# Encounter Battle: Engaging ISIL in Cyberspace

Dr. Chris Bronk
Gregory S. Anderson

## INTRODUCTION

Although the United States withdrew its last remaining combat forces from Iraq in December 2011, a significant insurgency spanning the territory of Iraq and Syria has evolved under a variety of names including the Islamic State, Islamic State in Syria (ISIS) and the Islamic State in Iraq and the Levant (ISIL)—for this work, we choose to employ the title ISIL. Since ISIL's break with al-Qaeda in February 2014, it has become the chief standard-bearer of a Salafi jihadist movement set upon forming a trans-regional caliphate. In its activities, ISIL has extended its territorial reach across North Africa and the Arabian Peninsula as well as claiming credit for terror attacks from Belgium to Bangladesh. As much as a movement, ISIL is the contemporary brand for Jihadist insurgency in the Middle East and beyond.

While ISIL forces have made impressive territorial gains in Iraq and maintained a viable resistance to Syria's Assad government, it is now extending its reach into the digital domain, cyberspace, to further its ambitions in intelligence collection, propaganda, and recruitment. Also, ISIL is perhaps the first violent insurgent or terror group to seriously consider developing at least modest cyberattack capabilities as well as developing strength in sophisticated computing and communications technologies designed to defend the identity of its adherents and the security of their digitally-mediated interactions. [1]

For the US, the fight against ISIL also represents a significant test of its offensive cyber capabilities. Yes, ISIL has put US allies on the defensive, but if U.S. Cyber Command (USCYBERCOM) is to be a viable part of the Department of Defense's (DoD) mix of forces going forward, it will need to demonstrate how it can be of utility in the counter-insurgency and counter-terrorism struggle against ISIL and its confederates. The fight against ISIL will represent a significant test of USCYBERCOM's ability to

Dr. Chris Bronk is an Assistant Professor of computer and information systems at the University of Houston's College of Technology. He holds or has previously held appointments in Rice University's computer science department and Baker Institute for Public Policy and at the University of Toronto's Munk School of Global Affairs. Until 2006, he served as a career diplomat with the U.S. Department of State on assignments both overseas and in Washington, D.C. He recently published the book, *Cyber Threat: The Rise of Information Geopolitics in U.S. National Security.*

operationalize tactical capabilities in line with strategic goals of marginalizing and eventually defeating this organization.

Provided here are observations of ISIL cyber power, from digital information operations and intelligence, to operational security and desired future capabilities. We also examine open-source material and reporting on US cyber operations against ISIL and leadership statements from the DoD and others in US government. Finally, we offer a prescriptive component that connects desired outcomes for diplomatic activities and military operations aimed against ISIL in the U.S. Central Command (CENTCOM) area of responsibility (AOR)—20 nations in the Middle East, Central and South Asia with cyber options, both known and desired.

### *Contemporary Counter Insurgency Operations in the Middle East*

Although ISIL's roots are with the al-Qaeda terror organization in Iraq, it has embarked upon a far more ambitious agenda for Islamic statehood that combines previous operational tradecraft in terror operations with a clear desire to capture and hold significant territory and generate economic activity sufficient to challenge state authority in its primary operating theater—Iraq and Syria. Combat operations against ISIL by outside military forces, including those of Iran, the US (along with Coalition allies), and Russia began in the summer of 2014. Russia deployed air and ground forces to Syria; however, fighting ISIL has created a coalition of rather unusual bedfellows.

Iran, a US adversary since the 1979 Revolution, has a significant stake in supporting the Iraqi coalition government, with its large Shia representation.[2] To this end, Iran has provided both military advisers to the Iraqi army and pro-government Shia militias. In parallel with the

Gregory Anderson is a master's candidate for the Information Systems Security program at the University of Houston and is currently a research assistant under Dr. Chris Bronk and Dr. Arthur Conklin. He earned his bachelor's degree in Business Computer Information Systems from the University of North Texas.

Iranian intervention, the US has gradually reintroduced forces into Iraq, a number that stands at 4,650 as of July 2016. In addition to advisers and logistical support, the US maintains significant numbers of manned and unmanned aircraft in the region that have been employed in intelligence, surveillance and reconnaissance (ISR) missions as well as air strikes against ISIL forces. Russia's involvement appears confined to Syria, in the form of air power and limited numbers of ground forces. Russia has also aided autonomous Kurdish forces in Syria. [3]

