A HOOVER INSTITUTION ESSAY

An Intelligence Reserve Corps to Counter Terrorist Use of the Internet

DANIEL BYMAN

Aegis Series Paper No. 1810

"Never before in history have terrorists had such easy access to the minds and eyeballs of millions," declared one journalistic account of the Islamic State's propaganda machine and proficient use of Twitter, Facebook, bots, and other modern means of getting its message out. Such views that the group's "mastery of modern digital tools" has transformed terrorism are commonplace and, though usually presented breathlessly, contain some basic truths.[1] Successful terrorist groups are good communicators and they employ the technology of their times. Fighting terrorism today thus requires fighting terrorism on the Internet and otherwise countering the use of advanced communications technologies. President Trump himself stressed this in a tweet after a 2017 terrorist attack in London: "Loser terrorists must be dealt with in a much tougher manner. The internet is their main recruitment tool which we must cut off & use better!"[2] Terrorists are only one dangerous actor on the Internet—and the one this paper focuses on—but other dangers ranging from hostile state intelligence services to criminal groups are also lurking. The above journalist's quote could also apply to Russian disinformation, sophisticated criminal phishing attempts, and other malicious uses of the Internet.

Technology companies have devised an array of innovative approaches to counter terrorist use of the Internet, ranging from using clever algorithms to disrupt extremist accounts to hiring large numbers of skilled personnel to monitor suspicious content.[3] Despite these measures, the US and European governments have considered more regulation.[4] One area that is largely neglected, however, is government personnel policy, a topic that usually produces yawns in the policy world and is beyond the private sector's reach. The US government faces difficulties when malefactors exploit the Internet in part because its personnel are often poorly equipped to handle cutting-edge technological problems. Compared with the private sector, government employees often are poorly paid, while technology companies are suspicious of government—or want to be seen as such by many of their customers. Many companies are multinational and must manage competing goals of different governments around the world and an international workforce. There is often a time-lag issue: the government moves slowly, devoting resources and training to problems as they become acute. In the short- and medium-term, however, the government often lacks capacity to manage a new challenge. This is particularly likely with technological challenges, as the pace of change is so rapid, and this allows terrorists and other bad actors freedom to exploit new developments as governments struggle to catch up.

One way to mitigate this personnel problem is to expand partnerships outside government, drawing on individuals in the private sector where much of the expertise lies. This paper proposes an Intelligence Reserve Corps modeled loosely after military reserve programs. The corps would bring in part-time government personnel with a technical background who would expand the range of skills available to government and increase private sector awareness of government needs. It would mitigate some (though hardly all) of the problems the government faces, including helping make up for salary disparities, strengthening surge and niche capacities, and improving the government's short-term responsiveness, among other benefits. Many companies, however, would not support participation, and cultural and other differences are likely to limit the extent of progress.

This paper proceeds as follows. First, it examines some of the ways in which terrorist groups use the Internet, focusing on the Islamic State in particular, and the limits and problems they have had. Second, it looks at several of the historical problems the US government has had in stopping this use and at the general issues that are likely to plague future efforts regarding terrorist use of new technologies. Finally, the paper details some of the parameters of an Intelligence Reserve Corps, describing its benefits and its limits.

How Terrorists Use the Internet: A Brief Review

Terrorists' use of the Internet can be broken down into at least three categories: propaganda to inspire and terrorize, direct recruitment, and operational direction. Different parts of the terrorist movement respond to each category.

Perhaps the most-discussed terrorist use of the Internet is to disseminate propaganda. Terrorists have always used the technology of their times. Arabs fighting in Afghanistan created *Jihad* magazine to spread their message and encourage other Arabs to join the caravan of jihad. In the early 1990s, an Osama bin Laden-backed organization used faxes to disseminate criticism of the royal family in Saudi Arabia, roiling politics there. The Saudi jihadist Ibn al-Khattab inspired many Muslims to try to go to fight in Chechnya, disseminating CDs with videos documenting his exploits. After the 2003 US invasion of Iraq, Abu Musab al-Zarqawi became a jihadist superstar when he uploaded video of himself beheading Western hostages there. So it is no surprise that groups active in the Syria conflict, particularly the Islamic State, capitalized on the Internet—and social media in particular—to spread their message.[5]

