-rights activists and journalists around the world. Websites such as Security-in-a-Box provide

robust collection points for digital-security tools and training. Organisations such as Amnesty International, Pen International, the National Democratic Institute, Open Technology Fund, Tactical Tech, Front Line Defenders, Global Voices, Access, Internews, Riseup.net, Reporters without Borders and many more fund, or receive funding for, efforts to train, develop and implement digital security. Taken together, they have created or conducted hundreds of training manuals, resource websites, blogs, applications and in some cases even physical devices. The work these organisations conduct is done with the expressed intent of safeguarding individuals working under the threat of oppressive states.

Yet these tools, often funded with the help of the United States government, are also used for illicit purposes. Few of the organisations listed above are directly referenced by jihadists, but the applications, tactics, techniques and procedures they have developed or trained activists on are. (It is worth noting that, after exhaustive research, we were unable to find even the smallest of direct connections between any of these organisations and terrorist groups in jihadist posts or the organisations' public statements.)

Nevertheless, jihadists' awareness of the skill and scale of their adversaries means they will take advantage of all the tools on offer to them. And as the privacy community increasingly develops software- and hardware-based solutions to counter heavy-handed state actions against journalists and activists, the result, ironically, is proliferation of technologies to organisations that pose a clear and present danger to national governments. One of the more popular suites of applications discussed on the forums concerns those developed by the Guardian Project, designed to enhance privacy and secure communications on mobile devices. In response to a question about how to use applications on Android to communicate, for example, user 11120 on Fida provides detailed instructions on Orbot, one of 15 applications provided by the Guardian Project: 'Usually, our brothers need something simple and clear to understand, and there is a simple way that you can connect all the apps of your Android to the Tor without the need of the root; which is by using the VPN.' (He incorrectly calls Orbot a VPN; it is, instead, an encrypted proxy to Tor.) By running web traffic through Tor, users of Orbot are 'provided access to network services that may be

blocked, censored or monitored, while also protecting the identity of the user requesting those resources'.[50]

The Guardian Project is funded by the Open Technology Fund, the Knight Foundation, Free Press Unlimited, Tibet Action Institute and others. The developers and communities behind such products seek to facilitate privacy and human-rights protection, and they serve valuable, legitimate purposes in less-than-democratic states where civil liberties are under sustained threat. Many of these tools are also extremely important to individuals wishing to protect their personal information when travelling and accessing insecure public Wi-Fi networks or when crossing into countries with known economic, industrial and political espionage operations directed against foreign nationals. This does not alter the fact, however, that digital-security tools ostensibly developed for use by human-rights activists and journalists are also being used to support terrorist activities, including the training and indoctrination processes that help to separate and differentiate users within an organisational structure that is decentralised through digital means.

OPSEC in print

The majority of the examples provided above originated either online in forums or on social media. An analysis of innovation and adaptation would be incomplete without at least a partial examination of efforts to disseminate OPSEC advice in printed form (or at least in PDF). The most famous jihadi publication, al-Qaeda's *Inspire*, includes pages replete with stories of heroism, how-to guides for bomb-making and interviews with celebrity jihadists. Issues can also contain subtle reminders of digital security and the occasional piece of digital OPSEC advice. On page 41 of the June 2010 *Inspire*, for example, instructions are provided on how to use Asrar al Mujahideen, a bespoke cryptographic program, to send encrypted messages. The article ends with further advice on when to access the internet in messaging and recruitment processes, the need for proxies, anonymous emails and abstaining from using USB drives. In the subsequent issue of *Inspire*, the authors explained in detail how to encrypt, decrypt and shred files (permanently deleting them, thus rendering them safe even from forensic analysis). In addition to discussing the use of encrypted communications platforms, most

issues of *Inspire* also include a communication section with a public-key block to facilitate secure communications. The Middle East Media Research Institute notes that Ansar al-Mujahideen, an English-language forum, was also a prolific source of information on digital OPSEC.[51]

Once the cyber-security community had had a chance to analyse Asrar al Mujahideen, the tool faced challenges from intelligence and law enforcement, and was briefly discontinued before being redeveloped. No technological solution is permanent, yet the iterative processes of innovation and adaptation across organisations is growing in importance. Asrar al Mujahideen demonstrates home-grown development of a software package for the purpose of obfuscating and hiding from intelligence services. In the face of extremely well-resourced adversaries, this constitutes a win for a terrorist organisation. The life cycle of secure technology is short, yet the attempts to leverage these tools shows a desire and an attention to detail far in excess of the average internet user.