The Kurdish dimension to the ISIL conflict in Iraq and Syria further broadens the set of interested parties, most significant among them Turkey. Considerable US and coalition resources have gone into supporting Kurdish military forces in Iraq. While the Iraqi Army collapsed in the face of the 2014 ISIL offensive, Kurdish troops have been viewed as more effective in protecting territories viewed as their own, but they are not without internal issues. [4] Also, Iraq's current president, Fuad Masum, is an ethnic Kurd. While the interplay of Iraqi internal politics is of limited salience here, the Kurdish issue and the threat to Turkey produces interesting cyber geopolitics relevant to the conflict as the Erdogan government has routinely found issue with the actions of its internal opponents on social media. [5]

Military operations against ISIL undertaken by the US-led coalition cohere well with the form of conflict summarized by now retired Admiral James Stavridis, the former NATO commander. His view of contemporary and future conflict is that it will be dominated by drones, special operations forces (SOF), and cyber. [6] This is the force mix that the US and its allies have fielded in Iraq and, to a lesser degree, Syria. Besides the US, Australia, Canada, Denmark, Germany New Zealand, Norway, Spain, and the United Kingdom have deployed ground contingents, primarily composed of military advisers in Iraq and Iraqi Kurdistan along with an air component. Many of the SOF are called upon for direct action operations aimed to rescue hostages, identify targets for precision munitions, or neutralize ISIL leadership targets.

The other highly visible activity in counter ISIL operations is air power. The Russian and Coalition air forces have used precision air strikes and drone attacks to counter ISIL. Among the US-led coalition conducting air strikes has been Arab nations Jordan, Morocco (withdrew 2015), and the United Arab Emirates. Michal Eisenstadt stresses that "The campaign against ISIS cannot be won by airpower alone."[7] While it can be and likely has been useful in breaking up large concentrations of ISIL ground forces, it is less so as ISIL goes to ground. As former MI6 officer and EU adviser Alastair Crooke observed, air strikes, "'are more likely to kill people who are not involved because the practice of these groups is to break up their formations, dissipate and then move on to built-up areas and hide within the populations.'"[8]

There are concerns for spillover of the conflict into neighboring countries, including Turkey, Saudi Arabia, and Jordan. With a lengthy land border with Iraq and Syria as well as its concerns regarding its Kurdish minority, Turkey has much to fear regarding Islamic terrorism on its soil as well as strong Kurdish forces in the region. Less a factor in counter-ISIL operations has been Saudi Arabia, which has trained token numbers of fighters for operations in Syria. However, the Kingdom has been a target of violence by ISIL confederates in recent months, including the holy city of Medina.[9] Finally, Jordan, which hosts more than a million Syrian refugees, is already stretched thin in extending its national resources to provide humanitarian support.

> ISIL is perhaps the first violent insurgent or terror group to seriously consider developing at least modest cyberattack capabilities

***Why They Fight—ISIL Social Media & Propaganda***

Use of social media to distribute Jihadist messages arose almost as quickly as the technology was invented. In the hands of Jihadist groups, it is an outgrowth of a socially mediated network in which video and audiotape messages are copied and recopied then passed across the Middle East and beyond. Popular are videotapes of hostages (usually Western) employed to demonstrate strength and opposition to the West. These videos were previously used to demonstrate proof of life, after 9/11, Abu Musab al-Zarqawi and other al-Qaeda leaders released execution videos of hostages. The brutal videos are now a staple of ISIL propaganda.[10] Their stature rose significantly in 2014 when ISIL officially parted ways with al-Qaeda and released the beheading video of American journalist James Foley. ISIL pushes its media through online sites as well as major American platforms, including YouTube and Twitter.

> The fight against ISIL will represent a significant test of the ability of USCYBERCOM to operationalize tactical capabilities with strategic goals of marginalizing and eventually defeating this organization.

To understand the ISIL narrative, it is important to grasp the medium it attempts to master. ISIL has maintained a heavy presence on social media platforms including Twitter, [11] Instagram, and YouTube to maximize exposure for their propaganda related activities. While the Twitter platform is not built for sustained diatribes, their brief 140 character updates allow for a constant flow of reinforcement. Instagram represents another vehicle for propaganda distribution available to ISIL and a useful image-based complement to Twitter. Instagram's primary function is sharing videos and pictures. The proliferation of high-quality cell phone cameras and Go-Pro type lightweight mobile cameras, allows ISIL to share, in morbid detail, their most violent exploits with just a few clicks. [12] These activities plainly violate the terms of service of these sites, and both Twitter and Instagram have taken steps to stop the spread of ISIL propaganda, including, but not limited to, blocking known ISIL accounts. [13]

The Internet provides ISIL unique reach across the world to "become pen pals with a lonely teenager in small-town America." [14] Not only are their social media attempts to recruit fence-sitters and sympathizers to travel to the Middle East or carry out terror attacks in their home country; they are forcing the West to send troops to combat ISIL on the ground. By provoking a US and coalition military response, ISIL plays the victim and reinforces their claim that "the West is engaged in a crusade against Muslims." [15]