At its peak, some of the Islamic State maintained active media services such as al-Hayat Media Center and Amaq News Agency that created and disseminated slick online magazines and developed innovative propaganda platforms like a mobile Android-based app for broadcasting its al-Bayan radio station. Much of this media presence was generated or directed from the group's self-proclaimed caliphate in Iraq and Syria. As such, it has been disrupted as the United States and its allies have forced the Islamic State underground. But

much of the propaganda effort is bottom-up, with low-level fighters, sympathizers outside of Iraq and Syria, and other supporters tweeting and otherwise promoting the Islamic State's cause. Islamic State supporters produce videos, poems, and essays and spread official Islamic State pronouncements and images.[6] This enables the Islamic State to have a vast propaganda apparatus without significant official infrastructure.[7]

The Islamic State proved particularly successful in leveraging social media such as Twitter and Facebook to spread its message. In 2015, the Islamic State had over 40,000 Twitter accounts, with about 2,000 of them in English. A RAND study found that the Islamic State drew on almost 80,000 accounts in total, including informal supporters and surrogates who were not directly tied to the group but passed on its propaganda.[8] Part of this presence is simply a reflection of its demographics. The Islamic State's average recruit in the United States is twenty-five years old (European figures are roughly comparable), and younger people are frequent social media users.[9] However, it also reflects the centrality of social media to Islamic State recruiting and propaganda efforts. The RAND study found that many of the Islamic State accounts were exceptionally active—far more so than those of the group's opponents and critics.[10]

Social media offered cheap and effective propaganda capabilities, making it easy to disseminate information, including powerful media images. The Islamic State's 2014 videos of beheading Western journalists were among the most impactful media events of the year and served the group's purpose of inspiring fear among its enemies (although I would argue the resulting policy response proved a disaster for the Islamic State). Internet propaganda in general allows users to bypass established media outlets and create their own messages. No longer are terrorist groups dependent on traditional media outlets which, in the eyes of terrorists, distort their heroic narrative and wrongly portray them as thugs and sadists.[11] Social media in particular are beneficial for creating a narrative, as large numbers of users can tailor the images the Islamic State generates (or that the users generate themselves) to appeal to a host of micro-communities. Beyond the propaganda itself, social media create networks that can complement face-to-face contacts and enable individuals to form relationships outside their neighborhood, country, or even region. Social media also enable risky behaviors because a user's identity can be concealed—curious individuals can interact with dangerous people with low initial risk, luring them toward the group over time.[12]

Islamic State leaders invested considerable effort and resources into their social media presence. Much of their effort went into creating material for propaganda, which served as "evidence" of their successes and good intentions.[13] The Islamic State put out propaganda in Arabic, English, Russian, French, German, Turkish, Uighur, and even Kurdish, among other languages. Islamic State leaders recognize that their importance and impact can grow in the media even as they lose territory and suffer other reverses, as they have since 2015.[14] In addition, the huge number of images they have generated in the last seven years of fighting and the almost four years of the caliphate will endure: jihadists promoted images of the

anti-Soviet struggle in Afghanistan and the anti-US struggle in Iraq many years after their role in these conflicts peaked.

The propaganda has several audiences. One goal is to attract individuals to the movement and otherwise serve as an aid to recruitment. Even when groups like the Islamic State do not direct an attack, they can encourage attackers through their propaganda. This can range from promises of rewards in the afterlife to images of civilian deaths attributed to US bombing or other supposed atrocities that demand revenge. Martyrdom videos are specifically meant to inspire others, and both al-Qaeda and the Islamic State record and release them systematically. The themes in this propaganda can at times lead individuals with other grievances or psychological problems to latch on to the Islamic State, conducting attacks that are labeled terrorism and seen as part of the group's campaign even when the attacker himself had little if anything to do with the group. Both Europe and the United States have seen attacks by individuals who pledge loyalty to the Islamic State but have had little direct contact with the group. Perhaps more important, official and unofficial recruiters often serve up a steady diet of propaganda to move individuals from curious to committed. In addition, propaganda is a way of sending messages to the enemy, explaining the supposed purpose of the terrorist violence and otherwise telling the story of the terrorist group and trying to maximize its psychological impact.

