How Terrorists Use Encryption

By Robert Graham

As powerful encryption increasingly becomes embedded in electronic devices and online messaging apps, Islamist terrorists are exploiting the technology to communicate securely and store information. Legislative efforts to help law enforcement agencies wrestle with the phenomenon of "going dark" will never lead to a return to the status quo ante, however. With the code underlying end-to-end encryption now widely available, unbreakable encryption is here to stay. However, the picture is not wholly bleak. While end-to-end encryption itself often cannot be broken, intelligence agencies have been able to hack the software on the ends and take advantage of users' mistakes.

Counterterrorism officials have grown increasingly concerned about terrorist groups using encryption in order to communicate securely. As encryption increasingly becomes a part of electronic devices and online messaging apps, a range of criminal actors including Islamist terrorists are exploiting the technology to communicate and store information, thus avoiding detection and incrimination, a phenomenon law enforcement officials refer to as "going dark."

Despite a vociferous public debate on both sides of the Atlantic that has pitted government agencies against tech companies, civil liberties advocates, and even senior figures in the national security establishment who have argued that creation of "backdoors"[1] for law enforcement agencies to retrieve communications would do more harm than good, there remains widespread confusion about how encryption actually works.[a]

Technologists have long understood that regulatory measures stand little chance of rolling back the tide. Besides software being written in other countries (and beyond local laws), what has not been fully understood in the public debate is that the "source code" itself behind end-to-end encryption is now widely available online, which means that short of shutting down the internet, there is nothing that can be done to stop individuals, including terrorists, from creating and customizing their own encryption software.

The first part of this article provides a primer on the various forms of encryption, including end-to-end encryption, full device encryption, anonymization, and various secure communication (operational security or opsec) methods that are used on top of or instead of encryption. Part two then looks at some examples of how terrorist actors are using these methods.

Part 1: Encryption 101

End-to-End Encryption

A cell phone already uses encryption to talk to the nearest cell tower. This is because hackers could otherwise eavesdrop on radio waves to listen in on phone calls. However, after the cell tower, phone calls are not encrypted as they traverse copper wires and fiber optic cables. It is considered too hard for nefarious actors to dig up these cables and tap into them.

In a similar manner, older chat apps only encrypted messages as far as the servers, using what is known as SSL.[b] That was to defeat hackers who would be able to eavesdrop on internet traffic to the servers going over the Wi-Fi at public places. But once the messages reached the servers, they were stored in an unencrypted format because at that point they were considered "safe" from hackers. Law enforcement could still obtain the messages with a court order.

Newer chat apps, instead of encrypting the messages only as far as the server, encrypt the message all the way to the other end, to the recipient's phone. Only the recipients, with a private key, are able to decrypt the message. Service providers can still provide the "metadata" to police (who sent messages to whom), but they no longer have access to the content of the messages.

The online messaging app Telegram was one of the earliest systems to support end-to-end encryption, and terrorists groups such as the Islamic State took advantage.[2] These days, the feature has been added to most messaging apps, such as Signal, Wickr, and even Apple's own iMessage. Recently, Facebook's WhatsApp[3] and Google[4] announced they will be supporting Signal's end-to-end encryption protocol.

a For example, General Michael Hayden, the former head of the NSA and CIA, stated "America is more secure—America is more safe—with unbreakable end-to-end encryption," arguing that the vulnerabilities created by removing unbreakable code outweighed the advantages of detecting nefarious communications. Tom Di Christopher, "US safer with fully encrypted phones: Former NSA/CIA chief," CNBC, February 23, 2016.

b Secure Sockets Layer (SSL) is the standard security technology that is used for creating an encrypted link between a web server and internet applications such as browsers and chat apps. This prevents anyone who is eavesdropping on the network from reading the original, unencrypted data. Only those on either end of the SSL link can read the data.