ISIL has successfully made full use of so-called 'viral' marketing campaigns to establish itself on the Internet. ISIL has created its own brand, networked with other terrorist groups, and engaged with their supporters through social media. [16] Through their media campaign, ISIL recruits from around the world, including Usaamah Rahim of Boston, Massachusetts, who sought to kill police officers. [17] Rahim was radicalized via internet correspondence and expressed sympathies for ISIL on social media. [18] As with al-Qaeda, ISIL has a well-staked interest in radicalizing persons already living in the US and other Western countries to engage in terror attacks. These individuals, exemplified by San Bernardino terrorist shooters Rizwan Farook and Tashfeen Malik, often operate alone or in small tightly knit groups, represent the most paradigmatic ISIL assets to strike targets beyond the Middle East. ISIL also calls for adherents to travel to the Middle East for training and participation in military action in Iraq, Syria, or other operational areas. [19]

As of August 2014, "as many as 3,000 Westerners" were recruited and fighting alongside ISIL and related jihadist groups in Syria and Iraq. [20] ISIL constructed a sophisticated online media machine masterfully crafted for recruiting Westerners. One such media activity is the Al Hayat Media Center, established in May of 2014, and publishes in French, German, and English. Most of the posted content is in English, which strongly "suggests that they are specifically designed as a recruitment tool for Western audiences." [21] One of the programs run by Al-Hayat is called mujatweets (mt), which showcases the group's domestic efforts of winning support by showing the "lighter side of life in ISIS." One example is called "Cats of Jihad," in which ISIL fighters pose cats with their weapons. [22]

The U.S. Department of State has estimated that roughly 12,000 foreigners from 50 different countries have traveled to Syria to fight with ISIL, with most between the ages 15 and 25. [23] It is alleged that one-third of the 12,000 foreign ISIL fighters are from Western countries. [24] ISIL tends to focus their recruiting efforts on Western youth (evident by the high amount of English propaganda). ISIL recruiters discern if the potential fighters are more likely to join ISIL in the Middle East or carry out terrorist attacks in their home country. ISIL recruiters create an online community encouraging recruits to break ties with any outside channel that could disrupt the recruitment process (e.g. family and friends). [25] Many ISIL recruits become cannon fodder and are encouraged to further the brutal propaganda campaign by creating videos and "blowing themselves up." [26]

Contemporary and future conflict will be dominated by drones, special operations forces (SOF), and cyber.

The recruits that do not head to Syria or Iraq are strongly encouraged through the online ISIL community to carry out terrorist attacks in their home country. As the organization has said of the West, "the tiniest action you do in the heart of their land is dearer to us than the biggest action by us. There are no innocents in the heart of the lands of the crusaders." [27] Online recruiters offer guidance on how to carry out an attack and offer resources on how to construct or acquire materials if necessary. ISIL considers Western Lone Wolves a relatively cheap resource for ISIL. If a Lone Wolf carries out a terrorist attack, ISIL can choose to claim credit or not, depending on its outcome. Lone Wolves are also incredibly useful as they typically use their financial resources to carry out attacks.

### *ISIL's Cyber Capabilities and Intent*

While the Internet has served as an important vehicle for recruiting adherents to Jihadist causes, the US and its allies must prepare for ISIL's expanding capabilities. Recruitment is but one measure of ISIL's power. There are many others, including its financial resources, the capacity to communicate at a distance, ability to plan and execute coordinated operations, and acquire increasingly sophisticated armaments and use them effectively in traditional and unconventional combat operations.

ISIL has also made liberal use of Facebook Groups to conduct arms trafficking, including the sale and transfer of small arms and other munitions. [28] These Facebook Groups closely mimic American legal counterparts with the open posting of ads with pictures, descriptions, and prices for everyone to see. However, Facebook's terms and policies updated in January 2016 have disallowed all open trading of firearms and other munitions for all users regardless of country or affiliation. [29] Unfortunately, Facebook relies heavily on the user to report violations of these terms.

ISIL and other groups aligned with it have also started moving secure activities to other social media websites such as Diaspora. [30] Diaspora is a decentralized social network with data stored on private servers (called pods) not controlled by Diaspora's staff. This leaves the removal of ISIL (and ISIL-related) content up to the owner of the pod. These additional platforms do not allow for the widespread dispersal of propaganda of Twitter and Instagram, however, it does let them operate with more impunity. Also, ISIL appears to have a growing awareness of digital operational security. Although many of the group's operations have employed open, unencrypted communications, researchers from the Combating Terrorism Center (CTC) at West Point located a 34-page operational security manual originally drafted by a Kuwaiti firm as advice to journalists and activists in Gaza, which ISIL now uses as an essential training tool. [31]

ISIL maintains a heavy presence on social media including Twitter, Instagram, and YouTube to maximize exposure for their propaganda related activities.