Propaganda helped attract potential supporters and inspired the occasional "lone wolf" (especially in the United States). But by itself it was not enough to fill the group's ranks. To identify and enlist potential recruits, Islamic State members monitored sites that were ostensibly peaceful but contained content sympathetic to more radical teachings, such as the websites of groups like Tablighi Jamaat or Al-Muhajiroun in Europe. Potential supporters were identified and then separated and "groomed," using direct messaging or private, and potentially more secure, platforms like Telegram, Surespot, WhatsApp, Kik, and Skype, to provide more focused attention.[15]

As individuals engaged more with social media, an "echo chamber" effect occurred. Like-minded individuals reinforced the radical message, often at a rapid pace with extensive back-and-forth, with individual tweets being reposted by hundreds of others. When successful, individuals became isolated, exposed only to the ideas of the Islamic State—a process recruiters encouraged by citing religious teachings that called for shunning non-Muslims and Muslims they considered to be insufficiently zealous.[16] Such efforts paid off. In his studies of American supporters of the Islamic State, analyst Peter Bergen found, "The only profile that ties American militants drawn to the Syrian conflict is that they are active in online jihadist circles."[17]

The virtual and personal interacted via social media. Individuals were able to meet former or current fighters or more experienced recruiters virtually.[18] Whereas in the past,

individuals had to go to a radical mosque or community center for such exposure, they can now hear war stories and gain practical advice on logistics without ever leaving their apartments.[19] Even more important, the process is an interactive one, so they can receive encouragement and advice tailored to their individual circumstances.

Terrorists also use the Internet to direct operations and coordinate logistics with their operatives, though this is increasingly fraught. Anwar al-Awlaki, for example, engaged in a back-and-forth with Fort Hood, Texas, shooter Nidal Malik Hasan, who shot thirteen people there in 2009, convincing him that the attack was justified. *New York Times* reporter Rukmini Callimachi found that Islamic State operatives often kept in near-constant virtual touch with attackers, especially in Europe, prodding them on and guiding their actions. This "cybercoaching" ranged from simple encouragement to help with arranging weapons systems in countries with strict gun laws.[20]

Limits and Disadvantages for Terrorists

Although the Internet offers terrorists many advantages, the effectiveness of terrorists' use of the Internet is often exaggerated and the costs and disadvantages poorly understood.

Terrorists use the technology of their times—they are rarely pioneers, innovators, or otherwise on the edge of the curve. Although the Islamic State is often painted as technologically brilliant, it would be odd if an organization with tens of thousands of young people, many of whom are well educated, did *not* use the Internet extensively. Afghan jihadists' use of magazines, bin Laden's use of faxes, and the Islamic State's use of social media should be expected. Terrorist use of technology usually lags behind more sophisticated criminal organizations and hostile foreign government agencies, to say nothing of cutting-edge technology firms.

Terrorists' personnel resources are often thin. Although large groups may have many highly skilled individuals, it is rare for them to have a critical mass of technology experts. Many recruits are criminals, have violent proclivities, worked in menial jobs, or are otherwise unsuited for cutting-edge technological roles.[21] Most groups cannot pay their people well, at least for extended periods of time, and are vulnerable to arrest and targeting. Groups like al-Qaeda and the Islamic State have tried to recruit experts to their cause with mixed success at best.

Nor is the Internet a particularly effective means of recruitment. Part of the reason the United States had far fewer volunteers for Iraq and Syria was because, unlike Europe, potential recruits had to use the Internet more and had less face-to-face contact with actual jihadists through existing extremist networks. Even for this small number of US recruits, one leading study found that it was personal networks, not online propaganda, that mattered most.[22]

From the Islamic State's point of view, cybercoaching is far less effective than being able to train and control members directly. As terror threat skeptic John Mueller points out, from afar it is hard for the coach to judge the quality of recruits. Failure is common—one recruit shot himself in the leg and another who was tasked to run people down with a car lacked a driving permit. Security is a constant problem: the cybercoach and the recruit must find each other on the open Internet, and if the government is watching (and it is) they are vulnerable. One of the Islamic State's few successful recruitments in the United States, Emanuel Lutchman, was a petty criminal with mental issues. He revealed his sympathies by posting pro-Islamic State content on the Internet (a constant problem for would be Islamic State recruits in the United States) and soon found himself in what he thought was a terrorist cell of four people—the other three being FBI informants.[23]

As Lutchman's experience suggests, many members are poorly trained at counterintelligence. Dependence on the Internet takes this weakness and makes it a broader vulnerability. Volunteers, many of whom see themselves as joining the jihadist equivalent of the marines rather than a clandestine terrorist group, often tweet about their activities, brag and post photos on Facebook, and otherwise incriminate themselves and reveal their membership in a terrorist group. In the beginning of the Syria war, some volunteers even left their location trackers active on their phones, allowing them to be traced in real time.

This poor counterintelligence is often a disaster for the terrorist group. Not only is the clueless volunteer often disrupted, but so too are the individuals who try to recruit him, help him travel, and direct any attack. In one case, a fighter in Syria posted a photo of himself and an Islamic State facility in Syria—a facility that coalition forces then targeted.

