The American Foreign Policy Council

Defense Technology Program Brief

September 2015 | Washington, D.C. | No. 12

The War Against ISIS Through Social Media

By: Abraham Wagner, Rand Waltzman, Alberto Fernandez

Briefing Highlights

Intelligence Community has failed to adequately support what was known as "open source" research. Social media, however, has radically changed this analytical landscape as new media sources have now become central to the operations of violent extremists.

• • •

The ability to influence is now democratized, in that any individual or group has the potential to communicate and influence large numbers of others online in a way that would have been prohibitively expensive in the pre-Internet era.

• • •

All of our adversaries possess an enormous asymmetric advantage over us as a result of policy, legal and organizational constraints that we are subject to and they are not.

• • •

Pro-ISIS accounts on Twitter peaked in late 2014 at around 50,000; about 2,000 do the bulk of the work. If you take all accounts on Twitter which are active in countering ISIS messaging (not just those of the U.S. gov.), you would total at most 200.

• • •

Social media platforms provide an opportunity for "cyberstalking" while ISIS terrorists use these platforms to identify and target specific military personnel and families.

• • •

The U.S. should focus on several critical areas to counter ISIS, including large-scale collection of social media, analytical tool development, understanding the radicalization process, and creating a countervailing social media message.

On July 7, the American Foreign Policy Council (AFPC) held the fourth installment of its Defense Technology Program's Understanding Cybersecurity lunch briefing series for Congressional Staffers. This event, entitled, "How the Caliphate is Communicating:" Understanding and Countering the Islamic State's Messaging outlined how and why the Islamic State has been winning the "war of ideas" through the use of social media, and how the group is using social media to further its operations.

The event was moderated by AFPC Defense Technology Program Director Rich Harrison and featured cyber and social media experts Dr. Abraham Wagner, Dr. Rand Waltzman, and Amb. Alberto Fernandez.

The experts addressed areas where ISIS has been successful, discussed social media trends, and identified areas where the West can take advantage of ISIS' vulnerabilities and disrupt its propaganda campaign, recruitment efforts and other means of attack. The three articles enclosed herein are based on the speakers' presentations.

Table of Contents

Dr. Abraham Wagner *is a Lecturer in Law at Columbia Law School and Senior Fellow at the Center for Advanced Study on Terrorism. Dr. Wagner served for over 30 years in various U.S. Government posts including the Defense Advanced Research Projects Agency (DARPA) at the time of the transition to the Internet.* ***Dr. Rand Waltzman*** *joined the Software Engineering Institute of Carnegie Mellon University as Associate Director of Research in May 2015 after a five-year tour as a Program Manager in the Information Innovation Office of DARPA. At DARPA, he created and managed the Social Media in Strategic Communications program.* ***Ambassador Alberto M. Fernandez*** *is MEMRI Vice President. Amb. Fernandez served as a U.S. Foreign Service Officer from 1983 to 2015, and as the State Department's Coordinator for the Center for Strategic Counterterrorism Communications from March 2012 to February 2015. He speaks fluent Spanish and Arabic. The opinions expressed by the author do not reflect those of the U.S. government.*

8th Century Ideology and 21st Century Technology

By: Abraham R. Wagner

The rising tide of violence from radical extremists, including ISIS and other Islamist groups, presents a new set of challenges to U.S. public policymakers. Unlike traditional threats from state actors, ISIS is operating on an increasing number of fronts in the Middle East and continues to make ever greater use of social media to support its operations. The threat it poses to the American homeland as well as U.S. personnel abroad is also increasing, as is support to "lone wolf" terrorists within our borders.

This situation presents both an organizational and technical challenge. Traditionally, national security threats have been situated outside the U.S., and have been the domain of the Department of Defense as well as the Intelligence Community—both of which are prohibited from operating within the U.S. itself. While the 9/11 attacks forced the nation to alter this traditional assumption, as well as to create a Department of Homeland Security and reorganize the Intelligence Community, it is still unclear that these changes have been either adequate or effective. The question, then, is what can be implemented to effectively deal with this evolving threat?

