Digital Counterterrorism: Fighting Jihadists Online

March 2018

Task Force on Terrorism and Ideology

Co-Chairs

Governor Thomas H. Kean
Former Chairman, 9/11 Commission; Former Governor of New Jersey

Representative Lee H. Hamilton
Former Vice Chairman, 9/11 Commission; Former Representative from Indiana

Staff

Blaise Misztal
Director of National Security

Nicholas Danforth
Senior Policy Analyst

Michael Hurley
Contributor

Jessica Michek
Policy Analyst

Table of Contents

4 **Introduction**

5 **Social Media**
5 Terrorists' Use of Social Media
8 Counter-Messaging
10 Removing Jihadist Messages

15 **Encryption**
15 Strong Encryption Since the Snowden Leaks
16 Terrorists' Use of Encrypted Communications
18 Addressing the Encryption Challenge

20 **Implications for Policymakers**

26 **Conclusion**

27 **Appendix A**

30 **Endnotes**

Introduction

Mohammed Yazdani seemed to be on the path to success. As *The New York Times* reported, despite being born in a poor area of Hyderabad, India, he had earned an engineering degree and landed a job in Saudi Arabia, where he worked for four years.[1] During his time abroad, Yazdani was captivated by the Islamic State's lightning-quick military advance and sophisticated online propaganda. Inspired to join the caliphate, he "logged onto Twitter and searched the hashtags #ISIS and #Khilafa," quickly making contact with an Islamic State (also known as ISIS) recruiter. The conversation then hopped over to Telegram, an encrypted messaging service. Using Telegram and other encrypted messaging applications, ISIS planners helped Yazdani recruit conspirators, locate weapons caches that had been prepositioned around India, swear allegiance to ISIS, and attempt to manufacture explosives.

> *"It is impossible to conclude that the enemy has been defeated. Rather, the threat of terrorism has metastasized."*

Fortunately, Indian police rolled up the new cell before it could strike. The case nevertheless illustrates how new technologies have dramatically expanded terrorist groups' global reach. Social media allows terrorist groups to distribute propaganda—including slickly produced videos and Instagram-ready photo streams—and to recruit potential followers instantly, at no cost, anywhere in the world. Encrypted messaging applications provide no-cost global communications secured by virtually unbreakable cryptography—a level of secure communications previously available only to the most advanced states. In the battle against jihadist terrorism, the digital world is the new ungoverned territory. To prevail, governments will have to deny jihadists the ability to operate securely in these digital realms.

Social Media

Social networks are less than two decades old, yet it is no overstatement to say that they have already reshaped many aspects of modern life. No earlier medium combined such a vast audience with social media's personalized experience, tailored by sophisticated algorithms to each user's interests—or, skeptics would argue, to each user's cognitive susceptibilities. That social media can influence and even drive world events is now beyond dispute. The 2016 U.S. presidential election is one of many examples: The Trump campaign, despite its lower budget, deftly used Facebook and other social-media tools to reach voters with micro-targeted, personalized messages. "Ineffective ads were killed in minutes, while successful ones scaled. The campaign was sending more than 100,000 uniquely tweaked ads to targeted voters each day."[2] Meanwhile, entities linked to the Russian government ran "scores" of paid ads on Facebook and Twitter; the polarizing ads, which appealed to both the left and right, reached hundreds of thousands, if not millions, of Americans.[3]

Terrorists' Use of Social Media

Terrorists have always adapted new technologies to their purposes, and social media is no exception. Indeed, social media has proved particularly well-suited for terrorist propagandizing and recruiting for several reasons.

> *"Social media has proved particularly well-suited for terrorist propagandizing and recruiting for several reasons."*

First, social media enables terrorists to communicate radicalizing messages to a far wider circle of potential adherents than they could have reached with traditional media. Previously, radicalization required personal contact with someone who could provide materials, ideological grooming, and connections to wider jihadist networks. Decades ago, when the global jihadist movement was in its infancy, the followers of radical clerics circulated their sermons on audiotapes, reproduced one at a time and passed from one follower to another. Desperate to reach a wider audience from his bases in Sudan and Afghanistan, Osama bin Laden faxed his diatribes and fatwas to media outlets in London.[4] Today, social-media platforms like Twitter, Instagram, Facebook, and YouTube offer the ability to instantaneously convey one's message to users around the world, often in the form of captivating images or video. What's more, unlike hosted websites, which one might argue also offer global reach, these services are free, user-friendly, and most can be used pseudonymously. While terrorists have used password-protected forums since the beginning of the internet age, the pool of potential recruits, supporters, or sympathizers that can be reached on social media is vastly larger than the pool of potential visitors to a password-protected forum. As senior Homeland Security Department official Robin Taylor noted in recent testimony, "The reach and popularity of social media has enabled HVEs [homegrown violent extremists] to connect more easily with terrorist organizations, such as ISIS."[5] A senior FBI official echoed that concern: "Through the internet, terrorists overseas now have access into our local communities to target and recruit our citizens and spread the message of radicalization to violence faster than we imagined just a few years ago."[6] Put simply, social media allows terrorists to recruit and propagandize across borders, in a way that 20th-century technology never allowed.

Another salient feature of social media, less obvious but highly relevant for terrorists, is that on social-media platforms all content looks more or less the same. With modest exceptions (Twitter's blue check mark, for example), content posted to a social-media platform by a veteran investigative journalist or a Harvard-trained physicist bears the same visual indicia of reliability as content posted by a fringe conspiracy theorist. On social media, there are no editorial gatekeepers, nor is cost a barrier to entry.

Instead, production value serves as the most readily available indicator of quality, and terrorists have grown adept at using desktop software to turn out propaganda materials that are as polished as traditional media. An analysis of American jihadists by the Program on Extremism at George Washington University found, "Two features that seemed to distinguish the media operations of IS [Islamic State] from previous jihadist organizations' material was their professional-quality productions and their ability to disseminate this content through social media."[7] As one researcher found, based on 30 days of following ISIS propaganda at the height of its pseudo-caliphate: "In just 30 days, IS's official propagandists created and disseminated 1,146 separate units of propaganda. Photo essays, videos, audio statements, radio bulletins, text round-ups, magazines, posters, pamphlets, theological treatises, … [r]adio bulletins and text round-ups were released in six languages. … All of it was uniformly presented and incredibly well-executed, down to the finest details."[8] Much of this material is designed to influence young men of prime recruiting age, for whom social media is the most important information source.[9] Meanwhile, the "multi-lingual approach IS implements" in its propaganda has another "clear objective: targeting non-Arabic speaking potential recruits."[10] This seems to have worked. Danish researchers found "that the foreign fighter flow to Syria [was] younger than for past conflicts, with typical recruits being between 16 and 25 years old—a prime social media age."[11]

Another advantage of social media is that it enables terrorist sympathizers to engage directly, and publicly, with more credible figures, hijacking those figures' visibility to amplify the terrorists' own messages. Sometimes this means riding in the wake of a more-prominent user's messages, a now familiar tactic for social-media self-promotion; "being the first to reply to a Trump tweet," for example, "promises someone an enormous audience."[12] But it can also entail baiting, debating, or harassing more prominent figures, to gain prominence or to win plaudits from like-minded users. Terrorist propagandists have capitalized on this aspect of social media, eagerly trading rhetorical salvos with U.S. government accounts. For example, the State Department's widely derided "Think Again Turn Away" Twitter account traded snarky jabs with ISIS sympathizers, inadvertently "providing jihadists legitimacy and a stage on which to project their messages."[13] Since 2015, the State Department's counter-narrative strategy has shifted "away from the earlier, 'snarky' tone and toward a fact-based message."[14] But the program remains emblematic of the risks and unintended consequences of counter-messaging campaigns in the era of social media, a decentralized ecosystem in which lumbering bureaucracies have frequently been bested by leaderless swarms of like-minded individuals.

The final reason why social media is such an effective amplifier for terrorists is the power with which platforms' algorithms connect users to content that resonates with their existing inclinations and preferences. Columbia University Professor Tim Wu has dubbed the internet giants that control the major social-media platforms "attention merchants"; like newspapers and television networks before them, their business models depend on selling advertising, which means that their profits depend on attracting as much of users' scarce attention as possible. Social-media platforms possess two assets that enable them to capture attention more durably than any prior medium: reams of detailed, personal information about their users' preferences, and algorithms

that analyze that data to determine what the user wants to see, read, or buy. This enables them to tailor the content the user sees in order to keep the user glued to the platform. The news that Facebook users see in their news feed "is personalized based on past clicks," including the "like" button, and on an items' popularity among other users with similar preferences.[15] Similarly, Google sorts and filters search results based on the user's "location and previous searches and clicks."[16] Engineers working on YouTube's recommendation engine, which determines which videos a user will see in the "up next" column, "continuously experiment[ed] with new formulas that would increase advertising revenues by extending the amount of time people watched videos."[17] The result, according to sociologist and technology expert Zeynep Tufekci, is that "the videos recommended and auto-played by YouTube get more and more bizarre or hateful."[18] Ensconced in a "filter bubble" created by algorithms designed to give the user what he or she wants, a user may rarely, if ever, encounter any opinion with which he or she disagrees. Indeed, this effect tends to become more pronounced over time: As the platforms acquire more information about the user's exact preferences, the algorithms become progressively better at anticipating the user's desires.

The result is that the sharpest-edged, least-nuanced content, which tends to be the most emotionally resonant, is also the most widely disseminated. Illustrative Facebook news feeds produced by this approach look less like traditional newspapers and more like "red" and "blue" propaganda channels, as a recent *Wall Street Journal* feature illustrated.[19] Users become enmeshed in feedback loops that confirm, and therefore *strengthen*, their preexisting beliefs about the world—their hatreds, their fears, their preferred accounts of the causes of their grievances, and their sense of what is to be done.

To be sure, the process of radicalization in online echo chambers resembles radicalization in any other closed environment: The vulnerable mind is fed a steady diet of narrative, cherry-picked facts, and encouragement to act, all of which point in the same direction. The difference is that analog-era radicalization required direct contact with a tutor who would personally lead the recruit down the intellectual and emotional path away from past associations and beliefs and toward radicalism. For example, as al Qaeda's message began to spread in the late 1990s and early 2000s, mainstream Islamic leaders and counterterrorism officials feared that radicalization was occurring in intimate "storefront" mosques, often beyond the control of established Islamic authorities, where young men fell under the influence of a charismatic radical preacher. Ironically, in 2000, Dar Al-Hijrah, a large mosque in Northern Virginia, hired future terrorist recruiter Anwar Awlaki as an imam to lure young men away from such a storefront mosque, Dar Al-Arqam.[20] Osama bin Laden was groomed by a Muslim Brotherhood-affiliated teacher at the school he attended as a boy in Saudi Arabia.[21] Social media creates a similar intellectual and emotional climate, enabling radicalization without the need for direct personal contact. As such, it dramatically expands the set of young Muslims vulnerable to radicalization; anyone with an internet connection can now receive the jihadists' call.

Social media has also given sympathizers a new way to support jihadist causes without committing or financing attacks themselves. This new class of "virtual [terrorist] entrepreneurs," as Seamus Hughes and Alexander Meleagrou-Hitchens have described them, have "acted in a more auxiliary capacity, plugging their Western contacts into wider extremist milieus (both online and offline) and encouraging extreme beliefs, while offering suggestions and options for mobilization."[22] Sometimes the assistance extends to the direct planning of an attack, but often "encouragement, reassurance, and comradery" is all a potential terrorist needs. Hughes and Hitchens describe an extensive U.S.-based network of such virtual entrepreneurs, who were linked to ISIS propagandists and planners in Syria. Jalil ibn Ameer Aziz "was heavily involved in online extremist networks, creating at least 57 pro-Islamic-State Twitter accounts."[23] When he was

arrested, authorities found a stash of high-capacity magazines and ammunition in his home in Pennsylvania. Aziz served as a node connecting Junaid Hussain, a notorious online propagandist and recruiter based in Syria, with Americans interested in carrying out attacks on behalf of the Islamic State. Safya Yassin, a Missouri woman, used at least 97 Twitter accounts to spread ISIS propaganda; she even tweeted the names and addresses of three federal employees under the words "Wanted to Kill."[24] Elton Simpson, one of the two men who attacked a free-speech event in Garland, Texas, in 2015, "had been in direct contact with at least two virtual entrepreneurs using Twitter direct message and SureSpot," an encrypted messaging application.[25] With social media as a meeting place, it is easy for curious and disaffected young people to connect with such online facilitators. These facilitators, in turn, are often only one step removed from operational terrorists, who, if needed, can provide the specific direction or know-how to execute an attack.