Despite social media sites attempts at preventing the spread of ISIL imagery, news, and other content, they are operating within the watchful eye of the world in most forms of commonly accessed social media. America's long history of trying to 'win the hearts and minds' of civilians in counterinsurgency operations stretches back as far as the Philippine-American War (1899-1902). ISIL recognizes the ideological struggle with the US and employs the Internet as its most valuable outlet for promoting public narratives useful to the organization. With regard to combat operations, this places US and Coalition forces in a precarious position, just as insurgencies can wreak havoc to an organized force with strictly enforced rules of engag ment, the fight against ISIL adds the additional concern of a global audience witnessing any misstep resulting in collateral damage and civilian fatalities. Finally, ISIL overarching information operations intimidated 1,700 Iraqi forces into surrender when some 1,500 ISIL fighters took control of Mosul from some 30,000 Iraqi soldiers and police in June 2014. ISIL's effective use of social media has brought further support to their cause.[32]

Through social media ISIL seeks to internally produce malware for future attacks while also accessing code manufactured by hackers for hire.

ISIL has so far proven itself very adaptable to the changing terror environment by seeking new ways to impose its jihad on the West. For now, these attacks have largely remained rudimentary in nature. In a few cases, they have gained access to Twitter feeds of US military members involved in CENTCOM operations or defaced websites of US military spouses.[33] These attacks have failed to influence military operations, but represent early steps in the development of an offensive cyber platform. Furthermore, ISIL is openly talking online about hacking aviation instruments of large passenger aircraft as well attacking nuclear power plants to release deadly radiation.[34] While these attacks have yet to materialize, ISIL is in the early stages of intrusion into the US power grid.[35] These attacks have been entirely unsuccessful and low level, however, it paints a clear picture of ISIL intent. These intrusions were executed with basic attack software purchased through online Dark Net market websites such as the Silk Road and its successors. By using social media, ISIL seeks to internally produce malware for future attacks while also accessing code manufactured by hackers for hire.

Additionally, ISIL will make better use of bot software to spread their message through Twitter. Currently, the traditional system of making thousands of accounts to swarm feeds and hashtags, both items that increase message visibility, is being countered by Twitter.[36] However, new apps (such as the Android app *The Dawn of Glad Tidings*) are now built allowing predetermined messages by ISIL social media coordinators to slowly spread through users with real accounts who choose to opt in.[37] When a user opts-in, their account functions 'normally', but will periodically broadcast ISIL tweets that are also sent around at the same time to thousands of other accounts.[38] These accounts are difficult to detect and allow for users who already have large amounts of followers to get their message out.

Usage of the app even varies the timing of posts to minimize detection and to maximize exposure during offenses. During the Mosul offensive, the ISIL controlled accounts sent out over 40,000 tweets.[39] ISIL has recognized the new threat network that advanced attacks on US systems can provide through cyber warfare, and the US must counter this adversary.

### *The ISIL Cyber Complex*

ISIL can and will conduct cyber warfare operations, which poses a significant threat to US interests and security. Through cyber operations, ISIL's sphere of influence extends beyond Iraq and Syria. While capabilities do not yet meet ambitions, ISIL is focused on conducting cyberattacks against critical infrastructure targets, including the US electrical grid.[40] Unlike cyberattacks from China, Iran, and Russia; ISIL hackers are more devoted to their cause and will overtly engage in hostilities against the US and its allies. ISIL cyber capabilities are not on par with nation-state actors, but their determination is found in the exploits of two ISIL-aligned computer hackers: Junaid Hussain and Ardit Ferizi. Neither Hussain's nor Ferizi's origins are in Syria or Iraq, but rather Europe.

Junaid Hussain rose to prominence in Jihadist hacking circles in 2011 when he compromised the digital address book and personal accounts of former UK Prime Minister Tony Blair. Using the hacker handle, TriCk, Hussain was just 17 years old when British authorities jailed him. Hussain, a British-born hacktivist turned pro-ISIL hacker of Pakistani descent became involved with the TeaMp0isoN Islamic hacking organization, contributing to the group's efforts. Other members of his hacking group, TeaMp0isoN, reputedly overloaded MI6's counter-terror hotline later that year. He was politicized through violent videos against children in Palestine and Kashmir, Hussain told an interviewer of his motivations in 2012:

As hackers around the world become more sophisticated, terrorist groups are likely to follow their lead and use the same tools to further their ends

