Georgetown Journal
of International Affairs

International Engagement on Cyber VII

Unveiling the "United Cyber Caliphate" and the Birth of the E-Terrorist

Christina Schori Liang

June 2017 marked the third anniversary of the self-proclamation of the so-called Islamic State in Iraq and Syria (ISIS, Islamic State, or IS). In the last few years IS's strategic military campaign rapidly took over large swaths of Syria and Iraq, taking its opponents by surprise. But the so-called caliphate is currently on the retreat, having lost over 60 percent of the territory in Syria and Iraq that it captured nearly three years ago. While IS is increasingly under pressure in the physical world, it is boldly conquering the digital domain, where IS is taking advantage of many conflicts across the globe; the growing duality of our virtual/physical reality; its own dynamic meta-narrative, which has a special appeal to the millennial generation; and most important; the Internet. Never in history has an organization with so few people and so little means managed to acquire so much wealth ($2 billion in 2015), a global following (30,000 IS aspirants from 80 countries in Syria and Iraq alone), with such geopolitical reach (operational in 18 countries across the world), and created so much terror (attacks in 14 countries in the first half of 2017 alone, killing over 660 people and injuring over 7,363).

Regardless of a US-led opposition coalition that includes seventy countries, IS is still far from being disrupted. While some policymakers and analysts believe that expelling the self-proclaimed "Islamic State" from its territory will be the key to its destruction, this seems unjustified. In a recent Pew survey, eighteen countries regarded IS as their leading security threat.[1] Many IS fighters will survive by simply going underground, keeping out of sight until they can join others in jihadist theaters further afield, or taking cover in Syria and Iraq, only to regroup in order to conduct sporadic raids or spectacular suicide attacks later.

This paper analyzes the continuing appeal of IS's meta-narrative while describing the current political situation that is feeding its success. It will also define the new digital battlespace and outline how IS is scaling up its use of the Internet not only as a proselytism, propaganda, recruitment, and fundraising tool but, more recently, as a weapon of war. IS is building up its new "cyber caliphate" and cyber army focused on collecting intelligence, coordinating operations, and unleashing cyber jihad. While still using mostly conventional practices, it is looking to acquire innovative new cyber weapons. Finally, the paper will describe what is currently being done to confront this extremely innovative form of terror.

The Continuing Appeal of a Jihadist Identity

The battle against IS is still mostly limited to the physical world. Since 2014, the global coalition has spent over $22.2 billion in support of humanitarian assistance, stabilization, explosive hazards removal, and economic support in Iraq and Syria.[2] The US spent nearly $11.5 billion from August 2014 to January 31, 2017, on the fight against IS.[3] Nearly 40 percent of US funds

Christina Schori Liang is leading the Terrorism and Organized Crime Cluster at the Geneva Centre for Security Policy and is a visiting professor at the Paris School of International Affairs, Sciences Po.

spent—$4.6 billion—has been for military actions or missions. The average cost of fighting the terrorist group is now $12.7 million a day. Money spent on intelligence, surveillance, and reconnaissance (ISR) has been less than 1 percent of the costs so far.[4] Many experts have concluded that these efforts, which have led to IS's expulsion from Mosul and Raqqa, mark the beginning of the end of the terror state.

Yet this assessment ignores other developments. In August 2016, it was reported that groups affiliated with IS were operational in eighteen countries, and as the US National Counterterrorism Center recently stated, there is clear evidence of "aspiring branches" in Mali, Egypt, Somalia, Bangladesh, Indonesia, and the Philippines.[5] IS is now in the process of mutating, like al-Qaeda did several times after the September 11, 2001, attacks, and the final model has yet to be understood. At the same time, a new global terrorist diaspora is forming made up of old and new terrorist fighters who will either go on to support other civil wars or who will try to reach other IS strongholds in Afghanistan, Algeria, Libya, and parts of West Africa.[6] And simultaneously, a new and more nefarious jihadi cyber army is being born, attacking websites, spreading worms, and posting "kill lists" that include the founders of Facebook and Twitter.

IS has managed to attract a global following of transnational actors that Gunaratna claims include a million followers worldwide.[7] As IS shrinks in the physical world, it seems to be creating a new identity and repositioning itself as a cyber caliphate, undertaking operations in the digital world from its relatively secure encrypted cyber domain.

