JARED COHEN is Director of Google Ideas and Adviser to the Executive Chair of Alphabet Inc. He is an Adjunct Senior Fellow at the Council on Foreign Relations.

THE POST-AMERICAN MIDDLE EAST

The Islamic State, or ISIS, is the first terrorist group to hold both physical and digital territory: in addition to the swaths of land it controls in Iraq and Syria, it dominates pockets of the Internet with relative impunity. But it will hardly be the last. Although there are still some fringe terrorist groups in the western Sahel or other rural areas that do not supplement their violence digitally, it is only a matter of time before they also go online. In fact, the next prominent terrorist organization will be more likely to have extensive digital operations than control physical ground.

Although the military battle against the Islamic State is undeniably a top priority, the importance of the digital front should not be underestimated. The group has relied extensively on the Internet to market its poisonous ideology and recruit would-be terrorists. According to the International Centre for the Study of Radicalisation and Political Violence, the territory controlled by the Islamic State now ranks as the place with the highest number of foreign fighters since Afghanistan in the 1980s, with recent estimates putting the total number of foreign recruits at around 20,000, nearly 4,000 of whom hail from Western countries. Many of these recruits made initial contact with the Islamic State and its ideology via the Internet. Other followers, meanwhile, are inspired by the group’s online propaganda to carry out terrorist attacks without traveling to the Middle East.

The Islamic State also relies on the digital sphere to wage psychological warfare, which directly contributes to its physical success. For example, before the group captured the Iraqi city of Mosul in June 2014, it rolled out an extensive online campaign with text, images, and videos that threatened the city’s residents with unparalleled death and destruction. Such intimidation makes it easier to bring populations under the Islamic State’s control and reduces the likelihood of a local revolt.

Foiling the Islamic State’s efforts on the Internet will thus make the group less successful on the battlefield. To date, however, most digital efforts against the Islamic State have been too limited, focusing on specific tactics, such as creating counternarratives to extremism, in lieu of generating a comprehensive strategy. Instead of resorting to a single tool, opponents should treat this fight as they would a military confrontation: by waging a broad-scale counterinsurgency.

KNOW YOUR ENEMY

The first step of this digital war is to understand the enemy. Most analyses of the Islamic State’s online footprint focus on social media. In a Brookings Institution report, J. M. Berger and Jonathon Morgan estimated that in late...
2014, 46,000 Twitter accounts openly supported the group. Back then, strategies for fighting the Islamic State online centered on simply removing such accounts.

Social media platforms are just the tip of the iceberg, however. The Islamic State’s marketing tools run the gamut from popular public platforms to private chat rooms to encrypted messaging systems such as WhatsApp, Kik, Wickr, Zello, and Telegram. At the other end of the spectrum, digital media production houses such as the Al-Furqaan Foundation and the Al-Hayat Media Center—presumably funded by and answering to the Islamic State’s central leadership—churn out professional-grade videos and advertisements.

Yet understanding the full extent of the Islamic State’s marketing efforts without knowing who is behind them is not an actionable insight; it is like understanding how much land the group controls without knowing what kinds of fighters occupy it and how they hold it. An effective counterinsurgency requires comprehending the Islamic State’s hierarchy. Unlike al Qaeda, which comprises a loose cluster of isolated cells, the Islamic State resembles something akin to a corporation. On the ground in Iraq and Syria, a highly educated leadership sets its ideological agenda, a managerial layer implements this ideology, and a large rank and file contributes fighters, recruiters, videographers, jihadist wives, and people with every other necessary skill. This hierarchy is replicated online, where the Islamic State operates as a pyramid consisting of four types of digital fighters.

At the top sits the Islamic State’s central command for digital operations, which gives orders and provides resources for disseminating content. Although its numbers are small, its operations are highly organized. According to Berger, for example, the origins of most of the Islamic State’s marketing material on Twitter can be traced to a small set of accounts with strict privacy settings and few followers. By distributing their messages to a limited network outside the public eye, these accounts can avoid being flagged for terms-of-service violations. But the content they issue eventually trickles down to the second tier of the pyramid: the Islamic State’s digital rank and file.

This type of fighter may or may not operate offline as well. He and his ilk run digital accounts that are connected to the central command and disseminate material through guerrilla-marketing tactics. In June 2014, for example, Islamic State supporters hijacked trending hashtags related to the World Cup to flood soccer fans with propaganda. Because they operate on the frontline of the digital battlefield, these fighters often find their accounts suspended for terms-of-service violations, and they may therefore keep backup accounts. And to make each new account appear more influential than it really is, they purchase fake followers from social media marketing firms; just $10 can boost one’s follower count by tens of thousands.