Robert Graham is a specialist in cyber security, who created the first intrusion prevention system (IPS). He is the creator of the cyber security tools BlackICE, sidejacking, and masscan, and he authors the blog Errata Security. Follow @erratarob

On personal computers, the software known as PGP,[c] first created in the mid-1990s, reigns supreme for end-to-end encryption. It converts a message (or even entire files) into encrypted text that can be copy/pasted anywhere, such as email messages, Facebook posts, or forum posts. There is no difference between "military grade encryption" and the "consumer encryption" that is seen in PGP. That means individuals can post these encrypted messages publicly and even the NSA is unable to access them. There is a misconception that intelligence agencies like the NSA are able to crack any encryption. This is not true. Most encryption that is done correctly cannot be overcome unless the user makes a mistake.

Such end-to-end encryption relies upon something called public-key cryptography. Two mathematically related keys are created, such that a message encrypted by one key can only be decrypted by the other. This allows one key to be made public so that one's interlocutor can use it to encrypt messages that the intended recipient can decrypt through the private-key.[d] Al-Qa`ida's Inspire magazine, for example, publishes its public-key[5] so that anyone using PGP can use it to encrypt a message that only the publishers of the magazine can read.

Full Device Encryption

If an individual loses his iPhone, for example, his data should be safe from criminals.[e] Only governments are likely to have the resources to crack the phone by finding some strange vulnerability. The FBI reportedly paid a private contractor close to $1 million to unlock the iPhone of San Bernardino terrorist Syed Rizwan Farook.[6]

The reason an iPhone is secure from criminals is because of full device encryption, also full disk encryption. Not only is all of the data encrypted, it is done in a way that is combined or entangled[7] with the hardware. Thus, the police cannot clone the encrypted data, then crack it offline using supercomputers to "brute-force" guess all possible combinations of the passcode. Instead, they effectively have to ask the phone to decrypt itself, which it will do but slowly, defeating cracking.[f]

Android phones work in much the same manner. However, most manufacturers put less effort into securing their phones than Apple. Exceptions are companies like Blackphone, which explicitly took extra care to secure their devices.

c PGP, or Pretty Good Privacy, was software written in the 1990s for encrypting any information, though primarily emails. A version known as GPG, or Gnu Privacy Guard, exists, which is open-source, meaning anyone can download the code and build their own apps that include this encryption standard.

d The most common use of PGP involves the creation of two extremely large prime numbers, then multiplies them together. The original two numbers form the private-key, the multiplied result forms the public-key that anyone can know. It is secure because it is too difficult for even the most powerful supercomputer to work backward and discover the original primes from the public-key. The public-key is then posted to public-key servers so that if somebody knows the associated email address, they can find the key. Or the key can be sent directly in an email message, and the recipient can then use the public-key to encrypt messages that only the other party can decrypt.

e This is assuming the owner is using the newer iOS 9 operating system as hackers found vulnerabilities in earlier versions.

f The precise delay is 80 milliseconds, or 12 guesses per second. If the passcode is "1234," it will be guessed quickly. But if the passcode uses six alphanumeric characters, it will take more than five years to guess it.

"A survey of terrorist publications and details from interrogations suggest that terrorists are at least as concerned about hiding metadata as they are about encrypting communications."

Full disk encryption is also a feature of personal computers. Microsoft Windows comes with BitLocker, Macintosh comes with FileVault, and Linux comes with LUKS. The well-known disk encryption software TrueCrypt works with all three operating systems as does a variation of PGP called PGPdisk. Some computers come with a chip called a TPM[g] that can protect the password from cracking, but most owners do not use a TPM. This means that unless they use long/complex passwords, adversaries will be able to crack their passwords.

These programs can also produce volume or container files. They will exist as a normal file on the disk, like foobar.dsk. But the contents of this file will look like random gibberish. When the file is opened with the encryption software, it will appear as a disk drive (like F:) on the computer. Anything written to this virtual drive F: will, in fact, be encrypted and written to foobar.dsk.

Anonymization

In 2013, Edward Snowden released documents from the NSA[8] revealing widespread mass surveillance, even of U.S. citizens. This surveillance did not eavesdrop on the phone calls of people in the United States but instead collected the metadata about the calls: who was calling whom and for how long. Reportedly[9] the United States has targeted overseas terrorists with drone strikes based on this metadata. A survey of terrorist publications and details that have emerged from interrogations suggest that terrorists are at least as concerned about hiding metadata as they are about encrypting communications. But the various chat apps/services now available on the market do little to hide metadata. Servers must know the address or phone number in order to know where to forward the message.