There are multiple reasons why such a strategy might give IS a new lease on life. There is a growing spirit of restlessness across the globe, in which many youth no longer find hope in a world seemingly poised for even greater conflict and instability. Political uncertainties are fueling nationalist political rhetoric that is linking terrorist acts with specific ethnicities and Islam. This rising Islamophobia has helped populist groups in the West, and especially in Europe, gain power. Political leaders, journalists, and social media are propagating messages about a "global war on terrorism" and a "clash of civilizations." US president George W. Bush's initial announcement of a global war on terror in 2001 has in fact become a self-fulfilling prophecy driving the globalization of terrorism, since it is largely supporting IS's own rhetoric about a clash of civilizations worldwide. In its first edition of its widely disseminated electronic journal *Dabiq*, IS claimed that "the world has divided into two camps"—"the camp of Islam and faith" and "the camp of the *kufr* (disbelief) and hypocrisy." For them there is indeed a global war between "the camp of Muslims and the mujahideen everywhere and the camp of the jews [*sic*], the crusaders, their allies, and with them the rest of the nations and religions of the *kufr*, all being led by America and Russia, and being mobilized by the jews [*sic*]."[8]

The current anti-jihadist rhetoric that is sometimes repackaged into anti-Muslim rhetoric by Western government officials and the media has created an environment that has allowed jihadist websites to propagate conspiracy theories in a process that has become all the more resonant in the era of "fake news" and "post-truth." Some policymakers have realized that the stereotypes about Muslims and terrorists that are constantly being paraded through the media are serving to support IS's strategic messaging that claims that the West is at war with Islam. In a dramatic turnaround, the Associated Press has recently announced that, among other words and expressions,

"Islamist" and "terrorist" are no longer acceptable. The term "Islamist" will be dropped altogether and the perpetrators of Islamist terrorist attacks are to be called "militants," "attackers," or "lone wolves."[9] This is a step in the right direction, and politicians must also now ensure that they do not vilify Muslims or Islamic values in order to ensure that grievances exploited by extremists are not exacerbated. This type of rhetoric also derails prevention programs and counternarratives employed against IS recruitment.

The current anti-jihadist rhetoric that is sometimes repackaged into anti-Muslim rhetoric by Western government officials and the media has created an environment that has allowed jihadist websites to propagate conspiracy theories in a process that has become all the more resonant in the era of "fake news" and "post-truth."

The extensive period of conflict in the Middle East and North Africa (MENA) has created thousands of disaffected Muslims who are either displaced, homeless, or undocumented refugees or migrants in search of new identities. The global coalition against Daesh, militias, and ethnic groups is deeply embroiled in protracted proxy wars aimed at changing borders, dividing states, and giving birth to new ones. Many states in the MENA already fear that the conflict will spill over and terrorist attacks will play out within their borders must also worry about 25.4 million refugees escaping conflict, exacerbating the problems faced by already fragile governments.[10] These refugees are seeking a new narrative and identity. IS fills the void and helps provide them with one.

Another new source of recruitment is constituted by the thousands of Syrian children affected by war who represent a lost generation—uneducated, malnourished, and orphaned. They are perfect victims to be recruited by Salafi jihadists and military groups that need only promise them a meal a day and salvation to win their devotion. If nothing is done now to save them, they will help proliferate terrorism for years to come, as has been evidenced by Taliban and Northern Alliance soldiers who were products of their traumatic and violent childhoods.[11]

Terrorism in Europe has illuminated the growing ethnic and social enclaves in some European cities where multiculturalism is still not acknowledged and where governments are imposing cultural conformity, creating alienated, unhappy, and disgruntled youth. With the ongoing political rhetoric and negative news cycle, second- and third-generation young Muslim citizens in sectarian countries no longer feel respected or wanted in their own homelands. Roy argues that it is not the radicalization of Islam, but "the Islamification of radicalism" that is at work, maintaining that second-generation immigrants were caught between the tradition-bound world of their parents and the secularism of modern Europe.[12] Without a home or a place in society, young Muslims adopted a nihilistic rejection of society, not in the Marxist language of the 1960s and 1970s, but in the language of its current equivalent: Islam. Adolescents are searching for meaning through faith but do not have the level of religious background to understand the nuances of the "religion" they are signing up for. They are thus easily manipulated by the Salafi jihadists who offer them simple answers to complex problems. They can either choose *hijrah* (migration to the so-called caliphate) or conduct jihad at home. Countries are targeted not only for what they "represent" (blasphemy, moral decay), but also for what they "do" (support for the global coalition against Daesh).