When these limits are exploited properly, terrorist groups find the Internet risky, not enabling. In the United States starting around 2014 and in most European countries by 2016, governments monitored social media closely and terrorist groups became highly vulnerable.

Government Limits in Stopping Terrorist Internet Use

Just as terrorist groups have their limits in using technology, so too do governments hunting them. Although parts of the US government, such as components of the National Security Agency (NSA), are cutting-edge, much of the government is not. Susan Landau, an expert on cryptography, noted that the FBI "has long had a technology problem," often making basic mistakes and lacking sufficient numbers of computer-savvy investigators. Homeland Security has similar issues. Many state and local investigators, who are often vital for particular counterterrorism investigations, are even further behind.[24]

The average age of federal government employees is forty-seven, older than both the median age for US workers (forty-two) and people working in the technology sector, who are mostly

in their twenties. As Facebook CEO Mark Zuckerberg once claimed, "Young people are just smarter."[25] Former CIA and NSA director Michael Hayden similarly noted the "massive gap" between technologically smart people in business and the policy world.[26] In addition, the government procurement process is slow, making it hard to keep up on the latest technology. By the time a typical contract is proposed, vetted, approved, and executed, the technology itself may have changed. This problem is even more acute when technology has to be approved for work in a secure environment.

Government also has difficulty attracting top technical talent. In addition to competing for programmers and engineers in general, private sector firms now eagerly seek out individuals with skills once more appropriate to government, such as geospatial data analysis. A conservative estimate is that entry level data analysts earn between $25,000 and $50,000 more in the private sector than in government.[27] As a result, the government often relies on contractors to fill gaps.

Governments thus are often behind the curve or overstretched on expertise on how terrorists are using particular technologies and how to counter it. It may not be until after an attack or major plot that awareness of the importance of a particular platform spreads. At the end of the last decade, terrorists felt their chat rooms were penetrated and otherwise worried that using the Internet would reveal their locations and other dangerous information.[28] However, groups like the Islamic State (and its predecessor organizations) began using Facebook, Twitter, and other platforms to recruit and otherwise advance their operations from the start of the Syrian civil war in 2011. These new platforms were not as well monitored. By 2013, terrorist groups had developed a massive online apparatus—well ahead of when many Western governments began to detect, disrupt, and exploit it. As a result, for several years there was a gap that helped the Islamic State operate recruitment networks in the West, where thousands volunteered to fight for the group. Governments, of course, caught on to this, but it took time for them to formulate and then implement a policy. Indeed, this time-lag problem is structural when it comes to technological issues: the slow government response may always be behind the rapid pace of change.

Technology companies are often suspicious of government. In contrast to the nuclear research community, which grew out of the World War II atomic bomb program and continued with government funding, most Internet companies proudly operate independently of government. The lack of a draft or other government service has also meant that many young professionals have little sense of the realities, both good and bad, of government service. Some tech company employees object to defense-related work on moral grounds. Internet companies fear losing their talent—a vehement internal debate within Google erupted in 2018, for example, over whether to help develop artificial intelligence for the Department of Defense.[29] Part of the suspicion is also due to commercial pressures, as at least some users are vocal in their concerns over government eavesdropping and data privacy in general.[30] Companies may also be particularly concerned about exposing data to

personnel with government links, fearing these personnel will act as government agents, not as company employees.

Increasing both the suspicion and the practical coordination issues, the leading Internet companies are international. Both laws and norms vary considerably between the United States and Europe, let alone between the United States and a range of countries in the developing world and various dictatorships. As a result, government pressure often varies by location, incentivizing companies either to seek out jurisdictions that are the most permissive or, conversely, to bind themselves by policies of their most restrictive important customer. Some may also worry that ties to the United States or another Western government will discredit them with other important customers, such as China.

Counter-messaging on the Internet is often invoked as a solution on the assumption that our message is better than the terrorists'.[31] This, I hope, is true, but it misses the heart of the problem: the terrorists are not trying to win over the majority of the population, or even the majority of the young Muslim males of fighting age who make up their primary source of recruits. The Islamic State, for example, attracted more than five thousand Europeans to fight in Iraq and Syria—a wildly successful recruiting effort by historical standards. Yet this is only a tiny fraction of the more than twenty-five million Muslims in Europe.[32] Messaging has to focus on a very narrow demographic. Even if it is 99 percent successful, that may not be enough.