The most common way to deal with this problem on the internet is through a service called Tor (The Onion Router).[h] It passes traffic (encrypted) through multiple proxy servers around the internet controlled by different organizations, often private individuals. This makes it sometimes very difficult and at times even impossible to figure out the source of network traffic.

The process is not perfect. For example, when the FBI went after Jeremy Hammond, the perpetrator of the Anonymous Stratfor attack, they collected[10] traffic on both ends. The Tor traffic coming from his home matched activity by the targeted hacker in a chat

g Trusted Platform Module stores the encryption keys in the hardware, similar to how phones store keys in their hardware. It also provides physical protection for the keys so that no one can crack open the chip to access them.

h Tor runs on Windows, Macintosh, and Linux computers. It is mostly used with its own built-in web browser based on Firefox, but it can be used to proxy almost any internet traffic.

room. The correlation was robust enough to secure court orders.

Tor also requires great care to use. The leader of the Anonymous faction called "LulzSec" was discovered[11] because one time when he logged onto a chat room, he forgot to enable Tor first. This one time that he slipped up defeated the hundreds of times he did it right, revealing his internet address to police.

As the Snowden leaks revealed,[12] Tor is a double-edged sword for intelligence services. Reportedly, U.S. government agencies had a role in Tor's development, have provided funding for it, and have used it to hide their own activities. Yet intelligence agencies spend significant resources trying to defeat it when terrorists use it.[13]

Opsec Methods

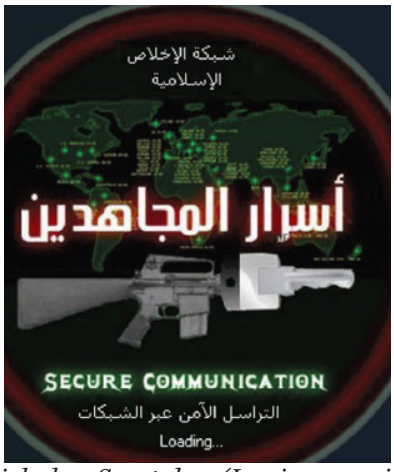
Encryption is only one way of hiding. There are alternatives. For example, the Paris terrorists congregated in safe houses in Belgium to plan their attack, and while some had downloaded messaging apps with encryption, to a significant degree they used burner phones[14] to coordinate during the attack.[i] To describe this, technologists often use the word opsec, or operational security.

Most chat apps (like Telegram and Wickr) now have a feature where old messages automatically self-destruct after an hour or a day, as well as the option to manually delete messages. It means incriminating evidence disappears without any interaction by the user. For law enforcement, this can mean that when a terrorist's phone is obtained, most of the evidence may already be gone. On desktops/laptops, there is special software, such as "Windows Washer" on Windows, for wiping the disks, designed to get rid of any remaining information. It is also a feature on web browsers, which can automatically delete browser history.

One industry leader for opsec is "Tails," which is frequently mentioned on terrorist forums.[15] It contains all the encryption tools described in this paper and more. Tails is a live flash drive, which means when a user inserts it into the computer, no trace is left on the computer. A typical computer boots Windows or Linux or macOS because the operating system is on the internal drive. When a live USB drive is inserted, however, the computer can instead boot the operating system from the external drive, ignoring whatever operating system is on the internal drive.

Tails boots the Linux operating system, which is similar to Windows or Mac OS in most ways. It is a bit clunky but easy enough to use. Most importantly, it reduces the chance that the user will make a mistake because once the USB drive is removed and the computer is shut down, there will be no accidental evidence left behind. Tails includes a normal web browser like Firefox that runs through Tor. It includes PGP and Pidgen+OTR for end-to-end encrypted email/messages. It includes LUKS (Linux Unified Key Setup) for full disk encryption of the USB drive, so that even if the user loses it, no one will be able to decrypt the lost drive.

i The three Paris attack teams kept in touch with each other by burner phones during the night of the attacks. The trio of terrorists who attacked the Bataclan music hall downloaded the Telegram encryption messaging app onto their phones several hours before the attack, but they also made unencrypted calls and text messages to co-conspirators on burner phones. Paul Cruickshank, "The inside story of the Paris and Brussels attacks," CNN, March 30, 2016.