The jihadists manage to make it everyone's personal obligation to defend their fellow Muslims. They promise martyrdom and paradise for those who die defending their fellow Muslims against persecution. Their literature is highly persuasive and their online, paid recruiters are relentless.

European secularist governments, unwilling to acknowledge and accept their increasingly multiethnic, multicultural, and growing Muslim diaspora, have helped to create an environment that has allowed Salafist jihadism to thrive. The ecosystem of the threat of terror and the violence that is carried out in the West is helping to feed Islamophobia, which creates more violence against Muslims, which drives more Muslims to radicalize, thus becoming a self-perpetuating cycle of hate and violence.

> **The ecosystem of the threat of terror and the violence that is carried out in the West is helping to feed Islamophobia, which creates more violence against Muslims, which drives more Muslims to radicalize, thus becoming a self-perpetuating cycle of hate and violence.**

The Digital Battlespace

The persistence of a jihadist identity in a world riddled with conflict, migration, and Islamophobia has allowed IS to send its message unimpeded in cyberspace, where it has global access to anyone who owns a computer or a smart phone. Most militaries have not yet grasped the fact that the world's most dangerous influences can be transmitted by phone. While countless terrorist organizations are also successful in maintaining power, the speed and power of the global IS phenomenon has yet to be fully analyzed and acknowledged. Both policymakers and analysts are still grappling with IS's ability to structure messages and use the Internet to attract a global following.

IS is tapping into a new phenomenon that policymakers and military cadres do not acknowledge: the fact that modern society maintains a double life—real and virtual. Both young and old are increasingly online, and technology has become a significant part of daily life. IS has identified the growing trend of video games, copying online games and Hollywood-style action movies by producing Clang of Swords videos and mimicking Call of Duty and Grand Theft Auto online games. These games allow the player to mimic an experience they can have in real life while serving the "caliphate," blowing up tanks and killing enemies, which will lead to martyrdom and eternal life.

IS is exploiting this new online life that modern youth are adopting by reaching out to disaffected individuals on a global scale, evoking the creation of not only a new physical "caliphate," but also a "cyber caliphate."

The Alluring, Inclusive, and Dynamic "Caliphate" Narrative

IS propagates an inclusive, fluid, and dynamic global caliphate narrative, winning support from groups spanning from Africa to Southeast Asia. IS reaches out to all walks of life, ranging from the low-hanging fruit of convicted criminals to elite professionals—doctors, professors, cyber technicians, and engineers. The group has enough resources to send its messages in twenty-eight languages and through multiple social media platforms, such as AskFM, WhatsApp, Tumblr, Instagram, Facebook, SoundCloud, and Twitter. It is consequently the most globalized terrorist organization in the world. At the founding of the so-called Islamic State, the new "caliph," Abu Bakr al-Baghdadi, proclaimed that the caliphate

would ultimately encompass Caucasians, Indians, Chinese, Iraqis, Syrians, and even Americans.[13] Foreseeing that ultimately IS would lose ground and would find it difficult to hold land, in August 2016 Abu Muhammad al-Adnani, shortly before he was killed, published the following message:

> O America, would we be defeated and you be victorious if you were to take Mosul or Sirte or Raqqa? . . . Certainly not! We would be defeated and you victorious only if you were able to remove the Koran from Muslims' hearts.[14]

Following this statement, IS is promoting a new digital future in which there is no need for land, since the "caliphate" can now be virtual in a digital domain.

IS has therefore defined land/territory as lying in the heart of every Muslim who supports its caliphate online, so even if cities and states are recaptured, or it is physically impossible to travel to the caliphate, the virtual caliphate will always exist and cannot be destroyed (in a similar way, e-Estonia has planned to maintain its entity should the physical Estonia be overcome).[15]

IS has therefore defined land/territory as lying in the heart of every Muslim who supports its caliphate online, so even if cities and states are recaptured, or it is physically impossible to travel to the caliphate, the virtual caliphate will always exist and cannot be destroyed.