But while social media offers terrorists valuable capabilities, it also brings vulnerabilities. Foreign fighters' ostentatious use of social media in Syria—documenting their violent exploits like a grisly reality show—helped inspire new recruits to travel to the pseudo-caliphate, but it also handed reams of open-source materials to Western intelligence services. As many millennial job applicants have found out, personal details posted on social media can be discovered by anyone, to the user's detriment. Foreign-fighters' selfies and social-media bragging may have drawn new recruits, but the accounts also gradually "[went] silent, presumably as their owners [we]re killed," many in U.S. airstrikes.[26] Information in the posts helped intelligence agencies and other analysts to locate individual terrorists, observe how terrorist groups operated in Syria, and learn how foreign fighters traveled from Europe to Syria. Private messages sent on these platforms were vulnerable to surveillance by Western officials—leading terrorist groups to shift most of their communications to encrypted platforms, a trend discussed later in this report. Social networks provide a detailed map of who is linked to whom in a given organization or movement—a basic task of intelligence analysts seeking to understand a terrorist group. And if the first stages of recruiting take place on a publicly visible forum, counterterrorism operatives have an opportunity to identify potential recruits in real time and either divert them away from terrorism or recruit them as potential double-agents.

Counter-Messaging

Governments were initially caught off guard by the Islamic State's sophisticated social-media campaign, but they quickly began to contest this virtual terrain. One element of governments' response has been counter-messaging: attempting to refute or undercut the messages propagated by terrorist groups and their sympathizers. Those efforts, while laudable in theory, have struggled in practice. More recently, governments and the social-media platforms themselves have shifted their focus away from competing with terrorists in the marketplace of ideas and toward denying terrorists the ability to use prominent platforms for recruiting and propaganda.

In the wake of the Islamic State's blistering ascent, the State Department's Center for Strategic Counterterrorism Communications (CSCC) began to aggressively challenge ISIS and its sympathizers and amplifiers on social media.[27] The center's aim, explained then-head Ambassador Alberto Fernandez, was "not to make people love the U.S.," but "to make al-Qaeda look bad."[28] That approach was informed by the Bush administration's experience attempting to boost the positive image of the United States in the Middle East using such traditional news media as radio and television. The U.S.-created broadcasters Al Hurra TV and Radio Sawa were intended to "improve America's image in the Middle East," but "a 2006 study of university students in five Arab countries … found their attitude toward U.S. foreign policy *worsened* after tuning into the channels."[29] Given that experience, it made

sense to pursue a "negative" campaign focused on bringing down the Islamic State's favorability, rather than quixotically seeking to persuade committed or potential Islamic radicals to favor the United States.

Unfortunately, the CSCC's direct online engagement with terrorist groups and their sympathizers had unintended and unhelpful effects. By directly debating previously obscure jihadist sympathizers, the U.S. government inadvertently elevated their status, allowing them to build their credibility by directly confronting the hated enemy. Conversely, critics believed that some of the CSCC's activities eroded the prestige of the U.S. government. Trading snarky, juvenile jabs on Twitter with jihadist nobodies was beneath the dignity of the State Department. What's more, posting grisly videos that incorporated brutal ISIS propaganda, like the CSCC's infamous "Welcome to ISIS Land" montage, raised ethical concerns.[30] In 2016, the CSCC's responsibilities were transferred to a new, interagency "Global Engagement Center" (GEC) also housed at the State Department. The GEC has used social media to micro-target users vulnerable to radicalization, but experts have questioned its effectiveness.[31] More recently, the GEC has stalled under the Trump administration; the GEC is a casualty of doubts about its value and disputes about Russian propaganda and its effect on the 2016 election.[32]

Counter-messaging efforts outside the State Department have been even less successful. WebOps, a Defense Department program created to thwart ISIS propaganda and dissuade potential recruits, was an expensive fiasco. Program employees described to the *Associated Press* "multiple examples of civilian Arabic specialists who have little experience in counter-propaganda, cannot speak Arabic fluently and have so little understanding of Islam they are no match for the Islamic State's online recruiters."[33] Translators repeatedly confused the Arabic words for "authority" and "salad," referring to the Palestinian Authority as the "Palestinian salad," eliciting ridicule from the very audience the program aspired to persuade. Operators also lacked adequate knowledge of sectarian or local variations in Islamic practice and the language used to describe it. By contrast, the jihadists and sympathizers with whom they were debating were adept at deploying religious doctrines and attuned to the linguistic and cultural subtleties that tripped up the U.S.-based contractors. As the *Associated Press* put it, "Engaging in theological discussions on social media with people who are well versed in the Quran is not for beginners."[34]

This speaks to a broader challenge in post-9/11 efforts to counter Islamist ideology: Western governments' lack of fluency in the languages, ideas, traditions, history, and mores of the Islamic world. In the Cold War, the battle of ideas was fought largely *within the West*, between economic and governmental systems that were both the products of Western thought. In the struggle against Islamist terrorism, the arguments that move public opinion draw upon traditions that few Americans understand, often expressed in languages that few Americans have mastered.

These epistemic limitations are especially problematic for counter-messaging operations that take place on social media. Verbal combat on Twitter calls for the quick stings of a yellow jacket, not the cautiously aimed salvos of an artillerist. There is no time to pause to consult an expert. And because the volume of jihadist messages is so huge, it takes a swarm of yellow jackets, not just a few. Yet precious few Americans have the cultural, linguistic, and religious fluency to beat a jihadist sympathizer on these terms. Ideally, these few would have been recruited into higher-value intelligence and counterterrorism work than tweeting snark at jihadist fanboys.

Another defect in U.S. approaches to countering ISIS messages is that ISIS, in contrast to al Qaeda, has been less concerned with building support and consent among Muslim populations. As terrorism expert William McCants explained, ISIS's strategy is to use fear and violence to cow populations

into submission, not to win hearts and minds.[35] For that reason, highlighting ISIS's violence against other Muslims, as the State Department did in YouTube videos like "Welcome to ISIS Land," did not necessarily undermine the Islamic State's message among its target audiences: young men, whom it hoped to recruit, and local populations, whom it hoped to intimidate. In the words of McCants: "When we advertise the Islamic State's brutality, the Islamic State loves it."[36] This may change, however, with the collapse of the Islamic State's territorial caliphate. Now that ISIS has reverted from a quasi-state, which can command and extract resources from its population through terror, back to being a clandestine insurgency, a reputation for brutality to fellow Muslims may become a liability rather than an asset.

A final downside of a focus on counter-messaging is that salvos of saucy social-media messages—as if Twitter and Facebook were themselves fields of battle—obscured the underlying factors that drove some Muslims to support the Islamic State's messaging and most others to ignore or oppose it. To be sure, the channels of communication and persuasion are important, but it is the underlying content of the messages and the receptiveness of those who see them that ultimately determine whether and how the recipients act. As former CSCC Chief Richard LeBaron put it, "We count tweets and forget that they are just tweets—they are not a very good indicator of ISIS recruiting abilities." He argued:

> *Social media provides access to a large audience but it rarely is an independent force that mobilizes an individual to take off for the Turkish border. Otherwise there would be a lot more recruits. Motivations for taking the step from sympathy for a cause to individual action are varied: personal circumstances of social isolation, resentment in one form or another, the urge to "do something" in the face of persecution of fellow Muslims, the lack of other things to do, and political marginalization. The motivation of a former Iraqi army major is quite different from that of a teenager from Wales.*[37]

On the other hand, it may be that America's ability to influence the underlying "motivations" that compel individuals to action are very constrained, and that online counter-messaging operations directed at the small number of "people on the cusp of radicalization who live in a constructed world of conspiracy and isolation" are thus a reasonable, cost-effective, relatively low-risk way to target that decisive group. And to be fair to the CSCC, and other U.S. government entities that have undertaken counter-messaging efforts in social media, this discipline is still in its infancy. Finding viable formulas for counter-messaging, particularly in the unique environment of social media, will take trial and error, which means that some flops are inevitable.

Removing Jihadist Messages

Alternatively, it may be that the primary lesson of these struggles is that counter-messaging is not the right way to prevent terrorists from exploiting social media; instead, denying them that forum outright may be more effective. That seems to be the lesson Western governments have drawn. In recent years, attention has shifted to removing terrorist content from social-media platforms, rather than seeking merely to debunk or discredit it.

Because "terrorist content" is often political speech, this raises constitutional concerns. European countries' constitutions give them substantial latitude to prohibit speech where doing so advances social cohesion. Germany and France, for example, have long criminalized Holocaust denial and *Mein Kampf* only recently went back on sale in Germany after being banned for decades.[38] European governments have also used prohibitions against "hate speech" or "incitement" to criminalize speech that maligns recent immigrants or religious or ethnic minorities.

Given these more permissive constitutional frameworks, European nations have more latitude than the United States in mandating that social-media platforms remove jihadist

speech. The most notable new effort in that vein is Germany's 2017 *Netzwerkdurchsetzungsgesetz (NetzDG)*, which requires companies to take down "hate speech," including terrorist speech, within 24 hours in the case of "obviously illegal" speech and seven days in closer cases.[39] Facebook "now has more than 1,200 people based in Germany helping it to check content, part of a global team it has rapidly expanded to around 7,500."[40] In June 2017, France and the United Kingdom jointly announced that they are "exploring the possibility of creating a new legal liability for tech companies if they fail to remove content," including "penalties such as fines for companies that fail to take action."[41]

In the United States, by contrast, the First Amendment to the Constitution provides that "Congress shall make no law … abridging the freedom of speech," and the U.S. Supreme Court has consistently held that this includes speech that offends, insults, or foments hatred. As relevant here, even speech that advocates the use of force, lawbreaking, or the overthrow of the government is protected, "except where such advocacy is directed to inciting or producing *imminent lawless action* and is likely to incite or produce such action."[42] And while much jihadi speech surely is directed to "producing imminent lawless action," other constraints make it difficult for the government to legislate prospectively to effectively target that speech. For example, courts will not permit the government to enforce criminal laws that are unconstitutionally vague, fail to provide fair notice of what is criminal, or are "overbroad" in that they would bar a substantial amount of constitutionally protected speech in addition to unprotected speech.[43] Requiring companies to screen messages for illegal content before publishing them would be even more fraught: "Prior restraints" banning publication outright are even more constitutionally disfavored than after-the-fact punishments for prohibited statements.[44]

Nonetheless, some legal experts have floated theories that would allow social-media companies to be held liable for permitting jihadist content on their platforms. The families of victims of several terrorist attacks have sued social-media companies, arguing that the companies provided "material support" by permitting terrorists to use their platforms. The plaintiffs also claim, with support from some legal experts, that Section 230 of the Communications Decency Act, which shields internet platforms from liability for user-created content, should not apply to the act of knowingly permitting terrorist groups to maintain accounts.[45] Thus far, however, Section 230 has been held to bar these suits.[46]

A more promising vein of progress, in both the United States and Europe, is voluntary cooperation by social-media companies to remove extremist content. Social-media platforms are owned by private companies, which are not subject to constitutional free-speech guarantees. Executives of these companies have a personal motivation, as citizens, to help their governments combat terrorism to the extent that such cooperation is consistent with their other personal and corporate values. Other incentives favor such cooperation as well: Legitimate users and advertisers dislike being associated with jihadist materials. And these corporate behemoths have powerful economic incentives to get on well with the governments that regulate their businesses and that can threaten harsh sanctions, such as tax crackdowns, antitrust investigations, data-privacy regulation, and more. Voluntarily taking down terrorist content is an unobjectionable way to get on the government's good side.

