ONE

MASTERS OF THE DIGITAL UNIVERSE

Islamic State could never have achieved its territorial ambitions, nor could it have recruited such a large army in so short a time, without its mastery of the Internet.

Al Qaeda was the first major jihadist network to sense the potential of the World Wide Web, using its darker recesses in a covert manner to share ideology, information, plans, and correspondence. Its younger operatives also launched early cyber attacks on "enemy" websites, presaging the emergence of the cyber jihad that is raging today.

Today, Islamic State and its supporters use the Internet and social networking platforms in a brazen, overt way, marketing their "brand" and disseminating their material via mainstream networks such as Twitter. For those already in the territories of Islamic State, as much as for potential recruits on their laptops in a thousand bedrooms across the globe, concealing identity and location remains a priority. But there are myriad ways this can be done. Advice on the wide range of "anonymity products" available online is freely available for those who seek it—much of this advice is produced by Islamic State recruiters for the would-be jihadist. Those who fail to ensure their online anonymity are those we see detained and prosecuted. Sadly, this is only a tiny minority.

Most Islamic State commanders and recruits are tech-savvy; coding (writing software programs, inputting information in html) is as familiar to them as their mother tongue. Most of the digital caliphate's business is conducted online, from recruitment and propaganda to battlefield strategy and instruction. What the jihadists lack in the way of sophisticated weaponry they more than make up for with their online expertise.

The range, quality, and availability of today's digital equipment, such as HD cameras, editing software, special effects libraries, and so on, enable Islamic State's professional media teams to produce the slick and gruesome high-definition videos and glossy online magazines for which they have become infamous.

The Digital Generation

Most people who participate in, or are attracted to, Islamic State are in their late teens and early twenties. Researchers have shown that, among this age range in the developed world, 89 percent are active online, 70 percent use social networks daily, and each spends an average 19.2 hours a week on the Internet.[1] The jihadists are no exception and may spend even more time on their laptops, tablets, and smart phones, since their output across social media platforms is vital to maintaining the digital health of their project.

The paradoxical clash between advanced twenty-first-century technology and the Salafist-jihadist interpretation of Islam, which espouses the values of life in the seventh century, ceased to be a topic for heated debate among extremist ideologues and clerics when the potential of the Internet was fully realized. The Taliban smashed televisions in the 1990s, but al Qaeda led the way online with email lists being used to disseminate information as early as 1995. Encrypted communications were used to orchestrate all al Qaeda's major attacks from the 1998 embassy bombings in Nairobi and Dar-es-Salaam on, and Osama bin Laden's organization had its first website up and running by 2000. The Taliban followed suit soon after. By 2003, cyber jihad was cited as one of al Qaeda's widely circulated *39 Principles of Jihad*.

Al Qaeda attempted to free itself from its dependence on mainstream media exposure by starting its own online news service, The Voice of the Caliphate, in 2005. At that time, however, there was no obvious way to disseminate its content, apart from among a small pool of subscribers. It continued to rely on television channels such as Al Jazeera for the wide exposure it sought for videos featuring bin Laden's increasingly empty threats and for the ultra-violent Abu Musab al-Zarqawi, who would become al Qaeda's emir in Iraq. Zarqawi pioneered the tactic of recording every successful attack on coalition targets in Iraq on digital video, complete with cries of "Allahu Akbar" ("God is Great") and a soundtrack of the rather beautiful, stirring *nasheeds.* (These Islamic hymns are specifically written for the purpose of praise, adoration, or prayer, and are typically addressed to a deity or to a prominent figure.) YouTube, which was launched in 2005, provided the perfect forum for these videos, as well as for the filmed posthumous "wills and testaments" of suicide bombers, which could be uploaded anonymously.