Then there are the vast numbers of radical sympathizers across the globe, who constitute the Islamic State’s third type of digital fighter. Unlike the rank and file, they do not belong to the Islamic State’s official army, take direct orders from its leadership, or reside in Iraq or Syria. But once drawn into the Islamic State’s echo chamber by the
rank and file, they spend their time helping the group disseminate its radical message and convert people to its cause. These are often the people who identify and engage potential recruits on an individual level, developing online relationships strong enough to result in physical travel. In June, for example, The New York Times documented how a radical Islamist in the United Kingdom met a young woman from Washington State online and convinced her to consider heading to Syria.

Although joining the Islamic State’s operations in Iraq and Syria may be illegal, spreading extremism online is not. These fighters are masters at taking advantage of their right to free speech, and their strength lies both in their numbers and in their willingness to mimic the Islamic State’s official line without having to receive direct orders from its leadership.

The Islamic State’s fourth type of digital fighter is nonhuman: the tens of thousands of fake accounts that automate the dissemination of its content and multiply its message. On Twitter, for example, so-called Twitter bots automatically flood the digital space with retweets of terrorist messages; countless online tutorials explain how to write these relatively simple programs. In comment sections on Facebook, YouTube, and other sites, such automated accounts can monopolize the conversation with extremist propaganda and marginalize moderate voices. This programmable army ensures that whatever content the Islamic State’s digital central command issues will make its way across as many screens as possible.

**RECAPTURING DIGITAL TERRITORY**

Much of the debate over how to combat the Islamic State on the ground has been binary, split between those proposing containment and those insisting on its defeat. The best strategy for fighting it online, however, is something else: marginalization. The result would be something similar to what has happened to the Revolutionary Armed Forces of Colombia, or FARC, the narcoterrorist group that grabbed headlines throughout the 1990s for its high-profile kidnappings and savage guerrilla warfare. Today, the group has been neither disbanded nor entirely defeated, but its ranks have largely been driven into the jungle.

Along the same lines, the Islamic State will be neutered as a digital threat when its online presence becomes barely noticeable. The group would find it either too risky or tactically impossible to commandeer control of social media platforms and public chat rooms, and its digital content would be hard to discover. Incapable of growing its online ranks, it would see its ratio of digital fighters to human fighters fall to one to one. It would be forced to operate primarily on the so-called dark Web, the part of the Internet not indexed by mainstream search engines and accessible to only the most knowledgeable users.

Compelling terrorist organizations to operate in secret does make plots more difficult to intercept, but in the case of the Islamic State, that is a tradeoff worth making. Every day, the group’s message reaches millions of people, some of whom become proponents of the Islamic State or even fighters for its cause. Preventing it from dominating digital territory would help stanch the replenishment of its physical ranks, reduce its impact on
Fangirls: two women charged with plotting ISIS-inspired attacks in New York, April 2015

the public psyche, and destroy its most fundamental means of communication.

It will take a broad coalition to marginalize the Islamic State online: from governments and companies to nonprofits and international organizations. First, they should separate the human-run accounts on social networks from the automated ones. Next, they should zero in on the Islamic State’s digital central command, identifying and suspending the specific accounts responsible for setting strategy and giving orders to the rest of its online army. When that is done, digital society at large should push the remaining rank and file into the digital equivalent of a remote cave.

The suspension of accounts needs to be targeted—more like kill-or-capture raids than strategic bombing campaigns. Blanket suspensions covering any accounts that violate terms of service could not guarantee that the leadership will be affected. In fact, as Berger and Morgan’s research highlighted, the Islamic State has learned to protect its digital leadership from suspension by keeping its activities hidden behind strict privacy settings.

This is not to downplay the importance of banning users who break the rules and distribute terrorist content. Technology companies have become skilled at doing just that. In 2014, the British Counter Terrorism Internet Referral Unit, a service run by London’s Metropolitan Police, worked closely with such companies as Google, Facebook, and Twitter to flag more than 46,000
pieces of violent or hateful content for removal. That same year, YouTube took down approximately 14 million videos. In April 2015, Twitter announced that it had suspended 10,000 accounts linked to the Islamic State on a single day. Such efforts are valuable in that they provide a cleaner digital environment for millions of users. But they would be doubly so if the leadership that orders terrorist content to be distributed were also eliminated.

That, in turn, will require mapping the Islamic State’s network of accounts. One way law enforcement could make inroads into this digital network is by covertly infiltrating the Islamic State’s real-world network. This technique has already achieved some success. In April, the FBI arrested two young women accused of plotting attacks in New York City after a two-year investigation that had relied extensively on their social media activity for evidence. Law enforcement should scale such efforts to focus on the digital domain and target the Islamic State’s digital leadership, suspending the accounts of its members and arresting them in certain cases.

