Digital Developments: Extremists' Use of Modern Communications Tools

March 2019

COUNTER EXTREMISM PROJECT

Digital Developments
Extremists' Use of Modern Communication Tools

The rapid adoption of state-of-the-art communication tools—with an emphasis on Internet-based applications—has been critical to the organization, expansion, and success of terrorist networks. Terror groups use modern communication technology in myriad ways, from fundraising, radicalization, and recruitment, to issuing threats, inciting violence, and planning attacks.

While Osama bin Laden used fax machines and satellite phones in the 1990s, the early 2000s saw a boom in new media applications that enabled terrorists to communicate undetected across borders more swiftly and effectively. The Internet essentially became another extremist battlefield. Encrypted software became a popular modus operandi for jihadists, and many groups established media departments and online recruitment magazines such as al-Qaeda's *Inspire.*

ISIS's communications tactics, such as its high production value beheading videos and its "Mujatweets," have grabbed international headlines. The terror group has hacked thousands of international websites, replacing their content with pro-ISIS messages. In January 2015, ISIS hacked the social media accounts of the U.S. Central Command and posted the personal contact information of numerous retired military officers, waging psychological warfare on men and women in uniform. Lone-wolf terrorists have also taken advantage of advancements in digital communications. In March 2019, a suspected white supremacist livestreamed shooting attacks on two New Zealand mosques that left at least 50 people dead. The suspect broadcasted the massacre on his Facebook account, where he also posted his manifesto. Terrorists' use of communication technology has shifted tremendously in the past two decades, demanding a greater understanding of these new threats—and a strategy to deal with them.

"The time has come to have the media take its rightful place, to carry out its required role in confronting this aggressive campaign and the open declared Crusader war by all means that can be seen, heard, and read." – Osama bin Laden, 2002 (Source: Terrorism and Political Violence)

1990-1996

Payphones, Cellphones, and Encrypted Emails

Throughout the 1990s, al-Qaeda operatives communicate via public pay phones, cellphones, and encrypted emails sent from Internet cafés throughout Asia and the Middle East. Osama bin Laden's operatives also store and disseminate information on CD-ROM disks. (Source: PBS NOVA)

1996-1998

Satellite Telephones

In November 1996, al-Qaeda operative Ziyad Khalil purchases an *Inmarsat Compact M* satellite phone and more than 3,000 pre-paid hours from a suburb in upstate New York. It retails at $15,000 and is the size of a laptop computer. The phone is for Osama bin Laden, who uses the device to coordinate terror activities from his hideout in a mountainous region of Afghanistan. The satellite phone works by bouncing phone calls off of an Inmarsat satellite in orbit above the Indian Ocean. For two years, bin Laden and his military operations chief Mohammed Atef use the satellite phone to make more than 900 calls to al-Qaeda operatives in Britain, Pakistan, Saudi Arabia, the U.S., and Yemen. Using the satellite phone, bin Laden organizes the 1998 bombings of the U.S. embassies in Kenya and Tanzania.

Bin Laden stops using the satellite phone in August 1998 following the embassy bombings in Kenya and Tanzania out of fear that the connection is not secure. Instead, he begins to rely on couriers to hand-deliver his messages.

(Sources: Bloomberg Business, PBS Frontline, RAND, *Wall Street Journal*, BBC News, Secret Intelligence: A Reader, PBS NOVA)

August 1996 / Fax Machines, Television, Radio and Print Media

Osama bin Laden releases a video of his first *fatwa*, or religious decree. He also faxes the text of the *fatwa* to Arab newspaper *al-Quds al-Arabi* in London for publication. The *fatwa*, titled "Declaration of War against the Americans Occupying the Land of the Two Holy Places," authorizes attacks on Western military targets in the Arabian Peninsula. Bin Laden declares there is "no more important duty than pushing the American enemy out of the holy land."

In the following years, al-Qaeda releases numerous video and audiotapes—often through mail or messenger—to Arab news stations such as Qatari-owned Al Jazeera and Saudi-owned al-Arabiya.

(Sources: NBC, *Telegraph*, PBS Newshour, Heritage Foundation, U.S. Congress Archive, NBC)

1997-present / The World Wide Web, Online forums, and Television Programs

Controversial Egyptian Muslim Brotherhood cleric Yusuf al-Qaradawi founds Islamonline.net in Doha, Qatar in 1997. The website serves as a forum providing young Muslims with information on politics, family, and social issues. Around the same time, Qaradawi launches a television program on Al Jazeera called al-Sharia wa al-Hayah, "Sharia and Life," on which he lectures on extremist Islam. Through his website and television series, Qaradawi calls for the murder of British and American troops in Iraq, the execution of homosexuals, and the murder of Jews. He also supports domestic violence to enforce a woman's submission.

(Sources: *Guardian*, MEMRI, *Guardian*, Middle East Forum, Spiegel)

Yusuf al-Qaradawi (Source: AFP)

1998 / Al Jazeera

In February 1998, Osama bin Laden faxes his second *fatwa*, "Declaration of the World Islamic Front for Jihad against the Jews and the Crusaders," to *al-Quds al-Arabi* for publication. (Source: *Foreign Affairs*)

During the summer, bin Laden sends a fax from Afghanistan to London-based cleric Omar Bakri Mohammed, a militant Islamist leader who claims to be the "mouth, eyes and ears of Osama bin Laden." The fax contains instructions for holy war against the U.S.: "Bring down their airliners. Prevent the safe passage of their ships. Occupy their embassies. Force the closure of their companies and banks." (Source: *Los Angeles Times*)