The problem of dissemination remained, however. Even on YouTube, the potential viewer would need either to have been informed about a video's existence or to have conducted an almost intuitive search. Anwar al-Awlaki, a US-born, youthful cleric prominent in al Qaeda–offshoot AQAP (al Qaeda in the Arabian Peninsula), was the first to suggest exploiting social networking platforms to spread jihadist material more widely and reach new recruitment pools. The so-called bin Laden of the Internet created his own blog, Facebook page, and YouTube channel, and used them to distribute the online magazine *Inspire*, which included recipes for bomb-making and increasingly sophisticated films. Awlaki's over-confident use of social media platforms almost certainly led to his death from a US drone attack in Yemen in September 2011. Facebook use in particular was very easy to track at that time, as it did not accommodate anonymous operating systems such as Tor (see below).

Islamic State's Internet strategy has taken Awlaki's innovations one step further. In the past, the leadership would produce and release material; now, every jihadist is his or her own media outlet, reporting live from the frontline in tweets, offering enticing visions of domestic bliss via short films and images posted to JustPaste.it and Instagram, entering into friendly conversations via Skype, messaging on anonymous Android platforms, and posting links to the group's propaganda material and its infamous catalogue of videos. All of this output is systematically re-tweeted and, by clever use of hashtags, generates a huge audience.

Islamic State has made a point of recruiting IT specialists and those with online marketing experience. As a result, its social media activists are well versed in the most effective brand-sharing strategies—except its brand is death. One very effective method is to hijack Twitter storms: the activists include high-trending hashtags in their own tweets, which then include a link to Islamic State material hosted on an anonymous, unpoliced platform such as JustPaste.it. In August 2014, for example, IS activists included Scottish Independence hashtags, such as #VoteNo and #VoteYes, in their tweets during the run-up to the referendum. Trending celebrity stories are also exploited in this manner. People searching for #LewisHamiltonGrandPrix in November 2014 received instead a link to an Islamic State video showing child soldiers training with Kalashnikovs. Activists realize that material has to be widely distributed in as short a time as possible—and uploaded to safe archiving platforms—before YouTube, Facebook, and Twitter administrators are alerted and they remove the material and disable their accounts.

Islamic State's recruitment machine is largely online. In the course of researching this book we communicated in a variety of ways with young men and women who had either joined or were considering joining Islamic State. In Islamic countries, initial approaches were more often made via an intermediary or recruiter, but in the West, most said they had either direct messaged someone (via Twitter or Facebook) or had been contacted by a friend, relative, or acquaintance already inside Islamic State who initiated their "migration" and provided practical advice and logistical instructions. After the initial contact has been made, anonymous smart phone instant messaging platforms such as Kik and WhatsApp are used to deepen the contact. These are completely unpoliced and unregulated. The former, with 14 million users, appears to be largely used for pornography and drug dealing—it is easy for jihadists to hide here. Skype, the Internet telephone system, is another favorite means of communication, allowing real-time reporting by jihadists, and dialogue between recruiters and potential recruits. It is encrypted and can be used in conjunction with so-called dark Internet service providers and anonymous operating systems. Secret discussions, via messaging or telephone applications, conducted via a laptop or smart phone in a teenager's bedroom, are extremely difficult for parents and the authorities to police, which makes these digital devices perfect recruiting instruments.

Twitter and Facebook profiles are also used to cyberstalk and to identify and locate enemies. Military personnel, politicians, and journalists are particularly at risk; many have not taken even the most basic security precautions to conceal their work and home addresses, their daily schedule, where their children go to school, and so on.

The jihadists have their own community of web developers who pool their knowledge and developments, producing online resources such as *Technical Mujahid*, a training manual for jihadists released every two months. Extremists have developed their own closely guarded version of Facebook—Muslimbook—and Islamic State recently launched a mobile phone app: Dawn of Glad Tidings updates users on IS's news and uses their Twitter accounts to automatically disseminate information and reach potential funders.[2]

Islamic State has also produced its own video game, hijacking and modifying the extremely popular Grand Theft Auto, which it has renamed Salil al-Sawarem (Clashing of Swords). The game takes place in terrain resembling that of northern Iraq; players can ambush and kill American soldiers or plant improvised explosive devices (IEDs) that blow up military vehicles transporting groups of Western soldiers to shouts of "Allahu Akbar" (God is Great).