Mujahedeen Secrets logo (Inspire magazine)

Part 2: How Terrorists Use Encryption

Encryption in the Age of al-Qa`ida

In the years after 9/11 U.S. intelligence intercepts helped thwart a string of al-Qa`ida plots, including the 2006 transatlantic airplane plot, a plot by al-Qa`ida-linked terrorists to bomb U.S. soldiers in Germany the following year, and the 2009 plot by Najibullah Zazi to bomb New York. Well before the 2013 Snowden revelations of NSA capabilities, the earlier NSA successes, widely reported on in the media at the time, resulted in the group increasingly moving toward encrypted communications.[16]

In early 2007, al-Qa`ida released an encryption tool called "Mujahedeen Secrets" (or Asrar al Mujahideen) and then in January 2008 issued an update to the software called "Mujahideen Secrets 2."[17] It was used in 2009 by al-Qa`ida in the Arabian Peninsula (AQAP) cleric Anwar al-Awlaki to communicate with operatives in the West,[18] and Inspire magazine included a four-page, step-by-step tutorial on how to use it in June 2010.[19] A group of German foreign fighters recruited for a plot to hit Europe the same year were instructed on how to use the software in the tribal areas of Pakistan by al-Qa`ida operative Younes al Mauretani.[20]

While Mujahedeen Secrets was described as a kind of custom encryption tool, it was just a friendly wrapper around PGP. Its developers did not write encryption code themselves; they used the code written by others. It was fully compatible with other versions of PGP and could be used to encrypt messages using keys such as those found in Inspire magazine. In other words, it was an end-to-end encryption tool not because the terrorists designed it that way but because they inherited the code from cryptographers. Creating original source code for encryption that actually worked would have been too difficult, but they certainly could make existing encryption easier to use. One lesson policy makers can learn from this is that the software code for encryption is out there. Attempting to regulate software or devices will not prevent terrorists from creating their own software with the encryption features they want.

Al-Awlaki placed a significant emphasis on secure communications. Between 2009 and 2010 he and Rajib Karim, a British Airways call center worker based in Newcastle, set up an elaborate system of encrypted communications to plot attacks against British and American aviation. The intricate system, outlined in a 2011 trial in which Karim was convicted of terrorism offenses, involved Karim using end-to-end encryption to send messages to his brother

in Yemen, who was in contact with al-Awlaki.

They used a multi-layered process to encrypt the messages. First, the text message was pasted into an Excel document, which used their own macros to encrypt the message. Second, the result of that encryption was copied and pasted into a Word document, then saved with Microsoft's "password protect" feature, which is unbreakable if long and complex passwords are chosen. Third, the Word document was compressed and encrypted using the RAR program, which is also unbreakable if long and complex passwords are chosen. Lastly, they uploaded to web hosting sites through a URL shortener in an attempt to anonymize the metadata.[j] Police described his use of encryption as "the most sophisticated they had seen in a British terrorist case."[21]

When he was arrested, court documents show that he was calm, apparently secure in his knowledge that he did encryption right. In reality, while Western intelligence agencies were not able, as far as is known, to intercept any of his communications in real time, he made some mistakes.[22]

Karim practiced good opsec by using the program "Windows Washer" and other Windows tools to keep his laptop clean of any incriminating evidence. He used full disk encryption in order to put all of his plans as well his encrypted communications with al-Awlaki on an external hard disk, separate from his laptop.[23] He used volume/container files for full disk encryption. He named the files like "Quran DVD Collection 1.rar,"[24] where the ".rar" extension indicated the use of a popular compression program. However, the files were in fact PGPdisk encrypted volumes. Changing the extension from ".pgd" to ".rar" failed to fool investigators because, regardless of extension, RAR files start with the string "Rar!" and PGPdisk files start with the string "PGPdMAIN." This is an example of the fallacy of security through obscurity.[25] Noticing the ruse, British police technicians were able to decrypt the disk volumes.[k]