It is most likely that just as currently cyber-warriors are being asked to join IS, there will be a call for e-citizens to join the cyber caliphate. There are already calls to support the cyber caliphate by donating time, expertise, and money. IS is offering young people meaning and purpose by giving them tasks to support the caliphate. In a recent online guidebook, *Advice to Those Who Cannot Come to Shām* by Abū Sa'aeed Al-Britāni,[16] which was posted on Telegram, a chapter titled "Working for the *Dawlah* through Social Media" gives a list possibilities for how IS supporters can work for the organization online, including spreading material such as articles, books, posters, and videos, which can be posted to new links, or uploading new videos on the website JustPaste.it. A second task for those with knowledge of Photoshop is assisting in graphic design. A third task is to hack into people's email to get home addresses. IS also looks for expertise in credit card fraud, including stealing people's bank details. If recruits need help, they can contact Al-Britāni via Kik. Al-Britāni states that this is only temporary work: the real goal should be martyrdom, and everyone should always have an escape plan in place for when it might be needed.

The "United Cyber Caliphate" and E-Terrorists

The future of IS will undoubtedly include a strong cyber presence at all levels of the World Wide Web. Most people surf the surface web, the online world that contains Google, Facebook, and Twitter. But not far below the surface lurks another hidden network of sites—the Deep Web—that hosts communities and platforms where people can meet only if they are invited or if they already know the relevant IP address. Here IS convenes in chat rooms and web forums away from the prying eyes of intelligence actors and security forces. One layer deeper is an even more secure part of the web known as the Dark Web, which can be accessed only through specialized browsers. Over half of its content is occupied by illegal content, illicit finances, and drug and weapons hubs.[17]

Terrorists have been active in this domain since the late 1990s. Many have migrated to the Dark Web after the Snowden revelations and when hundreds of IS websites were taken down after the November 2015 terrorist attacks in Paris. IS's Al-Hayat Media Center has recently posted links and information on how to access the Dark Web. Telegram has become the preferred application since it went live in August 2014 and announced its Channel application in September 2015. By March 2016 IS had opened over 700 channels. They include a staggering number of members, with one channel hosting over 10,000.[18] Terrorists use the Dark Web for propaganda, fund-raising, purchasing illegal weapons, and soliciting online donations, including Bitcoin. Terrorists store their illegal propaganda (videos, books, articles) here safely behind encrypted applications. IS will most likely search for vulnerabilities in the Deep Web by attacking banks and medical institutions. For an overview of the many apps and websites that IS uses to spread its propaganda while remaining anonymous for its operations, see figure 1.

> **Terrorists use the Dark Web for propaganda, fund-raising, purchasing illegal weapons, and soliciting online donations, including Bitcoin. Terrorists store their illegal propaganda (videos, books, articles) here safely behind encrypted applications.**

Several hacker teams have conducted cyber operations under the IS banner. In April 2016, many of these teams united to form the so-called United Cyber Caliphate (UCC); the group comprises the subgroups known as the Cyber Caliphate Army, Ghost Caliphate Section, Sons of the Caliphate Arms, and Kalachnikov E-Security.[19] In the last six months, the UCC has carried out cyber operations, recruited new followers, and offered security advice on how not to be detected and how to conduct terror operations. UCC recently released a video message threatening the US and President Trump, together with a "kill list" of 8,786 names and addresses, commanding IS followers to "kill them wherever you find them." It has also called Muslim hackers to join its ranks against the "disbelievers." In February 2017, it published four *Security Tips* manuals covering issues such as Windows 10, password managers, and how to patch security vulnerabilities. In January 2017, the UCC and the Cyber *Kahilafah* disseminated a PDF copy of the *Anarchist Cookbook*, a 1971 book that contains instruction manuals on bomb making, firearms use, and building traps.