Information Hub

IS realizes that it has to keep pace with the Internet generation in order to remain relevant. Thousands of Twitter accounts, RSS feeds (a form of automatic digital distribution), and messaging networks provide a constant stream of battle reports and news about life in Islamic State. Thus they keep potential recruits and supporters engaged, counteract the propaganda efforts of the enemy, and share news, such as the loss of Kobani in early February 2015. Although most online material is still in Arabic, English is fast catching up; and a lot of Arabic material that is considered important is subtitled in English. Much material is also available in many other languages, including Russian, Urdu, and Chinese. After all, the jihadist network is now more or less global.

The relentless stream of information from the extremists is also used to build up the image of Islamic State as an emotionally attractive place where people belong, where everyone is a "brother" or "sister." A kind of slang—melding adaptations or shortenings of Islamic terms with street language—is evolving among the English-language fraternity on social media platforms in an attempt to create a "jihadi cool." A jolly home life is portrayed via Instagram images, where fighters play with fluffy kittens, and jihadist poster girls proudly display the dishes they have created. These Muslimas also tweet about domestic concerns or the absence of decent clothing: "Honestly we need some professional dressmakers for sister in Islamic State," tweeted one young woman, @UmmMariAndaluciya.

The jihadists' social media output also works hard to maintain a consistency of message, reminding the network that the enemy is the apostate and *kufr* (denier), who must convert or die. The menace is often embellished with a quote from the Qur'an. A recurrent thread upholds a mindset where the desire for martyrdom is normalized and death is sought and celebrated. This is the jihadists' most potent weapon. A soldier who does not fear death is an invincible enemy, and close-up photos of dead fighters' smiling faces are frequently posted across all platforms. The Islamic State salute—the index finger of the right hand pointing heavenward—reflects this ideology. The female jihadist holder of one Twitter account I investigated had posted a shocking photograph as wallpaper: two little boys, presumably her own, aged around four and six, are dressed in black and masked; they are dwarfed by the Kalashnikov rifles supported by their left hands while their right hand index fingers point to the sky. On February 3, 2015, one female resident of Islamic State, Al-Britaniya (British), shared "glad tidings" via Twitter: "My husband Rahimuh Allah has done the best transaction you can make his soul [sic] and in return Jenna [heaven] may Allah accept you *yaa shaheed* [martyr]." Five hours earlier she had posted a picture of a bowl of ice cream with bits of Toblerone chocolate stuck on top.

The head of the Islamic State's media department is Ahmed Abousamra, a Syrian who was born in 1981 in France and then brought up in Massachusetts where his father is a well-known endocrinologist. He obtained a degree in IT and worked in telecommunications before becoming self-radicalized; he encountered no obstacles in relocating to Aleppo in 2011 thanks to his dual Syrian-American nationality. Under Abousamra's direction are several media organizations with full-time staff, the main ones being al-Hayat, al-Furqan, and al-Itisam. These are solely for the purposes of propaganda. Al-Hayat was formed in May 2104, and its operations offices are based in Syria. Iraqi al-Furqan, originally the media mouthpiece of the Islamic State of Iraq (ISI), has been going since 2006. Al-Itisam is a film production unit based in Syria and is responsible for most of the slick, high-production-value videos al-Hayat disseminates.

It employs professional journalists, filmmakers, photographers, and editors (who must swear allegiance to Caliph Ibrahim as part of their contract) and has brought in cutting-edge technology and qualified operators. As a result, its film output is of a quality more usually associated with national broadcasters or even Hollywood. A slick recruitment video titled "What Are You Waiting For?" features attractive youths with dramatic long black hair, including a Frenchman with blue eyes. Al-Hayat releases regular short, snappy films called MujaTweets which show scenes of daily life among the *mujahideen* (those engaged in jihad). One, shot during Ramadan in a large canteen where a cook ladles stew into bowls, shows fighters breaking their fast with local children, laughing and joking; another shows fighters helping an old Kurdish lady, abandoned by her family, onto the back of a moped to be taken to other relatives; a seventy-year-old white-haired fighter is interviewed in one called "Why Did You Come to Jihad, Uncle?," which has become a great hit on YouTube.