In the wake of horrific terrorist attacks in Europe in 2015 and 2016, Facebook, Twitter, and Google responded to European pressure by stepping up efforts to remove extremist content from their platforms. In 2015, French Interior Minister Bernard Cazeneuve excoriated U.S. internet companies for their failure to police extremist content. A year later, he praised their cooperation, declaring in January 2016, "There is now a wide-ranging and effective dialogue based on mutual trust between the French government and Internet companies."[47] In February 2016, Twitter announced that it had suspended more than 125,000 accounts since mid-2015 for "threatening or

promoting terrorist acts";[48] in June of that year, Facebook, Twitter, YouTube, and Microsoft agreed with the European Commission to adhere to a "code of conduct" for combating "illegal online hate speech."[49] Under the code of conduct, the companies committed to working toward the goal of "review[ing] the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remov[ing] or disabl[ing] access to such content, if necessary," and to creating processes and providing information to ensure that such content is identified, efficiently reviewed, and removed.[50]

With attacks in Europe continuing, however, pressure on the companies to address extremists' use of their platforms has continued to mount. A 2017 report by the U.K. House of Commons' Home Affairs Committee found that "nowhere near enough is being done" and that "the biggest and richest social media companies," including Google, Facebook, and Twitter, were "shamefully far from taking sufficient action to tackle illegal and dangerous content."[51] After Britain's third terrorist attack in 2017, Prime Minister Theresa May placed responsibility directly on tech companies: Governments, she argued, "cannot allow this ideology the safe space it needs to breed. Yet that is precisely what the internet and the big companies that provide internet-based services provide."[52]

Facebook, Google, Twitter, and Microsoft responded by creating the "Global Internet Forum to Counter Terrorism," intended to "share technical solutions for removing terrorist content, commission research to inform their counter-speech efforts and work more with counter-terrorism experts."[53] Facebook also announced in June that it would "bolster its automated and human-powered efforts to flag and take down extremists' posts," increasing the number of humans on its "community operations" team, and deploying artificial-intelligence tools to "keep certain images and videos that have been flagged from being uploaded again."[54] Google recently revealed that it had "begun removing from YouTube extremist videos that do not depict violence," including the videos of influential radical preacher Anwar Awlaki, who became a prominent recruiter for al Qaeda in the Arabian Peninsula before being killed in a U.S. drone strike.[55]

In the once-Sisyphean task of keeping terrorist content off their platforms, the companies are using their technological mastery to become faster and nimbler than the terrorists. Techniques like "hash sharing," which "allows a company that discovers terrorist content on one of [its] sites to create a digital fingerprint and share it with the other companies," means that once terrorist content is identified, it can quickly be barred from every platform.[56] Because of this and other technological advances, Google's general counsel reported in September 2017 that "75 percent of the violent extremism videos" the company had "removed in recent months were found using technology before they received a single human flag."[57] Meanwhile, "Facebook is using new advances in artificial intelligence to root out 'terrorist clusters' by mapping out the pages, posts, and profiles with terrorist material and then shutting them down."[58] Just one year ago, terrorists could post new material faster than human moderators could review, identify, and remove them; now, automation is making this a much closer contest.

During a visit to Washington in November 2017, U.K. Home Secretary Amber Rudd acknowledged significant progress, noting that companies were now taking down roughly two-thirds of violent terrorist material within two hours of its discovery and that ISIS was now "struggling" to get some materials online.[59] Between January and June 2017, Twitter "suspended almost 300,000 terrorist accounts," of which 75 percent were blocked "before their first tweet."[60] Blocking appears to be effective, despite the fact that terrorists quickly create new accounts to replace those suspended: Research suggests that "after suspension," "returning accounts" fail to gain the same level of traction they once enjoyed, and the number of English-language tweets by ISIS sympathizers has fallen by around 50 percent.[61] (Blocking is only one possible

cause of this decline; users who previously generated substantial numbers of pro-ISIS tweets in English may have migrated to other platforms, or simply lost enthusiasm for ISIS as it hemorrhaged territory in Iraq and Syria. Some may even have been killed themselves during coalition military operations.) Energetic cooperation by platforms to remove content has produced results, and it has likely forestalled government efforts to impose legal mandates.

Nonetheless, radicalizing individuals are still able to access terrorist materials online. The Uzbek immigrant who killed eight in a Manhattan truck attack had "90 videos and 3,800 photos of ISIS-related propaganda on one of two cell phones found in the truck he had rented."[62] The Bangladeshi man who attempted to conduct a suicide bombing in New York's Port Authority bus terminal reportedly downloaded bomb-making instructions and read al Qaeda in the Arabian Peninsula's English-language *Inspire* magazine on the internet, prompting New York Governor Andrew Cuomo to "urge Internet companies to reassess their approach to extremist content."[63] Similarly, the bomber who killed 22 at a concert in Manchester, England, in May 2017 "used YouTube videos to learn how to build the explosive device."[64]

One challenge is that material is frequently posted in multiple places, including, ironically, on sites that host it for purposes of counterterrorism analysis. After December's Port Authority bombing, police officials criticized Google and even academic institutions that host this material; in the words of one New York Police Department deputy commissioner, "You can't make the argument that, well, maybe some scientist wants to learn this."[65] Another is that certain non-terrorist content with legitimate news value—videos of Syrian Islamism militias in combat, for example—can serve as an online gathering point for terrorist recruiters and curious neophytes open to radicalization. From there, a user "commenting on" the unblocked videos might then receive "a short-term link to a private discussion on an encrypted platform such as Telegram," where terrorist content is readily available.[66] This echoes Peter Neumann's concern, paraphrased by CNN, that "efforts by major social media firms to crack down on extremist accounts have pushed their conversations off public sites and onto encrypted messaging platforms."[67] As the next section explains, addressing recruitment and radicalization on those encrypted platforms remains a daunting challenge for counterterrorism officials.

Overall, in the past year, technology companies have made it harder for jihadists to openly propagandize on prominent, widely accessible social-media platforms. While jihadist messages remain easily accessible online, removing them from the most widely used platforms will make it harder for curious individuals who are vulnerable, but not yet committed, to radicalism to find those materials.

On the other hand, encouraging—or, in Germany's case, requiring—Facebook, Twitter, and YouTube to become censors, or even to merely bury disfavored speech in search results, raises uncomfortable questions. In the United States, even "hate speech" is constitutionally protected, and unpalatable speakers have a right to communicate their ideas in the public square. Social-media platforms may be the 21st century's public square—the place to spread one's message to the broader public—but unlike the traditional public square, these private companies are not subject to constitutional limits, including the First Amendment. Companies have already shown themselves willing to censor speech that is controversial but not illegal in order to avoid bad publicity or to curry favor with government officials.[68] Such voluntary, private censorship is within the companies' legal rights, but if social-media platforms are the new public square, this practice sits awkwardly with traditional American notions of untrammeled public debate and free expression. Paradoxically, it also risks fueling extremism by

nourishing a sense that paternalistic elites are choking off political debate and burying true but inconvenient information on sensitive topics.[69]

Ultimately, jihadist terrorism will fade only when the terrorists' ideas are discredited. Making their messages harder to access may reduce the number of new recruits, but it will be a half-measure as long as those messages continue to resonate with many Muslims. That is a longer-term challenge, which, even after 15 years of counterterrorism struggles, governments have only begun to confront.

Encryption

Terrorists have capitalized with equal rapidity on another disruptive digital-communications technology: strong encryption that is impenetrable even to the most advanced nation-state cryptographers. For terrorists, this has been a godsend. Electronic communications have long been a prime vulnerability for terrorist plotters and, conversely, a prime opportunity for intelligence services seeking to divine their plans. As strong encryption spreads, that vulnerability is being closed off.

> *"Terrorists have capitalized with equal rapidity on another disruptive digital-communications technology: strong encryption that is impenetrable even to the most advanced nation-state cryptographers."*

Strong Encryption Since the Snowden Leaks

The 2013 leaks by National Security Agency (NSA) contractor Edward Snowden had profound effects for the U.S. technology industry. The public was shocked to learn that the government had been using an obscure section of the USA PATRIOT Act to collect records of *all* phone calls placed on major U.S. telecommunications carriers. (The program pulled in "metadata," such as the phone numbers involved, when the call was placed, and the duration, but not what was said on the call.) This "bulk collection" of telephone call records, including the records of completely innocent Americans, had been approved by the Foreign Intelligence Surveillance Court and briefed to Congress, but a federal court of appeals later held that the statute did not authorize it. Snowden's leaks also highlighted a program, known as PRISM, conducted under Section 702 of the Foreign Intelligence Surveillance Act. Media reports suggested, based on purloined NSA training slides, that the program gave NSA direct access to tech companies' servers. That was not true: The government could demand account data from the companies, but only by serving the company with a legal directive based on individualized suspicion. Yet the damage was done.

U.S. tech firms immediately faced a global backlash over suspicions that they were complicit in government surveillance. Companies were also angered by other Snowden documents, which alluded to operations that sought to access U.S. companies' data without permission or to conduct espionage by clandestinely modifying their products. Foreign tech companies sought to capitalize on the revelations by advertising their products as safer from putative "mass surveillance" by the United States. For example, Deutsche Telekom touted "Email Made in Germany," a local and purportedly safer alternative to U.S.-based providers.

U.S. companies responded by moving quickly to demonstrate their independence from the government and to reassure their users that their data was private. Expanding strong encryption, which companies had already begun deploying, was one such response. Google's Eric Schmidt argued that the "solution to government surveillance is to encrypt everything."[70] Which many companies then attempted to do. Roughly one year after the first Snowden leaks, Apple released "full-disk" encryption keyed only to the user's password; it came standard with iOS 8. This means that even Apple cannot unlock an iPhone without the user's password. For devices running all earlier versions of iOS, law enforcement could send a locked device to Apple, which could then download and provide the data stored on the device in response to a search warrant or other legal authorization.

Companies also began to apply user-controlled encryption to messaging services. Apple's iMessage and the massively popular messaging service WhatsApp (now owned by Facebook) rolled out "end-to-end" encryption, meaning that the unencrypted, plain text of the message is viewable only by the end users and can't be accessed by the company. Other encrypted messaging apps proliferated; the most popular include Signal, Kik, Viber, Wickr, and Telegram. Harvard Professor Yochai Benkler explained the post-Snowden turn to encryption as "a response to users' thirst for technology that can secure their privacy and autonomy in a world where they cannot trust any institutions, whether government or market."

But while this trend enhances users' privacy, it creates new challenges for law enforcement and counterterrorism. Officials describe this problem as "going dark": Valuable evidence that could once be obtained is now inaccessible, even if authorities obtain a search warrant or other legal process. In a recent speech, FBI Director Christopher Wray disclosed that in fiscal year 2017, the FBI was "unable to access the content of 7,775 devices," more than half of those it attempted to access in that year, "even though it had the legal authority to do so."[71] Civil libertarians counter that the nation is in fact in a "golden age of surveillance," because digital technologies produce a huge volume of previously nonexistent data, which can be used as evidence and relatively little of which is encrypted. (Routing information, for example, is usually not encrypted. Nor are messages whose contents are scanned by providers to serve advertising, to detect malware, or for other business purposes.) That is true, but only up to a point: Metadata (the sender, recipient, size of a message, time it was sent, location from which it was sent, etc.) can arouse suspicion and inform hypotheses, but it is often the content of communications that provides the telltale clue and that can prove a crime beyond a reasonable doubt.