Al-Qaeda begins using Al Jazeera as a conduit for broadcasting bin Laden's messages. Al Jazeera then provides the videos to CNN and other Western media outlets. Bin Laden eventually agrees to an interview with Al Jazeera, hoping to help disseminate al-Qaeda's message. Critics of the television station claim that by cooperating with bin Laden, Al Jazeera becomes a participant in the conflict rather than just an impartial observer. (Sources: Marshall Center, *Guardian*, NBC)

Bin Laden's second fatwa published in Al-Quds al-Arabi newspaper (Source: BBC)

Early 2000s

Media Departments

Al-Qaeda launches the Global Islamic Media Front (GIMF) and the Al-Fajr Media Center. GIMF provides translation and dissemination, while Al-Fajr supports network usage and enables numerous websites and media outlets to host the same video content. (Source: Forensic Science Communications- FBI)

September 2000

Al-Qaeda launches its new media department, "As-Sahab." In one of its first videos, also aired by Al Jazeera, bin Laden calls for more attacks on the U.S. The video is released just three weeks before the bombing of the USS *Cole*.

As-Sahab proves to be an important force for al-Qaeda. The media arm is responsible for producing video files of interviews, documentaries, speeches, and news programs, and disseminates these videos from central and southeastern Afghanistan. As-Sahab also serves as an official source, verifying the legitimacy of al-Qaeda's videos. By 2005, As-Sahab produces its videos in formats that can be watched on a cellphone, broadening its reach and influence. The video and audiotapes serve to galvanize recruits and fighters, provide footage of attacks, claim responsibility for attacks, issue threats, and offer incentives to fighters.

(Sources: Marshall Center, NBC, *Telegraph*, PBS Newshour, Heritage Foundation, U.S. Congress Archive, NPR, NBC, *Washington Times*, The Globalization of Martyrdom)

As-Sahab Media Department Logo (Source: As-Sahab)

2001

The American-Yemeni Islamist militant [Anwar al-Awlaki](#), dubbed the "bin Laden of the Internet," releases hundreds of his sermons online. The videos and recordings are further disseminated by jihadi websites. By 2008, Awlaki is "all over YouTube and the rest of the Internet, and his website [is] skyrocketing in readership," according to the U.S. Department of Homeland Security. (Sources: [ICSR](#), *[Huffington Post](#)*, [USA Today](#))

June 2001

Osama bin Laden celebrates the October 2000 attack on the USS Cole in a recruitment video released by As-Sahab. Bin Laden calls on Muslims to join his jihad, and urges viewers to distribute the video. The Associated Press and Reuters publish the video. (Sources: [NBC](#), [ABC News](#), [The Globalization of Martyrdom](#))

September 11, 2001

The 9/11 hijackers use conventional email and online chat rooms to gather basic intelligence on targets, share information, and coordinate the attacks. They also use the Internet to steal Social Security numbers and obtain fake drivers' licenses. Any messages sent between the hijackers are coded or encrypted. (Sources: [United States Institute of Peace](#), [MIT Technology Review](#))

Following 9/11, al-Qaeda moves towards a more decentralized structure resulting in its heavy reliance on new media. The simultaneous expansion of the World Wide Web enables continued communication between its operatives. The terror group expands its influence through the online publication of written statements, blogs, online Arabic-language magazines, and articles written by its ideological leaders.

The number of jihadi websites metastasizes in the wake of the 9/11 attacks. Notable websites include al-Qaeda's "Alneda.com" and the online jihadi forum "Qalah." Alneda.com acts as a

clearinghouse for al-Qaeda leadership statements, and displays pictures of the 2001 Afghan war, celebrations of the 9/11 hijackers, and lengthy theological justifications for jihad. In July 2002, a statement on Alneda.com reads: "The U.S. enemy, unable to gain the upper hand over the mujahedin on the battlefield, has since Sept. 11 been trying to gag the world media… America will lose the media war, too." During this time, Anwar al-Awlaki becomes involved in Qaradawi's Islamonline.net.

The Qalah forum and similar websites host computer hacking techniques, claim credit for recent attacks, and air beheading videos from Iraq. Most of the websites are written in Arabic, and the text is encrypted, which makes it difficult for officials to find or read. Such websites are centered on preaching, recruitment, training, and broad incitement. (Sources: Marshall Center, *Washington Post*, USA Today, Anti-Defamation League)

February 5, 2002

CNN airs a controversial interview between Al Jazeera reporter Tayseer Alouni and Osama bin Laden. Al Jazeera refuses to air the video for its incendiary content. In the interview, bin Laden declares that the Americans in Afghanistan will be defeated more easily than the Soviets. Bin Laden declares: "We experienced the Americans through our brothers who went into combat against them in Somalia, for example…America exited dragging its tails in failure, defeat, and ruin, caring for nothing." (Source: NBC)

February 21, 2002 / Beheading Videos

The first of its kind, a video depicting the beheading of American-Israeli journalist Daniel Pearl by Pakistani militants circulates on the Internet. In the video Pearl discusses his Jewish roots, which is followed by his graphic beheading. (Source: *Washington Post*)

2003 / Online Magazines

Al-Qaeda releases two Arabic-language online magazines: *The Call of Islam and Voice of Jihad*, which seek to radicalize and mobilize recruits. (Sources: Terrorism and Political Violence, Beyond al-Qaeda)

2004-2006 / Al-Qaeda Beheading Videos Gain Sophistication

The Internet erupts with videos of hostage beheadings perpetrated by al-Qaeda in Iraq (AQI) emir Abu Musab al-Zarqawi. The videos are downloaded by tens of millions of people. According to former CIA counterterrorism analyst Aki Peritz, AQI's beheading videos become increasingly sophisticated over time. The May 2004 video depicting the beheading of American hostage Nick Berg is a "shaky, blurry product." By 2006, AQI's beheading videos are "far superior, complete with smooth edits, audio dubbings and computer graphics."