Al-Furqan has produced whole television series glorifying Islamic State's achievements and deeds, including *Messages from the Land of Epic Battles* and *Flames of War*. They feature IS fighters, many of them foreign, in the midst of fierce battles. Its most infamous productions show increasingly barbaric executions designed to terrify enemies and the world at large with horrifying, unforgettable images: a small young boy personally executes adult hostages; a fighter holds up two severed heads; a woman is stoned to death; an old man alleged to be a pedophile is tipped off a white plastic chair from the top of a high building; and in February 2015 came the repellent, high-production-value video of a captured Jordanian pilot, Moaz al-Kasasbeh, being burned alive in a cage.

The latter was disseminated within seconds of being released, enabling me to trace the method by which it reached hundreds of thousands of people and all the media outlets. First, operatives tweeted that something was going to happen and recommended followers set up several duplicate accounts in case of suspension. Next came links to copies of the film on JustPaste.it (this anonymous message board, run by a twenty-six-year-old Pole, has become an integral part of Islamic State's media machine) and its Arabic equivalents, Nasher.me and Manbar.me, among many other anonymous platforms. These were tweeted with messages urging followers to re-tweet widely and for "people with hi-speed connections" to download and archive the film either on anonymous clouds or mirror websites (whereby the content of a known jihadist website is reproduced on hundreds of others under different names and identities). However fast the authorities removed Twitter accounts and sites that were hosting the film, it remained, and still remains, available. The same is true of the files the group Cyber Caliphate managed to download when it hacked the US Army's Central Command accounts in January 2015.

The murder of al-Kasasbeh immediately divided the followers of Twitter accounts I was monitoring. Some expressed horror and sadness and said this had nothing to do with Islam; others reveled in the cruelty, with one account holder, Faris al-Britani, chillingly tweeting, "Burn baby Burn!!! Starring 'best scream' award winner Moaz al Kassasbeh."

Islamic State also runs its own radio station, al-Bayan, which is based in Mosul, and a satellite TV station, Tawheed, based in Libya. In January 2015, a trailer announced the imminent arrival of a twenty-four-hour Internet television channel, The Islamic Caliphate Broadcast, to be hosted on one of the group's websites, KalifaLive.info. The channel will host a series of videos by John Cantlie, the British photojournalist kidnapped by ISIS in November 2012, along with James Foley, who was subsequently executed. Cantlie has appeared in eight Islamic State propaganda videos to date, a cause of much debate and speculation.[3]

The group's websites also contain or link to a huge archive of ideological treatises, monthly reports, sermons, Qur'anic interpretations, fatwas, magazines, training manuals, and guidance on issues such as how to treat slaves or life for women in the Islamic State.

Security Matters

"You are engaging in war tactics so that you can spread the true dawah and discuss matters of jihad, to uncover news about your mujahid brothers, to dismiss lies. You are entering into a sort of psychological warfare with them; they do not take it lightly, and we do not take it lightly. Therefore, we can trick them and it is totally permissible." So begins the welcome on a website called Al-Khilafah Aridat (The Caliphate Has Returned), which aims to keep cyber-jihadists up to date with security developments.

Islamic State's activists are able to be brazen online because they understand security issues and keep one step ahead of government agencies and service providers seeking to close them down. I have been able to put together the following overview of how the more canny activists and fighters navigate and exploit the Internet without fear of detection.

Key to anonymity are the virtual private networks (VPN) that conceal the user's IP address and instead create a false location in another country, usually in the middle of nowhere. Ghost VPN is one such program and is particularly effective when used in conjunction with an anonymous browser such as Tor (The Onion Router), which was initially developed for US Navy intelligence and remains the most effective product. Tor conceals the user's location by sending his or her Internet signal through nodes in dozens of different countries; it also enables the user to access the dark Internet, the anonymous zone of criminals and child pornographers. The recommended combination for maximum security, according to Al-Khilafah Aridat, is Ghost VPN with an operating system called Tails (The Amnesic Incognito Live System), which boots from an exterior source—a CD or flash drive for example—and therefore leaves no trace of activity on the computer hard drive. Tails has Tor pre-installed, enables multiple desktops, and can be switched off instantly if the user fears detection. Tails also has a suite of cryptographic tools for files, email, and instant messaging. With these security features in place, and provided the user does not make a basic mistake and betray his or her real identity voluntarily (by checking personal email or Facebook, for example), it is possible to remain entirely anonymous and conduct a false, untraceable, online life with a series of aliases inhabiting social media platforms. Twitter is Tor-compatible, and Facebook recently enabled it too.