Beyond this significant limit, government messaging programs tend to be quite bad.[33] Despite the intelligence and hard work of many of those involved, it is difficult to come up with a consistent narrative that will compel the narrow target demographic. Part of the problem is that the reality of US policy—the United States does kill civilians when it bombs terrorist groups, sides with dictatorial regimes in the Middle East, proudly supports Israel, and so on—often involves unpopular stances for Middle Eastern audiences and drowns out more positive messaging. In addition, government agencies demand a certain degree of top-down control. Leaders do not want a twenty-seven-year-old GS-11 tweeting out statements that will be taken as US policy without supervision, which would lead to mistakes and policy confusion. Top-down control and micromanagement go against the spirit of the rapid back-and-forth of social media exchanges. Finally, the government does many things, in contrast to even the largest and most diverse companies, making it hard to develop a single narrative.

An Intelligence Reserve Corps: Functions, Advantages, and Limits

The creation of an Intelligence Reserve Corps (IRC), modeled after the reserves the army and other services use, would be a valuable way to offset several problems the government currently has regarding terrorist use of the Internet. Such a program, however, would face

many limits and would at best ameliorate, rather than eliminate, the problems the United States and other countries have faced in stopping terrorist use of the Internet.

An Intelligence Reserve Corps could be created that is loosely modeled after the reserves maintained by the US Army and other services. Some members of the military go directly to the reserves, while others enter on leaving the active force. The reserves initially train their members as they would full-time, permanent soldiers but then allow them to go to school or work in a civilian job. Reserves attend training one weekend a month to maintain their military-relevant skills and ability to integrate into their home units and organizations. Some go for advanced training and many focus on niche areas such as the specialized programs for physicians and dentists. During the 1980s and 1990s, much of the army's civil affairs and psychological operations capacity was in the reserves. The relative percentage of such specialists in the active force grew as their services were heavily needed in Iraq and Afghanistan. But even in the late 2000s they remained predominantly reservists, as did judge advocate units, chemical battalions, and other specialists. Depending on the nature of the crisis, the government can mobilize individual reserve members, portions of a unit, or an entire unit for a length of time that varies according to the nature of the crisis.

The IRC could draw on two streams for personnel. Some would be individuals familiar with the intelligence community and associated agencies through past service who then sign on for a part-time commitment while working in the private sector. They would spend several days a month on average working in government and play a more significant role during crises. The second stream would be individuals from the technology sector. They would receive a training session on their particular agency and its needs and, like those already from government, would commit to spending on average several days a month working for the government. The corps would be a more formal version of several existing programs that allow government employees to temporarily work for the private sector and where private sector employees loan their skills to government.[34]

Companies would have a valuable role to play. At the very least, they would support staff who participate, as they do for those who are military reservists. Ideally, they would encourage such interaction, accepting mid-career intelligence officers as technology interns, for example, while making sure that participation is seen as professionally rewarding for their full-time employees. Not all, or even most, firms would do so, of course, but some may wish to be partners to Washington or at least be seen as doing so.[35] In addition, companies could train government personnel on the latest technologies.

IRC members could also provide niche capacity. Given the explosion in the number and types of communication, it is unrealistic for the government to have full-time employees who are experts on all of them. For example, part-time employees might examine less-used platforms like XING, monitor potentially violent organizations involved in causes not currently prominent on the radar screen (e.g., radical environmentalism or a particular

ethnic minority overseas), or otherwise cover technologies, issues, or problems that are not top government priorities but may matter in the future.

IRC members could play a valuable role in "surging" intelligence during crises or in response to surprises. The government has at times found itself shorthanded and with limited expertise, particularly in response to a platform or method being used with which the government was not familiar. Over time the government builds capacity, but there are often short-term gaps. Particularly in the event of a terrorist attack or other major problem, intelligence reservists would be "mobilized" and act as full-time personnel until the crisis passed. They could handle the myriad small tasks or briefings that often consume the time of the full-time experts, preventing burnout and freeing up the stronger experts to follow a crisis in more depth. For example, in the event of a 2015 Paris-style terrorist attack overseas, particularly one that involved American personnel, numerous reports from liaison services, speculation on social media, and other information would pour in. At the same time, US government agencies and foreign partners would seek greater situational awareness on the attack, on possible follow-on strikes, and on how to calibrate a response, especially if it involved military force. The resulting information flow and requests for information would be massive. Having trained personnel who could handle relatively easy turnarounds, basic briefings, triage information, and otherwise assist in a crisis would be beneficial.