Al-Zarqawi's AQI packages real-time war scenes with shock videos of suicide bombings and beheadings. According to journalists Susan Glasser and Steve Coll, it's almost as if "no act goes unrecorded and atrocities seem to be committed in order to be filmed and distributed nearly

instantaneously online." (Sources: *Washington Post*, BBC, MIT Technology Review, *Washington Post*)

Abu Musab al-Zarqawi (Source: U.S. Military)

September 2005 / Voice of the Caliphate

The underground Global Islamic Media Front (GIMF) launches Sawt al-Khilafa, "Voice of the Caliphate," a video newscast hosted on the Internet. GIMF's public relations director Sayf al-Din al-Kinani declares the newscast campaign will help in "galvanizing the fight against the enemy," and calls for active participation from youth in jihadi forums. The first video in the series shares headlines from around the world, including the "liberation of Gaza" and the "divine, just punishment" inflicted by Hurricane Katrina on New Orleans, the "city of homosexuals." (Sources: *Telegraph*, Integrated Threat Assessment Center, Jamestown Foundation)

2010-present

Online English-Language Magazines

Al-Qaeda in the Arabian Peninsula (AQAP), and specifically Anwar al-Awlaki, launch an English-language recruitment magazine called *Inspire*. The magazine is available online in PDF format and is disseminated via numerous online jihadi forums. According to *Inspire* editor-in-chief Yahya Ibrahim, the Boston Marathon bombers of April 2013 are motivated by the magazine, "not only because *Inspire* offers bomb recipes, but also because of the contents of the

magazine as a whole." Anyone with Internet access is susceptible to this radicalizing propaganda.

Awlaki, the "bin Laden of the Internet," produces *Inspire*'s content as a self-help manual for jihadists. The perpetrators of the 7/7 bombings— the 2005 London suicide attacks that killed 52—claim they researched bomb-making methods at home and were inspired by "[Awlaki's] rallying cry of 'just do it.'" Awlaki is also believed to have influenced Fort Hood shooter Nidal Hassan, Times Square bomber Faisal Shahzad, *Charlie Hebdo* shooters Chérif Kouachi and Saïd Kouachi, and Orlando shooter Omar Mateen, among dozens of other American and European extremists. CEP continues to identity these individuals in its online resource, Anwar al-Awlaki's Ties to Extremists. (Sources: Guardian, Defense One, Jihadology, Washington Post, Long War Journal, CNN, ICSR, Daily Mail, Huffington Post, USA Today)

A page from Inspire*'s Spring 2014 issue* (Source: Jihadology)

June 16, 2011 / Hit List

Top jihadist web-forum Ansar al-Mujahideen releases a "hit list" of U.S. officials including Pentagon directors, a member of Congress, executives of an American corporation that produces drones, and two prominent French executives. The hit list contains photographs and biographical

information of each of the 40 targets, and is released in response to al-Qaeda spokesman Adam Gadahn's June 3 call for lone wolf attacks on American public figures. (Source: ABC)

March 2012 - Ongoing / Jihadists Use GoPro Cameras to Capture Footage During Attacks

French-Algerian jihadist Mohammed Merah embarks on an eight-day shooting spree in southwest France, killing three off-duty soldiers, three Jewish schoolchildren, and a rabbi. Merah films the murders using a GoPro camera, a device designed for extreme athletes which allows users to produce action shots from their viewpoint. Merah edits the footage and sends it to Al Jazeera, though it is never released. In January 2015, ISIS sympathizer Amedy Coulibaly uses a GoPro camera to capture images while attacking a kosher supermarket in the days following the *Charlie Hebdo* murders. Coulibaly then uploads those photos onto his laptop while holding shoppers and store personnel hostage. The images are never broadcast. (Sources: *Washington Post*, *Guardian*, Combating Terrorism Center)

February 2013 / Jihadi-Approved Encryption Software

Jihadists release encryption software for instant messaging services called Asrar al-Dardashah, which is formally endorsed by the Global Islamic Media Front. In December 2013, Al-Fajr Media Center distributes an advanced encryption technology, a software dubbed "Security of the Mujahid." The program and its 28-page manual are then disseminated on numerous jihadi forums. In June 2014, Al-Fajr Media Center releases a version of the encryption software for android. (Sources: VICE News, MEMRI, Wilson Center)

April 2013 / Social Media

With the emergence of ISIS and its declaration of a caliphate, ISIS leaders turn to the Internet for radicalization and recruitment. Recruiters utilize social media outlets to "field questions about joining" the group, a process which resembles an "online version of [a] religious seminar." Social media platforms include Twitter, Facebook, YouTube, Tumblr, and Ask.fm. Recruiters also use encrypted messaging platforms such as Wickr, Kik, and YikYak to provide advice about logistical issues—such as transportation and finances—related to hijra, or migration to ISIS-controlled territory. (Sources: *New York Times*, *International Business Times*, *Atlantic*, Smithsonian, NPR, *International Business Times*, CNN Money, PRI)

2014 / Twitter

ISIS members and sympathizers mount a psychological campaign on Twitter in the hopes of drawing new recruits to its ranks. ISIS seeks to display its power and strength while deriding its enemy the Nusra Front, al-Qaeda's affiliate in Syria. The campaign continues as ISIS seizes more and more territory in Syria and Iraq.