Once equipped with VPN/Tails, cyber-jihadists can subscribe to the free email service Bitmessage, which allows them to send encrypted email. The intended recipient is given the key that unlocks the otherwise unintelligible code, but the email is also sent to hundreds of other random accounts that do *not* have the key. Anyone spying on the sender would never be able to deduce who the real, intended recipient was. Bitmessage is also used to establish and maintain social media accounts under aliases, and it enables anonymous communication, via direct messaging, from Twitter and Facebook. This is how jihadists are able to conduct their social media networking, overtly communicating the most extremist material with impunity. Jihadists do use open-source, decentralized, software-based networking platforms, such as Diaspora and Friendica, but these are not useful for outreach to the pool of potential recruits surfing the public information highways.

When operators are alerted to extremist accounts and material, they take it down. In the United States, the State Department's intelligence unit oversaw the removal of 45,000 items in 2014, while a specialist department within Britain's Metropolitan Police takes measures to delete around 1,100 items a week. An online cheerleader for Islamic State who goes by "Hamid," revealed to the *Guardian* newspaper that removal of a well-established Twitter account with thousands of followers is "a disaster " but requires patience. Hamid warned his followers not to give up, and tweeted: "Be ashamed if you worry about your account being deleted when there are other people willing to sacrifice themselves for their religion."

Like criminal gangs, jihadists need to be able to send and receive funds without security services being tipped off or spotting online transfers. They use cryptocurrency: bitcoins and dogecoins, Internet money "mining" systems that are popular with the underworld because they are bought in complete anonymity and their movements are untraceable. Recently available stored-value cards are another godsend to the underworld, forming part of another anonymous, untraceable method of transferring funds.

It works like this: senders load the amount they wish to transfer on a stored-value card; next they buy a prepaid, unregistered, disposable mobile phone with cash; then they register online with a mobile-payment service provider, using an anonymous, free email account, the number of the disposable mobile phone, and the money on the stored-value card. Using the mobile phone, they log on to the "m-payment" account and give the number of the mobile phone to which funds are to be transferred. This will also be a disposable, non-registered phone. Recipients then request the transfer of funds to their own anonymous and untraceable stored-value card, which can, in turn, be used to withdraw cash from an ATM, after which, both phones and cards are thrown away.

Mobile phones are an important part of the required communications arsenal, but until recently they were notoriously easy to pinpoint when in use. Disposable phones become traceable after time if they become part of a communications network that is under surveillance. A new Android phone is proving popular in the Islamic State. Nicknamed the Snowden Phone (after whistleblower Edward Snowden, who leaked classified information from the US National Security Agency to the media in 2013), it is sent in from the West by jihadists' friends and contacts. The phone can change numbers on demand and uses 128-bit encryption, VPN, and cryptocurrency to conceal all mobile footprints; it can be used for Skype, messaging, social media, and all other Internet activities with minimum risk of its user being traced. Tor has also developed a system that can be used with mobile phones in conjunction with Tails; the phone's memory is automatically erased as soon as the user removes the external booting device, so no trace of activity remains. ChatSecure is the instant messaging platform of choice for the anonymous phone user. It runs through Tor, and messages are encrypted.