Surge capacity may be even more necessary at the state and local level if there is a particular problem in one part of the country outside the Washington, DC, area (or other areas with a major federal presence). State and local agencies are often too small to develop technical expertise, yet may need it for particular investigations.[36]

An analyst could not just "drop in" and fully function, but he or she could still make an important contribution. For example, a financial analyst might offer insights into how a terrorist group could evade financial controls in its fundraising and money transfers. He or she would have less immediate knowledge of government processes than a full-time government analyst but would know more about aspects of the private sector and have better contacts there. In addition, because the analyst would regularly train and work with full-time analysts, the transition costs would be lower than bringing in new personnel. At the very least, the analyst could handle lower-skilled tasks, freeing up time for full-time personnel.

An IRC could also alleviate some of the financial differential that makes it difficult for government to attract and retain top technical talent. Given the gap between private and public sector wages, it is not realistic to expect large numbers of skilled technical personnel to forgo the greater income possibilities outside government. However, preserving at least some of the existing government knowledge and attracting public spirit-minded individuals from the private sector is possible. The sacrifices demanded on both ends would be less, making retention and recruitment more feasible.

Increasing the interaction between technology companies and government via the IRC would also reduce, though hardly eliminate, corporate suspicions of government. Too often, technology firms are hostile to the needs and realities of government, with government intentions often being caricatured or portrayed in worst-case scenarios. If more personnel worked for government agencies, they would better understand the often-mundane challenges they face and the legal and regulatory limits on their activities. And they would simply put a more human face on the government. For example, the vehement debate within Google about participating in defense work related to artificial intelligence and drones would benefit if more Google personnel knew the parameters of drone targeting, the problems with human operators that artificial intelligence could reduce, and other benefits of their participation. Reducing such suspicion may be vital in the event of a crisis. As Hayden has noted, Google, Facebook, and other technology companies can usually move much faster than the US government should a threat emerge.[37]

Government personnel, for their part, are often not aware of the personnel challenges, consumer demands, and multicountry legal jurisdictional issues facing technology companies. Greater mixing of personnel from both sectors would facilitate mutual understanding, enable the development of better procedures for sharing information, and otherwise reduce many problems.

It is possible—though by no means assured—that more expertise from the private sector could improve government counter-messaging. Google has pioneered a program that redirects general Internet searches for groups like the Islamic State to video or other content that highlights the group's deficiencies.[38] More broadly, Google, Facebook, and other companies excel at using personalized profiles to direct advertising or other information in a precise and tailored way. As part of this, they are also expert on collecting and analyzing which sales pitches and advertising approaches are most compelling.[39] This is particularly useful for groups like the Islamic State that recruit from only a few segments of the overall Muslim population.

More ineffable, but no less important, an Intelligence Reserve Corps could also involve citizens more in governance problems and challenges. Such interactions are an important way for government to increase awareness of problems and to broaden a sense of citizenship beyond military and government ranks.

Likely Limits

The bureaucratic and political difficulties involved in creating an IRC are considerable. The security clearance process is broken: the current backlog is at 700,000 people.[40] And now it would need to be expanded to bring in more part-time personnel, many of whom regularly work with foreign nationals on cutting-edge issues that the background investigator may not fully understand. In addition, individuals would have to be paid to participate and to

run the program—an expansion of government. This would be difficult to justify to some people as, almost by definition, much of the corps would never be called on or would at best play a supplementary role. Many minor accounts or unusual capabilities may never have their day in the sun.

Cultural differences are also likely to hinder cooperation. Hayden, for example, has attributed the Edward Snowden and Chelsea Manning leaks in part to different generational understandings of loyalty, secrecy, and transparency.[41] Such differences are often quite profound with the technology sector, which has less emphasis on hierarchy than government and stresses openness and global collaboration.

Even without cultural differences, companies have personnel and commercial reasons to limit ties to governments. These range from branding problems that might be linked to an association with unpopular government agencies to a desire to work with foreign governments that are rivals of the United States. For many countries, their workforce is global, and they will need to consider foreign employees' attitudes toward coworkers who associate openly with the US government. It may be smaller firms that have fewer personnel and commercial complexities that play a disproportionate role.

• • •

Terrorists will use the Internet and other new technologies in the future, but the government can limit their effectiveness and often turn the technologies against them. Doing so, however, will require the government to be able to draw more effectively on highly skilled technical personnel. Creating an Intelligence Reserve Corps is one way to bridge this gap.

NOTES

1 Brendan Koerner, "Why ISIS Is Winning the Social Media War," *Wired*, April 2016, accessed July 10, 2018, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat.