* * *

After 9/11, al-Qaeda appeared to have significantly scaled back its digital planning, but scaled up its broad-based communications. While the core leadership of the network became increasingly isolated, the periphery became empowered to spread the message of jihad in new ways. Whether this resulted in an increased operating capacity is up for debate in the case of al-Qaeda – but it has been found to be a significant advantage for ISIS.

This is not to say that ISIS is a fully decentralised, leaderless jihad, but rather that its online periphery – from which it facilitates recruitment, financial transfers, communications between the central administrative functions and decentralised cells, and the development of lone-wolf actors – is able to remain largely intact and robust. ISIS does have strong centralised features in zones where it maintains physical control.[52] Yet, beyond its zones of direct control, its online activities have resulted in a terrorist movement that facilitates complex, multi-nodal recruitment, organisation and planning.[53]

Increasing the security of recruits and recruiters helps keep open the supply lines of individuals joining the fight and the channels of information

coming from the zones of conflict. Yet jihadists' improvements in these areas are matched or exceeded by those of their adversaries. What would have worked in the pre-9/11 era would be considered poor digital hygiene today. Likewise, today's digital OPSEC tools, techniques and procedures will only be of benefit for a limited time. The treadmill of technology is incessant – and if a group stops running, it will fall off.

Acknowledgements

The author would like to give special thanks to Muhammad al-'Ubaydi for providing access to many of the primary-source documents examined in this work.

Notes

1 See Gabriel Weimann, 'Cyberterrorism: The Sum of All Fears?', *Studies in Conflict and Terrorism*, vol. 28, no. 2, February 2005, pp. 129–49; Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (New York: Columbia University Press, 2015); Lee Jarvis, Stuart Macdonald and Lella Nouri, 'The Cyberterrorism Threat: Findings from a Survey of Researchers', *Studies in Conflict and Terrorism*, vol. 37, no. 1, 2014, pp. 68–90; Gabriel Weimann, 'Cyberterrorism: How Real Is the Threat?', United States Institute of Peace Special Report, 17 December 2004, pp. 1–12; 'Virtual Threat, Real Terror: Cyberterrorism in the 21st Century', hearing before the Subcommittee on Terrorism, Technology and Homeland Security, United States Senate, 108th Congress, 2004, http://www.gpo.gov/fdsys/pkg/CHRG-108shrg94639/pdf/CHRG-108shrg94639.pdf; Gary R. Bunt, *iMuslims: Rewiring the House of Islam* (Chapel Hill, NC: University of North Carolina Press, 2009); Martin Bouchard, *Social Networks, Terrorism and Counter-Terrorism: Radical and Connected* (New York: Routledge, 2015); 'Al-Shabaab and Social Media: A Double Edged Sword', *Brown Journal of World Affairs*, vol. 20, no. 2, Spring/Summer 2015, pp. 309–27; and Jytte Klausen, 'Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq', *Studies in Conflict & Terrorism*, vol. 38, no. 1, November 2014, pp. 1–22.

2 The varying goals, objectives, and spatial and structural differences between terrorist organisations greatly influence their activities in this area. This article confines itself to the study of Islamic terrorism, with particular emphasis on ISIS and al-Qaeda.

3 See Fergus Hanson, 'Baked in and Wired: Ediplomacy@State', Brookings Institution, 24 October 2012, https://www.brookings.edu/wp-content/uploads/2016/06/baked-in-hansonf-5.pdf; and David Kaye, 'Report of the Special Rapporteur on the

Promotion and Protection of the Right to Freedom of Opinion and Expression', United Nations Human Rights Council, 22 May 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

4 Joseph Cox, 'Lawyer: Dark Web Child Porn Site Ran Better When It Was Taken Over by the FBI', Motherboard, 23 August 2016, http://motherboard.vice.com/read/lawyer-dark-web-child-porn-site-ran-better-when-it-was-taken-over-by-the-fbi.