In March, ISIS sympathizers launch a Twitter hashtag campaign, writing, "We demand Sheikh Al Baghdady declare the caliphate." ISIS declares a caliphate in June 2014 with Abu Bakr al-

[Baghdadi](#) as its caliph, or leader. (Source: ISIS: The State of Terror, Jessica Stern and J.M. Berger, p. 69)

April 2014 / ISIS app: "The Dawn of Glad Tidings"

ISIS releases an Internet application ("app") that sends subscribers tweets containing information, videos, and links to ISIS news. The tweets are written and disseminated by members of ISIS's social media department. The app automatically re-tweets each tweet onto the subscriber's personal Twitter account. The app, called "The Dawn of Glad Tidings," posts over 40,000 tweets per day during the terror group's advance on Mosul in June. Twitter and Google suspend the app after ISIS's seizure of Mosul. (Sources: ISIS: The State of Terror, Jessica Stern and J.M. Berger, p. 148, *[Atlantic](#)*, *[International Business Times](#)*)

May 2014 / ISIS's Al-Hayat Media Center

The Al-Hayat media center, launched in May 2014 and known for its recruitment and beheading videos, is ISIS's official media department and propaganda arm. Al-Hayat is notable for its videos' high production quality and consistent circulation. Long War Journal editor Bill Roggio comments on the fast turnout of the Al-Hayat's videos: "Al-Qaeda will issue a propaganda statement, what, once every month? With the Islamic State, I saw the aftermath of the battle of Tabqa that gave them full control of a province in Syria — I saw that video two days after the battle." (Sources: ISIS: The State of Terror, Jessica Stern and J.M. Berger, p. 113, [PRI](#))

Mujatweets Video Series

ISIS's al-Hayat Media Center launches an HD-quality video series called the Mujatweets to depict "snippets of day-to-day life in the 'Islamic State.'" The Mujatweets serve as explicit propaganda, aimed at depicting life under ISIS as bountiful and heroic. According to the Middle East Media Research Institute (MEMRI), "the purpose [of the Mujatweets] is to show that life under ISIS rule is peaceful and normal, and to shatter the image of the jihad fighters as fierce religious fanatics by presenting them as ordinary, friendly people eager to help the local population." (Sources: [Jihadology](#), [MEMRI](#))

Screen grab from Mujatweet episode 3, showing a chef praising the "Islamic State." (Source: Jihadology)

July 2014 / Dabiq: ISIS's English Language Magazine

ISIS's Al-Hayat media center releases the first issue of the terror group's online magazine, Dabiq. The magazine is circulated in print and online, and is available in English, French, German, Russian and Arabic. A new issue is released nearly every month detailing ISIS news and updates, theological justifications of ISIS's actions, and interviews with various ISIS leaders and members. The magazine has high production quality, both in terms of imagery and editing. In December 2014, ISIS launches a French-language magazine titledDar Al-Islam, and in May 2015 releases a Russian-language magazine called "Istok" aimed at recruiting fighters from post-Soviet countries. (Sources: Institute for the Study of War, MEMRI, Jihadology)

August 2014 / ISIS Drones

An ISIS web forum releases a promotional video demonstrating the terror group's purported deployment of remote-controlled drones. The 14-minutes video includes aerial shots of disputed regional territory allegedly filmed by ISIS-owned drones, which the terror group allegedly uses for reconnaissance. In December 2014, ISIS releases its second video including footage from remote-controlled drones, this time of the aerial view of the Syrian Kurdish town Kobani. (Sources: *International Business Times*, *Telegraph*)

Screen grab from ISIS's video purportedly showing footage shot by an ISIS-controlled drone
(Source: ISIS video, since removed)

August 19, 2014 / Message to America Beheading

ISIS posts a video to YouTube titled "A Message To America" showing ISIS militant Jihadi John beheading American journalist James Foley. The video concludes with the fighter threatening to kill American journalist Steven Sotloff, another hostage held by ISIS. YouTube removes the video the same day, but jihadist web forums, shock sites, and blogs have already reposted it. The Foley video is the first in a series of beheading videos in which Jihadi John graphically beheads Western hostages. (Sources: *New York Times*, CNN)

Screen grab from "A Message To America" (Source: Daily News)

Following the release of the video, Twitter begins to suspend pro-ISIS accounts spreading violent imagery and propagandizing material. (Source: ISIS: The State of Terror, Jessica Stern and J.M. Berger, p. 168)

September 2014 / Twitter Crackdown

In the weeks following James Foley's beheading, Twitter suspends the accounts of ISIS supporters, usually "dozens at a time." Some remaining ISIS members use Twitter to issue death threats to Twitter executives. Analysts estimate that at least 45,000 pro-ISIS accounts are active on Twitter between September-November 2014. (Source: ISIS: The State of Terror, Jessica Stern and J.M. Berger, p. 170-171)

September 18, 2014 / John Cantlie Video Series

ISIS releases its first episode of its "Lend Me Your Ears" video series starring British hostage and war journalist John Cantlie. As of February 2015, ISIS has released a total of seven episodes, with each new installment garnering considerable media attention. The video series has been

dubbed "vlogging" or video blogging by RYOT News, and has served as a propaganda tool for the terror group.

Cantlie appears seated at a table in an orange jumpsuit, similar to those worn by Guantanamo Bay prisoners and other ISIS hostages. He lectures to the audience, criticizing Western policies towards ISIS, asking "After two disastrous and hugely unpopular wars in Afghanistan and Iraq, why is it that our governments appear so keen to get involved in yet another unwinnable conflict?" While he is clearly a hostage speaking under duress, his sister has said that he most likely believes "two-thirds" of what he is saying.

In a few videos separate from the series, Cantlie is portrayed as a Western journalist in regular clothing, reporting on 'favorable' conditions in Mosul and Kobani. Indeed, ISIS has used Cantlie to its advantage, turning him into a perpetual propaganda machine. (Sources: BBC, *Daily Mail*, RYOT News + Action)

John Cantlie in an episode of "Lend Me Your Ears" (Source: U.S. News)

January 12, 2015 / The Cyber Caliphate Attacks U.S. Sites

Hackers claiming allegiance to ISIS and calling themselves the "Cyber Caliphate" hack the Twitter and YouTube accounts of the U.S. Central Command (CENTCOM). They post threatening messages, upload recruitment videos, and release non-classified military documents.

One Tweets reads: "*AMERICAN SOLDIERS, WE ARE COMING. WATCH YOUR BACK. ISIS.*"

One of the Tweets includes a link to a 52-page spreadsheet titled "Retired Army General Officer Roster" which includes the emails and home addresses of many retired military officers. This case of doxing—the act of publishing people's personal information online—is seen not only as a direct threat to the individuals whose privacy is breached, but also as a form of psychological warfare.

The main suspect in the hacking is Junaid Hussain, a young man from Birmingham, England, who is believed to have been in Syria at the time of the hacking. Hussain pleaded guilty in 2012 for publishing former Prime Minister Tony Blair's address book. (Sources: *Bloomberg*, *Guardian*, *Washington Post*)

CENTCOM's hacked Twitter account (Source: *Washington Post*)

January 7-15, 2015 / French Websites Targeted

In the wake of the Charlie Hebdo shootings, ISIS sympathizers hack approximately 19,000 French websites. The hacked websites belong to French businesses, religious groups, universities, and municipalities, and are altered to display pro-Islamist images and messages. For example, the website belonging to the municipality of Ezansville, a commune in the north of France, is changed to read: "The Islamic State Stay Inchallah [sic]. Free Palestine. Death To France. Death To Charlie." The French Defense Ministry's website is also hit with a denial of service (DOS) attack, causing it to be temporarily unreachable. (Sources: *Daily Mail*, CNN Money)

May 2015 / Garland, Texas Attack

American men—one in Somalia and one in the United States—use Twitter and private messaging services to communicate about an attack on U.S. soil.

On May 3, 2015, two lone-wolf terrorists armed with assault rifles and hundreds of rounds of ammunition open fire outside of a "draw Mohammad" contest in Garland, Texas. One of the terrorists, Elton Simpson, is in contact over social media for months before the attack with a Somali-based Minnesotan jihadist named Muhammed Abdullahi Hassan, or "Mujahid Miski." Miski, well known to FBI officials, communicates regularly with Simpson on Twitter before the pair take their communication to private messaging services. Simpson also communicates with ISIS hacker Junaid Hussain publically over Twitter—as well as on secure communication platforms—according to U.S. government sources.

Ten days before the shooting, Miski propagates violence by explicitly calling for an attack on U.S. soil. He tweets: "The Brothers from the Charlie Hebdo attack did their part. It's time for brothers in the #US to do their part."

Eight days before the attack, Miski tweets to Simpson: "One individual is able to put a whole nation onto it's [sic] knees."

Shortly after the shooting—which wounds one security official and leaves Simpson and co-shooter Nadi Soofi dead—Miski tweets that he will miss his daily correspondence with Simpson. (Sources: CNN, ABC News)

August 2015 / The Cyber Caliphate and Targeted U.S. Airstrikes

ISIS hackers release the details of 1,400 Americans, including members of the Marines, the Air Force, NASA, the State Department, and the FBI. The details are tweeted and retweeted by ISIS supporters who urge lone wolves to hunt down and kill. (Source: *Guardian*)

On August 26, 2015, the United States confirms that it has targeted and killed Junaid Hussain. The U.S. had listed Hussain as a high priority target and placed him third on the Pentagon's kill list, only under ISIS leader Abu Bakr al-Baghdadi and British executioner Mohammed Emwazi. The U.S. accused Hussain of recruiting Westerners to ISIS and calling for lone-wolf attacks in their home countries. (Sources: *Sunday Times, Newsweek*)

September 2015 / ISIS Releases Cyber Security Handbook

ISIS releases an English-language handbook on how to take photos with false geographic location stamps, privately connect to sites such as Twitter, and connect to encrypted communication networks on mobile devices. The resource suggests messaging apps and browsers including: Firechat, TorBrowser, Orweb, Onion Browser, WhiteHat Aviator, Opera Mini, TrueCrypt, VeraCrypt, Hushmail, ProtonMail, Threema, Telegram, Surespot, Wickr, Linphone, and SpiderOak. The end of the resource reads: "This short guide ask God's faithfulness in it, and we hope to be published and participation on a wider scale." (Source: Wired)

Late September 2015 / ISIS on Telegram

ISIS begins to operate on the encrypted social media app Telegram. The terror group runs numerous "channels," which allow users to disseminate encrypted information to a large number of viewers. ISIS broadcasts announcements including claims of responsibility for attacks. Researchers warn that jihadists are also using the app to fundraise for ISIS, with users able to designate their donations toward specific weaponry.

ISIS uses Telegram to announce its responsibility for the October 31 downing of the Russian airliner over the Sinai Peninsula, as well as the November 13 Paris attacks and the March 22, 2016 Brussels attacks.
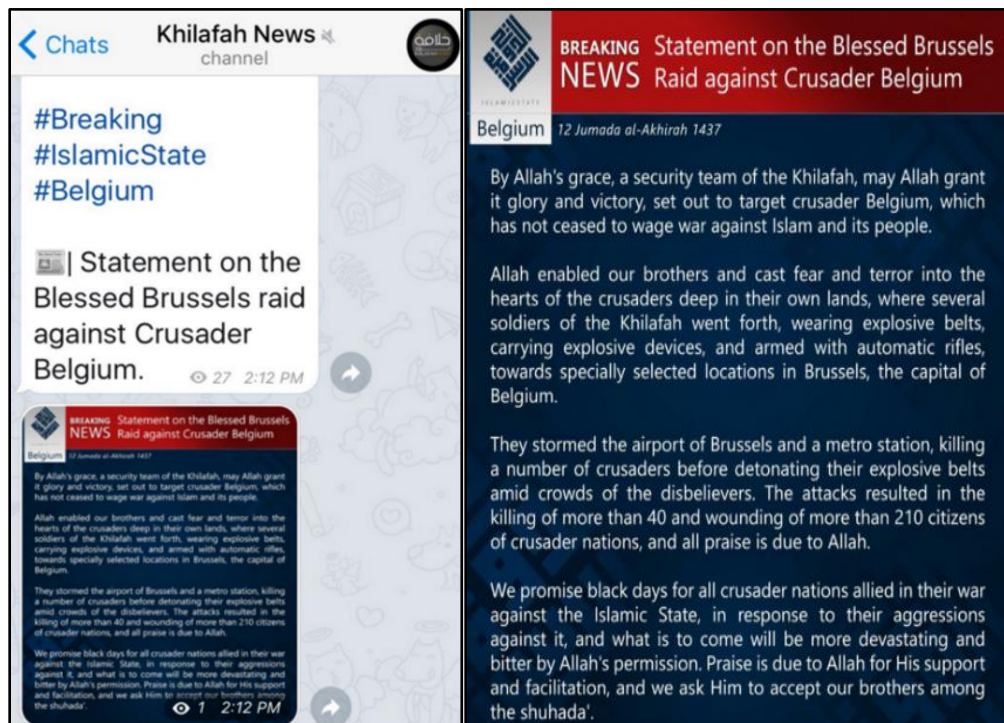
ISIS takes responsibility for the March 22, 2016 Brussels attacks via Telegram (Source: Twitter)

Telegram's founder Pavel Durov rebukes concern from law enforcement agencies regarding terrorists' use of the app. He claims that dying from slipping on a wet bathroom floor is 1,000 times more likely than dying from terrorism. He says, "Our right for private communication and privacy is more important than the marginal threats that some politicians would like to make us afraid of." (Sources: *Financial Times*, CNN Money)

September – December 2015 / The Debate on Social Media Responsibilities and Encryption Platforms

The Obama administration explores ways in which tech companies might allow law enforcement to decrypt coded messages on encrypted messaging platforms. The administration finds that although it is "technically feasible" for tech companies to provide agencies with decryption abilities, these solutions come with technical limitations. Law enforcement authorities urge tech companies to develop decryption abilities specific to their unique systems. These developments come amid a year-long battle between the Obama administration and encryption companies over government access to potentially crucial encrypted data in terrorism cases. (Source: *Washington Post*)

In October, the Obama administration steps down in its fight with tech companies. Obama announces that tech firms should not decrypt data for law enforcement agencies because it might expose users to abuse by Chinese and Russian intelligence agents, cybercriminals, and terrorists. FBI Director James Comey tells the Senate that the Obama administration will not seek legislation that would force tech companies to decrypt and share coded data. But the head of the FBI's Dallas unit, Tom Class, tells NBC that tracking terrorists and the new technologies they use is the "most significant issue right now with the FBI." (Sources: *New York Times*, *Washington Post*, NBC News)

The Obama administration changes course again in the wake of the November 13 Paris attacks and the December 2 San Bernardino shootings. The administration increases pressure on tech companies to grant law enforcement "backdoors," the codes needed to decrypt data.

The debate reignites as tech companies stand firm in their defense of encryption. Tech companies argue that creating a back door for the government would allow terrorists to exploit that vulnerability. The Software Alliance (BSA), a group representing some of the world's largest software providers, says, "Encryption - rather than something to be feared - is a valuable tool millions of people rely on every day to secure their online privacy." Meanwhile, numerous unnamed officials claim that the Paris terrorists used encrypted apps to plan the attacks. Investigators later name Telegram and WhatsApp as the apps most likely used by the perpetrators. (Sources: NDTV, Fortune, NPR, BGR)

Five days after the Paris attacks, Telegram tweets that it has blocked 78 ISIS-related channels in 12 languages. This is considered a major policy shift for the company, whose founder had previously diminished the threat of terrorists' use of the app. In an official statement, Telegram

says "We were disturbed to learn that Telegram's public channels were being used by ISIS to spread their propaganda." (Sources: Twitter, *Business Insider*)

In his address from the Oval Office on December 6, Obama says he will "urge high-tech and law-enforcement leaders to make it harder for terrorists to use technology to escape from justice," hinting that the Congress might propose legislation requiring tech companies to decrypt and share data. (Source: White House)

The female San Bernardino shooter pledges allegiance to ISIS on Facebook as the Wednesday morning attacks begin. It takes Facebook one day to act, finally removing her profile. A Facebook Inc spokeswoman says, "We don't allow people to praise acts of terror or promote terrorism. We also work aggressively to ensure that we do not have terrorists or terror groups using the site." The social media company reportedly cooperates with law enforcement following the incident. Facebook's head of content policy tells USA Today, "If we become aware of a threat of imminent harm or a planned terror attack, our terms permit us to provide that information to law enforcement, and we do." (Sources: Reuters, Wired, Fox Business, USA Today)

In the hours after the San Bernardino attack, a pro-ISIS Twitter account calling itself "Asawitiri Media" tweets: "California, we have already arrived with our soldiers. Decide how to be your end, with knife or bomb." The account is on its 335th iteration after continued suspensions by Twitter. (Source: *New York Times*)

On December 6, Hillary Clinton speaks at the Brookings Institution and urges social media and encryption communication services to remove, destroy, and "disrupt" terrorist content and activities on their platforms. "Resolve means depriving jihadists of virtual territory, just as we work to deprive them of actual territory," she says. "They are using websites, social media, chat rooms and other platforms to celebrate beheadings, recruit future terrorists and call for attacks. We should work with host companies to shut them down." (Sources: *New York Times*, *New York Times*)

Other voices join Clinton's. Donald Trump suggests asking Bill Gates to "close that Internet up in some way." On December 8, Sen. Dianne Feinstein (D-CA) and Sen. Richard Burr (R-NC) introduce legislation that would require social media companies to alert law enforcement agencies about terrorist activity on their sites. (Sources: *Fortune*, MSNBC)

Hany Farid, the chairman of computer science at Dartmouth College, says there's no "fundamental technology" limitation keeping social media companies from developing widespread tracking technologies. "This is a business or policy decision. Unless the companies have decided that they just can't be bothered." And even though Twitter says that it has teams "actively investigating reports of rule violations," Rita Katz from SITE Intelligence, a group that tracks online terrorist activity, says: "The bottom line is that Twitter is not doing enough." (Source: *New York Times*)

On December 9, FBI Director James Comey testifies at a Senate Judiciary Committee, calling for more cooperation between law enforcement and tech companies offering encryption services. While he does not provide details on the use of encryption apps during the recent attacks, ABC News reports that the couple responsible for the San Bernardino shootings used devices with "some form" of encryption, making it difficult for law enforcement to collect all personal information on the shooters. (Source: C-Span, ABC News)

Comey testifies that one of the two Garland, Texas shooters exchanged 109 encrypted messages with overseas terrorists on the morning of the May attack. "Before one of those terrorists left to try and commit mass murder, he exchanged 109 messages with an overseas terrorist. We have no idea what he said, because those messages were encrypted. And to this day I can't tell you what he said with that terrorist 109 times the morning of that attack. That is a big problem. We have to grapple with it," he says. (Sources: The Intercept, *Business Insider*)

November 13, 2015 / Anonymous vs. ISIS

Directly following the November 13 attacks in Paris that leave 130 dead, the international hacker group Anonymous declares a "war" on ISIS. The group releases a video in which a voice warns: "We will launch the biggest operation ever against you. Expect massive cyber attacks. War is declared. Get prepared. The French people are stronger than you and will come out of this atrocity even stronger."

While Anonymous has repeatedly targeted ISIS sympathizers online since the January 2015 *Charlie Hebdo* attacks, the group releases its biggest offensive yet, vowing to hunt down and expose the terror group's supporters.

Specifically, Anonymous operatives—who claim to operate internationally—report ISIS accounts to social media authorities and call for their removal. As of November 2015, the group has reportedly identified more than 39,000 ISIS accounts on Twitter, and has been instrumental in the suspension of at least 25,000 of these. The group does this by crowdsourcing to create a list of pro-ISIS social media accounts, which is then shared among Anonymous operatives. Anonymous also deploys automatic filter tools to search keywords on social media, as well as a bot to report accounts.

Ghost Security (Ghostsec), an offshoot of Anonymous, also works to remove extremist content online. Ghostsec carries out cyber-attacks (including "distributed denial of service," or DDoS attacks) of extremist websites, and reports extremist content to Facebook, Twitter, YouTube, and other social media sites.
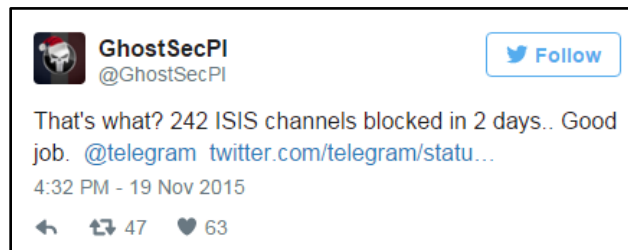
(Sources: *Independent*, *New York Times*, Reuters, *Foreign Policy*, Reuters)

Anonymous launches "OpParis" following ISIS's November 13 attacks in Paris
(Source: *New York Times*)

Ghostsec reports its role in blocking 242 pro-ISIS accounts on the social media site Telegram
(Source: *New York Times*)

November 2015 / Continued Hacking and Doxing Attacks

In revenge for Junaid Hussain's death in August, the "Cyber Caliphate" hacks more than 50,000 Twitter accounts, urging ISIS sympathizers on Twitter to take control of the accounts and spread the terror group's propaganda. The Cyber Caliphate also hacks and releases personal phone numbers of heads of the CIA, FBI, and NSA. The Cyber Caliphate tweets: "We need years to publish what we have…We will raise our flag in the heart of Europe." (Source: *Daily Mail*)

December 2015 / ISIS App

Ghostsec announces that ISIS has created an app for the Android phone called "Amaq Agency" in reference to the ISIS-affiliated Amaq News Agency. The app provides ISIS news and videos—including beheadings and battlefield victories—to its members and sympathizers. (Source: *Fortune*)

January 2016 / Kybernetiq Magazine

Jihadists take to Twitter and Telegram to disseminate the online "Kybernetiq" magazine—a new German-language periodical intended to instruct "muhajideen" on encryption and identity protection. An article in the magazine titled "Digital Branding" decries the weak security of oft-used encryption services—specifically jihadist-branded encrypted chat platforms.

"As a brother in Islam, I feel obliged in this post-Snowden era to strongly discourage crypto-programs with a mujahid branding. This includes programs like Asrar al-Mujahideen, Amn al-Mujahid, Asrar al-Ghurabaa and various mobile applications… The thoughtless use of specific software can reveal your identity. Software with weak or broken encoding algorithms can convey a false sense of security to you. Act inconspicuous and operate under the radar…Now it lies on you. Be attentive and always one step ahead of your enemies."

The magazine suggests using the Amnesic Incognito Live System commonly known as "Tails," as well as the GNU Privacy Guard encryption program. Tails—an operating system that ensures privacy and anonymity—can be used on personal computers via DVD or USB. The GNU Privacy Guard is a software application that encrypts all personal data and communications. It can be easily downloaded for free. (Sources: Site Intelligence, *International Business Times*, Tails, GnuPG)

The cover of the first issue of the German-language Kybernetiq magazine. (Source: Kybernetiq)

February – March 2016 / The FBI vs. Apple

The debate over encryption between tech companies and law enforcement agencies comes to a head. On February 16, a U.S. federal court—on the Justice Department's request—orders Apple to aid the FBI in unlocking the iPhone of Syed Rizwan Farook, one of the shooters in the December 2 San Bernardino terrorist attack.

Farook owned an iPhone 5c. Like all newer iPhones, 10 failed passcode attempts results in a wipe of the phone's data. The FBI requests Apple's aid by allowing the government to enter an unlimited number of passcode attempts. This "brute force" attack requires time and persistence in trying a multitude of passcodes, commonly entered with the help of a computer. FBI Director James Comey says, "We simply want the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it. We don't want to break anyone's encryption or set a master key loose on the land." (Sources: *New York Times*, *Los Angeles Times*, Reuters)

Apple remains staunchly opposed to the court order. On February 17, Apple CEO Tim Cook sends a letter to his employees, stating, "The case is about much more than a single phone or a single investigation. At stake is the data security of hundreds of millions of law-abiding people, and setting a dangerous precedent that threatens everyone's civil liberties." But the FBI argues that it is requesting access to Farook's iPhone only, and not to iPhones everywhere. "I hope folks will take a deep breath and stop saying the world is ending, but instead use that breath to talk to each other," Comey says. (Sources: *New York Times*, *Los Angeles Times*, Reuters)

In an official statement, the Justice Department says, "It is unfortunate that Apple continues to refuse to assist the department in obtaining access to the phone of one of the terrorists involved in a major terror attack on U.S. soil." (Source: CNN)

A Pew Research Center survey conducted in the days following the court order finds that 51 percent of Americans believe Apple should assist the FBI in unlocking the iPhone. According to the poll, 38 percent say Apple should not unlock the phone, and 11 percent have no opinion. (Source: Pew Research Center)

On March 21, the FBI announces that it may not need Apple's help in unlocking Farook's iPhone, which is in government custody. Reports emerge that an Israeli tech firm specializing in data extraction, called Cellebrite, is helping the FBI unlock the iPhone. (Source: Reuters)

One week later, on March 28, the FBI says that it has successfully unlocked the iPhone without Apple's help and has filed to drop the court case. Details regarding the data extraction—including which company may have helped the government in unlocking the phone—are not revealed. The nearly two-month row between the government and the tech giant constitutes an important chapter in the debate on privacy versus security. (Source: *New York Times*)

June 2016 / French Jihadist Broadcasts Rant on "Facebook Live" Following Murder

French extremist and ex-convict Larossi Abballa murders a senior police official and his partner in their home in Magnanville, a small town northwest of Paris. After stabbing the couple to death, Abballa opens his smartphone and records himself using Facebook Live, a feature that allows Facebook users to produce live stream videos for view on their profiles. Abballa broadcasts a 12-minute rant in which he pledges allegiance to ISIS leader Abu Bakr al-Baghdadi, cites his motives for the attack, and calls for further attacks on French targets. While filming, he also questions what to do with the couple's three-year-old child, saying, "I don't know what I'm

going to do with the boy." Police storm the residence hours later, killing Abballa and rescuing the child. ISIS claims responsibility for the attack. (Sources: Combating Terrorism Center, Reuters, *Daily Mail*, *Guardian*)

Mid-Late 2016 / French Foreign Fighter Directs Domestic Attacks in France Via Telegram

Syrian-based Frenchman Rachid Kassim grows increasingly popular among French jihadists on Telegram, where he circulates attack plots and lists of targets inside France. Kassim is also believed to host a group chat on Telegram called "Sabre de Lumiere," or "Sword of Light," which allows him to communicate with French-based extremists. French officials believe Kassim directly communicates with Larossi Abballa, allegedly influencing the latter's 12-minute rant on Facebook Live following the June 2016 murders in Magnanville. French officials also suspect that Kassim uses Telegram to help introduce Abdel-Malik Petitjean to Adel Kermiche who, in late July 2016, murder an elderly priest in Normandy on behalf of ISIS. Kassim also reportedly uses Telegram to introduce three French women who are arrested in September 2016 for parking an explosive-laden car next to the Notre Dame Cathedral. (Sources: Combating Terrorism Center, Jihadology, BBC News, BBC News)

March 15, 2019 / New Zealand Mosque Attacks Livestreamed on Facebook

A gunman wearing a helmet-mounted camera goes on a shooting spree at the Al Noor Mosque in Christchurch, New Zealand, and the Linwood Mosque in a suburb three miles away, killing at least 50 and wounding 50 others. The attacker livestreams the attack on Facebook. The video also shows the gunman preparing for the attack with semiautomatic weapons brandishing neo-Nazi slogans. The attacker continued to shoot at people from his car when police dragged him out and arrested him. The suspect is identified as Australian citizen Brenton Tarrant, who had posted a manifesto on his Facebook page claiming responsibility shortly before the attacks began. He is charged with murder. (Sources: *New Zealand Herald*, *Wall Street Journal*, *Wall Street Journal*, CNN, CNN, CNN, CNN, *Washington Post*, CBS News)

Facebook deletes the video and the attacker's Facebook and Instagram accounts but only after police notify the company. Despite claims by Facebook, Twitter, and YouTube to contain the video, it continues to circulate online. Facebook subsequently responds to critics by cherry-picking statistics. The company claims that it removed 1.5 million videos from its site within the first 24 hours of the attack and that 1.2 million of those were blocked before upload, but fails to explain why 300,000 videos were not caught by Facebook's content moderation systems. Police urge the public not to share the 17-minute video of the attack. News outlets largely refuse to show the video and analysts warn that sharing the video only helps terrorism. (Sources: *Wall Street Journal*, CBS News, Twitter, TechCrunch)