Cyber Jihad

In January 2015, Islamic State dominated world headlines yet again through a group of "black hat" (i.e., maliciously destructive) hackers calling themselves the Cyber Caliphate. They took control of the social media platforms run by the US government's Central Command (CentCom), which oversees military operations in Iraq and Syria. The authorities were quick to say that no harm had been done but immediately rendered this claim implausible by offering the explanation that the hackers had simply "guessed the password." The preceding section on the many available layers of encryption and other security precautions should make the unlikelihood of this obvious. On CentCom's YouTube platform, the hackers discovered files that contained personal details of hundreds of US military personnel who were either veterans of, or currently deployed in, the Middle East. Clearly this greatly compromised their personal safety and that of their families. The files were swiftly disseminated and duplicated onto mirror sites and stored in anonymous archive clouds. It *could* have been worse—the hackers did not manage to get into the main information handling system or the organization's websites—but it was a declaration of cyber jihad with the American military.

The Cyber Caliphate had built up a solid presence on Twitter in the run-up to the attack, with 110,000 followers—a very large amount for extremist accounts, which are usually shut down before they achieve such numbers. A man's head entirely masked by a black and white keffiyeh (headscarf) serves as the account's wallpaper and "gravatar" (a globally recognized avatar, or trademark image). As of February 2015, the account had been deleted, and there was no active account for the group. That is not to say that they have ceased their activities; they have simply changed identity in the anonymous world of cyberspace.

In February 2015, French Minister of the Interior Bernard Cazeneuve revealed that since the previous month's *Charlie Hebdo* atrocities, the country had been hit by 25,000 cyber attacks by at least twenty-seven hacker groups claiming allegiance to Islamic State. The French cyber defense chief, Admiral Arnaud Coustillière, told a press conference that this was "the first time that a country has been faced with such a large wave."[4] Most of the attacks, on targets ranging from tourism pages to military defense websites, resulted in denial of service (DoS), which clogs a site with traffic and renders it unusable. There are no reports that any of the attacks resulted in data theft, but viruses may have been left, and nearly all affected sites were left displaying pro-Islamic State messages on their homepages. Many of the hacker groups were based in North Africa and the Sahel, and warned that another, more devastating wave of attacks would follow, targeting higher-level organizations.

There is some speculation that another very active group of black hat hackers calling themselves The Lizard Squad are linked to Islamic State. On January 25, 2015, they hijacked the website of ill-fated Malaysia Airlines, who had lost one plane and had another crash in 2014. For several hours the homepage displayed the words "ISIS will prevail" and "404—Plane Not Found: Hacked by Cyber Caliphate" over an image of a Malaysia Airlines plane in flight.

Islamic State's most likely "cyber emir"—and almost certainly the man behind the CentCom hack—is a UK citizen, twenty-one-year-old Junaid Hussain (aka Abu Hussain al-Britani) from Birmingham. Hussain spent six months in jail in 2012 for hacking into the personal Gmail account of Katy Kay, special advisor to former British Prime Minister Tony Blair. He obtained the emails and phone numbers of Blair's family and of various members of Parliament and the House of Lords, then posted them on various social media platforms across the Internet. Hussain also led a gang of teenage hackers called Team Poison that blocked a police anti-terror hotline by bombarding it with more than 100 prank calls. Undergraduate Hussain was on bail following separate allegations regarding a violent disorder offense when he evaded surveillance and fled to Syria, where he joined ISIS in 2013.

Apart from crashing websites, experienced and inventive hackers like Hussain can use their skills to intercept real-time battle information, giving Islamic State's fighters and commanders an obvious advantage and opportunities for ambush. Less tech-savvy fighters in rival opposition groups, militias (such as the Kurdish PKK), and even Iraqi and Syrian state forces rely on digital, hackable means to communicate battle plans, the location of protected supply routes, ammunition requirements, and strategy. In addition, phones, screens, and laptops not using Tails will also reveal records of previous emails, messaging, and Skype calls.