> I wanted to know why this was happening and who was doing it; there were loads of questions in my head. It made me angry; it changed the way I lived my life and the way I saw the world. I then started using hacking as my form of medium by defacing sites to raise awareness of issues around the world and to 'bully' corrupt organizations and embarrass them via leaks etc., which is how I got into hacktivism.[41]

Upon release, Hussain made his way to Syria with his British wife, a convert to Islam, and set to work training the ISIL organization in cyber tradecraft. He was an associate of Mohammed "Jihadi John" Emwazi, the ISIL spokesperson known for his role in killing Western hostages James Foley and Steven Sotloff. Hussain achieved results hacking CENTCOM Twitter and YouTube accounts.[42] More threatening was Hussain's employment of a technique known as 'doxing' to build dossiers of personally identifiable information found online regarding Coalition service members and their families.[43] The capacity for

ISIL digital operatives to pass such information along to confederates in the US or Western Europe willing to attack relatively soft targets is a serious concern.

For some time, scholars of the law of armed conflict have considered the question of when a nation-state would meet a cyberattack with a kinetic response. The killing of Junaid Hussain on August 24, 2015, during a US airstrike in Syria appears to have answered that question. [44] In killing Junaid Hussain, the Pentagon displayed a capacity to meet cyber power with kinetic force. It appears that Hussain is the first terrorist hacker to be explicitly targeted by the US in a military campaign—the 2011 killing of Anwar al-Awlaki in Yemen via a September 2011 drone strike offers an example of prior military action to disrupt terrorist recruiting via the Internet.

Beyond the Hussain strike, the US has initiated a 'doxing' prosecution of Ardit Ferizi, a Kosovar studying computer science in Malaysia. He was arrested in October 2015, after allegedly breaching a retailer's database and lifting records of all its military and government customers. US prosecutors allege, "Ardit Ferizi is a terrorist hacker who provided material support to ISIL by stealing the personally identifiable information of U.S. service members and federal employees and providing it to ISIL for use against those employees," and provided Hussain with this information between June and August 2015. [45]

Since Hussain's death, ISIL has continued to mount cyber campaigns, but its aspirations appear far greater than its capabilities. [46] Yes, ISIL can hire individuals online to act on the group's behalf in launching cyberattacks, but likely only to a limited degree. [47] ISIL cyber operatives continue to develop their technological skills as they shield their communications from eavesdropping, utilize encrypted chat systems and employ fake phone numbers. Although, cyberattacks are low threat and can be stopped, ISIL is beginning to learn and hone their skills. [48] As hackers around the world become more sophisticated, terrorist groups are likely to follow their lead and use the same tools to further their ends. Soon the US will face a major cyber capability in the hands of a Jihadist group or groups.

> Translating desired policies into a real, viable cyber campaign is the unique challenge of the moment.

***Policy Options—Cyber Offense Against ISIL***

Although ISIL's military capabilities in Iraq and Syria have been significantly blunted, the organization remains a potent force. The challenge in further reducing ISIL's cyber capabilities is two-fold. The US and its allies must work to harden military, critical infrastructure, and economic targets. Mitigating the ISIL social media machine is a difficult but necessary task. There is no silver bullet available to resolve the power of pro-ISIL narratives particularly since Muslims living in the West face hostility and even persecution. [49] As spectacular terror attacks generate considerable fear among the western electorates, ISIL's use of cyber intelligence collection, recruitment, and kinetic attack will elicit louder calls for intensive Internet monitoring to support the counter-terror mission.

Translating desired policies into a real, viable cyber campaign is the unique challenge of the moment. In June 2016, a dissenting memorandum signed by 51 US Department of State diplomats argued for a more rigorous effort to bring about a cessation of hostilities in Syria. While the diplomats argued for, "a more militarily assertive US role in Syria," they preferred to leverage kinetic technologies such as precision-guided weapons and air defense systems for offensive and defensive roles, respectively.[50] The memo stressed a new policy where belligerence by any of the warring parties, i.e. the Syrian regime and ISIL, would be met with force. The question is how cyber forces could be employed to degrade further ISIL's ability to wage war as well as forcing the Assad government to acquiesce to a ceasefire.

> Cyber warriors will need to create a capability at the intersection of Silicon Valley and the Pentagon that delivers innovative, unorthodox cyber tools.

Top Pentagon leadership mentioned cyber "bombs" that it wishes to deploy against ISIL.[51] The US military is considering what sort of cyber munitions, capabilities, or tactics might make the most headway in reducing ISIL's battlefield capabilities. The US military must map desired capabilities to an assessment of what is technically feasible now or with varying degrees of effort. There are likely three desired cyber combatant areas in which most activity should fall: intelligence gathering from cyberspace's fixed and mobile computational infrastructure including networks both wired and wireless; cyberattack capabilities designed to degrade or damage battlefield effectiveness of targeted forces; and cyber-information campaigns against enemy messaging.