During his tenure in office, former FBI Director James Comey frequently raised the "going dark" trend as a growing problem for law enforcement. Facing a backlash from the tech industry and civil libertarians, however, the Obama administration decided not to seek legislation that would require companies to retain the ability to provide their users' communications in unencrypted form. In 2016, Sens. Richard Burr (R-NC) and Dianne Feinstein (D-CA), then chair and vice chair of the Senate Select Committee on Intelligence, released a discussion draft of legislation to that effect, but it was not enacted or even reported out of committee. Since Comey's departure, Deputy Attorney General Rosenstein has taken up the "going dark" cause on behalf of law enforcement. In a recent speech at the U.S. Naval Academy, Rosenstein argued for "responsible encryption" that would "protect privacy and promote security without forfeiting access for legitimate law enforcement needs supported by judicial approval."[72] Despite these efforts, however, there is little reason to believe that mandatory-decryption legislation is more politically viable now than it was during the last years of the Obama administration.

Terrorists' Use of Encrypted Communications

Terrorists have long been aware that their electronic communications were a point of vulnerability and have refined their operations accordingly. In the 1990s, bin Laden reportedly stopped using his satellite phone after a media report disclosed that the U.S. government had been using it to track him. Instead, bin Laden's inner circle relied heavily on human couriers—one of whom, ironically, eventually led the U.S. government to find his post-9/11 hideaway in Pakistan.

Terrorists had attempted to use encryption before the Snowden revelations, but, until very recently, powerful end-to-end encryption had not been built into software that was simple enough for ordinary users with little technical skill.[73] After the Snowden leaks revealed how valuable terrorists' unencrypted communications were for U.S. counterterrorism efforts, terrorist groups swiftly tightened up their operational security. Jihadi "talent-spotters" on publicly visible social-media sites began routinely inviting potential

recruits to switch to encrypted platforms. Telegram, founded by an enigmatic Russian émigré, has become especially popular with terrorists, because it offers encrypted messaging both one-on-one and in group chats. One of ISIS's most prolific virtual planners, former French rapper Rachid Kassim, used his Telegram channel, "Sabre de Lumière," to facilitate and direct "at least a dozen successful and thwarted plots in France" from ISIS territory.[74]

Encrypted messaging often supplements terrorists' use of social media, rather than replacing it altogether. A senior official at the National Counterterrorism Center explained that "terrorists have begun widespread use of private groups in encrypted applications to supplement traditional social media for sharing propaganda in an effort to circumvent the intelligence collection and private sector disruption of their public accounts."[75] ISIS even distributed an operational-security manual recommending specific encrypted apps and providing other technologically astute advice on avoiding surveillance by counterterrorism officials.[76] By toggling between publicly visible social media and encrypted messaging applications, terrorist recruiters can share their message with a vast global audience and then communicate securely with individuals lured in by that public outreach.

Encrypted messaging has been prominently involved in several high-profile attacks in recent years. Abdelhamid Abaaoud, who directed the cells that perpetrated the horrific November 2015 terrorist attacks in Paris and subsequent atrocities in Brussels, gave each member of his team a USB stick bearing an encryption key the operative was to download onto his computer and use as part of an elaborate clandestine communications channel.[77] Members of the cells then used Telegram and WhatsApp to communicate securely with planners in Syria while they hid from police and plotted during the interlude between the Paris and Brussels attacks. European counterterrorism officials attributed their failure to find the terrorists before they struck again in part to the terrorists' use of encrypted communications, which even the U.S. government reportedly could not penetrate.[78] As one American official told *ProPublica*: "New technologies that enable encryption… allow them to be fairly confident that they are communicating in a way that can't be detected. They know how to communicate securely. Often we are inhibited: We know the fact of the communications taking place without knowing the content."[79]

Other examples abound. Junaid Hussain, a U.K. citizen who journeyed to Syria and became an infamous Islamic State recruiter and propagandist, used encrypted messaging apps to encourage and instruct ISIS-inspired plotters in the United Kingdom and the United States. On the morning of the 2015 attack on an event in Garland, Texas, Hussain exchanged more than 100 encrypted messages that featured drawings of Mohammed with one of the shooters. The ISIS operatives directing the Hyderabad-based cell (described in this paper's introduction) "insisted on using a kaleidoscope of encrypted messaging applications, with [the operatives] instructed to hop between apps so that even if one … was discovered and cracked, it would reveal only a portion of their handiwork."[80] Because encrypted messaging apps are so easy to use, even technically mediocre operatives find it easy to cloak their messages behind world-class encryption.

Encrypted devices have also made investigating past terrorist attacks more difficult. The best-known example was the 2016 San Bernardino shooting by husband-and-wife jihadists who pledged allegiance to ISIS. Because the husband's work-issued iPhone was running iOS 9, Apple was unable to unlock the phone even though the government had legal authorization to access the data stored on it. The government then sought a federal court order to compel Apple to upload a new operating system onto the phone that would circumvent the encryption, effectively seeking to force Apple to hack its own product. Ultimately, the dispute became moot after the government paid a private firm more than $1 million to use a proprietary technique to break into the phone.

Addressing the Encryption Challenge

Despite intense advocacy, law enforcement and counterterrorism officials in the United States and western Europe have been unable to secure legislation or court orders compelling device manufacturers and communications providers to decrypt the communications of terrorists and criminals, even where authorities obtain a search warrant. The issue is deeply contentious, with weighty issues on both sides. Policymakers considering encryption legislation must balance libertarian principles, commercial interests, and cybersecurity against powerful public-safety considerations.

The encryption issue is particularly thorny because any legislative "solution" targeting the communications of terrorists and criminals would affect technology used by hundreds of millions of ordinary, completely innocent people. A law requiring companies to decrypt on demand would require that every device sold, or, in the case of communications apps, the software run by every user, incorporate whatever technical means the company developed to enable decryption. This has potential implications for privacy and individual rights, for international human rights, for cybersecurity, and for the commercial strength of a key export industry and source of future economic dynamism.

At the most basic level, prohibiting citizens from encoding their speech to protect it from prying eyes, including government eyes, is anathema to many Americans. There is no historical precedent for a law barring individual citizens (as opposed to such regulated industries as banking) from communicating in a manner inhospitable to government surveillance. The Constitution's Fourth Amendment protects Americans' "papers," which in the founding era always included stored letters, from unreasonable searches and seizures, demonstrating the Framers' solicitude for the privacy of correspondence.

Human rights and privacy advocates have also raised concerns that requiring U.S. companies to decrypt on demand would have spillover effects for internet freedom abroad, particularly in authoritarian countries where activists rely on encryption and anonymization technologies, such as the Tor browser, to communicate securely and to access information that diverges from their governments' agendas. Sen. Ron Wyden (D-OR) has argued that a mandatory-decryption law would "give repressive regimes in Russia and China a blueprint for forcing American companies to create a backdoor."[81] If the United States demanded that companies build particular technology or capability into devices sold in the United States, it would be difficult for the companies to resist other governments' demands to do the same. On the other hand, some companies are already taking measures to comply with Russian and Chinese policies that enable those governments to monitor their citizens. Apple moved all iCloud backups for its Chinese users to servers in China, enabling the Chinese government to access that trove of stored data.[82] Apple has also faced unanswered questions about whether it modified iPhones sold in China in ways designed to facilitate Chinese government surveillance.[83] Russia banned LinkedIn for not storing user data in Russia and is now threatening to do the same to Facebook if it does not move its user data to Russian servers.[84] And both Russian and Chinese law already strictly regulate encryption technologies used within their borders.[85] These developments suggest that powerful authoritarian states are not waiting to see what the United States does, meaning that U.S. forbearance on encryption regulation may not influence them much.

Another frequently raised concern with legislating limits on encryption is the potential effect on the security of user data. Encryption helps secure web browsing, underpins electronic banking, and can ensure that stolen data, including passwords, are illegible to the thief. (Unfortunately, the U.S. Office of Personnel Management failed to encrypt security clearance records, allowing a foreign power to steal and exploit these highly sensitive files.) This concern should not be overstated, however: Law enforcement advocates make clear that they support encryption generally and seek to limit only a narrow subset of applications that are abused by terrorists and other criminals. Analysis of the potential security risks of laws limiting encryption should focus on the specific

applications at issue. For example, it is fair to question whether legislation requiring Apple to retain the capability to access encrypted data stored on an iPhone would materially increase the risk that an unauthorized third party could unlock it; doing so would presumably far exceed the technical capabilities of pickpockets, identity thieves, or other malefactors who might come into physical possession of purloined phones. Similarly, communications platforms such as Gmail that are supported by high-quality security teams but that are not end-to-end encrypted are widely viewed as secure, and the company retains the ability to provide stored data to law enforcement if served with a court order.

A final concern is that U.S. encryption legislation would undermine the commercial prospects of American technology providers. The tech sector has been a key driver of dynamism and growth in the U.S. economy, and will presumably become even more important as digital technologies pervade ever more areas of life. That countries envy American leadership in this field is amply demonstrated by the "many other countries and foreign cities … desperately imitating Silicon Valley in the hopes of igniting their own startup booms."[86] The aftermath of the Snowden leaks revealed, however, that U.S. companies' credibility overseas depends to a significant extent on foreign users' trust that U.S. companies will place their interests and privacy above allegiance to their government. The post-Snowden perception that U.S. technology products had been penetrated by the government perceptibly harmed technology exports, forcing companies to expend "huge amounts of money, engineering time, and other resources" to reassure their customers that their products were secure.[87] While this effect would be hard to quantify, requiring American companies to redesign their products to facilitate law enforcement and intelligence activities could affect international users' confidence that U.S. technology products protect their privacy.

For these reasons, efforts to mandate that law enforcement and counterterrorism officials can access encrypted data have not succeeded. The Obama administration, prompted by the FBI's and local law enforcement's struggles with encrypted devices, completed an internal review of encryption policy in 2015, opting not to seek legislation.[88] The 2016 draft legislation released by Burr and Feinstein in the United States stimulated useful discussion but had little prospect of passing. In the wake of the Paris attacks, France's National Assembly considered legislation imposing draconian penalties on companies that did not help the government decrypt the messages of users under investigation, but the final bill declined to adopt the measure. In the United Kingdom, the initial draft of the Investigatory Powers Bill of 2016 would have imposed a stringent decryption mandate; in response to company concerns, however, the final bill qualified the mandate by specifying that companies would only have to provide the government with assistance that is "technically feasible."[89]

But while the debate appears stalemated today, future events could dramatically reshape public opinion. As one senior American intelligence official reportedly wrote in an email quoted by *The Washington Post*, while "the legislative environment is very hostile today, it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."[90] A mass-casualty attack in the United States in which law enforcement had previously intercepted, but was unable to read, the perpetrators' encrypted messages, could create a political tsunami that would carry a mandatory-decryption law to swift passage.

Implications for Policymakers

Both issues, encryption and social media, resist easy resolution. Even where the technological challenges can be surmounted, any intervention to address terrorists' use of these domains would have collateral effects on other important values: cybersecurity, free speech, economic dynamism, and human rights, among others. That makes it unlikely, and perhaps undesirable, that the policymaking process will yield the optimal end state for counterterrorism in either domain. End-to-end encryption is likely to persist, at least for some time. And social media, at least in the United States, is likely to remain open to messages that, if not constituting outright incitement, at least point toward radicalization.

> *"Policymakers should aim to construct a "layered" defense against terrorist operations in the digital realm."*

This suggests that rather than a complete victory in either domain, policymakers should aim to construct a "layered" defense against terrorist operations in the digital realm. As the 9/11 Commission explained in the context of transportation security, a "layered security system" recognizes that "[n]o single security system is foolproof."[91] Instead, the various layers must support one another to improve the security of the system overall. In digital counterterrorism, a layered approach would entail making each stage at which terrorists exploit the digital realm less hospitable to their operations. That includes the posting and re-posting of extremist content on social-media platforms, vulnerable individuals' searches for and viewing of that content, jihadist sympathizers' or recruiters' outreach to those potential new recruits, the shift of those conversations to secure encrypted platforms, and terrorist networks' use of encrypted platforms for ongoing communications and planning.

At the same time, counterterrorism policymakers must accept that they have limited political capital and that attempting to push through reforms that would make any one of these steps impossible—for example, banning end-to-end encrypted communications apps, or imposing harsh liability regimes on social-media companies—would consume all of it. That means that policymakers' goal in developing a layered defense strategy in digital domains should be to make terrorists' tasks at each step as difficult as realistically possible, at the lowest possible political cost, rather than trying to eradicate these vulnerabilities completely.

On the encryption front, this should entail moving forward now with measures, short of decryption mandates, that can help law enforcement and counterterrorism officials cope with a world in which strong encryption is widespread and continues to present obstacles for investigators. The most promising option is "lawful hacking"—that is, legally authorized efforts by government agencies to penetrate the devices and services used by terrorists and other criminals. One example of lawful hacking is the FBI's hiring of a private firm to hack into the San Bernardino shooter's iPhone after Apple refused to do so.[92] Lawful hacking can also penetrate end-to-end encrypted communications by placing spyware on the PC or mobile device, called the "endpoint," at which the communications are decrypted for the intended user to see. The FBI has had great success using analogous techniques to uncloak anonymous users in child-pornography cases.

Lawful hacking is not a panacea: Even when it works, it is labor- and resource-intensive. The latest iPhones running up-to-date software may be un-hackable. End-to-end encrypted communications can be penetrated only if the user is still actively using the service and can be tricked into downloading spyware. More subtly, if governments are

forced to use hacking instead of "front-door" access, they will have a higher incentive to hoard software vulnerabilities rather than disclosing them to vendors so that they can be patched. This allows insecurities to persist in widely used products, increasing insecurity for all users. Absent decryption legislation, however, counterterrorism, intelligence, and law enforcement officials will need hacking capabilities to do their jobs.

To that end, political leaders should ensure that security agencies have adequate funding, personnel, and authorities to acquire and deploy the latest technologies. Germany, for example, has forsworn a decryption mandate for companies but also created a new agency to help law enforcement and intelligence agencies gain unilateral access to devices, without compelled assistance from providers. Put simply, it is allowing companies to race forward with the best technology they can muster but giving government agencies the resources to try to keep up. Given America's federal system, with more than 10,000 state and local police agencies, Congress should also ensure that the FBI has dedicated funding, personnel, and authorities to help state and local officials cope with encryption in high-value cases.

The United States should also coordinate its approach to encryption with international partners, particularly in Europe, that face similar counterterrorism challenges, and whose law enforcement and intelligence services also operate under the rule of law. Over the past several years, in the wake of horrific terrorist attacks in their cities, cabinet officials in the United Kingdom, France, and Germany have hinted at tougher measures to ensure access to encrypted data.[93] On a March 2017 trip to Washington, European Union Justice Commissioner Věra Jourová discussed the challenge of encrypted evidence with U.S. Attorney General Jeff Sessions, a strong supporter of a lawful-access mandate.[94] Given that technology products trade on a global market, if the United States and European governments ultimately opt for lawful-access mandates, they should coordinate the technical requirements imposed by their respective laws. Alternatively, if the U.S. government declines to seek a mandate out of concern for its potential effect on the privacy of activists, journalists, and dissidents living under authoritarian regimes, that policy would have its desired effect only if U.S. partners in Europe forgo such mandates as well.[95]

Legal changes may also be needed to ensure that the rules governing law enforcement's use of these technologies reflect the realities of digital-age investigations. This process is already underway: A 2016 change to Rule 41 of the Federal Rules of Criminal Procedure enables federal judges to issue search warrants for police hacking operations without regard to the target's physical location, if that location "has been concealed through technological means."[96] This reflects the fact that technologically sophisticated cyber-criminals, including child pornographers, typically disguise their locations and identities while conducting illegal activities online.[97] Further updates may be needed to enable police to effectively use these modern investigatory techniques to make cases. For example, federal courts have disagreed on whether Federal Rule of Criminal Procedure 16 requires the government to disclose the source code of software "exploits" the FBI has used to ferret out the identity of anonymous visitors to websites dedicated to illegal child pornography.[98] In some cases, the government has been forced to abandon prosecutions in those cases in order to "protect highly sensitive" source code "from criminal discovery" ordered by judges under Rule 16.[99] Legislators and legal experts should consider whether there is a better way to balance a defendant's right to see information material to the defense with the government's interest in protecting valuable law enforcement tools.

One other intriguing new front in the encryption arms race between industry and law enforcement is subterfuge: gaining access by old-fashioned deception or lawful strong-arm tactics rather than high-end hacking. For example, in cases where a suspect is believed to be using encryption, police have arrested him or her while the device is unlocked and in use, distracting the arrestee so that he or she cannot quickly lock the device before police seize it. Police have also begun compelling arrestees whose phones unlock with a fingerprint to touch the scanner, a practice upheld by some court decisions.[100] Phones that unlock using facial recognition will

be even easier to unlock in this manner, which likely raises fewer constitutional questions than compelled fingerprint scanning, as it can be accomplished without any coerced action by the arrestee.

Where encrypted devices can't be unlocked, cloud backups are often the next best alternative. Certain data stored on an iPhone, for example, is backed up to the cloud by default, and can be provided to government officials bearing a valid legal process. Congress should consider creating, and mandating corporate participation in, a national clearinghouse that would help law enforcement at all levels understand what data companies store in the cloud, how that data is classified and subdivided, and how to draft clear, well-tailored search warrants and other legal process that will elicit useful responses from companies. The judiciary should do its part to ensure that judges receive appropriate training in these subjects, so that they are able to rigorously evaluate whether search warrants and other requests for data are appropriately tailored.

Finally, absent access to the content of encrypted messages, counterterrorism officials will be forced to extract more value from communications metadata, which is rarely encrypted. If policymakers are unwilling or unable to mandate that providers decrypt on demand, they could instead consider mandating that if communications platforms do not retain the ability to decrypt upon receipt of lawful process, they must retain communications metadata for a specified period. Lawmakers might also consider whether to grant authorities expanded power to obtain metadata from such providers.

Meanwhile, as they quietly explore these alternatives to mandatory decryption, policymakers can also develop options for future scenarios in which legislative action could be possible. These preparations should entail considering which potential regulatory models to ensure lawful access would offer the greatest law enforcement benefit in exchange for the least possible reduction in security. Having good models on the shelf will increase the likelihood that any post-attack legislation will be well-considered rather than hastily drafted and later regretted. The Burr-Feinstein draft legislation, though harshly criticized by strong-encryption advocates, was a useful thought experiment, even if such legislation is never enacted.[101] Viable proposals will almost certainly have to be technology-neutral—that is, they should impose a performance standard (for example, that companies must provide technical assistance, retain the capability to decrypt in response to a court order, and so on) rather than specifying a particular technical mechanism that companies must employ. "Magic key" proposals, which give the government the ability to obtain unilateral access to encrypted data, are presumptively inferior, for two reasons: (1) requiring the government to request data from companies, rather than taking it unilaterally, heightens transparency and accountability; and (2) the government's track record in protecting its highest-priority data is not good, creating an unacceptable risk that governmental magic keys will be lost or misused.

Deputy Attorney General Rosenstein's November 2017 speech acknowledged as much: He acknowledged that any legislation should be technology-neutral and conceded that requiring companies to entrust the government with a "magic key" would likely be a nonstarter. He noted that "the law need not mandate any particular means in order to achieve" what he defined as "the crucial end: When a court issues a search warrant or wiretap order to collect evidence of crime, the provider should be able to help."[102] Similarly, in a speech in January 2018, FBI Director Wray disclaimed any effort to obtain a "backdoor," instead citing extant systems in which either providers or independent custodians retain keys to encrypted data.[103] These concessions notwithstanding, policymakers should be under no illusions: Even a performance standard that allows industry to choose and control the technological mechanism will arouse ferocious opposition from civil libertarians, privacy advocates, and the tech industry. A study convened by the National Academies of Sciences, Engineering, and Medicine is expected to report in 2018 and should inject additional technical insight into this policy debate.[104]

While the changes proposed here can help law enforcement cope

and plan for the future, the reality, however, is that end-to-end encryption is almost certainly not going away. Terrorists will continue to be able to use powerful end-to-end encryption to shield many of their communications—meaning that they can remain networked *whether or not* they possess a geographic sanctuary. This is a critical difference from the pre-9/11 era, when al Qaeda needed the breathing room provided by its physical safe haven in Taliban-ruled Afghanistan to convene and plot attacks. As the Islamic State's territorial caliphate disintegrates, the secure, global communications enabled by widespread end-to-end encryption will provide an alternative forum for widely dispersed ISIS operatives to virtually convene and conspire. Worryingly, this cohort will likely include foreign fighters returning to Europe and—in far smaller numbers—the United States.[105]

But while the encryption challenge is likely to be an enduring one, there are promising openings in efforts to stop terrorist propaganda. Companies that will almost certainly be unwilling to cooperate on strong encryption are proving to be far more cooperative on halting terrorist propaganda. Indeed, while government counter-messaging has faltered, leading technology companies are bringing their talent for innovation to the challenge of uprooting terrorists' presence on social media.

Google's ideas lab, Jigsaw, created by the company to "tackle some of the toughest global security challenges facing the world today," has pioneered a data-driven approach to thwarting terrorist messages, which avoids many of the stumbling blocks that have frustrated government attempts to counter jihadist messages. Instead of relying on government officials or contractors to create and disseminate messages, Jigsaw's pilot project redirected YouTube users who search for radicalizing content away from that material and toward user-created, de-radicalizing content that similarly situated users have found persuasive. This approach, dubbed the "Redirect Method," uses Google's sophisticated AdWords targeting tools to redirect "the slice of ISIS' audience that is most susceptible to its messaging … towards curated YouTube videos debunking ISIS recruiting themes."[106] Wisely, Jigsaw's team "avoided government produced content and newly or custom created material, using only existing … YouTube content" that users already found compelling. The final list of redirect content "had videos sourced from 83 different YouTube creators."[107]

Jigsaw's approach has several advantages over government-driven counter-messaging. First, the content it serves to users is perceived as more authentic than messages manufactured by the U.S. government—presumably because it *is* more authentic. Second, and more subtly, Jigsaw's empirical, data-driven approach enabled it "to identify 'hidden' counterargument content"—that is, videos that were not *designed* to refute ISIS, but that in practice did so quite effectively.[108] These included "citizen journalism and documentary footage" presenting, in a factual manner, life on the ground in the ISIS pseudo-caliphate, and "[v]ideos featuring clerics and other religious figures who refute violent extremist narratives."[109] Third, the success of such data-driven approaches—unlike some of the top-down broadcasting or counter-messaging schemes described earlier in this report—is not contingent on the government possessing the regional, linguistic, or religious expertise to determine which messages or messengers will be credible. Instead, those insights are derived by analyzing the real-world behavior of users on the platform, and a campaign can be constantly, instantaneously adjusted in response to user behavior after it goes live. This approach has already proved successful in political campaigns,[110] and Jigsaw has demonstrated that it has immense potential to undercut the effect of jihadist messages on social media as well.

