FLASHPOINT

Tech for Jihad:

Dissecting Jihadists' Digital Toolbox

By Laith Alkhouri & Alex Kassirer

July 2016

Introduction

Over the past two years, the media has tended to sensationalize jihadists' rapid adoption and strategic use of social media. Despite perpetual news coverage on the issue, the general public remains relatively uninformed about the complex ways in which many jihadists maintain robust yet secretive online presences. To accomplish their goals — ranging from propaganda dissemination and recruitment to launching attacks — jihadists must skillfully leverage various digital technologies that are widely advertised and freely accessible online.

Just as smart phones and portable devices have transformed the way much of the world communicates and interacts, jihadists, too, have rapidly adopted and availed themselves of these technologies. Their savvy grasp of technology presents one of the most frequently asked questions about jihadists today: what is in their digital toolbox and how do they exploit these technologies to benefit their activities?

This report explores these questions by elucidating 36 of the most noteworthy tools and technologies behind the online presence of jihadist groups such as ISIS. Flashpoint analysts have examined primary sources from the Deep and Dark Web to identify and analyze the key digital technologies facilitating the proliferation of these actors' radical agendas.

Why is digital technology critical for jihadists?

Today's jihadists rely heavily on the Internet, and their defense systems are increasingly shifting toward digital mediums. Consequently, this expanding online presence ignites an entirely new host of security concerns. As a result, many jihadists now depend on specialized security technologies. These technologies are imperative to jihadist operations — whether for escaping surveillance, maintaining presences in underground channels, or obscuring tracks to war zones. Jihadist groups undeniably owe countless aspects of their perpetuated existence to the Internet.

Indeed, social media is integral to this robust online presence; it has truly transformed the global jihadist movement. Platforms such as Twitter and Facebook inflate jihadist notoriety, driving unlimited traffic, new recruits, and a global audience. Inevitably, this social media presence has generated pushback from certain platforms. Twitter in particular has been highly aggressive against pro-ISIS accounts. In response, today's tech-savvy jihadists have demonstrated their keen adaptability; they now frequently leverage digital technologies to circumvent these barriers.

It is no secret that confidentiality and privacy are paramount to jihadists' survival. However, most communication platforms lack the sophistication necessary to ensure sufficient security. As a result, today's jihadists constantly seek alternative ways to advance their agendas and communicate securely. The 36 digital tools discussed within this report represent only a small sampling of the technologies required to overcome security challenges that would otherwise render jihadists' daily tasks and crucial operations impossible.

I. Secure Browsers

Jihadists worldwide rely heavily on various web browsers to maintain operations. Firefox, Google Chrome, and Safari are among the most popular but provide little anonymity. As such, these browsers pose serious security threats, often placing jihadist users within the crosshairs of intelligence agencies. Consequently, tech-savvy jihadists have been forced to seek alternative, secure browsers to avoid scrutiny.

In particular, **Tor Browser** is a favorite among jihadists. Long before ISIS emerged as a global threat, jihadists were circulating detailed instructions on installing and utilizing Tor, which anonymizes Internet browsing activity. In fact, data from Flashpoint's Deep and Dark Web forum archives indicate that jihadists have been evaluating secure browsers, particularly for use disseminating propaganda and communicating via email, since May 2007.

During the summer of 2008, Tor's popularity grew sharply within jihadist Deep and Dark Web forums. This time frame also marks the inception of the first proprietary jihadist encryption tool, Asrar Al-Mujahideen. Shortly thereafter, a top jihadist web forum was abuzz with deeper discussions of encryption, privacy, and naturally — Tor. In particular, one forum member distributed guidelines describing Tor's implications and best practices for jihadists. These guidelines recommended that, in addition to using Tor for encrypted browsing, jihadists should download Tor onto a portable USB drive for easy use at Internet cafes. Jihadists frequently visit these cafes because they provide an additional layer of privacy in areas laden with Internet censorship.

Another jihadist-approved alternative browser is called **Opera Browser**, which contains a free VPN service and ad-blocker. Opera Browser is also compatible with Android, which seems to be jihadists' preferred mobile operating system. These useful features make Opera extremely popular today. In an April 2016 posting on ISIS's top web forum, one member raved about Opera and released detailed instructions for fellow jihadists on using the browser to obfuscate their digital fingerprints.