Islamic State hackers have also taken to laying cunning cyber traps for their opponents away from the battlefield. In Raqqa, one of the group's Syrian strongholds, a grassroots organization that calls itself "Raqqa is Being Slaughtered Silently" (RSS) set up a website to highlight human rights abuses perpetrated by Islamic State and to document the hardships of daily life under their interpretation of Sharia. Posing as a group of Syrians in exile in Canada, Islamic State hackers sent RSS an email expressing support and thanks for their "efforts to deliver a true picture of the reality of life in Raqqa." They told RSS that they were sending them the first draft of a news report they were preparing in order for them to comment and amend if necessary. The document contained images and, being a large file, was stored on a file-sharing site: links were provided in the email. On opening the link, RSS activists found the report and some satellite images of Raqqa, but while they were viewing them, malware files were secretly downloading into their system with one very simple purpose: to obtain the IP addresses of members of the network. Anybody who had worked on or visited the site would be vulnerable because the system stored IP addresses that can reveal the actual location of the computer being used. As a result of this sting, members of RSS were attacked by Islamic State "police"; their houses were raided, two of them were kidnapped and tortured, and at least one was murdered.

A similar ruse involves extremists setting up fake websites purporting to be against them in order to identify their enemies. When visitors click on a link, malware is downloaded to their systems and their IP addresses are obtained.

Hacking can be a useful source of funds, too. Without a fraud squad to bother them, cybernauts in Islamic State are having a field day hacking unsuspecting retail sites in the West from which they can extract thousands of credit card details. These can then be used to charge pre-paid, anonymous stored-value cards (as discussed above), enabling the hackers to withdraw large sums in cash from ATMs. Although other systems can be hacked, hackers are aware that Windows XP's security protocol has not been updated because it is now obsolete—yet this is the operating system many retailers are still using. Despite showing the locked padlock symbol indicating that a Secure Socket Layer (SSL) is in place, the system can be infected with malware that can initiate a Random Access Memory (RAM) scraper attack that downloads all the data in the targeted system to the hacker's computer.

Islamic State's friends abroad are also exploiting the opportunities the Internet affords them. The Tunisian Cyber Army and al Qaeda's Electronic Army have both launched successful cyber raids on US targets, including Customs and Border Protection and the Office of Personnel Management. Boko Haram produced a hacker who obtained from the Nigerian Secret Service's digital records the personal details of sixty spies, which were then published online.[5]

Governments appear relatively powerless to confront these attacks. Most social media platforms will voluntarily delete obviously extremist content, and many have a fast-track system for government agencies reporting it (Twitter, apparently, does not);[6] but there are political sensibilities around issues of free speech, privacy, and—crucially—very real technical obstacles.

To date, the most effective cyber retaliation on Islamic State for the murderous January 2015 Paris attacks (on satirical magazine *Charlie Hebdo* and a kosher supermarket) has come from an unlikely source—the veteran anarchist hacking collective Anonymous. Anonymous declared war on IS in January 2015 by means of a dramatic video and swiftly followed with a DoS attack, destroying an extremist website, ansar-alhaqq.net.[7] Anonymous also started a Twitter campaign #OpCharlie, which has leaked a list of Islamic

State recruiters and go-betweens uncovered on JustPaste.it, and it has acquired more than 900 links to IS-linked accounts, websites, and assorted online material, which it then hacks or denounces to service providers. Paradoxically, the group reports that Twitter administrators have twice deleted their burgeoning following on @OpCharlie handles.

In October 2013, a group of countries opposing Islamic State formed an informal US-led technical coalition to combat its cyber activities. The coalition includes Britain, France, Egypt, Saudi Arabia, and the UAE but has little to show for its efforts. International cooperation is impeded by legislation, bureaucracy, and, quite simply, lack of knowledge and experience. The serious curtailment of Internet usage proposed by more draconian regimes does not sit well with the more liberal Western countries, and, as many security analysts have pointed out, much of what they actually know about extremist groups has been gleaned from online sources.

The digital caliphate's young warriors are certainly working on, and may soon discover, ways to compromise the military superiority its opponents enjoy—if they learn how to hack the control systems of drones, for example, or jam communications between the alliance's commanders and pilots. The battle in cyberspace is not going the way of governments. It is one that Islamic State and other outlaw agencies can continue to dominate, so long as the world's most tech-savvy youth—who hold the key to the codes required for effective cyberwarfare—do not want to fight in the same trench as the authorities.