Once the Islamic State’s online leadership has been separated from the rank and file, the rank and file will become significantly less coordinated and therefore less effective. The next step would be to reduce the group’s level of online activity overall, so that it is forced into the margins of digital society. During this phase, the danger is that online, the Islamic State might splinter into less coordinated but more aggressive rogue groups. With a higher tolerance for risk, these groups might undertake “doxing” of opponents of the Islamic State, whereby the private information (such as the address and social security number) of a target is revealed, or “distributed denial-of-service attacks,” which can take down an entire website.

To mitigate this threat, the digital fighters’ activities need to be diverted away from extremism altogether. This is where counternarratives against violent extremism can come in. Over the last two years, several notable efforts have been launched, including video series produced by the Arab Center for Scientific Research and Humane Studies and the Institute for Strategic Dialogue. To be effective, these campaigns need to reflect the diversity of the group’s ranks: professional jihadist fighters, former Iraqi soldiers, deeply religious Islamic scholars, young men in search of adventure, local residents joining out of fear or ambition. Moderate religious messages may work for the pious recruit, but not for the lonely British teenager who was promised multiple wives and a sense of belonging in Syria. He might be better served by something more similar to suicide-prevention and anti-bullying campaigns.

For maximum effect, these campaigns should be carefully targeted. An antie xtremist video viewed by 50,000 of the right kinds of people will have a greater impact than one seen by 50 million random viewers. Consider Abdullah-X, a cartoon series marketed through a YouTube campaign funded by the European Union. Its pilot episode was promoted using targeted advertising oriented toward those interested in extremist Islam. Eighty percent of the YouTube users who watched it found it through targeted ads rather than through unrelated searches.
Given the diversity of the Islamic State’s digital rank and file, however, betting on counternarratives alone would be too risky. To combat extremists who have already made up their minds, the coalition should target their willingness to operate in the open. Al Qaeda has taken pains to keep its digital operations secret and works under the cover of passwords, encryption, and rigid privacy settings. These tactics have made the group notoriously difficult to track, but they have also kept its digital footprint miniscule. Likewise, the Islamic State’s rank and file should be forced to adopt similar behavior.

Achieving this will require creativity. For example, governments should consider working with the news media to aggressively publicize arrests that result from covert infiltration of the Islamic State’s online network. If any new account with which a digital soldier interacts carries the risk of being that of an undercover agent, it becomes exponentially more hazardous to recruit new members. Law enforcement could also create visual presentations showing how police investigations of digital extremists’ accounts can lead to arrests, thereby telling the cautionary tale that a single mistake can cause the downfall of a digital soldier and his entire social network.

Within the next few years, new high-tech tools may become available to help governments marginalize digital rank-and-file terrorists. One is machine learning. Just as online advertisers can target ads to users with a particular set of interests, law enforcement could use algorithmic analysis to identify, map, and deactivate the accounts of terrorist supporters. Assisted by machine
learning, such campaigns could battle the Islamic State online with newfound precision and reach a scale that would not be possible with a manual approach.

It is worth noting that just like a physical counterinsurgency, a digital counterinsurgency is more likely to succeed when bolstered by the participation of local communities. All the online platforms the Islamic State uses have forum moderators, the equivalent of tribal leaders and sheiks. The technology companies that own these platforms have no interest in seeing their environments flooded with fake accounts and violent messages. They should therefore give these moderators the tools and training to keep their communities safe from extremist messaging. Here again, machine learning could someday help, by automatically identifying terrorist messages and either highlighting them for moderators or blocking them on their behalf.

ACCESS DENIED
At first glance, the Islamic State can look hopelessly dominant online, with its persistent army of propaganda peddlers and automated trolls. In fact, however, the group is at a distinct disadvantage when it comes to resources and numbers. The vast majority of Internet users disagree with its message, and the platforms that its fighters use belong to companies that oppose its ideology.

There is no doubt that undertaking a digital counterinsurgency campaign represents uncharted territory. But the costs of failure are low, for unlike in a real-world counterinsurgency, those who fight digitally face no risk of injury or death. That is yet another factor making the Islamic State particularly vulnerable online, since it means that the group’s opponents can apply and discard new ways of fighting terrorism quickly to hone their strategy.

The benefits of digitally marginalizing the Islamic State, meanwhile, are manifold. Not only would neutering the group online improve the lives of millions of users who would no longer be as likely to encounter the group’s propaganda; it would also make the group’s real-world defeat more imminent. As the Islamic State’s digital platforms, communication methods, and soldiers became less accessible, the group would find it harder to coordinate its physical attacks and replenish its ranks. And those fighting it online would gain valuable experience for when the time came to fight the next global terrorist group trying to win the Internet.