Another promising approach is peer-to-peer messaging, which has shown results in related social-media contexts. In a report for the Organization for Security and Co-operation in Europe, Peter Neumann highlights the #Rewind campaign, created by Spanish university students. The social-media campaign "encouraged people to 'rewind,' that is, to re-consider their comments and stop engaging in abusive or offensive behavior."[111] The campaign cost less than 3,000 euros, reached "more than two million people in less than a year," and "often had the intended effect of mobilizing

users to push back against hateful and abusive comments."[112] Peer-generated messages may be more effective than messages created by governments or other authorities because they are likely perceived as more authentic. Similar approaches could be effective in pushing back against extremist content—particularly against radicalizing content that, because it is within the law and platforms' terms of use, will not be taken down.

Voluntary efforts by social-media companies to remove terrorist or extremist content, while slightly more coercive than counter-messaging or redirection, comport with the First Amendment and are palatable to the companies' global user base. Given those legal realities, voluntary removal of terrorist content is at present the most promising avenue for progress against terrorist messages on social media. Facebook and Google, which owns YouTube, have expanded their moderation teams and sharpened their guidelines as to what constitutes extremist content. Perhaps most promising, however, is the companies' development of tools driven by artificial intelligence (AI) that could ultimately enable platforms to identify and remove terrorist content faster than its creators can put it up. AI will never be a complete solution; determining which content violates the law, or a service's terms of use, calls for subtle legal and ethical judgments that only human beings will be able to make for the foreseeable future. But technological solutions can prevent terrorists from reposting *known* terrorist content or resuscitating blocked accounts under slightly different names.

Under pressure from governments, particularly in Europe, developments on this front are proceeding apace. The new Global Internet Forum to Counter Terrorism, discussed above, is actively "working on technological solutions to help thwart terrorists' use of our services."[113] These include "a shared industry hash database, where companies can create 'digital fingerprints' for terrorist content and share it with participating companies."[114] As of December 2017, the database contained more than 40,000 hashes, each representing a different video or image, enabling companies to easily identify and remove these media from their platforms—or even block them from being posted in the first place.[115] Facebook, YouTube, and Twitter are all using automation to take down terrorist content far faster than humans alone and, often, before its intended audience even sees it.

Terrorists' use of social media is an international problem, on international platforms, so the solution should transcend borders as well. Specifically, the U.S. government should coordinate with European allies and other affected governments to monitor companies' efforts to neutralize terrorist content and to encourage companies to continue deploying innovative tools. While quiet coordination is already taking place, a publicly visible, prominent united front will be most compelling as companies weigh how great an investment of their own resources to make in this space. At the same time, policymakers must be sure to ensure that U.S. participation in such initiatives is consistent with the First Amendment and traditions of free and open public debate. For example, Germany's *NetzDG* law, which compels companies to censor speech that would be lawful in the United States, may be appropriate in the German constitutional order but would not be appropriate for the United States to explicitly or implicitly endorse.

A broader question is whether social-media companies will consider—or be forced to consider—broader reforms to address filter bubbles, algorithmic promotion of conspiracy theories, and other unintended consequences that affect public discourse and have increased terrorists' ability to exploit these platforms. Russia's apparent exploitation of social media to micro-target Americans with tailored, conspiratorial, radicalizing messages during the 2016 election has created a new impetus in Congress to address this issue. As companies' calculated targeting of psychological vulnerabilities becomes more and more apparent, traditional media outlets and academic researchers are coming to regard the social-media giants with skepticism. Society is at the very early stages of wrestling with the titanic question of how to reconcile democratic politics with social media and other digital technologies, and it is impossible to predict how these debates will be resolved. Social-media companies may be able to blunt calls for regulation by re-engineering their recommendation engines to privilege credible

content over clickbait conspiracy theories, or to ensure that diverse points of view are presented.[116] Given the broad and fundamental implications for all areas of society, however, counterterrorism issues are not likely to drive these debates.

Ultimately, counterterrorism policymakers have limited political capital with technology companies and the public—capital they can expend on either addressing encryption or social media, and on either coercive or cooperative approaches. Seeking to force companies and users to accept mandatory backdoors to encrypted communications would burn that limited political capital, with an uncertain return.

Instead, officials and legislators would be better served by focusing their limited bandwidth and political capital on cooperative approaches, which are showing real returns. That means keeping up the pressure on companies to further increase the human and financial resources devoted to removing terrorist messages; to develop and deploy new automated tools as fast as possible; to share those technologies across the industry, including with small tech companies that have fewer resources to devote to compliance; and to provide the greatest possible transparency about these efforts' effectiveness and terrorists' presence on their platforms. In this vein, the European Commission recently called for social-media platforms to "step up and speed up their efforts" to remove terrorist propaganda, "including closer cooperation with national and enforcement authorities, increased sharing of know-how between online players and further action against the reappearance of illegal content."[117] Focusing on cooperative approaches will also make it easier for governments to seek quiet cooperation from companies on other priorities, including "encryption workarounds"[118] like accessing cloud backups or other potential unencrypted substitutes for needed evidence.

Conclusion

Social media and encryption undoubtedly pose counterterrorism challenges. Any efforts to address those challenges, however, will resonate far beyond the narrow realm of counterterrorism. These technologies implicate the freedom of expression, individual privacy, constitutional law, international human rights, technological innovation, and the future prosperity of the United States. They also affect every day domestic law enforcement, cybersecurity, and other public-safety efforts. In considering policy responses to the counterterrorism challenges these technologies present, governments must consider these other efforts as well.

That means that the likely end result will be imperfect for counterterrorism. For that reason, when the most direct possible solutions—for example, laws requiring companies to take down extremist speech or to decrypt content created by their users—are precluded, policymakers must think creatively to identify other, less-fraught tools that enable counterterrorism officials to do their jobs.

Recent developments offer some reason for optimism, particularly in the social-media realm. Governmental pressure has driven companies to develop new AI tools enabling them to identify and take down far more terrorist content than humans alone could remove. Data-driven approaches to counter-messaging, as pioneered by Google's Jigsaw project, also suggest a promising new opportunity in an area where, until recently, governments have lagged. Even with these new techniques, however, the digital realm will remain contested; many experts predict that the decline of the Islamic State's territorial caliphate will lead it to redouble its efforts in the digital realm, seeking to remotely inspire and direct violence in the West.

> *"Social-media and encrypted communications platforms are but a channel through which terrorists transmit their ideas; it is the ideas themselves, and whether they resonate or repel, that will decide whether young Muslims choose terrorism or peace."*

Finally, and most importantly, the focus on these technologies should not obscure the larger struggle of ideas that will decide the success of the campaign against jihadist terrorism. Social-media and encrypted communications platforms are but a channel through which terrorists transmit their ideas; it is the ideas themselves, and whether they resonate or repel, that will decide whether young Muslims choose terrorism or peace. Ultimately, jihadist terrorism will be defeated "only when the ambitions that motivate groups such as al Qaeda and the Islamic State return to the obscurity they richly deserve."[119]

Appendix A

Summary of Key Findings

Social Media

- Government-directed counter-messaging efforts on social media have been largely ineffective and may have inadvertently elevated the prestige of their targets while eroding that of the U.S. government.
- American officials or contractors typically lack the linguistic, cultural, and religious expertise to effectively out-duel terrorist sympathizers in fast-moving debates on social media.
- A focus on social-media showdowns risks obscuring the underlying factors that drive some Muslims to support radical messages and most others to ignore or oppose them.
- Despite these struggles, effective counter-messaging remains a worthwhile goal. Early efforts, while checkered, should not be condemned: Finding methods that work in the unique environment of social media will require trial and error.
- Given their limited political capital with social-media companies and the public, counterterrorism policymakers should adopt a layered defense strategy that aims to make each digital domain as inhospitable as possible at a reasonable potential political cost, rather than trying to eradicate these vulnerabilities completely. Voluntary or cooperative approaches are likely to be more realistic and promising than coercive approaches.
- One promising approach, pioneered by Google's Jigsaw ideas lab, is redirecting users away from radicalizing material and toward user-created, de-radicalizing content that similarly situated users have found persuasive. This approach requires the capabilities and cooperation of large social-media platforms.
- Peer-to-peer counter-messaging may also be perceived as more authentic than government-generated messaging and should be explored as a potential approach.
- Voluntary efforts by social-media companies to suspend jihadist accounts and remove jihadist messages have reduced, but not eliminated, terrorists' ability to propagandize and recruit online.
- New AI and machine-learning tools now enable the most prominent social-media platforms to take down previously identified terrorist content much faster than human moderators.
- European countries, whose constitutional frameworks are less protective of incendiary speech, have imposed or considered laws requiring companies to remove terrorist messages and "hate speech" within specified periods.
- Because extremist content is political speech, requiring companies to remove radicalizing messages would raise constitutional concerns in the United States. But even voluntary takedowns, if extended beyond incitement that is plainly illegal, raise important questions about unpopular messengers' ability to access this new public square.

- The U.S. government should coordinate with European allies and other affected governments to monitor companies' efforts to neutralize terrorist content and to encourage companies to continue deploying innovative tools, but the U.S. government should also ensure that any coordination only supports initiatives that comport with the First Amendment.
- Despite companies' efforts to take down known terrorist content, extremist materials remain widely available online.
- Making jihadist messages harder to access may reduce the number of new recruits, but it will be a half-measure as long as those messages continue to resonate with many Muslims.

Encryption

- Since the 2013 Snowden leaks, companies have dramatically expanded their use of strong encryption in consumer-communications technologies.
- Encrypted devices and messages have created new challenges for law enforcement and counterterrorism officials, as evidence that was previously available is now inaccessible.
- Terrorists, long aware that their electronic communications are a point of vulnerability, now enthusiastically use off-the-shelf encryption to secure them.
- The secure, global communications provided by end-to-end encryption will allow terrorists to remain networked *whether or not* they possess a geographic sanctuary.
- Encrypted messaging has been prominently involved in several high-profile attacks in recent years. Encrypted devices have also made investigating past attacks more difficult.
- Any legislation targeting the communications of terrorists and criminals would affect technology used by hundreds of millions of ordinary, innocent people.
- Encryption legislation would affect privacy and individual rights, international human rights, cybersecurity, and the U.S. tech industry.
- The United States should coordinate its approach to encryption with European partners facing similar counterterrorism challenges.
- Prohibiting citizens from encoding their speech to protect it from prying eyes, including government eyes, is anathema to many Americans and would be historically unprecedented in the United States.
- U.S. legislation could have spillover effects for activists and journalists overseas who use encryption to shield their activities from authoritarian governments. On the other hand, aggressive efforts by Russia and China to limit encryption within their borders suggest that U.S. actions may have little influence on powerful authoritarian states.
- Restricting encryption could also undermine cybersecurity for ordinary users, although any effect on security would be limited to the specific applications at issue.

- Encryption legislation could affect U.S. technology companies by undermining foreign users' confidence in the security of their products.
- The debate over encryption and "going dark" appears politically stalemated. Mandatory-decryption legislation appears unlikely to pass in today's political climate, but it could succeed after a future attack in which encryption played a decisive role.
- Policymakers should quietly prepare for a future in which legislative action could be possible, by considering now which potential regulatory models would offer the greatest law enforcement benefit with the fewest ancillary harms.
- Viable options will almost certainly be technology-neutral rather than specifying a technical mechanism.
- Technical mechanisms to meet a hypothetical decryption mandate should be designed and controlled by companies rather than by the government.
- Policymakers should also move forward now with measures, short of decryption mandates, that can help officials cope with strong encryption.
- Policymakers should ensure that agencies have adequate funding, personnel, and authorities to acquire and deploy the latest technologies for "lawful hacking."
- This should include dedicated funding, personnel, and authorities for the FBI to help state and local officials cope with encryption in high-value cases.
- Legal changes may also be needed to ensure that the rules governing law enforcement's use of these technologies reflect the realities of digital-age investigations.
- Congress should consider creating, and mandating corporate participation in, a national clearinghouse that would help law enforcement at all levels understand what data companies store in the cloud, how that data is classified and subdivided, and how to draft clear, well-tailored search warrants and other legal processes that will elicit useful responses from companies.
- The judiciary should ensure that judges are equipped to rigorously evaluate whether search warrants and other requests for data are appropriately tailored.
- If Congress chooses not to mandate that providers retain the ability to decrypt upon the receipt of lawful processes, it could consider requiring that if communications platforms do not do so, they must retain communications metadata for a fixed period.
- Lawmakers might also consider whether to provide expanded authority to obtain metadata from providers that do not retain the ability to decrypt upon receipt of lawful processes.