5 Joshua Sinai, 'Innovation in Terrorists' Counter-Surveillance: The Case of al-Qaeda and Its Affiliates', in Magnus Ranstorp and Magnus Normark, *Understanding Terrorism Innovation and Learning* (New York: Routledge, 2015), pp. 196–210.

6 Aaron Brantly, 'Defining the Role of Intelligence in Cyber: A Hybrid Push and Pull', in Mark Phythian, *Understanding the Intelligence Cycle* (Abingdon: Routledge, 2013), pp. 76–98.

7 Aaron Franklin Brantly, 'The Cyber Losers', *Democracy and Security*, vol. 10, no. 2, 2014, pp. 132–55.

8 Scott Gates and Sukanya Podder, 'Social Media, Recruitment, Allegiance and the Islamic State', *Perspectives on Terrorism*, vol. 9, no. 4, 28 August 2015, pp. 107–16.

9 Daniel Milton, 'Communication Breakdown: Unraveling the Islamic State's Media Efforts', Combating Terrorism Center at West Point, October 2016, https://www.ctc.usma.edu/v2/wp-content/uploads/2016/10/ISIL-Media.pdf.

10 Michael Chandler and Rohan Gunaratna, *Countering Terrorism: Can We Meet the Threat of Global Violence?* (London: Reaktion, 2007), pp. 178–93.

11 James P.G. Sterbenz et al., 'Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation', *Telecommunication Systems*, December 2011, pp. 1–33.

12 Ali Fisher, 'How Jihadist Networks Maintain a Persistent Online Presence', *Perspectives on Terrorism*, vol. 9, no. 3, 2015, pp. 3–20.

13 Data derived through big-data collection using the ForSight Platform by Crimson Hexagon and analysis of the number of tweets, followers of @ThinkAgain_DOS and 'Falluja the pride of Tikrit' and 'The Islamic State of Iraq' (author's translation of Arabic usernames) ISIS media accounts.

14 See Rita Katz, 'The State Department's Twitter War with ISIS Is Embarrassing', *Time*, 16 September 2014, http://time.com/3387065/isis-twitter-war-state-department/; and Greg Miller and Scott Higham, 'In a Propaganda War Against ISIS, the U.S. Tried to Play by the Enemy's Rules', *Washington Post*, 8 May 2015, https://www.washingtonpost.com/world/national-security/in-a-propaganda-war-us-tried-to-play-by-the-enemys-rules/2015/05/08/6eb6b732-e52f-11e4-81ea-0649268f729e_story.html.

15 Jessica Stern and John Berger, *ISIS: The State of Terror* (New York: Harper Collins, 2015), p. 154.

16 Weimann, *Terrorism in Cyberspace: the Next Generation*, pp. 125–46.

17 See 'U.K. Struggles to Stop Islamic Radicalization Spike', PBS *NewsHour*,

27 January 2015, http://www.pbs.org/newshour/bb/u-k-government-community-groups-struggle-stop-islamic-radicalization-spike/; 'A Community Based Approach to Countering Radicalization', World Organization for Resource Development and Education, 10 December 2010, pp. 1–34; and Organization for Security and Co-operation in Europe, 'Preventing Terrorism and Countering Violent Extremism and Radicalization That Lead to Terrorism: a Community-Policing Approach', 13 March 2014, pp. 1–200.

18 Suzanne Kelly, 'A Classic Case of Self-Radicalizing', CNN, 28 February 2012, http://security.blogs.cnn.com/2012/02/28/a-classic-case-of-self-radicalizing/.

19 Christopher Anzalone, 'Zachary Chesser: An American, Grassroots Jihadist Strategist on Raising the Next Generation of Al-Qaeda Supporters', *Perspectives on Terrorism*, vol. 4, no. 5, 2010.

20 The author has observed this non-trust environment on a regular basis within various jihadist forums and chatrooms.

21 Paul Szoldra, 'This Hacker Has Fought Terrorists Online Since 2010, and He's Not Impressed by Anonymous', *Business Insider*, 9 November 2015, http://www.businessinsider.com/anon-war-isis-jester-hacking-2015-11.

22 JustPaste.it and Dump.to are anonymous document-sharing sites that allow users to post and link to content, and edit and share that content with limited or no attribution.

23 See http://www.afterwestphalia.org/p/opsec-data.html.

24 Ghrib al-Ghuraba, user number 16219, post to Shumukh on 14 December 2014, https://shamikh1.info/vb/showthread.php?t=239928 [link no longer active]. The user posted a link to a document written by Islamic State Tech; the post and document made reference to Edward Snowden and included classified documents.

25 To gather this data no Institutional Review Board was necessary because, in keeping with US federal guideline §46.102 on the protection of human subjects – '(f) Human subject means a living individual about whom an investigator (whether professional or student) conducting research obtains (1) Data through intervention or interaction with the individual, or (2) Identifiable private information' – no interventions, interactions or private data not publicly available were used in this analysis. All data was collected passively in open-source formats and no direct questions, surveys or interactions with content generators occurred. Although individuals are identified within the data by username or pseudonym, such information was derived through open-source data collection.

26 Rick Gladstone, 'Twitter Says It Suspended 10,000 ISIS-Linked Accounts in One Day', *New York Times*, 9 April 2015, https://www.nytimes.com/2015/04/10/world/middleeast/twitter-says-it-suspended-10000-isis-linked-accounts-in-one-day.html?_r=0.

27 On 23 September 2015, 'Tiqani Dawat Al-Islam', username @Security-Exp82, tweeted a Dump.to link explaining how 'to get fake phone numbers that

can help the "brothers" to register in Telegram' (author's translation). But he noted that these phone numbers 'cannot be used to create accounts on Facebook, Twitter or WhatsApp'.

28 The following known ISIS Twitter accounts were used as a test of our big-data analytics platform: 'Falluja the pride of Tikrit' and 'The Islamic State of Iraq' (author's translation of Arabic usernames). Together they resulted in 36,217 tweets, retweets or quoted tweets between September 2014 and September 2015, of which almost 5,000 provided identifiable geo-location.

29 Thread by 'Ridak Rabi', user number 17530, Shumukh, 3 August 2013. See posts by Ridak Rabi, Abu Sumaya and Ala al-'Ahad.

30 David S. Cohen, remarks on 'CIA of the Future', CIA, 17 September 2015.

31 Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: W.W. Norton & Company, 2015).

32 A media-access control address (MAC address) is a unique identifier assigned to devices on a physical network, somewhat analogous to the way that a social security number is assigned to an individual. This is different from an Internet Protocol (IP) address, which is a numerical label assigned to each device within a computer network that uses the Internet Protocol for communication and can change based on network and network location.

33 See Daniel Moore and Thomas Rid, 'Cryptopolitik and the Darknet', *Survival*, vol. 58, no. 1, February–March 2016, pp. 7–38.

34 Barton Gellman, Craig Timberg and Steven Rich, 'Secret NSA Documents Show Campaign Against Tor Encrypted Network', *Washington Post*, 4 October 2013, https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html.

35 See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

36 See, for example, screenshots of three different posts on Tor, two from Shumukh and one from al-Fida. On Tor usage on Windows computers, see https://drive.google.com/open?id=0Bx_uTR8BHvoS-enU3bzhYdodxUVU (Shumukh). On using two copies of Tor simultaneously, see https://drive.google.com/open?id=0Bx_uTR8BHvoSSDQ1cFl-CVWRpWVU (Shumukh) and https://drive.google.com/open?id=0Bx_uTR8BHvoSQS1vRzNmNy1EclU (al-Fida). The images are cropped to hide login timestamps and user-account information.