While it is impossible to know much of the current US cyber-signals intelligence capabilities without moving into the classified space, we can conjecture on the sorts of capabilities that may be desirable in sweeping up additional intelligence resources. One of the items leaked by Edward Snowden was Tailored Access Operations (TAO),[52] the capacity to gain entry to important systems by either physical or virtual means.[53] What would be enormously useful is to have the capacity for TAO at a distance. Operational units would call upon lightweight off-the-shelf and open source technologies to pull intelligence, map digital points of presence, and see (in real time) data linkages on the battlefield and beyond it. Holding measurement and signatures mapping of the computer terrain might bring useful capabilities in intelligence collection and targeting as well.[54]

While ISIL's combatants are wedded to the same armaments used from conflicts in

Vietnam, Angola, Somalia, and Bosnia, chiefly the Kalashnikov assault rifle and the rocket-propelled grenade, the lure of adopting weaponry that is more sophisticated will likely grow. As the Internet of Things (IoT) extends to vehicles and other tools employed by ISIL and other insurgents, the potential will grow for cyberattacks against them. So far, US security experts have expressed concern over IoT vulnerabilities.[55] While hackers at DEFCON and Black Hat conferences have made news with car hacking, USCYBERCOM should begin thinking about how to get inside the computing components of the Toyota Hilux and Land Cruiser 4x4 vehicles that are key to the mobility of Jihadist elements from Mogadishu to the Maghreb.[56]

Today, as ISIL uses drones, USCYBERCOM should put resources into monitoring or disabling their control systems whether in defensive postures around vital installations such as nuclear power stations or government buildings, denying ISIL the drone intelligence and transport capability on the battlefield.[57] Non-lethal attacks would minimize collateral casualties and reduce insurgent capabilities. The US should accept a Harvey Sapolsky assertion on non-lethal cyber capabilities when he discussed non-lethal ammunition, “The first time a Marine shoots a bad guy with a beanbag, and the bad guy gets up and shoots back, will also be the last time the Marine uses the beanbag.” Nonetheless, there will be no shortage of kinetic hacking targets for the US military.

The cyber conflict against ISIL will serve as a template for future cyber action against terror groups, insurgents, and violent transnational criminal syndicates.

Also seemingly infinite are the Internet messages supporting ISIL’s war effort. While the platforms—such as Twitter, Instagram, and YouTube—are used to convey Jihadist messaging can police their content to some degree, the US government straddles a fine line in censoring ISIL and other Jihadist groups in cyberspace. The US Intelligence Community (IC) will no doubt continue its work examining social media outlets in a manner not dissimilar from how the Middle Eastern governments overthrown by the Arab Spring sought to accomplish. The key to short-circuiting communications for ISIL may be to borrow the concept of ransomware, the encryption of key data on important systems that have mushroomed into cybercrime. Encrypting stored data or even data in transit that threatens ISIL and its recruitment efforts may be a useful tool. So too might be technical failures of commodity computing hardware triggered by a cyberattack. Think of such tools as Stuxnet for data obfuscation or deletion.

It is important for the US to adopt a culture of innovation that is inclusionary of heterogeneous ideas and actors. The IC has employed its startup venture capital vehicle, In-Q-Tel, to develop desired capabilities where the commercial technology industry has not seen opportunity. As the Cold Warriors employed Lockheed’s Skunk Works to develop world-changing technologies like the U-2, SR-71, and F-117, the cyber warriors will need to create a capability at the intersection of Silicon Valley and the Pentagon that delivers innovative, unorthodox cyber tools and weapons that move from idea to deployment on a schedule far faster than current government acquisition. This would likely take form in a linkage between USCYBERCOM geeks and SOCOM's operators. Much as the US SOF community has developed unique transport, intelligence, and support capabilities, it will need a cyber echelon housed within its intelligence component as well. Already arguments have begun to emerge for a 'Cyber JSOC' (Joint Special Operations Command), the analog to SOCOM's JSOC force composed of Army Delta Force and Naval Special Warfare Development Force (DEVGRU) direct action units as well as its Intelligence Support Activity (ISA).[58]

There will no doubt be difficulties incorporating cyber operations components into overall US strategy countering ISIL and other non-state adversaries; however, it is clear national security leadership in Washington will leverage cyber capabilities more significantly. One issue that will continue to dog offensive cyber operations and intelligence activities is the equities question—should the US government turn over knowledge it accrues regarding cyber vulnerabilities to the technology industry so that they may be repaired. For instance, is it more desirable for USCYBERCOM and the National Security Agency (NSA) to keep information regarding broken encryption implementations or software as was alleged in the Heartbleed bug in the OpenSSL software libraries? Issues such as this will be a major policy question to consider.