While PGP was installed on the computer, Karim does not appear to have used it to encrypt and decrypt messages, perhaps out of paranoia about the capabilities of Western intelligence agencies, but instead used an unorthodox and complex technique based on cipher codes and passwords stored on Excel spreadsheets. His biggest slip-up was that he had saved this spreadsheet on his computer, allowing British police over a period of several months to decipher the messages stored on his external hard drive and use them as evidence against him. The computer had not been wiped in time. Booting a separate operating system, such as the aforementioned Tails, which the Islamic State is now encouraging their operatives to use, would have prevented this mistake.[26]

Encryption in the Age of the Islamic State

The ubiquity of encryption in commercially available messaging tools and devices has made it increasingly easy for terrorists to communicate securely. And it has become easier for terrorists to use the tools that already exist (Telegram, Whatsapp, Surespot, etc.) rather than build their own software like Mujahedeen Secrets. The main limiting factor appears to be terrorist distrust of some of these tools based on rumors that they contain backdoors and a general paranoia about the capability of Western intelligence agencies.[l]

In April the Islamic State released a 15-page guide titled "Sécurité Informatique" in its French online magazine Dar al-Islam, demonstrating the importance of secure communications for the group. It teaches how to setup Tails, connect to the Tor network to hide one's location and Internet address, create PGP keys, encrypt emails, and how to use a range of other secure communication tools.[27 m]

French police believe the Paris attackers used encryption in some of their communication, based on data collected from an abandoned Samsung phone they recovered outside the Bataclan concert hall after the attack. The Telegram app had been downloaded onto the phone seven hours before the attacks. No recovered content from the messaging app is mentioned in the French police documents, suggesting the technology allowed them to cover their tracks successfully and possibly by using the self-destruct feature within Telegram. Paris prosecutor Francois Mollins stated after the attacks that French investigators often encountered Telegram in their investigations and cannot penetrate its encryption.[28]

In August 2015, French authorities arrested and interrogated Reda Hame, a French Islamic State recruit who had gone to Syria where, over a period of several weeks in June 2015, he received rudimentary training in Raqqa and was tasked by Paris attack team leader Abdelhamid Abaaoud with returning to France to commit a terrorist attack. Hame was instructed in a rather bizarre technique to use a TrueCrypt volume file in which full disk encryption was used as a replacement for end-to-end encryption. The system involved creating text files with messages inside the virtual disk drive, then uploading the container file to file-sharing websites.[29]

On one hand, this technique provided good opsec. The normal method using PGP to encrypt a file means an unencrypted copy could still be left on the disk drive accidentally. By creating a file in a virtual disk drive, no other copy would exist on the system. But on the other hand, this technique is another example of the fallacy of security through obscurity. As with Rajib Karim, the obvious intent was to avoid NSA collection of email metadata by using an obscure method of uploading to file-sharing sites. However, this remains obscure only temporarily. Once Hame was caught and interrogated, his technique would have been conspicuous, making it easier for the NSA and its European counterparts to track the metadata of others using this technique.

j Karim's use of these sites may have helped evade NSA detection. On the other hand, once one member of this group was caught, it would make it even easier to track down all the rest of the members. A group is only anonymous as long as nobody in the group is known.

k They did not say how it was done. In all likelihood, they used a brute-force password cracker that can attempt a million passwords per second. Short passwords, especially those based on dictionary words, can quickly be cracked this way. Long passwords, especially complex ones using punctuation, would be beyond even the NSA's ability to crack, with all their billion-dollar supercomputers.

l For example, the Islamic State has instructed its followers not to trust Tor. "As to the question of whether the NSA can crack their code, the answer is probably yes. That's why you should never send anything personal or sensitive or that you do not want to be intercepted over Tor." Dar al-Islam issue 9, p. 38.

m An English Islamic State deep web forum user posted the same month also extolled the virtues of PGP encryption. "This method of encryption is the same one used by the assassins, drug dealers, and smugglers on the hidden internet, and this is due to its high level of security, such that one cannot even respond to a post or message without having the cypher," the user stated. See "Member of Top ISIS Deep Web Forum Releases First Lesson in Encryption Course." Flashpoint Intelligence, April 15, 2015.