37 See JustPaste.it link posted by Abu Khadija al-Muhajir, user number 18276, https://justpaste.it/h94v. For a PDF of this document in case the link is taken down, see https://drive.google.com/file/d/0Bx_uTR8B-HvoSUGhzM3VPS2pqUHM/view?usp=sharing.

38 On 19 January 2015, user @JladOmarov retweeted @Rohban_Al_Layl: 'no truth to the news of the Tor code decoding despite attempts

by many NSA leaks by Snowden activists and experts in information and encryption security and privacy'. JladOmarov also posts links on digital security and refers to himself as 'Umarov Executioner'. For further resources on @JladOmarov and his technical role, see https://drive.google.com/file/d/0Bx_uTR8BHv0SdUZwS1ZLMHlfZko/view?usp=sharing.

39 Abu Wiqar al-Gharib, user number 12848, post to Shumukh, February 2015.

40 See https://duckduckgo.com/privacy.

41 See https://startpage.com.

42 A cookie is a small piece of information sent by a web server to store on a web browser so it can later be read back from that browser.

43 A national-security letter (NSL) allows the FBI to demand information from service providers without prior authorisation by a judge.

44 Ben Sisario, 'U.S. Shuts Down Web Sites in Piracy Crackdown', *New York Times*, 26 November 2010, http://www.nytimes.com/2010/11/27/technology/27torrent.html.

45 Carmen Fishwick, 'How a Polish Student's Website Became an ISIS Propaganda Tool', *Guardian*, 15 August 2014, http://www.theguardian.com/world/2014/aug/15/-sp-polish-man-website-isis-propaganda-tool.

46 For an account of our discovery of this document, and a link to it, see Kim Zetter, 'Security Manual Reveals the OPSEC Advice ISIS Gives Recruits', *Wired*, 19 Novemebr 2015, https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.

47 Rakan al-Iraqi, post to Shumukh, 29 January 2015.

48 *Ibid*. Author's translation: 'Wickr software: Highly encrypted software that is preferred to be used in communications for the people who participate in demonstrations. The service provider cannot spy on your messages. To register in Wickr, you don't need to give your phone number or email address; therefore, your identity will be hidden. Wickr allows you to open groups, and shows you the date in which your message was deleted by the receiver. The creator of the software offered $100,000 for anyone who can find a gap that can lead to the breaking of the messages' protection. The software is closed, i.e., technicians cannot examine its codes. This software is a secure alternative for WhatsApp, and I recommend it to be used for secure communications … To install to your iPhone … https://itunes.apple.com/us/app/wickr-self-destructing-secure/id528962154?mt=8 … Android: … https://play.google.com/store/apps/details?id=com.mywickr.wickr'.

49 Wickr functions as a peer-to-peer encryption protocol eliminating the storage of encryption keys by a middleman.

50 'Secure Mobile Apps', Guardian Project, https://guardianproject.info/apps/.

51 'Asar Al-Mujahideen English Forum (AMEF) – the Main English Language Forum for Al-Qaeda and Its Western Followers: Information and Communication Technology Thread Offers a Virtual Training Center for Online Jihad and Cyber Warfare Including Weapons Training, Hacking & Encryption, and Lessons in

Becoming a Suicide Bomber', Middle East Media Research Institute, 20 April 2012, http://cjlab.memri.org/uncategorized/ansar-al-mujahideen-english-forum-amef-the-main-english-language-forum-for-al-qaeda-and-its-western-followers-information-and-communication-technology-thread-offers-a-virtual-training-center-for/.

52 For insights into the bureaucratic aspects of a terrorist organisation trying to establish regional control, see Brian Dodwell, Daniel Milton and Don Rassler, 'The Caliphate's Global Workforce: An Inside Look at the Islamic State's Foreign Fighter Paper Trail', Combating Terrorism Center at West Point, April 2016, https://www.ctc.usma.edu/v2/wp-content/uploads/2016/04/CTC_Caliphates-Global-Workforce-Report.pdf.

53 Marc Sageman, *Leaderless Jihad* (Philadelphia, PA: University of Pennsylvania Press, 2011), pp. 110–15.