Ultimately, the cyber conflict against ISIL will serve as a template for future cyber action against terror groups, insurgents, and violent transnational criminal syndicates. Looking backward, we can see the effective application of robust signals intelligence capabilities have been. Consider US support of Colombian operations against the Fuerzas Armadas Revolucionarias de Colombia (FARC). There can be little doubt that the Colombian military and police were made significantly more effective with the addition of US intelligence capabilities. Policymakers are keen to eradicate or at least damage ISIL but will need to ask how cyber weapons can frustrate it as much as anything else can. The more cyber tactics can short-circuit ISIL's operational capabilities, the better. What is necessary for US cyber operators are clear objectives from senior leadership on what they want to produce. The engineers that build USCYBERCOM's tools and the hackers that serve as its operational forces can easily enough push back on what they believe is the art of the possible.

*Special Contributors*

Fernando Barajas, Undergraduate Research Assistant, Rice University

Eric Brittain, Undergraduate Research Assistant, University of Houston

Mamie Sellam, Undergraduate Research Assistant, University of Houston

Jonathan Vallow, Undergraduate Research Assistant, University of Houston

## NOTES

1. Pierluigi Paganini, "Mikko Hyppönen Warns the ISIS Has a Credible Offensive Cyber Capability," *Security Affairs,* October 26, 2015.

2. Alireza Nader, *Iran's Role in Iraq,* RAND: Santa Monica, 2015.

3. Thomas Grove and Ben Kesling, "Russia Pursues Ties With Kurds to Keep Foothold in Region," *Wall Street Journal,* April 21, 2016.

4. Eduardo Gonzalez, "Kurdish Peshmerga: Divided from Within," *Harvard Political Review,* September 5, 2015.

5. Adam Taylor, "Why Turkey banned Twitter (and why banning Twitter isn't working)," *Washington Post,* March 21, 2014.

6. James Stavridis, "The New Triad," *Foreign Policy,* June 20, 2013.

7. Michael Eisenstadt, "Defeating ISIS: A Strategy for a Resilient Adversary and an Intractable Conflict," *Policy Notes – The Washington Institute for Near East Policy,* No. 20, November 3, 2014.

8. Jack Moore, "Why air strikes alone can't destroy ISIS," *Newsweek,* December 4, 2015.

9. Hamid Dabashi, "ISIL turns 'shock and awe' doctrine against Islam," *Al Jazeera,* July 5, 2016.

10. Holly Yan, "Showing off its crimes: How ISIS flaunts its brutality as propaganda", *CNN Regions,* September 4, 2014.

11. Sam Webb, "ISIS Use Instagram to Post Sickening Bodycam Footage of Murderous Assault on Civilians in Iraqi City," *Mirror,* May 15, 2015.

12. "ISIS Beheading Four Prisoners," *Zero Censorship,* February 3, 2016.

13. David Goldman, "Twitter goes to war against ISIS", *CNN Money,* February 5, 2016.

14.P. W. Singer and Emerson Brooking, "Terror On Twitter: How ISIS is Taking War to Social Media - and Social Media is Fighting Back," *Popular Science,* December 11, 2015.

15. David Blanchette, "Homeland Security Expert: ISIS Thrives on Social Media," *The State Journal-Register,* March 20, 2016.

16. P. W. Singer and Emerson Brooking, "Terror On Twitter: How ISIS is Taking War to Social Media - and Social Media is Fighting Back," *Popular Science,* December 11, 2015.

17. Steve Almasy, "Boston Shooting: Who Was Usaamah Rahim?" *CNN U.S.,* June 4, 2015.

18. Ray Sanchez, "ISIS Exploits Social Media to Make Inroads in U.S.," *CNN U.S.,* June 5, 2015.

19. Hassan, "The secret world of Isis training camps – ruled by sacred texts and the sword," *The Guardian,* January 25, 2015.

20. "ISIS Recruits Fighters through Powerful Online Campaign," *CBS News,* August 29, 2014.

21. Olivia Becker, "ISIS Has a Really Slick and Sophisticated Media Department." *VICE News,* July 12, 2014.

22. P. W. Singer and Emerson Brooking, "Terror On Twitter: How ISIS is Taking War to Social Media - and Social Media is Fighting Back," *Popular Science,* December 11, 2015.