II. Virtual Private Networks (VPNs) and Proxy Services

Jihadists have been leveraging VPNs and proxy services to further enhance online browsing security since long before ISIS developed a public Internet presence. These technologies first appeared within jihadist circles back in 2012, when members of an official Al-Qaida Deep and Dark Web forum discussed the use of CyberGhostVPN. They explained it as, "a new technology that uses (SSL/TLS) protocol through the local server you use, which makes your communication through the network create an encrypted and secure tunnel." One contributor even posted links to download the software, noting the differences between paid and free subscriptions. Such nuanced insight during the early adoption phase of these services further underscores their widespread appeal among jihadists.

> ***"As time progressed, jihadist forum dialogue continued to evolve from basic recommendations to the circulation of meticulous manuals and critical reviews."***

As VPNs and proxy services become more commonplace, jihadists' grasp of these tools has grown increasingly sophisticated. Indeed, in September 2014, a Deep and Dark Web forum member released a detailed manual encouraging jihadists to adopt the aforementioned CyberGhostVPN for masking IP addresses to ensure secure online browsing. In addition to discussing the basic functions of this service, the individual also alerted fellow members of weaknesses. Specifically, he warned that VPNs could not change the computer's hard disk serial number, which could be a digital identifier. To mitigate the risk presented by this shortfall, he recommended using the software HardDiskSerialNumberChanger, which is freeware that allows users to change the identifying serial number of their machine's hard disks easily and securely. This forum member's incisive knowledge clearly shows a deeper understanding of these technologies.

As time progressed, jihadist forum dialogue continued to evolve from basic recommendations to the circulation of meticulous manuals and critical reviews. For instance, in July 2015, a pro-ISIS actor released guidelines recommending a premium VPN service called F-Secure Freedome. Then in 2016, a notorious pro-ISIS hacking collective called United Cyber Caliphate (UCC) issued an advisory warning about the use of certain VPN services. The group indicated, "Not all VPNs r as secure or private as [the] company claims, but good way to tell: Does VPN keep logs of user data? If yes, what info is stored n how long? Beware of services that keep user logs n stores data." The warning then added that the best VPN services are company-based products and not merely "add-on" services. While "some safer VPNs require monthly subscription," UCC said, "not all" do.

For years, the jihadist community has discussed masking personal IP addresses and online activities with the aim of evading the surveillance. However, these actors have demonstrated more than just an interest in the subject; their sophisticated grasp of these complex technologies has shown their capacity for learning, adapting, and pivoting in the face of increased scrutiny.

III. Protected E-Mail Services

Jihadists are constantly on alert for ways to obfuscate their online activities. For intelligence agencies and eavesdroppers, e-mail surveillance is a primary way to monitor an actor. As such, today's jihadists take precautions to mitigate this risk. Over the past two years, jihadist chatter within Deep and Dark Web forums indicates that pro-ISIS and Al-Qaida actors employ numerous encrypted and temporary e-mail services to communicate confidentially and advance their digital agendas.

Jihadists highly recommend the following protected e-mail services:

Hush-Mail
This particular service provides enhanced security within e-mail communications via encryption between Hushmail account holders and others based on standard OpenPGP. The service also provides a two-step verification functionality and unlimited e-mail aliases.

In fact, Flashpoint analysts have identified various jihadist media logistical units using Hushmail. Specifically, Ibn Taimia Media Center, which officially represents pro Al-Qaida terror groups in Gaza, first began using Hushmail around February 2013. In other instances, the Dagestani Mujahideen, operating under Al-Qaida's North Caucasus branch, leverage Hushmail in tandem with PayPal for fundraising purposes.

ProtonMail
This is another noteworthy encrypted e-mail service popular among today's jihadists. Developed by CERN and MIT and based in Switzerland, ProtonMail offers end-to-end encryption, an anonymous e-mail account, and the security inherent to stringent Swiss privacy laws.

Tutanota
This is an open source, encrypted inbox service that, in addition to encrypting e-emails, encrypts e-mail subject lines and attachments. Compatible with all Android and iOS devices, Tutanota was developed in Germany.

GhostMail
This Swiss encrypted e-mail service has also been advised by tech-savvy jihadists as trusted for both Android and iPhone operating systems.

YOPmail
After the January 2015 terror attacks in Paris, Al-Qaida's branch in Yemen (AQAP), released an audio message about the attacks. This message was uploaded to the Internet Archives (archive[.]org), using an account from YOPmail – a disposable, temporary e-mail service that does not require registration or passwords. According to its website, YOPmail "guards you against spam, phishing and other online abuses". Even better, this temporary inbox lasts for only eight days. This feature further decreases the risk of having clandestine jihadist communications unveiled, even upon third-party investigation of associated email addresses. YOPmail is reportedly the same e-mail service used by the infamous Sony hackers in 2014.

IV. Mobile Security Applications

The digital communication landscape's rapid expansion to smart mobile devices has further catalyzed jihadists' online activities. Smart phones expedite many key components of jihadist communications. Specifically, they allow jihadists to upload, send, download, and view content with great ease and speed. In other words, this technology enables today's jihadists to spread propaganda and advance their agendas faster and farther-reaching than ever before.

While mobile technology's swift adoption has proven immensely beneficial for jihadists, these gains are not without downside. By default, most mobile devices are simply not secure enough for jihadists. Without proper precautions, it is relatively easy for third parties to obtain jihadists' sensitive identifying characteristics, such as the user's GPS location or IP address. Jihadists recognize that the risk of utilizing mobile devices is quite large.

Jihadist technology groups have long encouraged the use of various mobile phone applications to reduce the aforementioned security risks. One jihadist group, known as Horizons, runs two channels on Telegram, an encrypted communication platform. These channels exist primarily to educate supporters on how to leverage technology to further the jihadist agenda. Horizons released one particularly incisive multi-episode series highlighting information security in the realm of smart mobile devices. This series focused heavily on mobile security applications, otherwise known as "security apps".

Fundamentally, these security apps are designed to secure users' locations and data, clean their machines, and delete their browsing history. According to manuals from the Horizons series, the following security apps and services are highly recommended and growing increasingly popular with jihadists:

Locker
Automatically deletes user files once the number of incorrect lock-screen pass-code attempts crosses a certain threshold. It requires users to specify the number of incorrect unlock attempts allowed. If that number is exceeded, the app will completely wipe the user's phone, thereby protecting personal information.

FAKE GPS
Provides a false physical location when used in tandem with certain social media platforms. Facebook and Twitter in particular typically reveal or gather their users' location via GPS. FAKE GPS circumvents this feature, enabling users to choose and reveal their own false location.

D-Vasive Pro
Disables other apps from using the smart phone's camera, microphone, Bluetooth and WiFi to further enhance user privacy.

AMC Security
Consists of comprehensive antivirus and security tools.

ESET Mobile Security
Reportedly rated the best anti-virus app for Android devices, according to *Horizons*.

Battery Saver
Preserves a device's power supply.

Call/SMS Blocker
Rejects specified calls and text messages.

Privasy Locker
Hides sensitive images and files.

APP Manager
Deletes and relocates specified apps.

iSHREDDER PRO
Allows users to permanently delete sensitive files.

Override DNS
Obfuscates Android users' IP addresses by changing the DNS (domain name services). Users must first obtain **OpenNIC** — an app necessary for the use of Override DNS. Horizons recommends that users first shut down any Tor or VPN service before testing their IP location using the **IPleak[.]net** website to confirm their changed IP address.

DNSCrypt
Helps users improve DNS security. This app is an open protocol that encrypts DNS data between user and server. However, *Horizons* emphasizes that DNSCrypt is not a substitution for VPN or Tor services. Users are urged to employ DNSCrypt alongside these proxy services to enhance security.

Net Guard
An open source firewall that does not require root setup. This app allows users to specify which apps are connected to the Internet.

AFWall
An open source mobile firewall security app. When used with Linux's **IPtables** it empowers users with full control over which apps connect to the Internet.

F-Secure Freedome
An encrypted VPN service.

Hide.me
A Malaysian VPN service that preserves user privacy by not storing user data on company servers.

Tutanota
An encrypted e-mail service that comes especially recommended for use when registering VPN accounts.

V. Encrypted Messengers

For years, the jihadist community has employed a wide range of encrypted messaging applications to further conceal their communications. These applications are both accessible via computer and mobile devices. Among the tech-savvy jihadist community, however, not all encrypted platforms are created equal. The most popular messengers offer end-to-end encryption. This means that messages are encrypted and decrypted within the devices sending and receiving the messages themselves. Messages are thus unreadable in transit for maximum security.

Jihadists have evaluated the following encrypted messengers for use in their daily operations:

Threema

This Swiss application is an end-to-end encryption messenger. In April 2016, a pro-ISIS technology manual championed Threema, explaining how it "does not collect your personal info like phone numbers or email addresses, as it does not request you to enter identifiable information." Further, Threema will not "decrypt encrypted messages if the company faces government pressures." The manual added that Threema "virtually encrypt[s] pictures and files, audios and apps, and is strong against MITM [man-in-the-middle] attacks, and does not store any messages on the company's servers."

WhatsApp

End-to-end encryption does not, however, guarantee approval within the jihadist community. Following its April 2016 implementation of end-to-end encryption, ISIS supporters are still wary of using Facebook's WhatsApp. A major thought leader in the pro-ISIS technology community warned followers that, despite the new upgrade, "we cannot trust WhatsApp since WhatsApp is the easiest application for hacking and also one of the social messaging apps purchased by the Israeli Facebook program!"

Telegram

Despite the assortment of secure messaging platforms, Telegram, created by Russian VKontakte founder Pavel Durov, appears to be the top choice among both individual jihadists and official jihadist groups. These groups use Telegram for running media channels through which they disseminate official statements, claims of credit, videos, and propaganda.

Nevertheless, today's jihadists have emphatically urged their peers to rely solely on Telegram's "Secret Chat" service. Essentially, while all Telegram messages are encrypted, standard messages use client-to-server encryption. These standard messages are stored in the cloud and accessible across devices. Secret chats, on the other hand, use client-to-client encryption, which makes them readable only via the sending and receiving devices. Finally, when users delete a Secret Chat message from one device, it is automatically deleted from the other.

Asrar al-Dardashah

Regardless of a platform's sophistication, the skeptical jihadist trusts no service entirely because most are developed in

the West. However, jihadist-built services assuage these concerns. In February 2013, a jihadist media logistics unit called the Global Islamic Media Front (GIMF) introduced Asrar al-Dardashah (Secrets of Chatting), an encryption plugin compatible with various instant messaging platforms.

This plugin allows users to encrypt live conversations over instant-messaging platforms such as: Paltalk, Google Chat, Yahoo, MSN, and Pidgin. According to a tutorial from GIMF, "the plugin offers the highest level of encryption for secure communication through instant messaging. The plugin is small, installs in seconds, and it is trusted for use and secure communications…It supports most of the languages in the world through the use of Unicode."

> ***"Despite the assortment of secure messaging platforms, Telegram, created by Russian VKontakte founder Pavel Durov, appears to be the top choice among both individual jihadists and official jihadist groups."***

VI. Mobile Propaganda Applications

In part, jihadists obscure their online identities to access propaganda and media materials disseminated by their allegiant groups securely. ISIS in particular has numerous media units existing primarily to communicate these materials to members and supporters online. Jihadists require constant, uninhibited access to these critical materials, but often, such access is only available with a reliable Internet connection. While the aforementioned tools allow users to safeguard their activities and avoid detection, these tools do not ensure Internet connectivity. Since uninterrupted online browsing capabilities are crucial, many Jihadists take advantage of specialized smartphone applications to ensure consistent access to their desired propaganda media channels.

Over the past year, ISIS and other jihadist groups have developed their own proprietary mobile propaganda applications. The following apps offer jihadists constant access to their allegiant groups and propaganda media channels:

The A'maq Agency

A prolific ISIS-affiliated media unit, released one of the first jihadist-built Android mobile apps. Since its original release, A'maq has rolled out multiple updated versions, in both English and Arabic, delivering relevant news updates and war zone videos to ISIS supporters on-the-go.

Al-Bayan Radio

ISIS's official radio station, also released its own Android app. With this app, supporters can access broadcasts such as Qur'anic recitations, radical lectures, and public announcements relating to ISIS operations. Al-Bayan was originally broadcast solely in Mosul, Iraq, but by December 2015, Al-Bayan had aired broadcasts in 12 ISIS territories across Iraq, Syria, and Libya. Today, Al-Bayan Radio streams over three web domains and an Android app with news clips translated into several languages and uploaded daily. This effort has profoundly increased the size and scope of ISIS propaganda's target audience.

Recently, jihadists warned of fake A'maq and Al-Bayan Android apps circulating online. Alleged enemies released fake yet seemingly identical app versions corrupted with surveillance malware. To avoid confusion, Horizons released a manual explaining ways to differentiate between real and fake versions of these apps. It advised jihadists to compare the original MD5 hash, as advertised by A'maq and Al-Bayan on their official Telegram channels, to the downloaded file.

Voice of Jihad

On April 1, 2016, the Afghan Taliban launched the Voice of Jihad app, which was originally available in the Google Play store. Approximately 48 hours later and following substantial media scrutiny, Google removed the app. However, it resurfaced on Amazon's app store several days later. On April 7, the Afghan Taliban advertised the app as a way for users to "keep up to date with latest news, reports, statements, articles and videos."

Alphabet

ISIS's central media released what is perhaps the most unexpected propaganda app. The Alphabet app is primarily for children —to whom the product announcement refers to as "cubs." The app teaches children how to read and write Arabic letters through jihadist-oriented vocabulary. Alphabet's exercises reference rockets, cannons, tanks, and other militaristic terms as a means of teaching children the alphabet. Naturally, this further catalyzes ISIS's aggressive indoctrination strategy.

Key Findings

1. Jihadists enact stringent online security measures starting with the World Wide Web's most fundamental portal: browsers. While most of us access the web via popular browsers like Google Chrome, Firefox, and Safari, tech-savvy jihadists are increasingly turning to highly-secure, alternative browsers such as Tor Browser and Opera Browser, so they can operate online more clandestinely without easily divulging their IP address and risking third-party surveillance.

2. Virtual private networks (VPNs) and proxy services, often used in conjunction with secure browsers, help many jihadists further obfuscate their online identities. Members of a prominent Al-Qaida Deep and Dark Web forum first helped popularize these tools back in 2012. VPNs and proxy services, such as CyberGhostVPN and F-Secure Freedome, have since become commonplace among today's jihadists.

3. For intelligence agencies and eavesdroppers alike, e-mail surveillance is a primary way to monitor an actor. For jihadists, this necessitates certain precautionary measures when using e-mail. These precautions have taken the form of protected e-mail services equipped with popular features like end-to-end encryption and temporary, anonymous account capabilities. Among the most popular protected e-mail services today's jihadists utilize are Hushmail, Tutanota, and YOPmail.

4. The rapid, virtually universal adoption of smart mobile devices has accelerated the ease and speed at which jihadists communicate with one another. While the smart phone has been hugely influential for the global jihadist movement, this relatively new technology arrives with a host of new security concerns. In order to mitigate the risks inherent to smart phones, jihadists increasingly appear to be leveraging specialized mobile applications to bolster security.

5. Over the past few years, encrypted messaging platforms have become immensely popular among jihadists. These platforms provide an additional layer of security to conceal communications. The most favorable messengers offer end-to-end encryption, which means that messages are encrypted and decrypted within the sending and receiving devices so they are thus unreadable in transit. Despite the vast assortment of secure messaging platforms, a cloud-based app called Telegram appears to be the top choice among jihadists.

6. Propaganda plays an integral role within the daily operations of jihadist groups. In particular, ISIS and its supporters rely heavily on their affiliated media units to spread sensitive, vital materials ranging from breaking news and organizational updates to recruitment efforts and tactical instructions. Due to the critical nature of this information, jihadists must have constant, reliable access to the media. As such, various jihadist media units have released popular mobile applications allowing jihadists to disseminate and view propaganda with greater ease, speed, and accessibility.

Final Notes

Although technology is not typically associated with jihadists, it is their lifeblood. Jihadists' reliance on technology for survival pushes the jihadist community to constantly learn, adapt, and advance through various technological tools.

In order to both gain popularity among potential supporters and instill fear in their adversaries, jihadists need technology to provide consistent channels through which they can release propaganda. However, this propaganda distribution is a double-edged sword; it serves their goals, but also renders jihadists more susceptible to those who wish to disrupt, dismantle, and target them. Of course, jihadists can rely on that same technology to provide the stringent security measures necessary to conceal jihadists' identities and preserve their voice.

Today's jihadists' unrelenting drive to adapt and conceal their online operations presents unique challenges to monitoring them. While jihadists incessantly adapt their behaviors to evade surveillance, we must adapt our surveillance tactics to keep up. The more we understand about how jihadists leverage digital technologies to engage in nefarious activities, the better equipped we will be to defend ourselves and mitigate risk as effectively as possible.

About Flashpoint

Flashpoint delivers Business Risk Intelligence (BRI) to empower business units and functions across organizations to make better decisions and mitigate risk. The company's unique Deep & Dark Web data, expertise, and technology enable our customers to glean intelligence that informs risk and protects their ability to operate. Fortune 500 and government customers utilize Flashpoint's intelligence across the enterprise, including bolstering cybersecurity, confronting fraud, detecting insider threats, enhancing physical security, assessing M&A opportunities, and addressing vendor risk and supply chain integrity. For corporations with limited experience availing themselves of Deep & Dark Web intelligence, Flashpoint has tailored offerings that deliver comprehensive reporting and monitoring on their behalf.

Contact

web: www.flashpoint-intel.com
Email: info@flashpoint-intel.com