It appears that Hame never actually used the technique, however. According a transcript of his interrogation he forgot the passwords and names of the websites he was supposed to use. Instead, as it appears in most cases, most of the planning of his terrorist activities was by face-to-face contact, not electronic communication.[30]

Other Islamic State operatives resorted to a much more straightforward use of encryption. Junaid Hussain, a British Islamic State operative who had been involved in hacking before departing for Syria and was killed in a drone strike in August 2015,[31] was a prolific user of the encryption messaging app Surespot, using it to provide Islamic State sympathizers in the United Kingdom with bomb-making tips and encouraging them to carry out attacks.[32] For example, he used it to discuss targeting options with Junead Khan, a British extremist who was convicted of a plot to attack U.S. Air Force personnel in England that was thwarted in July 2015. In order to retrieve information from Khan's iPhone, British undercover offices employed an elaborate ruse to trick Khan into handing over his iPhone just before they arrested him so that they could change its password settings before it locked.[33]

Hussain also communicated using encryption with one of the American Islamic State followers who opened fire outside a "Draw the Prophet Mohammed" contest in Garland, Texas, in May 2015. The morning of the attack 109 encrypted messages were exchanged between Hussain and the gunman that were impossible for the FBI to read.[34]

According to reports, in the drone strike that killed Junaid Hussain (and fellow militant Reyaad Khan), British agents were able to find their physical location by "hacking" their end-to-end encrypted app Surespot.[35] Precise details are scarce, but it is unlikely that Surespot itself was hacked but merely used in the hack. Once British agents discovered their target's address (an opportunity may have been from Hussain posting it online or the phone acquired from Junead Khan, described earlier), they could send a phishing message with a link. This link could be as simple as a recording of their current internet address or as complex as a virus.

With an internet address, intelligence services could discover the unique identifier of the phone (known as the IMSI or International Mobile Subscriber Identifier). This would require intelligence services to hack into the phone company servicing the Islamic State or to utilize a paid informant on the inside. Then IMSI catchers in drones/airplanes flying overhead can be used to pinpoint the radio signals coming from the phone.

With a virus, they can do all that and more. Instead of grabbing the IMSI from the phone company, the virus can simply acquire it from the phone. Instead of planes flying overhead, the phone itself can report its GPS location on a regular basis via the internet. Intelligence services like the GCHQ and NSA have such viruses in their arsenal, known as implants, which use what is known as "0day[n] exploits" to break into the phone as soon as a user taps on a link within the Surespot app.

0days are the archetypal cyber weapon. Intelligence services can point them at a target, gain control of the computer, and implant a virus that allows them to maintain control.[o] This technique gets away from remote signals detection to find a target, which was the traditional role of the NSA, and moves toward subverting the device to monitor itself.

Islamic State-inspired terrorists have recently demonstrated good opsec. The San Bernardino terrorists used unencrypted burner phones[36] on the day of the attack, then destroyed them so that evidence could not be recovered. They also possessed an iPhone, provided by their employer, which the FBI could not crack due to Apple's powerful full device encryption. After four months of failing to gain access, the FBI reportedly paid close to $1 million to a hacker to find and exploit a vulnerability in Apple's software that allowed them to crack the password and access the phone.[37] [p]

To do this, the FBI likely bought an 0day,[q] which would have worked not by immediately hacking the phone but by allowing those trying to break into the phone to guess passcodes quickly, without the normal delay that iPhone uses to defeat brute-force cracking.[r]

Conclusion

The encryption used today was not developed by intelligence agencies or militaries but by university students and corporations. Even militaries, however, use this encryption because encryption they would develop themselves just is not good enough. And it is clear from a survey of jihadist publications that all encryption techniques

n An 0day is a software bug that can be used to break into a computer that no one, even the software maker, knows exists. The fact that intelligence services buy 0days from hackers but do not tell the manufacturers is controversial among those working in the tech field.

o They are extremely difficult to find. Intelligence services pay hackers in the controversial 0day market to find bugs and report them to the intelligence agencies. Every time that Microsoft updates Windows or Apple updates the iPhone, the 0days often break, requiring the intelligence agencies to go back to the hackers for replacements.

p After the San Bernardino iPhone was opened by a third party, Apple moved to tighten its full device encryption, recently hiring John Callas, a well-known encryption expert who helped develop both PGP and the Blackphone, to work on the problem in the belief that anything that weakens security for law enforcement ("backdoors") inevitably makes a phone insecure against all other threats. Russel Brandom, "Encryption expert returns to Apple in wake of San Bernardino standoff," The Verge, May 26, 2016.

q The iPhone uses full-device encryption with a hardware key that has been entangled with the passcode. Consequently, the only possible way to decrypt the iPhone is with that entangled key. One way to obtain it is by using acid to remove layers from the chip and read that hardware key, but this method carries a high chance of destroying the key before it's read. The only other way is to make frequent guesses of the passcode, and that can only work by using an 0day that bypasses Apple's software designed to prevent guesses. In other words, by design, the only two possible ways to decrypt an iPhone is either by attacking the hardware or brute-force guessing of the passcode using an 0day to disable the anti-guessing software.

r Normally, bad guesses cause the phone to wait longer and longer between guesses, and after 10 bad guesses, the phone is wiped. The 0day exploit the FBI likely purchased prevented both the long wait and the wipe so that an infinite number of guesses could be made as quickly as the phone would allow (roughly 12 guesses per second). Reports are conflicting, however. It may be that the FBI purchased the 0day technique so that they could use it on similar phones, or it may be that the hacker used the 0day and cracked the password for the FBI but did not give them the 0day. See, for example, "Ellen Nakashima, FBI paid professional hackers one-time fee to crack San Bernardino iPhone," *Washington Post*, April 12, 2016.

are known to terrorists.

Software must be written to perform encryption. This, too, is out in the world. The source-code for virtually all encryption is available to anyone who can write software. Indeed, paradoxically, the most trusted encryption software is also the software whose source-code is public, allowing anybody to read it and find flaws before the NSA or GCHQ can. That is why PGP appears so prominently among non-state actors seeking to communicate securely. They can read the code and verify for themselves whether an intelligence agency has inserted a backdoor.

The FBI has called for laws mandating encryption backdoors, but these laws would be mostly futile. They do not apply to software or phones created in other countries, for example. They do not apply to jihadist programmers who create their own apps based on open-source software. This is why many in the intelligence community, such as former head of the NSA Michael Hayden, oppose backdoors.[38]

So what are the options? Security agencies will need to outsmart the software. In end-to-end encryption, it is no longer viable to crack the encryption in the middle. Intelligence agencies must instead hack the software on the ends. 0day exploits will likely be the most common way the NSA will eavesdrop on communications in the future – by hacking the "ends" of end-to-end communication with an 0day.

Security services will also have to exploit poor opsec by terrorists. From the perspective of security services the most worrying software is not one with the best encryption but one that allows fewer user mistakes. The opsec feature of self-destructing messages, for example, is probably one of the most frustrating features for intelligence services.

In other words, instead of a team of code breakers, the future will see more and more teams of people dedicated to breaking into software and outwitting users. The NSA's vast compute power will not be dedicated to complex encryption algorithms but to the rather simple task of guessing that a terrorist's password is "Password1234."

Thus, while encryption is itself nearly perfect, the world is not about to enter an era of terrorists communicating with impunity. While end-to-end encryption means security agencies have little hope of cracking the middle, they will still have easy ways to attack the ends, either by hacking the software or outwitting the user. CTC