23. Francesca Trianni and Andrew Katz, "Why Westerners Are Fighting for ISIS," *Time,* September 5, 2014.

24. Rukmini Callimachi, "ISIS and the Lonely Young American," *The New York Times,* June 27, 2015.

25. Husna Haq, "ISIS Excels at Recruiting American Teens: Here Are Four Reasons Why (+Video)," *The Christian Science Monitor,* October 22, 2014.

26. John Hall, "European ISIS Fighters Who Are Seen as Cannon Fodder by Their Commanders Desperately Try to Prove Their worth by Committing the Most Sickening Atrocities, Says Former Prisoner," *Mail Online,* April 10, 2015.

## NOTES

27. "Isis Leader Encourages Lone Wolf Attacks on Civilians in Europe and US," *The Guardian,* May 22, 2016.

28. C. J. Chivers, "Facebook Groups Act as Weapons Bazaars for Militias," *The New York Times,* April 06, 2016.

29. Jessica Guynn, "Facebook Bans Private Gun Sales," *USA Today,* January 30, 2016.

30. Dave Lee, "Diaspora Social Network Cannot Stop IS Posts," *BBC News,* August 21, 2014.

31. Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired,* November 19, 2015.

32. Brendan Koerner, "Why ISIS Is Winning the Social Media War," *Wired,* April 2016.

33. Joseph Marks, "ISIL Aims to Launch Cyberattacks on U.S.," *Politico,* December 29, 2015.

34. Jess Mchugh, "ISIS Cyber Attack? US Government, Planes Threatened With Malware, Hacking By Islamic State," *International Business Times,* December 29, 2015.

35. Jose Pagliery, "ISIS Is Attacking the U.S. Energy Grid (and Failing)." *CNN Money.* October 16, 2015.

36. David Goldman, "Twitter Goes to War against ISIS," *CNN Money,* February 5, 2016.

37. "How ISIS Games Twitter," *The Atlantic,* June, 2014.

38. "ISIS Launches Twitter App For Android Phones," *CBS DC,* June 17, 2014.

39. Anthony Cuthbertson, "Iraq Crisis: Isis Launch Twitter App to Recruit, Radicalise and Raise Funds," *International Business Times,* June 18, 2014.

40. Jose Pagliery, "ISIS is attacking the U.S. energy grid (and failing)", *CNN Money,* October 16, 2015.

41. Lorraine Murphy, "The Curious Case of the Jihadist Who Started Out as a Hacktivist," *Vanity Fair Hive,* December 15, 2015.

42. Lorenzo Francecshi-Bicchierai, "How a Teenage Hacker Became the Target of a US Drone Strike," *Motherboard,* August 28, 2015.

43. Megan Garber, "Doxing: An Etymology," *The Atlantic,* March 6, 2014.

44.Kimiko de Freytas-Tamura, "Junaid Hussain, ISIS Recruiter, Reported Killed in Airstrike," *New York Times,* August 27, 2015.

45. "ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges," *Department of Justice Office of Public Affairs,* October 15, 2015.

46. Joseph Marks, "ISIL Aims to Launch Cyberattacks on U.S.," *Politico,* December 29, 2015.

47. Cory Bennett and Elise Viebeck, "ISIS Preps for Cyber War," *The Hill,* May 17, 2015.

48. Dan Lohrmann, "Cyber Terrorism: How Dangerous Is the ISIS Cyber Caliphate Threat?" *Government Technology,* May 18, 2015.

49. Rukmini Callimachi, "ISIS and the Lonely Young American," *The New York Times,* June 27, 2015.

50. "State Department Draft Dissent Memo on Syria," *The New York Times,* June 17, 2016.

51. Cory Bennett, "Pentagon hits ISIS with 'cyber bombs' in full-scale online campaign," *The Hill,* April 25, 2016.

52. Andrea Peterson, "The NSA has its own team of elite hackers," *Washington Post,* August 29, 2013.

53. Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired,* November 19, 2015.

54. A capability developed or under development by SRC, a defense contractor. "MASINT Systems," SRC, available at: http://www.srcinc.com/what-we-do/radar-and-sensors/masint-systems.aspx.

55. As Nicholas Weaver opined, "I don't do SCADA research because I like to sleep at night." Tom Simonite, *MIT Technology Review,* January 28, 2016.

56. Seth Rosenblatt, "Car hacking code released at Defcon", *CNET Security,* August 2, 2013.

57. David Hambling, "ISIS Is Reportedly Packing Drones With Explosives Now," *Popular Mechanics,* December 15, 2016.

58. "U.S. Needs 'Cyber JSOC' So It Can Strike Harder, Faster In Event Of Conflict: Experts," *CyberWar.News,* April 27, 2016.