The New Battlefield

Social media has evolved rapidly, bringing a host of benefits as well as new challenges to national security. Among the most pressing of these is the use of social media by ISIS and others to achieve their aims in the Middle East as well as in the U.S. and Europe.

While it is possible to debate the ideological roots of violent extremists, there is no question that they have embraced the use of social media to accomplish both near and longer term objectives. The most critical of these include:

- Radicalization of U.S. nationals to conduct terrorist operations within the U.S., and to increase support for those doing so.
- Recruitment of U.S. nationals to fight with ISIS in Syria and elsewhere.
- Use of social media to target U.S. nationals, particularly military service personnel and their families.
- Widespread use of social media for dissemination of propaganda and related literature.

It is certainly true that this issue area has not escaped the attention of the media, responsible government agencies or the broader research community. Rather, the operative question is why so little has been done to date, and what are the impediments to doing a better job?

For one thing, the research base in this increasingly critical area is relatively limited, both within the U.S. government as well as the scholarly community.[1] For decades, the Intelligence Community has failed to adequately support what was known as "open source" research, which was traditionally limited to analysis of broadcast and print media. Social media, however, has radically changed this analytical landscape, as new media sources have now become central to the operations of violent extremists.[2]

Public use of the Internet began in 1989, while the development and explosive growth in social media is far more recent. Recently the number of users has increased by several orders of magnitude, and now includes users of all ages and types. With no geographic or other limitations of any kind, the community of net users now includes terrorists, terrorist organizations and others seeking to harm the U.S.

ISIS in particular has worked to employ social media for education and training, including an on-line guide for mothers on how to raise extremist children. There has also been a major appeal to females and the "sisters' role in Jihad," who are urged to start training children when they are babies, while several jihadi web sites provide tales of jihad which tend to have a lasting effect on "little ears and eyes."

Likewise, social media is also used for the recruitment of fighters and other operatives for ISIS, including through YouTube videos, photos and hashtags as well

as dedicated web sites and specialized applications. It is impossible to discount the cost-effectiveness of this approach in light of the fact that there are some 1.6 billion Muslims worldwide. Even if only a small fraction of this number is actually radicalized, this itself will represent a large number. Here ISIS efforts are increasingly focused on the U.S., which ISIS sees as a significant threat to its success.

The impact of ISIS use of social media has been enormous. Thousands of images and videos have been uploaded to YouTube and Twitter alone, with the rate increasing. The organization is now producing "quality horror," with a measurable impact on the rate of recruitment among foreign fighters as a result.

New Vulnerabilities

Following the terrorist attacks of 9/11, the nation became sensitized to new threats as well as the use of new technologies by terrorist organizations. As increasing numbers of Americans, including military personnel, utilize social media, their online profiles render them vulnerable to hostile targeting. Meeting this challenge effectively requires new analytical tools to both assess the vulnerability of such personnel to hostile targeting through social media, as well as new techniques to detect the types of activity outlined.

Social media platforms provide an opportunity for "cyberstalking," and ISIS terrorists use them to identify and target specific military personnel and families.[3] How credible such threats may be, and what capabilities ISIS may have to operationalize this intent, are still open questions, but they cannot simply be dismissed.

Yet, looking at the current state of what the U.S. government now calls "countering violent extremism," the picture is not encouraging.[4] Multiple organizations are involved, led by a White House that lives in denial. The Department of Homeland Security now has a "CVE Coordinator" but no serious programs. The State Department has an operational program, but only very limited funds. As well, elements of the Intelligence Community and Defense Department are also involved, and they tend to treat the problem as a "boutique item" with little in terms of actual programs.

By all accounts, the U.S. is losing the battle, and losing it badly.[5] Very little exists in the way of serious, funded programs and any interagency coordination in this critical area is limited at best. Making matters worse, there is no consensus within the government on what the U.S. can or cannot do in this arena.