Endnotes

1 Rukmini Callimachi, "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar," *The New York Times*, February 4, 2017. Available at: https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html.

2 Steven Bertoni, "Exclusive Interview: How Jared Kushner Won Trump the White House," *Forbes*, December 20, 2016. Available at: https://www.forbes.com/sites/stevenbertoni/2016/11/22/exclusive-interview-how-jared-kushner-won-trump-the-white-house/#1bcae6263af6.

3 Cecilia Kang, et al., "Russia-Financed Ad Linked Clinton and Satan," *The New York Times*, November 1, 2017. Available at: https://www.nytimes.com/2017/11/01/us/politics/facebook-google-twitter-russian-interference-hearings.html.

4 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2004), 46.

5 Robin Taylor, Prepared Statement: Acting Deputy Under Secretary for Intelligence Operations, Office of Intelligence and Analysis, U.S. Department of Homeland Security, before the Senate Homeland Security and Governmental Affairs Committee, December 6, 2017.

6 Nikki Floris, Prepared Statement: Deputy Assistant Director of Counterterrorism, Federal Bureau of Investigation, before the Senate Homeland Security and Governmental Affairs Committee, December 6, 2017.

7 Alexander Meleagrou-Hitchens, et al., *The Travelers: American Jihadists in Syria and Iraq*, George Washington University Program on Extremism, February 2018, 33. Available at: https://extremism.gwu.edu/events/travelers-american-jihadists-syria-and-iraq.

8 Charlie Winter, "Fishing and ultraviolence: So-called Islamic State is known for its brutality. But it's also hooking people in far subtler ways," *BBC*, August 1, 2015. Available at: http://www.bbc.co.uk/news/resources/idt-88492697-b674-4c69-8426-3edd17b7daed.

9 See, e.g.: Aris Roussinos, "Jihad Selfies: These British Extremists in Syria Love Social Media," *Vice*, December 5, 2013. Available at: https://www.vice.com/en_us/article/gq8g5b/syrian-jihadist-selfies-tell-us-a-lot-about-their-war.

10 Audrey Alexander, *Digital Decay: Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter*, George Washington University Program on Extremism, October 2017. Available at: https://scholarspace.library.gwu.edu/downloads/5425k9692.

11 Cited in: Daniel Byman and Jeremy Shapiro, *Be Afraid. Be A Little Afraid: The Threat of Terrorism from Western Foreign Fighters in Syria and Iraq*, Brookings Institution, November 2014, 15. Available at: https://www.brookings.edu/research/be-afraid-be-a-little-afraid-the-threat-of-terrorism-from-western-foreign-fighters-in-syria-and-iraq/.

12 Adrienne LaFrance, "The First Reply to a Trump Tweet Is Prime Media Space," *The Atlantic*, December 16, 2016. Available at: https://www.theatlantic.com/technology/archive/2016/12/weird-media-ecosystem/510911/.

13 Rita Katz, "The State Department's Twitter War With ISIS Is Embarrassing," *Time*, September 16, 2014. Available at: http://time.com/3387065/isis-twitter-war-state-department/.

14 Task Force on Terrorism and Ideology, *Defeating Terrorists, Not Terrorism*, Bipartisan Policy Center, September 2017, 28. Available at: https://bipartisanpolicy.org/library/counterterrorism-policy-from-911-to-isis/.

15 Mostafa El-Bermawy, "Your Filter Bubble is Destroying Democracy," *Wired*, November 18, 2016. Available at: https://www.wired.com/2016/11/filter-bubble-destroying-democracy/.

16 Ibid.

17 Paul Lewis, "'Fiction is outperforming reality': how YouTube's algorithm distorts truth," *The Guardian*, February 2, 2018. Available at: https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth.

18 Ibid.

19 *The Wall Street Journal*, "Blue Feed, Red Feed: See Liberal Facebook and Conservative Facebook, Side by Side," May 18, 2016. Available at: http://graphics.wsj.com/blue-feed-red-feed/.

20 Scott Shane, *Objective Troy: A Terrorist, A President, and the Rise of the Drone* (New York: Tim Duggin Books, 2015), 64.

21 See: Steve Coll, *The Bin Ladens: An Arabian Family in the American Century* (New York: Penguin Press, 2008), 144-147.

22 Seamus Hughes and Alexander Meleagrou-Hitchens, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," Countering Terrorism Center at West Point, *CTC Sentinel* 10, no. 3 (March 2017), 1. Available at: https://ctc.usma.edu/the-threat-to-the-united-states-from-the-islamic-states-virtual-entrepreneurs/.

23 Ibid., 3.

24 Audrey Alexander, *Digital Decay: Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter*, George Washington University Program on Extremism, October 2017, 6. Available at: https://scholarspace.library.gwu.edu/downloads/5425k9692.

25 Ibid., 5.

26 Aris Roussinos, "Jihad Selfies: These British Extremists in Syria Love Social Media," *Vice*, December 5, 2013. Available at: https://www.vice.com/en_us/article/gq8g5b/syrian-jihadist-selfies-tell-us-a-lot-about-their-war.

27 Task Force on Terrorism and Ideology, *Defeating Terrorists, Not Terrorism*, Bipartisan Policy Center, September 2017, 27-28. Available at: https://bipartisanpolicy.org/library/counterterrorism-policy-from-911-to-isis/.

28 Ibid., 27.

29 Ibid., 20.

30 Ibid., 28.

31 See: Joby Warrick, "How a U.S. team uses Facebook, guerrilla marketing to peel off potential ISIS recruits," *The Washington Post*, February 6, 2017. Available at: How a U.S. team uses Facebook, guerrilla marketing to peel off potential ISIS recruits.
See also: Thomas M. Hill, "Secretary Tillerson is doing the right thing, so why is Congress bashing him?" Brookings Institution, October 27, 2017. Available at: https://www.brookings.edu/blog/fixgov/2017/10/27/secretary-tillerson-is-doing-the-right-thing-so-why-is-congress-bashing-him/.

32 Nahal Toosi, "Tillerson spurns $80 million to counter ISIS, Russian propaganda," *Politico*, August 2, 2017. Available at: https://www.politico.com/story/2017/08/02/tillerson-isis-russia-propaganda-241218.

33 Desmond Butler and Richard Lardner, "US misfires in online fight against Islamic State," *Associated Press*, January 31, 2017. Available at: https://apnews.com/b3fd7213bb0e41b3b02eb15265e9d292.

34 Ibid.

35 William McCants, *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State* (New York: St. Martin's Press, 2015), 137.

36 Richard LeBaron and William McCants, "Experts weigh in: Can the United States counter ISIS propaganda?" Brookings Institution, June 17, 2015. Available at: https://www.brookings.edu/blog/markaz/2015/06/17/experts-weigh-in-can-the-united-states-counter-isis-propaganda/.

37 bid.

38 See: Robbie Gramer, "Sales of Hitler's 'Mein Kampf' Skyrocketing in Germany—But It's Not Why You Think," *Foreign Policy*, January 3, 2017. Available at: http://foreignpolicy.com/2017/01/03/sales-of-hitlers-mein-kampf-skyrocketing-in-germany-but-its-not-why-you-think/.

39 See: *Deutscher Bundestag, "Bundestag beschließt Gesetz gegen strafbare Inhalte im Internet,"* June 20, 2017. Available at: https://www.bundestag.de/dokumente/textarchiv/2017/kw26-de-netzwerkdurchsetzungsgesetz/513398.

40 Emma Thomasson, "Facebook makes German marketing push as hate speech law bites," *Reuters*, December 19, 2017. Available at: https://www.reuters.com/article/us-facebook-germany/facebook-makes-german-marketing-push-as-hate-speech-law-bites-idUSKBN1ED1BW.

41 U.K. Prime Minister's Office, Press Release: "UK and France announce joint campaign to tackle online radicalisation," *Gov.UK*, June 13, 2017. Available at: https://www.gov.uk/government/news/uk-and-france-announce-joint-campaign-to-tackle-online-radicalisation.

42 *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam).

43 See: *United States v. Stevens*, 559 U.S. 460 (2010).

44 See: *New York Times Co. v. United States*, 403 U.S. 713 (1971).

45 See: Benjamin Wittes, "Twitter, ISIS, Civil Liability, and Immunity: An Update," *Lawfare*, May 5, 2016. Available at: https://www.lawfareblog.com/twitter-isis-civil-liability-and-immunity-update-0.

46 See: Nina Iacono Brown, "Should Social Networks Be Held Liable for Terrorism?" *Slate*, June 16, 2017. Available at: http://www.slate.com/articles/technology/future_tense/2017/06/a_new_legal_theory_for_holding_social_networks_liable_for_terrorism.html.

47 Sam Schechner, "France's Top Cop Has More to Teach Silicon Valley," *The Wall Street Journal*, January 26, 2016. Available at: https://blogs.wsj.com/digits/2016/01/26/frances-top-cop-has-more-to-teach-silicon-valley/.

48 BBC, "Twitter suspends 125,000 'terrorism' accounts," February 5, 2016. Available at: http://www.bbc.com/news/world-us-canada-35505996.

49 European Commission, Press Release: "European Commission and IT Companies announce Code of Conduct on illegal online hate speech," May 31, 2016. Available at: http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

50 Ibid.

51 U.K. Parliament, *Hate crime: abuse, hate and extremism online*, House of Commons, Home Affairs Committee, Apr. 25, 2017, 11. Available at: http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/inquiries/parliament-2015/inquiry7/.

52 Quoted in: Charles Riley, "Theresa May: Internet must be regulated to prevent terrorism," *CNN*, June 4, 2017. Available at: http://money.cnn.com/2017/06/04/technology/social-media-terrorism-extremism-london/index.html.

53 Julia Fioretti, "Social media giants step up joint fight against extremist content," *Reuters*, June 26, 2017. Available at: https://www.reuters.com/article/us-internet-extremism/social-media-giants-step-up-joint-fight-against-extremist-content-idUSKBN19H20A.

54 Hamza Shaban, "Facebook wants to use artificial intelligence to block terrorists online," *The Washington Post*, June 15, 2017. Available at: https://www.washingtonpost.com/news/the-switch/wp/2017/06/15/facebook-wants-to-use-artificial-intelligence-to-block-terrorists-online/?utm_term=.d747930cdf51.

55 Paresh Dave, "Google broadens takedown of extremist YouTube videos," *Reuters*, November 1, 2017. Available at: https://www.reuters.com/article/us-tech-hatespeech/google-broadens-takedown-of-extremist-youtube-videos-idUSKBN1DE05X.

56 Kent Walker, "Working together to combat terrorists online," *Google Public Policy*, September 20, 2017. Available at: https://www.blog.google/topics/public-policy/working-together-combat-terrorists-online/.

57 Ibid.

58 Ibid.

59 See: Mark Hosenball, "British official urges social media companies to block militant content," *Reuters*, November 10, 2017. Available at: https://www.reuters.com/article/us-security-socialmedia-britain/british-official-urges-social-media-companies-to-block-militant-content-idUSKBN1DA065.

60 Elisabeth Weise, "Anti-extremist crackdown on YouTube, Facebook, Twitter only solves part of the problem," *USA Today*, November 1, 2017. Available at: https://www.usatoday.com/story/tech/news/2017/11/01/anti-extremist-crackdown-youtube-facebook-twitter-only-solves-part-problem/823111001/.

61 Audrey Alexander, *Digital Decay: Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter*, George Washington University Program on Extremism, October 2017, 7, 15. Available at: https://scholarspace.library.gwu.edu/downloads/5425k9692.

62 Ibid.

63 Jack Nikas, "Cuomo Points to Tech Companies After New York Bombing Attempt," *The Wall Street Journal*, December 12, 2017. Available at: https://www.wsj.com/articles/google-others-take-uneven-approach-to-policing-extremist-content-1513074601.

64 Elisabeth Weise, "Anti-extremist crackdown on YouTube, Facebook, Twitter only solves part of the problem," *USA Today*, November 1, 2017. Available at: https://www.usatoday.com/story/tech/news/2017/11/01/anti-extremist-crackdown-youtube-facebook-twitter-only-solves-part-problem/823111001/.

65 Zolan Kanno-Youngs and Scott Calvert, "After New York Attack, Investigators Ask: Should ISIS Material Be Online?" *The Wall Street Journal*, December 15, 2017. Available at: https://www.wsj.com/articles/investigators-looking-at-how-nyc-terror-suspect-found-radical-islam-online-1513339201.

66 Elisabeth Weise, "Anti-extremist crackdown on YouTube, Facebook, Twitter only solves part of the problem," *USA Today*, November 1, 2017. Available at: https://www.usatoday.com/story/tech/news/2017/11/01/anti-extremist-crackdown-youtube-facebook-twitter-only-solves-part-problem/823111001/.

67 Charles Riley, "Theresa May: Internet must be regulated to prevent terrorism," *CNN*, June 4, 2017. Available at: http://money.cnn.com/2017/06/04/technology/social-media-terrorism-extremism-london/index.html.

68 See, e.g.: Javier E. David, "Angela Merkel caught on hot mic griping to Facebook CEO over anti-immigrant posts," *CNBC*, September 27, 2015. Available at: https://www.cnbc.com/2015/09/27/angela-merkel-caught-on-hot-mic-pressing-facebook-ceo-over-anti-immigrant-posts.html.
See also: Timothy B. Lee, "Racist Daily Stormer goes down again as Cloudflare drops support," *Ars Technica*, August 16, 2017. Available at: https://arstechnica.com/tech-policy/2017/08/racist-daily-stormer-goes-down-again-as-cloudflare-drops-support/.

69 See, e.g.: Matthew Karnitschnig, "Cologne puts Germany's 'lying press' on defensive," *Politico*, January 20, 2016. Available at: https://www.politico.eu/article/cologne-puts-germany-lying-media-press-on-defensive-migration-refugees-attacks-sex-assault-nye/.

70 Nathan Ingraham, "Google's Eric Schmidt: 'the solution to government surveillance is to encrypt everything,'" *The Verge*, November 21, 2013. Available at: https://www.theverge.com/2013/11/21/5130472/googles-eric-schmidt-encrypt-everything-to-prevent-government-surveillance.

71 Christopher Wray, Federal Bureau of Investigation, Remarks before the International Conference on Cyber Security, January 9, 2018.

72 Rod J. Rosenstein, U.S. Department of Justice, Deputy Attorney General Delivers Remarks on Encryption at the United States Naval Academy, October 10, 2017.

73 See, e.g.: Robert Graham, "How Terrorists Use Encryption," Countering Terrorism Center at West Point, *CTC Sentinel 9*, no. 6 (June 2016), 15. Available at: https://ctc.usma.edu/how-terrorists-use-encryption/.

74 Lorenzo Vidino, Francesco Marone, and Eva Entenmann, *Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West*, George Washington University Program on Extremism, June 14, 2017, 75. Available at: https://icct.nl/publication/fear-thy-neighbor-radicalization-and-jihadist-attacks-in-the-west/.

75 Lora Shiao, Prepared Statement of Acting Director of Intelligence, National Counterterrorism Center, before the Senate Homeland Security and Governmental Affairs Committee, December 6, 2017, 5.

76 Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired*, November 19, 2015. Available at: https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.

77 Ibid.

78 See: Sebastian Rotella, "ISIS via WhatsApp: 'Blow Yourself Up, O Lion,'" *ProPublica*, July 11, 2016. Available at: https://www.propublica.org/article/isis-via-whatsapp-blow-yourself-up-o-lion.

79 Ibid.

80 Rukmini Callimachi, "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar," *The New York Times*, February 4, 2017. Available at: https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html.

81 Quoted in: Spencer Ackerman, "Apple encryption case risks influencing Russia and China, privacy experts say," *The Guardian*, February 17, 2016. Available at: https://www.theguardian.com/technology/2016/feb/17/apple-fbi-encryption-san-bernardino-russia-china.

82 Sam Oliver, "Apple now storing local China iCloud data in China Telecom datacenters," *Apple Insider*, August 15, 2014. Available at: http://appleinsider.com/articles/14/08/15/apple-now-storing-local-china-icloud-data-in-china-telecom-datacenters.

83 Stewart Baker, "Deposing Tim Cook," *The Washington Post, Volokh Conspiracy Blog*, February 25, 2016. Available at: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/25/deposing-tim-cook/?utm_term=.bca921b73e9e.

84 Damien Sharkov, "Russia is Threatening to Close Facebook Like it Did LinkedIn," *Newsweek*, September 26, 2017. Available at: http://www.newsweek.com/russia-threatening-close-facebook-it-did-linkedin-671263.

85 See: Adam I. Klein, *Decryption Mandates and Global Internet Freedom: Toward a Pragmatic Approach*, Hoover Institution, Aegis Paper Series, no. 1608 (2016), 14-15. Available at: https://www.hoover.org/sites/default/files/research/docs/klein_webreadypdf.pdf.

86 Adam Klein, Michèle Flournoy, and Richard Fontaine, *Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond*, Center for a New American Security, December 2016. Available at: https://www.cnas.org/publications/reports/surveillance-policy.

87 Ibid., 21.

88 See: Ibid., 45.

89 See: Alex Hern, "UK government can force encryption removal, but fears losing, experts say," *The Guardian*, March 29, 2017. Available at: https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act.

90 Ellen Nakashima and Andrea Peterson, "Obama faces growing momentum to support widespread encryption," *The Washington Post*, September16, 2015. Available at: https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html?utm_term=.1f9c8b6c4902.

91 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2004), 392.

92 Cyrus Farivar, "FBI paid at least $1.3M for zero-day to get into San Bernardino iPhone," *Ars Technica*, April 21, 2016. Available at: https://arstechnica.com/tech-policy/2016/04/fbi-paid-at-least-1-3m-for-zero-day-to-get-into-san-bernardino-iphone/.

93 See: Natasha Lomas, "Europe's justice ministers unsure on whether to push for decrypt law," *TechCrunch*, March 29, 2017. Available: https://techcrunch.com/2017/03/29/europes-justice-ministers-unsure-on-whether-to-push-for-decrypt-law/.

94 Věra Jourová, Remarks: "EU-U.S. Data Flows and Privacy Shield," Center for Strategic and International Studies, March 31, 2017.

95 See: Adam I. Klein, *Decryption Mandates and Global Internet Freedom*, Hoover Institution, September 26, 2016. Available at: https://www.hoover.org/research/decryption-mandates-and-global-internet-freedom.

96 Federal Rule of Criminal Procedure 41(b)(6).

97 See: Dustin Volz, "FBI to gain expanded hacking powers as Senate effort to block fails," *Reuters*, November 30, 2016. Available at: https://www.reuters.com/article/us-usa-cyber-congress/fbi-to-gain-expanded-hacking-powers-as-senate-effort-to-block-fails-idUSKBN13P2ER.

98 Compare *United States v. Pawlak*, no. 3:16-CR-306-D(1) (N.D. Texas, May 30, 2017) with *United States v. Michaud*, no. 15-CR-5351 (W.D. Washington, February 17, 2016).

99 *Michaud*, no. 15-CR-5351, Government's Unopposed Motion to Dismiss Indictment Without Prejudice (W.D. Washington, March 17, 2017), 3.

100 See, e.g.: *State v. Diamond*, 2017 WL 163710 (Minnesota Court of Appeals, January 17, 2017).

101 See: Compliance with Court Orders Act of 2016 (discussion draft). Available at: http://www.burr.senate.gov/imo/media/doc/BAG16460.pdf.

102 Rod J. Rosenstein, U.S. Department of Justice, Deputy Attorney General Delivers Remarks on Encryption at the United States Naval Academy, October 10, 2017.

103 Christopher Wray, Federal Bureau of Investigation, Remarks before the International Conference on Cyber Security, January 9, 2018.

104 National Academies of Sciences, Engineering, and Medicine, "Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs," Division on Engineering and Physical Sciences, September 7, 2016. Available at: https://www8.nationalacademies.org/cp/CommitteeView.aspx?key=49806.

105 See: Alexander Meleagrou-Hitchens, et al., *The Travelers: American Jihadists in Syria and Iraq*, George Washington University Program on Extremism, February 2018, 33. Available at: https://extremism.gwu.edu/events/travelers-american-jihadists-syria-and-iraq.

106 Jigsaw, *A Blueprint for Bypassing Extremism*, the Redirect Method, Google. Available at: https://redirectmethod.org/downloads/RedirectMethod-FullMethod-PDF.pdf.

107 Ibid.

108 Ibid., 5.

109 Ibid., 6.

110 Steven Bertoni, "Exclusive Interview: How Jared Kushner Won Trump the White House," *Forbes*, December 20, 2016. Available at: https://www.forbes.com/sites/stevenbertoni/2016/11/22/exclusive-interview-how-jared-kushner-won-trump-the-white-house/#1bcae6263af6.

111 Peter R. Neumann, *Countering Violent Extremism and Radicalisation that Lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region*, Organization for Security and Co-operation in Europe, Office of the Special Representative on Countering Radicalisation and Violent Extremism, September 28, 2017, 64. Available at: https://www.osce.org/chairmanship/346841.

112 Ibid.

113 *Google Public Policy*, "Update on the Global Internet Forum to Counter Terrorism," December 4, 2017. Available at: https://www.blog.google/topics/google-europe/update-global-internet-forum-counter-terrorism/.

114 Ibid.

115 Ibid.

116 See, e.g.: Adam Mosseri, "News Feed FYI: Helping Ensure News on Facebook Is From Trusted Sources," *Facebook Newsroom*, January 19, 2018. Available at: https://newsroom.fb.com/news/2018/01/trusted-sources/.

117 European Commission, Press Release: "Statement: Removing Illegal Content Online: Commission Calls for More Efforts and Faster Progress From All Sides," January 8, 2018. Available at: http://europa.eu/rapid/press-release_STATEMENT-18-63_en.htm.

118 See: Orin S. Kerr and Bruce Schneier, "Encryption Workarounds," *Georgetown Law Journal* (forthcoming), March 20, 2017. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033.

119 Task Force on Terrorism and Ideology, *Defeating Terrorists, Not Terrorism*, Bipartisan Policy Center, September 2017, 68. Available at: https://bipartisanpolicy.org/library/counterterrorism-policy-from-911-to-isis/.

BIPARTISAN POLICY CENTER

The Bipartisan Policy Center is a non-profit organization that combines the best ideas from both parties to promote health, security, and opportunity for all Americans. BPC drives principled and politically viable policy solutions through the power of rigorous analysis, painstaking negotiation, and aggressive advocacy.

bipartisanpolicy.org | 202-204-2400
1225 Eye Street NW, Suite 1000
Washington, D.C. 20005

@BPC_Bipartisan
facebook.com/BipartisanPolicyCenter
instagram.com/BPC_Bipartisan

BPC Policy Areas

Economy
Education
Energy
Evidence
Finance
Governance
Health
Housing
Immigration
Infrastructure
National Security

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000 | Washington, D.C. 20005
202-204-2400 | bipartisanpolicy.org