2 The tweet, accessed July 10, 2018, is available at https://twitter.com/realDonaldTrump/status/908643633901039617.

3 "Facebook Data Privacy Scandal Has One Silver Lining: Thousands of New Jobs AI Can't Do," *CNBC*, March 23, accessed July 10, 2018, 2018, https://www.cnbc.com/2018/03/23/facebook-privacy-scandal-has-a-plus-thousands-of-new-jobs-ai-cant-do.html.

4 Charles Riley, "Theresa May: Internet Must Be Regulated to Prevent Terrorism," *CNN*, June 4, 2017, accessed July 10, 2018, http://money.cnn.com/2017/06/04/technology/social-media-terrorism-extremism-london/index.html.

5 For a review of the Islamic State's media strategy, see Charlie Winter, "Media Jihad: The Islamic State's Doctrine for Information Warfare," International Centre for the Study of Radicalisation, February 13,

2017, accessed July 10, 2018, http://icsr.info/2017/02/icsr-report-media-jihad-islamic-states-doctrine-information-warfare.

6 Charlie Winter, "The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy," Quilliam, July 2015: 18; *Countering the Virtual Caliphate: Testimony before the House Committee on Foreign Affairs*, 114th Cong. 26–29 (2016) (statement of Peter Neumann, Director, International Centre for the Study of Radicalisation, Department of War Studies, King's College London).

7 On Islamic State media operations, see Craig Whiteside, "Lighting the Path: The Evolution of the Islamic State Media Enterprise, 2003–2016," International Centre for Counter-Terrorism, The Hague, November 2016.

8 Elizabeth Bodine-Baron, Todd Helmus, Madeline Magnuson, and Zev Winkelman, *Examining ISIS Support and Opposition Networks on Twitter* (Santa Monica, CA: RAND Corporation, 2016), 8.

9 *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment: Testimony before the Senate Committee on Homeland Security and Governmental Affairs*, 114th Cong. 47 (2015) (prepared statement of Peter Bergen, director of the International Security Program, New America).

10 Bodine-Baron et al., *Examining the Islamic State*, 8–11.

11 For a discussion, see Bruce Hoffman, *Inside Terrorism* (Columbia University Press, 2006).

12 This draws on the ideas of Tim Stevens and Peter Neumann, "Countering Online Radicalisation: A Strategy for Action," International Centre for the Study of Radicalisation and Political Violence, 2009: 11.

13 Winter, "The Virtual 'Caliphate,'" 7.

14 Charlie Winter, "ISIS Is Using the Media Against Itself," *Atlantic*, March 23, 2016, accessed July 10, 2018, https://www.theatlantic.com/international/archive/2016/03/isis-propaganda-brussels/475002.

15 J. M. Berger, "Tailored Online Interventions: The Islamic State's Recruitment Strategy," *CTC Sentinel* 8, no. 10 (October 2015): 19. See also Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel* 9, no. 6 (June 2016); and *Countering the Virtual Caliphate: Testimony before the House Committee on Foreign Affairs*, 114th Cong. 5–12 (2016) (statement of Seamus Hughes, Deputy Director, Program on Extremism, Center for Cyber and Homeland Security, George Washington University).

16 Lorenzo Vidino and Seamus Hughes, "San Bernardino and the Islamic State Footprint in America," *CTC Sentinel* 8, no. 11 (November/December 2015); Berger, "Tailored Online Interventions."

17 Bergen, testimony on *Jihad 2.0*, 48.

18 See Rukmini Callimachi, "ISIS and the Lonely Young American," *New York Times,* June 27, 2015, accessed July 10, 2018, https://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html.

19 Winter, "The Virtual 'Caliphate,'" 7.

20 Rukmini Callimachi, "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar," *New York Times*, February 4, 2017, accessed July 10, 2018, https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html. See also Daveed Gartenstein-Ross and Nathaniel Barr, "Bloody Ramadan: How the Islamic State Coordinated a Global Terrorist Campaign," *War on the Rocks*, July 20, 2016, accessed July 10, 2018, https://warontherocks.com/2016/07/bloody-ramadan-how-the-islamic-state-coordinated-a-global-terrorist-campaign.

21 For a discussion of terrorist personnel issues, see Jacob Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organizations* (Princeton, NJ: Princeton University Press, 2013).

22 Alexander Meleagrou-Hitchens, Seamus Hughes, and Bennett Clifford, *The Travelers: American Jihadists in Syria and Iraq* (Washington, DC: George Washington University, Program on Extremism, 2018), 9.