The Future of Cyber Operations

While IS members have yet to acquire the expertise of groups backed by nation-states, such as the Russian Bears, Iran's Kittens, and China's Pandas,[20] who have the ability to hack industrial infrastructure, IS has stated that it is interested in building up its cyber army to conduct future asymmetrical attacks. New destructive hacker technology has been leaked, creating new opportunities for terrorists and criminals alike. The US National Security Agency (NSA) subcontractor Equation Group was recently hacked, and destructive hacker toolkits that are capable of seizing control of computers, watching and capturing keystrokes, and penetrating security firewalls were stolen. The organization Shadow Brokers has acquired these cyber weapons and has attempted to sell them online for millions of Bitcoin. These weapons have the potential to be bought by IS supporters who could use them to cause widespread devastation. Shadow Brokers

App/website icon	Name of App/website
Surface web	
Reddit	Reddit
tumblr.	Tumblr
YouTube	YouTube
Instagram	Instagram
LinkedIn	LinkedIn
Twitter	Twitter
Facebook	Facebook
AskFM	AskFM
WhatsApp	WhatsApp
KIK	KIK
SoundCloud	SoundCloud
Deep web	
HSBC	HSBC (and most international banks)
Rod of Asclepius	Rod of Asclepius—a symbol frequently associated with medicine and health care (websites and organisations that store health and medical records)
Dark web	
Tor	The Onion Router
Bitmessage	Bitmessage
Dark Wallet	Dark Wallet
Telegram	Telegram
Silent Circle	Silent Circle
ProtonMail	ProtonMail
TrueCrypt	TrueCrypt
Signal	Signal
wickr	Wickr
Threema	Threema
Viber	Viber
Conversations	Conversations

Figure 1: IS Presence in the World Wide Web

has so far leaked over a gigabyte's worth of the NSA's weaponized software exploits and hacking tools since they were stolen in the fall of 2016.

In another security breach, WikiLeaks published a leak, called Vault 7, consisting of approximately 9,000 files that detail the activities and capabilities of the CIA Center for Cyber Intelligence to carry out surveillance and cyberwarfare, giving the tools that are used to break into phones and communication apps. This release has helped to close the gap between the capabilities of states and those of terrorists and criminals. IS has been trying to find ways to wage more effective asymmetric warfare and obtaining these toolkits and inside information would be its greatest prize.

Along with these new revelations, the head of the NSA, Mike Rogers, stated that "the NSA has never seen the field of signals intelligence change as rapidly as it is right now." Both IS and nation-states are constantly changing their communications strategies and are upgrading their technology with increasing complexity and speed. Rogers stated that "ISIS wants to break America's will," believes "we are inherently weak, that we can't stand the pressure," and "believes if they contest our ability to lead normal lives . . . they will break our will."[21] Defeating this goal has spurred a dialogue between the intelligence community and major information companies such as Google, Apple, Facebook, and Yahoo.

Global Internet Forum to Counter Terrorism

On June 26, 2017, the Global Internet Forum to Counter Terrorism was formed—formalizing and structuring areas of collaboration between giant tech companies, smaller tech companies, civil society groups, academics, governments, and supranational

organizations. The work of the forum focuses on the following three methods to tackle terrorism online:

1. Technological solutions
2. Research
3. Knowledge sharing

While the US and UK have improved their cybercapabilities, recent security leaks have put them on the defensive. The US Cyber Command, a six-year-old military branch, is planning to expand its force to 6,000 employees and will in the future use such tools as data dragnets, disrupted cell towers, compromised microwave relays, intercepted communications, and subverted satellites. The US is planning an independent cyber command that will be separate from the NSA and will put the digital fight on the same footing as US land, air, sea, and space defense efforts.
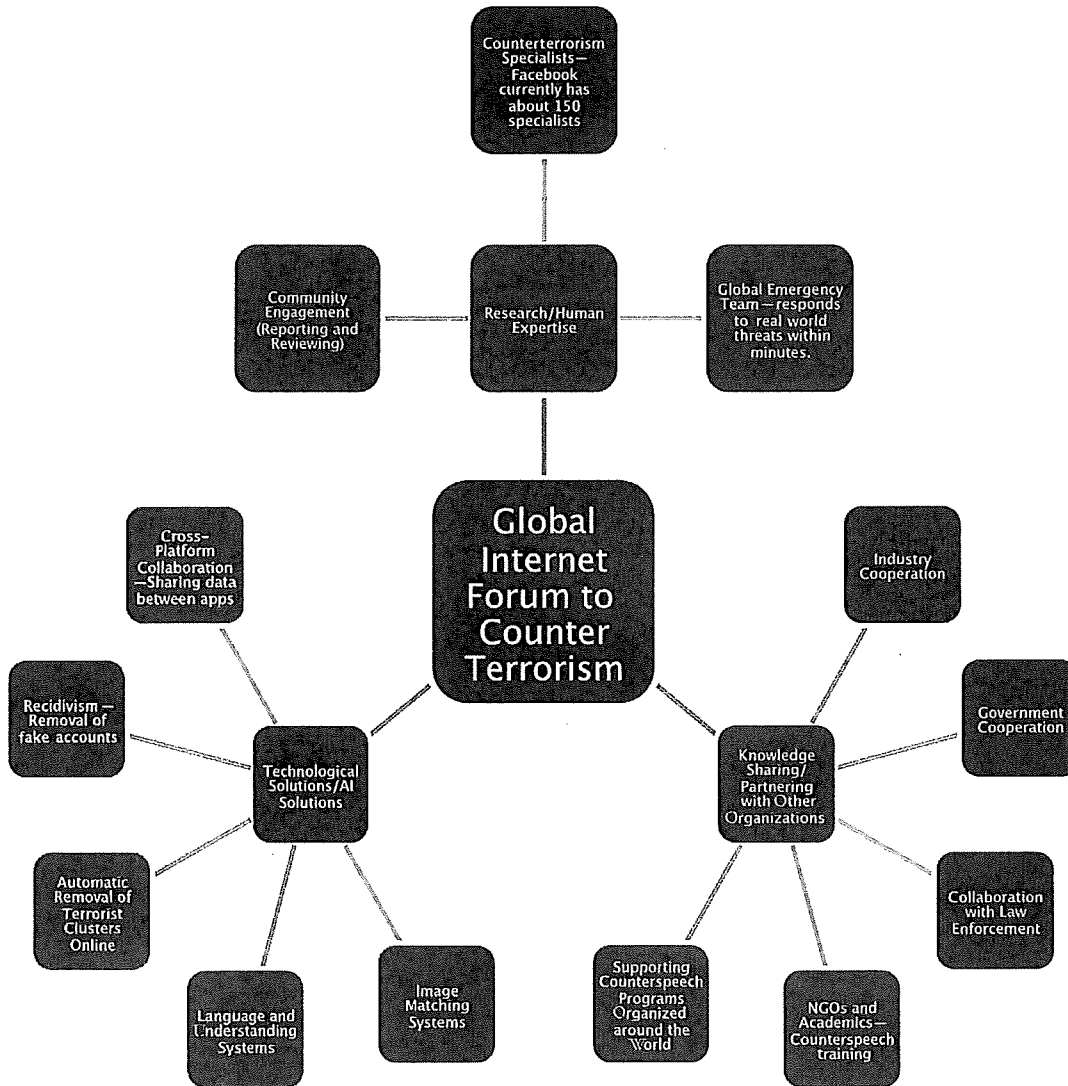

Figure 2: Global Internet Forum to Counter Terrorism

One of the greatest challenges that remain is the dearth of laws on how to deal with the new digital age. As Rogers stated, "Our challenge as a nation is . . . [that] technology has outstripped our legal framework." The key now is to "find a solution to deal with this issue that would give the government more power of access but will not be so invasive that it would not sit comfortably with innocent civilians."[22] While the will and collaboration is in place, the current political climate and dearth of appropriate responses to both the meta-narrative and the ongoing conflict and uncertainty in the MENA continue to embolden IS and have allowed the idea of a "United Cyber Caliphate" to take hold. This extremely modern and innovative form of terrorism will likely capture the imagination and loyalties of a whole new generation of e-terrorists, and security forces will have to be equally inventive to respond to this new threat.

This extremely modern and innovative form of terrorism will likely capture the imagination and loyalties of a whole new generation of e-terrorists, and security forces will have to be equally inventive to respond to this new threat.

Notes

1. Jacob Poushter and Dorothy Manevich, "Globally, People Point to ISIS and Climate Change as Leading Security Threats: Concern about Cyberattacks, World Economy Also Widespread," Pew Research Center, August 1, 2017, http://www.pewglobal.org/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/.
2. "The Global Coalition—Working to Defeat Daesh," *Global Coalition*, July 17, 2017, http://theglobalcoalition.org/en/the-global-coalition-working-to-defeat-daesh-july17/.
3. "Operation Inherent Resolve: Targeted Operations to Defeat ISIS," US Department of Defense, n.d., https://www.defense.gov/OIR/.
4. Lisa Chiu, "This Is How Much Money the U.S. Has Spent to Fight ISIL," CGTN America, March 2017, https://america.cgtn.com/2017/03/22/this-is-how-much-money-the-u-s-has-spent-to-fight-isil. As of March 14, 2017, the US and coalition forces have conducted a total of 18,948 strikes, nearly 80 percent of which were delivered by US forces.
5. "Islamic State and the Crisis in Iraq and Syria in Maps," BBC News, June 2017, http://www.bbc.com/news/world-middle-east-27838034.
6. While IS evacuates Mosul and Raqqa, it is moving its headquarters commanders and fighters to strongholds in al-Mayadeen City in the Deir Ezzor countryside. Other IS fighters have begun re-infiltrating villages throughout the Euphrates River Valley that were once cleared. Still others will try to bring terror to their former homes.
7. Rohan Gunaratna, "Best Practices: Rehabilitating and Reintegrating Foreign Fighters," *Countering Daesh Propaganda: Action-Oriented Research for Practical Policy Outcomes*, February 2016, 84–92, https://www.cartercenter.org/resources/pdfs/peace/conflict_resolution/countering-isis/counteringdaeshpropaganda-feb2016.pdf.
8. *Dabiq*, no. 1, 1435 Ramadan, July 2014, http://www.ieproject.org/projects/dabiq1.pdf.
9. Associated Press, *Associated Press Style Book 2017*, https://store.apstylebook.com/2017-ap-stylebook-print-edition.html.
10. "Figures at a Glance," UNHCR, June 30, 2017, http://www.unhcr.org/en-us/figures-at-a-glance.html.
11. The international community's lack of help will also lead them to revenge-seeking in the future, as has been evidenced by the Taliban and Northern Alliance soldiers, products of their violent childhoods. See Peter Singer, *Children of War* (Berkeley: University of California Press, 2006).
12. Olivier Roy, "Who Are the New Jihadis? Biographies of 'Homegrown' European Terrorists Show They Are Violent Nihilists Who Adopt Islam, Rather Than Religious Fundamentalists Who Turn to Violence," *Guardian*,

April 13, 2017, https://www.theguardian.com/news/2017/apr/13/who-are-the-new-jihadis.

13. Christina Schori Liang, "Cyber-Jihad: Understanding and Countering Islamic State Propaganda," GCSP Policy Paper, February 2015, http://www.gcsp.ch/News-Knowledge/Publications/Cyber-Jihad-Understanding-and-Countering-Islamic-State-Propaganda; and *Dabiq*, no. 1, 1435 Ramadan, July 2014, 7, http://www.ieproject.org/projects/dabiq1.pdf.

14. Robin Wright, "After the Islamic State: As the Caliphate Crumbles, Rival Movements Struggle for the Soul of Sunni Jihadism," *New Yorker*, December 12, 2016, http://www.newyorker.com/magazine/2016/12/12/after-the-islamic-state.

15. Eric Schnurer, "E-stonia and the Future of the Cyberstate: Virtual Governments Come Online, Snapshot," *Foreign Affairs*, January 28, 2015, https://www.foreignaffairs.com/articles/eastern-europe-caucasus/2015-01-28/e-stonia-and-future-cyberstate.

16. Abū Sa'aeed Al-Britāni, "Advice to Those Who Cannot Come to Shām," posted on Telegram.

17. Gabriel Weimann, "Terrorist Migration to the Dark Web," *Perspectives on Terrorism* 10, no. 3 (2016), http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html.

18. "Gov't in Talks to Restore Access to Telegram," *Jakarta Globe*, June 17, 2017, http://jakartaglobe.id/news/govt-in-talks-to-restore-access-to-telegram/.

19. Malcolm Nance and Chris Sampson, *Hacking ISIS: How to Destroy the Cyber Jihad* (New York: Skyhorse Publishing, 2017), 91.

20. Ibid., 80.

21. Jim Garamone, "Pace of Change Complicates Signals Intelligence World, NSA Chief Says," July 22, 2017, https://www.defense.gov/News/Article/Article/1255194/pace-of-change-complicates-signals-intelligence-world-nsa-chief-says/.

22. Ibid.