Citations

1 Matthew Deluca, "Draft Encryption Bill Would Mandate Companies Assist Investigators," NBC News, April 13, 2016.
2 Don Reisinger, "This is How ISIS Communicates Online," *Forbes*, November 19, 2015.
3 Cyrus Farivar, "WhatsApp is now most widely used end-to-end crypto tool on the planet," Ars Technica, April 5, 2016.
4 Russell Brandom, "Google's Allo runs on the same encryption tech that powers WhatsApp," The Verge, May 18, 2016.
5 "How to communicate with us," Inspire issue 10, spring 2013.
6 Mark Hosenball, "FBI paid under $1 million to unlock San Bernardino iPhone: sources," Reuters, May 4, 2016.
7 Apple, Inc., "iOS Security Guide – iOS 9.3 or later," May 2016.
8 Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *Guardian*, June 6, 2013.
9 Mike Masnick, "Michael Hayden Gleefully Admits: We Kill People Based On Metadata," Techdirt, May 12, 2014.
10 Nate Anderson, "Stakeout: how the FBI tracked and busted a Chicago Anon," Ars Technica, March 6, 2012.
11 John Leyden, "The one tiny slip that put LulzSec chief Sabu in the FBI's pocket," Register, March 7, 2012.
12 Glenn Greenwald, "NSA and GCHQ target Tor network that protects anonymity of web users," *Guardian*, October 4, 2013.
13 Yasha Levine, "Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government," PandoDaily, July 16, 2014; Barton Gellman, Craig Timberg, and Steven Rich, "Secret NSA documents show campaign against Tor encrypted networks," *Washington Post*, October 4, 2013; Alex Hern, "US government increases funding for Tor, giving $1.8m in 2013," *Guardian*, July 29, 2014.
14 Jeff Stone, "ISIS Terrorists Used Disposable Burner Phones, Activated Just Hours Before, To Carry Out Paris Attacks," International Business Times, March 21, 2016.
15 J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, and L. Ryge, "NSA targets the privacy-conscious," ARD 1 Das Erste, July 3, 2014.
16 Paul Cruickshank, "Did NSA leaks help al Qaeda?" CNN, June 25, 2013.
17 "Jihadi software promises secure web contacts," Reuters, January 18, 2008.
18 See Morten Storm, Paul Cruickshank, and Tim Lister, *Agent Storm: My Life Inside al Qaeda and the CIA*, (New York: Atlantic Monthly Press, 2014), pp. 182-183.
19 "How to use Asrar al-Mujahideen: Send and Receiving Encrypted Messages," Inspire issue 1, summer 2010.
20 Cruickshank, "Did NSA leaks help al Qaeda?"
21 Vikram Dodd, "British Airways worker Rajib Karim convicted of terrorist plot," *Guardian*, February 28, 2011.
22 Regina v. Rajib Karim, Woolwich Crown Court, Prosecution Opening Statement, February 1-2, 2011.
23 Ibid.
24 Alistair MacDonald and Cassell Bryan-Low, "U.K. Case Reveals Terror Tactics," *Wall Street Journal*, February 7, 2011.
25 Regina v. Rajib Karim.
26 Sheera Frankel, "Everything You Ever Wanted to Know About How ISIS Uses The Internet," BuzzFeed, May 12, 2016.
27 Ibid.
28 Leslie Stahl, "Encryption," CBS 60 Minutes, March 13, 2016.
29 Soren Seelow, "Est-ce que tu serais prêt à tirer dans la foule?" *Le Monde*, January 6, 2016; Proces Verbal: 6eme Audition de Reda Hame, DGSI, August 13, 2015.
30 Ibid.
31 Barbara Starr, "Prominent ISIS recruiter killed in air strike," CNN, August 28, 2015.
32 For example, see "I.S. Plot to Bomb UK Today," *Sun*, June 26, 2015.
33 Paul Cruickshank, Andrew Carey, and Michael Pearson, "British police tricked terror suspect into handing over phone, source says," CNN, April 1, 2016.
34 David E. Sanger and Nicole Perlroth, "FBI Chief Says Texas Gunman Used Encryption To Text Overseas Terrorist," *New York Times*, December 9, 2015; reporting of Evan Perez on CNN Situation Room, December 17, 2015.
35 Lizzie Dearden, "British Isis jihadists 'had phones hacked by GCHQ' before they were killed by drone strikes," *Independent*, September 16, 2015.
36 Jennifer Medina, Richard Pérez-Peña, Michael S. Schmidt, and Laurie Goodstein, "San Bernardino Suspects Left Trail of Clues, but No Clear Motive," *New York Times*, December 3, 2015.
37 Mark Berman and Matt Zapotosky, "The FBI paid more than $1 million to crack the San Bernardino iPhone," *Washington Post*, April 21, 2016.
38 Susan Page, "Ex-NSA chief backs Apple on iPhone 'back doors,'" *USA Today*, February 24, 2016.