Stopping ISIS use of social media is largely impossible and could be counterproductive. Tracking ISIS use of social media is important, but requires better programs with adequate funding. That leaves countering ISIS in social media as likely the most fruitful avenue of approach, but it is one that remains grossly underexplored and underfunded. Here, the U.S. should focus on several critical areas:

Large-scale collection of social media: This is essential for effective analysis and tracking of potential radical extremists;

Analytic tool development: Automated analysis of the vast amount of social media is the only hope, as it would be impossible to recruit, train and pay the number of human analysts required. Current efforts here are not coordinated, and there is no fundamental agreement was to who should be doing this.

Understanding the radicalization process: The method by which ISIS attracts and inspires adherents is still not widely understood, and there are important tools from neuroscience and related fields that could be applied here. Such efforts have been proposed since 9/11 in relation to extremist groups writ large, but to date have never implemented effectively.

Creating a countervailing social media message: It would be possible to match ISIS in scope, scale and quality, but current efforts simply don't exist or are grossly inadequate. Here, the State Department's Center for Strategic Counterterrorism Communication should be greatly expanded, While supplemental, highly-cost effective offshore efforts can and should be created.

The High Cost of Failure

One key question remains: what happens if we fail to respond to ISIS in this arena. In part, the answer is a matter of "optics." The conflicts in Iraq, Syria and Yemen will continue regardless of that takes place in social media, and the U.S. cannot seriously impact their outcomes via that medium. At the same time, other threats to the U.S. and Western nations remain uncertain. There are many posts and Tweets in social medial promising horrific and deadly attacks, but it is often hard to match real intent and actual capabilities.

Critical here is the recruitment and radicalization process, with social media at the heart of the problem. Almost all recent incidents and arrests have been tied to radicalization via social media, as has the recruitment of fighters for ISIS. All of this argues compellingly for developing the tools to gain a better understanding of ISIS use of social media, as well as to expand our ability to effectively counter the phenomenon.

The Weaponization of the Information Environment

By: Rand Waltzman

Both as individuals and collectively, we make decisions and behave in a way that reflects our perception of the world and our interpretation of the information available to us. Yet this construct is changing dramatically. The creation of the Internet and Social Media (ISM) has resulted in massive changes of scale in time, space and cost of information flows. The diffusion of information is now practically instantaneous across the entire globe.

This has resulted in a qualitatively new landscape of influence and persuasion. First, the ability to influence is now effectively "democratized," since any individual or group has the potential to communicate and influence large numbers of others online in a way that would have been prohibitively expensive in the pre-Internet era.

Second, this landscape is now significantly more quantifiable. Data from ISM can be used to measure the response of individuals as well as crowds to influence efforts, and the impact of those operations on the structure of the social graph.

Finally, influence is also far more concealable. Users may be influenced by information provided to them by anonymous strangers, or even in the simple design of an interface. In general, ISM provides new ways of constructing realities for actors, audiences and media. It fundamentally challenges the traditional news media's function as gatekeepers and agenda-setters.

Thinking About Influence

More often than not, the word "propaganda" is used in a negative or pejorative context. But this was not always the case. In 1622, Pope Gregory XV created the *Congregatio de Propaganda Fide* (Office for the Propagation of the Faith), whose purpose was to supervise the Church's missionary efforts in the New World and elsewhere. This was partly a reaction to the spread of Protestantism and intended to help people follow the "true" path.

Edward Bernays, considered by many to be the father of the modern field of public relations, had a perhaps somewhat more flexible interpretation. He said: "Modern propaganda is a consistent, enduring effort to create or shape events to influence the relations of the public to an enterprise, idea or group."[1] He also took note of its power, making clear that "[t] he conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in a democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country."[2]

An even more modern and flexible perspective has been offered by Dimitry Kiselev, the Director General of Russia's state-controlled *Rossiya Segodnya* media conglomerate, and the Kremlin's all-around media czar. According to him, "objectivity is a myth that is proposed and imposed on us."[3] He has accused the European Union of hypocrisy and violating his right to free speech

(which is protected by international law) for imposing sanctions on him for broadcasting propaganda (which, by the way, is not illegal under international law).

All of this is important context for thinking about the rapidly-changing Information Environment that we now confront.

The Information Environment

The U.S. Department of *Defense Dictionary of Military Terms* defines the Information Environment (IE) as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[4] The IE consists of a wide variety of complex interacting and interconnected components, ranging from individuals to groups at multiple scales of organization to physical systems such as the power grid and medical facilities. The decisions and actions taken by these components, individually and collectively, simultaneously shape and are shaped by the IE in which we live.

The nature of interaction within the IE is rapidly evolving and old models are becoming irrelevant faster than we can develop new ones. The result is uncertainty that leaves us exposed to dangerous influences without proper defenses.

The IE can be broadly characterized along both technical and psychosocial dimensions. IE security today (often referred to as cybersecurity) is primarily concerned with defense of its purely technical features—for example, defense against denial of service attacks, botnets, massive thefts of IP and other attacks that typically take advantage of security vulnerabilities. This view is too narrow, however. For example, little attention has been paid to defending against incidents like the April 2013 Associated Press Twitter hack,[5] in which a group used ("hijacked") the news agency's Twitter account to put out a message reading "Two explosions in the White House and Barack Obama is injured." The result of this message, with the weight of the Associated Press behind it, was a drop and recovery of roughly $136 billion in equity market value over a period of about 5 minutes. This attack exploited both the technical (hijacking the account) and psychosocial (understanding how the markets would react) features of the IE.

Another attack, exploiting purely psychosocial features, took place in India in September 2013.[6] It was an incident designed to fan the flames of Hindu-Muslim violence, involving the posting of a gruesome video of two men being beaten to death, accompanied by a caption that identified the two men as Hindu, and the mob as Muslim. It took 13,000 Indian troops to put down the resulting violence. It turned out that while the video did show two men being beaten to death, it was not the men claimed in the caption and in fact the incident had not taken place in India at all. The attack, moreover, required no technical skill whatsoever; it simply required a psychosocial understanding of the right place and right time to post it in order to achieve the desired effect.

These last two actions are examples of *cognitive hacking*. Key to the successes of these cognitive hacks were the unprecedented speed and the extent to which the essential disinformation could be distributed. Another core element of the success of these two efforts was their authors' correct assessment of a *cognitive vulnerability* of their intended audiences—a premise that the audience is already predisposed to accept without too much critical thinking, because it makes a fundamental emotional appeal to existing fears or anxieties. And while the execution of this strategy relies on fundamentally new features of the IE, some of the underlying principles have been known throughout recorded history.

A Call to Action

An important question regarding the survival of our nation is how we answer the increasing threats that we face in the Information Environment from adversaries who range from nation states large and small to criminal or terrorist organizations to a handful of people with malicious intent. At this time, *all* of our adversaries possess a significant asymmetric advantage over us as a result of policy, legal and organizational constraints that we are subject to and they are not. We need honest and open debate about how to meet these threats.

For example, both the research community and the operational community that is charged with defending us

are subject to suffocating constraints on access to data. To understand the absurdity of our current situation, consider the fact that many parts of the U.S. government that need access to open and public social media data are denied that access, while every single one of our adversaries has complete and ready access to that information.

This author, as a program manager at the Pentagon's Defense Advanced Research Projects Agency (DARPA), recently concluded what is probably the largest ever government sponsored research program in foundational social media technology, known as the Social Media in Strategic Communications (SMISC) program. SMISC researchers accomplished amazing things and significantly advanced the field resulting in over 200 publications in the open literature, as well as developing a number of groundbreaking technologies ready for application. At this point, the biggest fear is that, because of uninformed and antiquated policies and undue legal constraints, the principal beneficiaries of this work will end up being not the U.S. government but its adversaries.

To ensure this does not happen, the United States needs to create a new Center for Information Environment Security, the goal of which is to create and apply the tools needed to discover and maintain fundamental models of our ever-changing IE and to defend us in that environment, both collectively and as individuals. Such a Center would bring together experts in areas such as cognitive science, computer science, engineering, social science, security, marketing, political campaigning, public policy, and psychology, with the goal of developing a theoretical as well as an applied engineering methodology for managing the full spectrum of information environment security issues. The U.S. government has already laid the foundation for such a construct; now is the time to erect it.

Today, the manipulation of our perception of the world is taking place on scales of time, space and intentionality that were previously unimaginable. It is all shaped by the information we receive. And that, precisely, is the source of one of the greatest vulnerabilities we as individuals and as a society must learn to deal with.

Why ISIS Flourishes in its Media Domain

By: Alberto M. Fernandez

In June 2015, the leading U.S. official in charge of the propaganda war against ISIS was admitting defeat in a leaked memo.[1] Yet, the very next month, the same official, Undersecretary of State for Public Diplomacy and Public Affairs Richard Stengel, was claiming success in the "Hashtag Jihadi" struggle in no less prominent an outlet than the *Washington Post*.[2]

Both impressions, seemingly at odds with one another, give unnecessarily definitive judgments on what will be a long, twilight struggle. It is entirely possible that the physical phenomenon known as "the Islamic State," located in the hinterlands of Syria and Iraq, will face unprecedented pressure in 2015 which could lead to its shrinkage if not outright collapse. But the "virtual caliphate," the online realm sometimes jokingly referred to by ISIS fan boys as "Wilayat Twitter" (State of Twitter), will have ramifications long after the physical defeat of ISIS-land.[3]

Staying Power

It is no contradiction to say that while the overwhelming majority of the world's Muslims have rejected the siren call of ISIS, and while the total number of recruits is relatively small given the vast potential pool, the entity's social media success has still been remarkable. More foreign fighters and zealots have gone to Syria, most of them to join ISIS, than went to fight in Iraq when American troops were on the ground or Afghanistan when the Russians were there.[4]

ISIS burst into the popular collective memory with the fall of Mosul in June 2014, the declaration of a caliphate shortly thereafter, and with a series of telegenic outrages in the months that followed. But the organization's roots go back more than a decade, and its leadership was decapitated as recently as 2010.

The Islamic State of Iraq (ISIS), before Syria, was an

extremely violent and ambitious branch of Al-Qaeda – one with, at least rhetorically, boundless aspirations. Yet it was also largely focused on events within Iraq. If you look at ISIS videos in 2011 and 2012, they are light years behind the group's current media efforts, in terms of both quality and focus.[5] Not only were they less technically accomplished, their focus was also overwhelmingly internal, Iraq-focused. The dominant message was domestic, about Iraqi Sunni disenfranchisement and the corruption and brutality of the Baghdad government. This changed over time, as ISIS messaging adapted to take advantage of new political realities and new technologies.

The Syrian Front

Syria, which represents truly the first social media war, provided the experience and venue for ISIS to make a qualitative jump in its media outreach.

The ISIS media network today is always "on," whether from the organization itself or through its network of supporters. ISIS media has a dynamic strategy, and the general technical quality of production is constantly improving. It is a multimedia (image, video, music) effort that encompasses all aspects, from pre-production to distribution. It includes extensive post-production and sound design.

While the masterminds are unknown, at least some are likely to be either westerners or western trained.[6] Each ISIS "studio" has its own staff, and they compete with each other. ISIS media functions with an essential entertainment logic: to top previous productions, to increase shock effect and generally enhance viewer experience.

The central ISIS studios, Al Furqan Foundation, Al-'Itisam Foundation and Al-Hayat Media Center, have bigger budgets and means. Their staff appears more experienced as well, and likely has professional background. The important productions have a long pre-production process and are thought out, designed and staged meticulously. To that end, local media teams are embedded with fighters and filming assaults is common, both for media and for tactical purposes.

Music and sound design are key elements to ISIS media production success. Several ISIS *nasheed* (chants) are even well known and popular beyond *jihadi* circles. Individuals such as former German rapper Deso Dogg are involved, and often have English and Arabic subtitles. You can now find ISIS musical material online, embedded in non-*jihadist* Islamist channels on YouTube. This allows at least some of the group's material to reach a larger Salafi or conservative Islamist audience.

Productions are translated into several languages, while English material is subtitled in Arabic and shown throughout Iraq and Syria in corner "Dawa" kiosks in various cities.[7] One goal is to make the virtual presence of the Islamic State as large and as encompassing as possible.

Despite the media coverage, most ISIS propaganda is not particularly gruesome. Much of it focuses on building a special state along the lines that ISIS selectively chooses from examples taken from the early period of 7th century formative Islam, the time of the *Salaf* and *Sahaba*. The violent material is a small but significant part of this picture, designed to provoke reactions in the West and garner attention. It has succeeded spectacularly in doing so.

Twitter as Force Multiplier

To this impressive internal media operation, ISIS has – as a cutting edge *jihadist* counter-culture - created a large network of online supporters. Volume matters, and ISIS' online audience has grown exponentially. According to a recent study by the Brookings Institution, while in 2012 ISIS supporters established 2,380 accounts, in 2014 that number had grown to 11,902. Almost a thousand of those contained location metadata indicating they were from Saudi Arabia. Now, some of those accounts were lightly used or shut down by social media companies. Generally, it is possible to say that pro-ISIS accounts on Twitter peaked in late 2014 at around 50,000; the number is slightly less than that today. Of that amount, about 2,000 accounts do the bulk of the work.[8]

To give one a sense of scale, if you take all accounts on

Twitter – not just those of the U.S. government – which are active in countering ISIS messaging, you would total at most 200. Moreover, most of those are not "on" all the time. So on our best day, we are outnumbered 10 to one—but sometimes much more.

An essential part of the extremist – and in particular the ISIS – message in the key years of 2013-2014 was the sectarian carnage in Syria. This motif was powerful because it was true and compelling, and because no government had a ready answer for it. *Jihadist* groups, by contrast, offered righteous, religiously sanctioned violence against an evil force. The fact that ISIS was the grimmest, most extreme and noisiest of all the jihadist groups made them all the more attractive in what became seen by many as an existential struggle of good versus evil. Thus, on the most powerful element of ISIS propaganda, governments were hamstrung from the beginning, being forced to either change the subject or argue, implausibly, that ISIS and the Islamists were worse than Assad.

An ISIS message constructed from an actual urgent crisis (in Syria), an opportunity for individual agency by young people looking for identity, a seemingly austere and implacable persona as the avenging angel of Islam, and utopianism represents a heady propaganda cocktail. It is not one message, but several—affecting both the very worst and very best in human beings in a successful effort to provide what terrorism scholar Thomas Hegghammer has called "the cultural-emotional dimension" to radicalization.[9] ISIS messaging is as much or more about building as it is about destruction, whether it is the building of a physical state, a state of mind, or of authentic (Sunni) Muslim life. ISIS has succeeded, to the extent that for several million Muslims it seems to plausibly constitute a better political option than others currently available, especially in Syria and Iraq.[10]

Responding to Radicalization

This vision is important when we observe how ISIS recruits. While there is no one road to extremism, it is surely a mistake to think that individuals are radicalized by themselves or solely by the consumption of radicalizing social media. There is usually a personal dimension – a friend or relative or neighbor – or a virtual individual dimension providing remote intimacy through Skype or Twitter or instant messaging.[11]

Governments, if they can't do it themselves (and they probably can't), need partners who can try to replicate a personalized anti-*jihadist* intervention. While there are currently smart individuals, such as Humera Khan and Mubin Shaikh, who do work of this sort, the large numbers of ISIS supporters indicates the need for greater mobilization of those who can be vetted and empowered to reach out to these clusters of troubled individuals, as well as to the general public. You likewise need a wide variety of tailored material aimed at different potential audiences of importance to the extremists. As the Quilliam Foundation's Charles Winter has pointed out, what is needed is both volume and originality—a difficult combination for governments to fashion effectively.[12]

President Obama recently spoke about the need to combat ISIS as an ideology, without actually saying what that ideology is or what should replace it.[13] But how much does this ideology actually differ from that of al-Qaeda, or from the state Salafism practiced from the Kingdom of Saudi Arabia?[14] And whose role is it to counter the introduction (or reintroduction) of the poisonous lexicon which accompanies it: *rafidah*, *kufar*, *mushrikeen*, *taghut*, *jizya*, *dhimmah*?[15] There is a well-established body of extremist thought to draw from, even if the actual roots or history of this thought are debatable.[16]

In addition, if ISIS is offering a doubtlessly false but apparently sincere utopian vision of what society – for the right sort of Muslims – is, what is the appropriate response? What is wrong, exactly, with the caliphate or with *sharia* law?[17] What sort of arguments does one make to the ISIS target audience, namely Sunni Muslims in Syria and Iraq, when ISIS seeks to present itself as *the* defender of Sunni Muslim rights, especially in today's openly sectarian-drenched region with an empowered Iran and its proxies seemingly on the march?[18] This is especially a challenge when the discourse of some Arab regimes subtly (or sometimes not so subtly) echoes the same sectarian discourse, thereby reinforcing the ISIS argument.

Ultimately, mainstream Sunni Muslims are going to need to solve the issue of ISIS presenting itself as a credible option to millions. Many are already in the fight.

AFPC will continue to host lunchtime briefing series for Congressional Staff in the House and Senate, featuring presentations by noted subject matter experts focused on a wide array of defense technology issues. If you are a staffer interested in attending future briefings or would like to suggest briefing topics, please contact Defense Technology Programs director Rich Harrison via email at harrison@afpc.org.

Endnotes

8th Century Ideology and 21st Century Technology

1) To some extent this is part of a larger problem within the Intelligence Community to adequately support "open source" research and focus effectively on the evolution of non-state actors in the Middle East and elsewhere. There is also an organizational issue as to whether this is a "homeland security" issue and a DHS mission area, to be supported by the DNI and the NCTC – none of whom appear to have distinguished themselves in advancing the research base here.

2) There is, however, the precedent that for decades open source materials collected by CIA as the Foreign Broadcast Information Service (FBIS) were published daily and sold as hard copy. But this included translations of media, not analytic products done at CIA and elsewhere in the Intelligence Community.

3) For their part many service personnel and their families have become avid users of social media platforms, which enable communications and sharing of information with family and friends. See, for example, http://time.com/3612970/isis-military-social-media/.

4)As often noted in the media, the Obama administration refuses to use the term "Islamic" in referring to the problem or ISIS at all, notwithstanding the fact that the initial "I" stands for Islamic, and the organization self-describes itself as Islamic.

5) Within the administration a recent State Department Memo from Undersecretary Stengel (June 9, 2015) to Secretary Kerry and released to the media was brutally frank on this point.

The Weaponization of the Information Environment

1) Edward Bernays, Propaganda (Ig Publishing, 2005).
2) Ibid.
3) Joshua Yaffa, "Dmitry Kiselev is Redefining the Art of Russian Propaganda," The New Republic, July 1, 2014, http://www.newrepublic.com/article/118438/dmitry-kiselev-putins-favorite-tv-host-russias-top-propogandist.
4) United States Department of Defense, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, November 2010, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
5) Max Fisher, "Syrian Hackers Claim AP Hack that Tipped Stock Market by $136 Billion. Is it Terrorism?" Washington Post, April 23, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/.
6) Mark Magnier, "Hindu Gir's Complaint Mushrooms into Deadly Indian Riots," Lost Angeles Times, September 9, 2013, http://articles.latimes.com/2013/sep/09/world/la-fg-india-communal-20130910.

Why ISIS Flourishes in its Media Domain

1) As cited in Mark Mazetti and Michael R. Gordon, "ISIS is Winning the Social Media War, U.S. Concludes," New York Times, June 12, 2015, http://www.nytimes.com/2015/06/13/world/middleeast/isis-is-winning-message-war-us-concludes.html?_r=0.

2) Richard Stengel, "The United States is Gaining Ground Against the Hashtag Jihadis," Washington Post, July 23, 2015, https://www.washingtonpost.com/opinions/beating-the-hashtag-jihadis/2015/07/23/52e097ca-30a8-11e5-8353-1215475949f4_story.html.

3) "'Obama and Twitter' – Second Installment of Pro-ISIS Animation Series Called 'The Diaries of Jihadi John,'" Middle East Media Research Institute Video Clip no. 5015, July 2015, http://www.memritv.org/clip/en/5015.htm.

4) http://icsr.info/projects/western-foreign-fighters-syria/.

5) Al-Furqan Presents a New Video Message from the Islamic State of Iraq: "Risen Alive #5." December 3, 2011, http://jihadology.net/2011/page/16/

6) "Official: American May Be Key in ISIS Social Media Blitz," ABCNews.com, September 3, 2014, http://abcnews.go.com/blogs/headlines/2014/09/official-american-may-be-key-in-isis-social-media-blitz/.

7) "Inside Mosul: What's Life Like Under Islamic State?" BBC, June 9, 2015, http://www.bbc.com/news/world-middle-east-32831854.

8) J.M. Berger and Jonathan Morgan, "The ISIS Twitter Census: Defining and Describing the population of ISIS Supporters on Twitter," Brookings Institution Analysis Paper no. 20, March 2015, http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

9)Thomas Hegghammer, "Jihadism: Seven Assumptions Shaken by the Arab Spring," Project on Middle East Political Science, February 3, 2014, http://pomeps.org/2014/02/03/jihadism-seven-assumptions-shaken-by-the-arab-spring/.

10) See Alberto M. Fernandez, "ISIS Promotes Image of Building, Not Just Destruction," MEMRI Daily Brief no. 48, July 2, 2015, http://www.memri.org/report/en/0/0/0/0/0/0/8641.htm.

11) Rukmini Callimachi, "ISIS and the Lonely Young American," New York Times, June 27, 2015, http://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html?_r=0.

12) Charlie Winter, The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy (Quilliam Foundation, July 2015), http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf.

13) "Obama on ISIS Threat: Ideologies Are Not Defeated with Guns, They Are Defeated By Better Ideas" MSNBC, July 6, 2015, http://www.realclearpolitics.com/video/2015/07/06/obama_on_isis_threat_ideologies_are_not_defeated_with_guns_they_are_defeated_by_better_ideas.html

14) Aymenn Jawad Al-Tamimi, "Islamic State Training Camp Textbook: 'Course on Monotheism' – Complete Text, Translation and Analysis," aymennjawad.org, July 26, 2015, http://www.aymennjawad.org/17633/islamic-state-training-camp-textbook-course-in.

15) Alberto M. Fernandez, "Islamic Words That Kill," MEMRI Daily Brief no. 49, July 23, 2015, http://www.memri.org/report/en/0/0/0/0/0/0/8674.htm.

16) Yahya Michot, "Ibn Taymiyya's 'New Mardin Fatwa.' Is Genetically Modified Islam (GMI) Carcinogenic?" The Muslim World, 2011, http://www.muslimphilosophy.com/michot/ITA-Mardin-Conference.pdf.

17) Khaled Diab, "The Caliphate Fantasy," New York Times, July 2, 2014, http://www.nytimes.com/2014/07/03/opinion/the-caliphate-fantasy.html?_r=0.

18) Michael Weiss and Michael Pregent, "The U.S. Providing Air Cover for Ethnic Cleansing in Iraq," Foreign Policy, March 28, 2015, http://foreignpolicy.com/2015/03/28/the-united-states-is-providing-air-cover-for-ethnic-cleansing-in-iraq-shiite-militias-isis/.

ISIS AND SOCIAL MEDIA

About The Defense Technology Program

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at Harrison@afpc.org.

About AFPC

For over three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC Mission Statement

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

CONTACT

509 C Street NE
Washington, D.C. 20002
Telephone: 202.543.1006
Fax: 202.543.1007
www.afpc.org