23 John Mueller, "The Cybercoaching of Terrorists: Cause for Alarm?" *CTC Sentinel* 10, no. 9 (October 2017): 29–30.

24 "Henry Farrell, "The FBI Blunder on Phone Encryption, Explained," *Washington Post*, May 30, 2018, accessed July 10, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/30/the-fbi-blunder-on-phone-encryption-explained/?utm_term=.d3fe0d5e9b16.

25 Anaele Pelisson and Avery Hartmans, "The Average Age of Employees at All the Top Tech Companies, in One Chart," *Business Insider*, September 11, 2017, accessed July 10, 2018, http://www.businessinsider.com/median-tech-employee-age-chart-2017-8.

26 "Key to Cybersecurity Lies between Policy and Tech, Says Former CIA Director," Carnegie Mellon University, November 9, 2016, accessed July 10, 2018, https://www.cmu.edu/dietrich/news/news-stories/2016/november/michael-hayden-cybersecurity.html.

27 "Spooks for Hire: America's Intelligence Agencies Find Creative Ways to Compete for Talent," *Economist*, March 3, 2018, accessed July 10, 2018, https://www.economist.com/news/united-states/21737535-novel-ways-attract-and-retain-programmers-cyber-security-analysts-and-data.

28 Thomas Hegghammer, "The Future of Jihadism in Europe: A Pessimistic View," *Perspectives on Terrorism* 10, no. 6 (2016), accessed July 10, 2018, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/566/html.

29 Scott Shane, Cade Metz, and Daisuke Wakabayashi, "How a Pentagon Contract Became an Identity Crisis for Google," *New York Times*, May 30, 2018, accessed July 10, 2018, https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html?smprod=nytcore-ipad&smid=nytcore-ipad-share.

30 See Mary Madden and Lee Rainie, "Americans' Attitudes about Privacy, Security and Surveillance," Pew Research Center, May 20, 2015, accessed July 10, 2018, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance.

31 See generally Alberto M. Fernandez, "Here to Stay and Growing: Combating ISIS Propaganda Networks," Brookings Institution, October 21, 2015.

32 "Europe's Growing Muslim Population," Pew Research Center, November 29, 2017, accessed July 10, 2018, http://www.pewforum.org/2017/11/29/europes-growing-muslim-population.

33 For a critical view, see Rita Katz, "The State Department's Twitter War with ISIS is Embarrassing," *Time*, September 16, 2014, accessed July 10, 2018, http://time.com/3387065/isis-twitter-war-state-department.

34 "Spooks for Hire," *The Economist*, March 3, 2018.

35 M. L. Cavanaugh, "Don't Be Evil, Support the Troops," *Wall Street Journal*, April 16, 2018.

36 Farrell, "The FBI Blunder."

37 Ryan Francis, "Former NSA Chief Weighs in on Cyber Security, Cyberespionage at ZertoCon," *Computer World*, May 23, 2017, accessed July 10, 2018, https://www.computerworld.com/article/3198184/security/former-nsa-chief-weighs-in-on-cybersecurity-cyberespionage-at-zertocon.html.

38 Bethan McKernan, "Google's Battle to Stop Isis from Recruiting Online," *The Independent*, September 13, 2016, accessed July 10, 2018, https://www.independent.co.uk/news/uk/google-isis-twitter-facebook-propaganda-syria-war-iraq-plan-stop-recruits-online-a7245656.html.

39 Sara M. Watson, "Russia's Facebook Ads Show How Internet Microtargeting Can Be Weaponized," *Washington Post*, October 12, 2017, accessed July 10, 2018, https://www.washingtonpost.com/news/posteverything/wp/2017/10/12/russias-facebook-ads-show-how-internet-microtargeting-can-be-weaponized/?utm_term=.dcccaf154840.

40 "Spooks for Hire," *Economist*, March 3, 2018.

41 Lizzie Dearden, "Former Intelligence Chief Claims Millennials Leak Secrets Because of 'Cultural Differences,'" *The Independent*, March 11, 2017, accessed July 10, 2018, https://www.independent.co.uk/news/world/americas/wikileaks-cia-files-documents-vault-7-hacking-spying-phones-apple-millennials-blamed-cultural-a7624201.html.

The preferred citation for this publication is Daniel Byman, "An Intelligence Reserve Corps to Counter Terrorist Use of the Internet," Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1810 (July 24, 2018), available at https://www.lawfareblog.com/intelligence-reserve-corps-counter-terrorist-use-internet.

About the Author

DANIEL BYMAN

Daniel Byman is a professor and vice dean at Georgetown University's School of Foreign Service and a senior fellow at the Center for Middle East Policy at Brookings.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION