Digital Influencing for CVE

Counter-messaging and Digital Mobilization

February 2018

Yael Benkel, Stephanie Doucette, Christopher Godman, Katherine Hasty, Tom Hoffecker

Professors Jeffrey Connor & Carol Rollie Flynn
All statements of fact, opinion, or analysis expressed are those of the authors and do not reflect the opinion of any individual author’s employer and/or the US Government.
TABLE OF CONTENTS

I. EXECUTIVE SUMMARY ....................................................................................................................... 1

II. METHODOLOGY AND SCOPE OF RESEARCH .................................................................................. 2

III. KEY FINDINGS ................................................................................................................................. 3
   Key Finding #1: A Mismatch Exists Between USG Structures and the Threat .................................... 3
   Key Finding #2: The Threat Is Evolving and Requires a Multi-Stage Approach ................................. 7
   Key Finding #3: USG Must Identify and Employ the Best Available Technologies and Methodologies, Tailored to Each Adversary .................................................................................. 9

IV. RECOMMENDATIONS ......................................................................................................................... 12
   Recommendation #1: In the Near-Term, the USG Should Identify an Entity Responsible for Coordination Across the Enterprise .................................................................................................. 12
   Recommendation #2: In the Long-Term, USG Should Establish Hybrid NGO/USG Entity to Oversee Digital Influence Efforts .............................................................................................................. 13
   Conduct Digital Mobilization in the Medium-Term ............................................................................. 14
   Televisive Counter-Messaging Campaigns for the Long-Term ........................................................... 16

Understanding the Adversary: ISIL Case Study .................................................................................... 18
ISIL’s Digital Influence Strategy ........................................................................................................... 18
Target Audiences of ISIL’s Digital Influence ....................................................................................... 19
   Women .................................................................................................................................................. 19
   Children .............................................................................................................................................. 20
Best Practices in Counter-Messaging Campaigns Against ISIL ............................................................ 21
   Digital Disruption in the Short-Term (1–5 Years) .............................................................................. 21
   Digital Mobilization in the Medium-Term (5–10 Years) .................................................................. 21
   Effective Counter-Messaging in the Long Term (10+ Years) .............................................................. 24

VII. FUTURE RESEARCH ......................................................................................................................... 28
   #1: Understanding and Shaping ISIL’s Future ................................................................................... 28
   #2: Considering the Broader Applications of Countering Digital Extremist Influencing .................. 29

BIBLIOGRAPHY ....................................................................................................................................... 30

FIGURES AND TABLES

Figure 1: Illustration of USG Responsibility Based on Geography ......................................................... 7
Table 1: Example Framework for a Digital Mobilization Campaign ...................................................... 15
Table 2: Example Measures of Effectiveness ......................................................................................... 16
I. EXECUTIVE SUMMARY

Current thinking, methods, and structures used by the United States Government (USG) are inadequate to overcome challenges presented by extremist groups and nation-state adversaries in cyberspace. Different adversaries have different goals in this realm: among them, to inspire terrorist attacks, to sow doubt about the US government, or to influence public opinion. USG organizational structures and procedures, strictly bound by laws first written before the digital age, are insufficient to adapt to the quickly changing nature of the country’s adversaries not constrained by such limitations. The USG is currently unable to effectively respond to threats in cyberspace, largely due to the rigid legal system that makes coordination inefficient and ineffective and draws a distinction between “domestic” and “international” threats—a distinction that USG adversaries do not make.

There is not a one-size-fits-all solution to the digital influencing threats emanating from the cyber domain—a targeted response is necessary to achieve specific, desirable outcomes. To reduce waste, increase effectiveness, and better share lessons learned, USG efforts must be coordinated among the many government actors fighting against the same adversary. In the long-term, a new USG/NGO hybrid entity is needed to fully overcome obstacles related to organizational divisions, a lack of in-house flexibility or expertise, and legal limitations. In the meantime, a government group similar to the Department of State’s Global Engagement Center can play an essential coordinating role to eliminate duplicated efforts across agencies and partners by collecting, analyzing, and disseminating best practices from prior successes and failures.

To illustrate these current challenges and proposed solutions, this report presents a case study of the Islamic State of Iraq and the Levant’s (ISIL) digital activity. It analyzes its messaging techniques in the digital space, examines specific methods to counter the group’s online activities, and ultimately makes proposals about how to counter its messaging in the long term. In the short term, offensive cyber operations can be used to frustrate efforts of ISIL actors online. The USG and its partners can then fill in the open space left by the reduced ISIL presence by supporting “digital mobilization” campaigns that encourage and empower other credible voices. In addition, because extremists change their mindsets and behaviors through an active and (at least) two-way conversation—not by passively receiving information—having credible messengers and an interactive process is essential to long-term success.
II. METHODOLOGY AND SCOPE OF RESEARCH

This report is the result of a six-week-long task force established through Georgetown University’s Security Studies Program. The report is informed by research from a wide variety of sources, including 30 interviews with experts from the government, private sector, and academia; analyses of American policies; academic literature; countering violent extremism (CVE) and counterterrorism (CT) research and programs; empirical data; and foreign partner programs. While the key findings and recommendations in this report can be applied to a number of issues facing the USG, the task force examined best practices through the lens of a case study examining ISIL’s digital efforts.

The task force that authored this report, the National Security Critical Issue Task Force (NSCITF), focused on two primary research areas: common traits of effective messaging campaigns intended for large audiences, and the United States Government’s role in countering extremist efforts and promoting alternate messaging.

Throughout the research process, the NSCITF uncovered significant legal and organizational hurdles in combating digital extremism that still must be overcome, often the result of ever-changing policy and budget priorities. However, although the task force acknowledges these challenges, this report does not detail steps to address the legal and organizational barriers to effective extremist counter-messaging. Instead, this report focuses on short-term and long-term proposals for reshaping the structures and approaches the USG takes in its battle against digital extremist messaging.

The NSCITF would like to thank a number of parties without whom this report would not have come together. To the numerous guest speakers and interview subjects who volunteered their time to strengthen the content of this report, thank you. The NSCITF would like to acknowledge the sponsorship and support of the Department of State Global Engagement Center in providing the team with valuable perspective and guidance. The NSCITF relied upon prior scholarly work, especially Gabriel Weinmann’s writing on “narrowcasting” and the edited collection of works on cultivation theory by Michael Morgan, James Shanahan, and Nancy Signorielli. We would also like to recognize the research and writing of Maura McQuade, whose work on broader US government systems contributed to this report. Finally, the NSCITF would like to thank the Georgetown Security Studies Review for their review and editing of this report.
Key Finding #1: A Mismatch Exists Between USG Structures and the Threat

In the digital space, adversaries of the United States do not change their actions based on national boundaries or government structures and laws. Extremist organizations like ISIL, al-Qa’ida, or Boko Haram—and even state actors—can project their digital presence and influence to any part of the world and nimbly adjust their messaging, dissemination platforms, and objectives as their priorities change. The USG does not have a comprehensive and flexible approach to adversaries’ actions in cyberspace—instead, it is a mix of varying jurisdictions, authorities, and responsibilities that have accumulated over time. Adversaries who quickly adapt are able to stay ahead of a USG that is forced to spend more time coordinating and de-conflicting and less time responding to the threat.

USG legal and organizational structures and focus create boundaries that limit a comprehensive strategy to combat such a fluid global threat. This predominantly stems from the fact that governmental organizations are built to fulfill specific and narrow purposes. Many governmental organizations have a vertical design to ensure the institution can more effectively carry out missions related to its core functions. The operating boundaries of an organization are ultimately defined by its departmental policies, funding mechanisms, and legal authorities.1 Some refer to this type of organizational structuring as “government silos.”2 Government silos act as vertically-integrated entities that may stand next to one another, but operate independently. At least in some cases, this organizational design was also chosen to protect American civil liberties and ensure that USG agencies did not overstep their authority. However, in the digital age, what were once clear-cut rules have become less clear.3

Rapid technological advances have made communication and messaging significantly easier than before. Government organizations which were previously able to filter out at least some adversarial messaging are now unable to block such communications. Groups like ISIL are

1 National Countering Violent Extremism Task Force, interview; O’Flynn, Blackman, and Halligan, Crossing Boundaries in Public Management and Policy; Judge Advocate General subject matter expert, interview.
2 Tett, The Silo Effect.
3 US Federal Bureau of Investigation counterterrorism subject matter expert, interview; Lee, “The NSA Is Trying to Have It Both Ways on Its Domestic Spying Programs”.
no longer constrained by physical boundaries and can use the digital space to directly reach and influence US citizens domestically. The digital domain enables direct contact with target audiences, cutting horizontally across vertical governmental organizations. At the same time, however, reactions by USG organizations are constricted to the boundaries that exist inside their respective silos when contact via foreign adversaries is identified.

This becomes especially problematic when contact originates abroad and is transmitted directly into the United States, reaching US citizens within their own borders. USG organizations that are countering this threat are primarily built to keep domestic and international matters separate from each other. However, when a message is sent from a foreign country and arrives domestically, it crosses over those two distinct and separate jurisdictions.

Because foreign and domestic issues are handled separately, USG entities end up dividing and duplicating efforts to address the same threat. This also creates gaps as the USG agency with the international jurisdiction must immediately inform the domestic component any time there is a message sent to US citizens within US borders. The matter of deciding which USG organization is responsible for handling adversarial messaging or their international digital presence is also convoluted. It can take time to decide which USG agency or department has the lead or jurisdiction over the issue. As a result, an unintended consequence of such division of jurisdictions and responsibilities is that the USG has been unable to effectively respond to digital messaging from overseas adversaries.

Challenges are apparent from the beginning of the process; the initial evaluation of a threat can have a major impact on subsequent actions as a determinant of who takes the lead on the issue. Different bodies in the USG have different tools, legal mandates, and cultures that impact the way they frame and address the threat of extremist groups online.

A major challenge lies in the fact that there is no overarching or unified system to classify a threat. As it exists, the legal system is relatively well-structured to deal with domestic- or international-based threats, but issues arise as today’s digital threats are no longer easily classified as “domestic” or “international.” As a result, each USG agency is left to make its own determination about a threat as it is encountered. Coordination between the domestic-focused

---

4 For example, the FBI, Department of Homeland Security, Department of State, and Intelligence Community agencies each have strict limits on what they can do internationally vs. domestically.
and international-focused agencies does occur, but is significantly encumbered by a legal structure set up for the 20th century.

Each agency, depending on its legal mandate and the specifics of a case, characterizes the threats it encounters as either international or domestic in nature. Once an initial determination is made, (which is not always easy to do), a further determination is made as to whether use a CVE or CT approach. Most international issues are addressed through a CT framework (with some CVE overlap) while most domestic issues are addressed through a CVE framework (with some CT overlap).

This division has a significant impact on how the USG handles digital adversarial engagement domestically. Under Executive Order 13721, the Global Engagement Center (GEC) is responsible for international efforts while the Countering Violent Extremism Task Force (CVE TF) is responsible for domestic efforts established under the USG’s 2011 CVE Strategy. Additionally, whether a domestic case is viewed through a CVE or CT lens is influenced by the specifics of the case.

Both have clear legal limitations about what is permitted and both are responsible for CT and CVE coordination—however, they have different ways of implementing principles of CVE and CT. As of March 2017, GEC and the National CVE Task Force perform similar missions in their efforts to deter and confront extremist groups like ISIL in the digital space. Despite their similar missions, however, the two organizations have opposing geographical focuses with different funding mechanisms and legal authorities. Coordination and collaboration can meaningfully improve only once these structural gaps are reduced.

While the GEC and CVE TF do communicate about threats on a weekly basis, US adversaries launch cyber influence campaigns twenty-four hours a day, seven days a week. Coordination and collaboration cannot be consistent as each organization is focused on its own

---

5 US Federal Bureau of Investigation counterterrorism subject matter expert, interview.
7 For example: Is there an imminent threat? Is it connected to international terrorism? Is it connected to other criminal activities (e.g., money laundering, illegal weapons sales, etc.)? How those questions, and others, are answered play a part in determining whether a CT or CVE approach is used on domestic cases.
duties, responsibilities, and jurisdiction. This creates gaps as the threat crosses from one jurisdiction to another in real time.

Differing jurisdictions, organizational structures, and laws prevent a unified USG strategy to counter the same adversary. To illustrate the difficulty of a unified response, take two examples:

1. If an ISIL member sends a message that does not enter US networks or reach US persons in the US, GEC has jurisdiction over this case and it would likely be treated as a CT case (with some CVE overlap).\(^8\)
2. If that same message was sent by an ISIL member overseas, entered American networks, and was received by a US person, the CVE TF has jurisdiction over the domestic aspects and would likely treat it as a CVE case.\(^9\) GEC may also see this threat at some point before it enters the United States and would likely treat it as a CT issue. There are now two bodies addressing the same threat, at different times, using different approaches.

In this example, although the ISIL member is sending the same message, there are very different USG responses and mechanisms depending on details of where the message ends up. This illustrates how under the current system, it is very challenging to form a collective response because the threat is simultaneously moving through two separate jurisdictions and areas of responsibility.

Figure 1 illustrates the GEC and CVE TF areas of focus and responsibility. The adversarial message is sent out from a non-US location. Because it originates from overseas, it is under the GEC’s jurisdiction. However, when the message enters the US and US persons view the messages, it now falls under the CVE TF. The message is moving through both jurisdictions simultaneously. Because response times and how to handle the message is a factor, coordination and collaboration gaps are unintentionally created.

\(^{8}\) Judge Advocate General subject matter expert, interview; US Department of State, “Global Engagement Center.”
\(^{9}\) National Countering Violent Extremism Task Force, interview.
Key Finding #2: The Threat Is Evolving and Requires a Multi-Stage Approach

As adversaries change how they use the internet to spread their messages, a multi-stage plan with techniques and objectives adjusting over the short-term (disrupt the adversary), medium-term (spread new narratives through credible voices), and long-term (use other media, including television, to reach children) would increase chances of success.

Physically destroying extremist groups is only the first phase in eliminating their influence. This report focuses on the second phase (spreading new narratives) and the third phase (using other media to expand messages). In a 2016 report by the CSIS Commission on Countering Violent Extremism, former UK Prime Minister Tony Blair and former Secretary of Defense Leon Panetta addressed the fact that there are no quick military solutions to defeating extremist groups: “We will need to continue to take terrorists off the battlefield, disrupt plots, and safeguard our borders. But we will never eradicate the violence caused by these groups until we defeat their ideologies.”

To successfully counter violent extremism, the Commission called for a comprehensive strategy which included military and law enforcement action, a focus on

---

increasing education and economic prospects in vulnerable areas, and increasing cooperation with credible voices in regional and local civil society.\textsuperscript{11} This report shares some of the same findings and recommendations as the CSIS Commission’s report, but goes more in-depth on specific tactics and operations to defeat adversaries in the digital space.

As a previous NSCITF report emphasized, the public health model of primary, secondary, and tertiary prevention can be used to address CVE issues.\textsuperscript{12} This report builds on that analysis, detailing ideas for primary prevention (long-term messaging campaigns, especially through television), secondary prevention (reclaiming the narrative through credible voices), and tertiary prevention (in the short-term, eliminating certain digital safe spaces and interrupting an adversary’s ability to spread its messages).

While not sufficient to defeat an adversary, efforts to frustrate and disrupt the online activities of adversaries play an important role in setting the stage for follow-on messaging campaigns. During Congressional testimony in February 2017, Dr. Bruce Hoffman, a noted counterterrorism expert, said that when battling ISIL:

“First and foremost, there has to be a military answer to taking down the state...counter-propaganda messages and counter-messaging can be helpful. Until then, though, I would emphasize less the message and more the technological solutions of depriving the terrorists of the platforms that they use to communicate those messages...The counter-messaging should prevent the resurgence of these groups, not attempt to address them right now.”\textsuperscript{13}

As reported by the \textit{New York Times}, “cyberweapons buy time but rarely are a permanent solution.”\textsuperscript{14} This report proposes that as the adversary’s ability to openly communicate online is disrupted, there is space to fill with messages that support USG objectives.

By studying previous cases in which groups successfully influenced the beliefs and behavior of their target audiences, the USG can develop more robust and nimble responses to extremists online. Applicable lessons can be drawn from four different areas and case studies:

\textsuperscript{11} CSIS Commission on Countering Violent Extremism, “Turning Point: A New Comprehensive Strategy for Countering Violent Extremism,” V.
\textsuperscript{12} Challgren et al., “Countering Violent Extremism: Applying the Public Health Model”.
\textsuperscript{14} Sanger and Schmitt, “U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS.”
• Key features of adversaries’ digital activities, for example ISIL’s own tactics, techniques, and procedures (TTPs) in targeting and recruiting individuals;
• Lessons learned from de-radicalization efforts in the non-virtual world;
• Unique characteristics of recent American presidential campaigns; and
• Trends in the technological tools being developed for marketing and branding strategies.

Although it is challenging to develop measurements of effectiveness for messaging campaigns, this report makes an initial attempt to do so. By overlaying multiple types of quantitative and qualitative information, one can gain insight into the overall success of messaging campaigns—both those of the USG and adversaries.15

Finally, long-term efforts should focus on influencing the mindsets of those vulnerable to the propaganda of USG adversaries. Our research indicates that media aimed at children, especially television programs, can be effective at changing attitudes.16 Implementing such an approach can be difficult due to the challenge of measuring its effectiveness and the patience needed to see outcomes.

Key Finding #3: USG Must Identify and Employ the Best Available Technologies and Methodologies, Tailored to Each Adversary

Based on this task force’s research and interviews with experts, it is this report’s judgment that USG efforts to disrupt adversaries’ digital messaging efforts could be greatly improved if lessons learned from past efforts were readily shared and accessible when new efforts are being designed. The USG’s approach to countering ISIL and other groups online has adapted over time and has incorporated both new methodologies and technologies, but success continues to be

elusive. A major reason for this has been the lack of a centralized organization or entity responsible for overall sharing, communication, and leadership of the counter-messaging mission.

Recommendations for the future should be based on past efforts of the various entities involved in similar anti-extremist messaging projects, including across the USG, the private sector, and NGOs. While general best practices inform overall strategy, specific actions must be based on a nuanced understanding of the specific adversary against which they will be applied. There is a broad consensus that US efforts to counter ISIL online have, for the most part, been haphazard and clumsy. A January 2017 Associated Press report into the Pentagon’s WebOps counter-messaging program describes inept translators, “cronyism, and flawed data” to the point that the program is “having little impact,” with some specific issues drawing “open ridicule on social media.”

Rita Katz, founder of SITE Intelligence Group, described one early US-funded campaign as “playing into the Islamic State’s hands by bolstering its reputation for cruelty and expanding its audience.”

To overcome these hurdles, it is essential that relevant lessons learned from past efforts inform future efforts to counter extremists online. For example, the USG could adopt some recommendations from a thorough review of US military psychological operations in Afghanistan—another mission that requires a flexible response to messaging from adversaries—including increasing the role of credible messengers and bringing together counter-messaging practitioners from across the USG to share their experiences and identify best practices. The lack of a centralized process or entity responsible for collecting and disseminating lessons learned, including from efforts not obviously related to online counter-messaging, has resulted in excess inefficiency and waste.

While this report recommends that the USG should not direct most counter-messaging content, the USG will continue play an essential role in pushing back the online presence of adversaries through denying adversaries space on the internet and eliminating those who lead

---

17 Butler and Lardner, “US Misfires in Online Fight against Islamic State”; Nakashima, “U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies”; Miller and Higham, “In a Propaganda War against ISIS, the U.S. Tried to Play by the Enemy’s Rules”.
18 Butler and Lardner, “US Misfires in Online Fight against Islamic State.”
19 Miller and Higham, “In a Propaganda War against ISIS, the U.S. Tried to Play by the Enemy’s Rules.”
messaging efforts. While an in-depth discussion of private Internet companies is outside the scope of this report, they have a significant responsibility to monitor for extremist activity on their platforms (especially social media and messaging services). Beyond the private sector, the USG has significant SIGINT capabilities that can be used to identify and monitor extremists online. Information gathered by the USG can later be used to inform attacks which aim to reduce the digital footprint of an adversary, whether through DDoS attacks, destroying hardware, or sharing intelligence with the military to eliminate those who lead propaganda and messaging efforts. For these cases, technology should continue to be upgraded and efficient communication between the IC and DoD must be maintained.

A plethora of data, tools, and approaches exist that could be used to disrupt the digital messaging techniques of adversaries and directly influence their desired target audiences; the challenge lies in identifying which approaches would be most successful against which adversaries or audiences at any given time. Different tools may also be better suited to different objectives: an attack that takes down ISIL communication may be seen as a success by the military, but a lost communication channel to intercept by the intelligence community. These goals will have to be agreed upon and coordinated in an interagency process, potentially led by the GEC or at the National Security Council (see Recommendation #1 in the following section for more detail).

---

21 Nakashima, “U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies.”
IV. RECOMMENDATIONS

Recommendation #1: In the Near-Term, the USG Should Identify an Entity Responsible for Coordination Across the Enterprise

Given the large number of approaches that can be used in counter-messaging campaigns, there is a need for a central body within the USG to: 1) de-conflict efforts, 2) establish information-sharing mechanisms across participating agencies, and enable and encourage collaboration, 3) collect, analyze, and disseminate lessons learned, 4) monitor results, and 5) establish best practices. This central body must also have the ability to determine the actors best suited to conduct each campaign, and centrally delegate to and across barriers of jurisdiction.

As the lead for foreign counter-messaging campaigns, established in Executive Order 13721, the GEC is currently well suited to take on this role. Because the coordination efforts described above are resource and time intensive, the GEC should focus on these efforts rather than developing its own counter-messaging content. More broadly, whichever entity is ultimately charged with this responsibility should become a center of expertise and policy planning. USG agencies should coordinate clear objectives, strategies, and tactics through the coordinating entity before starting new counter-messaging efforts at multiple levels, including down to the tactical level. This further provides the coordinating entity with the ability to increase information flow, minimize unintended duplication, and increase resource efficiency—all of this can be accomplished while collecting and disseminating best practices and serving as an active repository of what approaches have been tried and their respective strengths and weaknesses.

While GEC is the government lead for such efforts, it lacks “directive authority” over other government efforts to fight ISIL and other adversaries in the information space, ultimately hampering its ability to effectively marshal resources. An alternative approach, suggested by Lt. Col. Bradford Burris, involves placing the National Security Council in charge of “coordination, integration, and synchronization” of counter-ISIL efforts. Given GEC’s expanded mandate to

---

23 Burris, “Countering ISIL’s Digital Caliphate: An Alternative Model.”
24 Ibid.
work against new, non-terrorist targets,\textsuperscript{25} government leaders must ask whether the current structure most effectively supports US policy goals. If the not, leaders should consider new proposals like Lt. Col Burris’.

**Recommendation #2: In the Long-Term, USG Should Establish Hybrid NGO/USG Entity to Oversee Digital Influence Efforts**

Friction from the legal and organizational barriers described in this report can be minimized from within the USG, but a more effective approach in the future would be to create a hybrid USG/NGO entity with greater flexibility. Such an entity would not be hampered by months-long interagency coordination processes. Instead, it would have more room to experiment with new approaches and be able to quickly adopt those that have been most effective. In the fight against extremist messaging in which adversaries quickly adapt, speed is essential, and this structure would allow a quicker US response.

Current USG counter-messaging efforts lack a dedicated mechanism to collect, analyze, and develop best practices (which includes methodology and technology) from multiple sources:

- The various agencies and entities focused on addressing extremist online activities;
- The private sector;
- US adversaries; and
- Academia (specifically, psychology).

Even if this report’s first recommendation to establish a unified coordinating body is implemented successfully, this entity would play a key role by stepping back from daily operations and focus on long-term strategic research and planning. The NGO/USG hybrid would be responsible for carrying out anti-extremism campaigns (operations), while the GEC (or other designated lead) would be responsible for collecting and disseminating best practices from around the world and funding longer-term research into counter-messaging (strategy).

Developing such recommendations requires an understanding of metrics of success. This entity would also need to conduct robust analysis to determine why a particular effort succeeded

\textsuperscript{25} Tucker, “Analysts Are Quitting the State Department’s Anti-Propaganda Team.”
or failed. Its staff will need an appreciation for the fact that no single effort will solve the problem of extremist messaging over the internet—instead, efforts need to be layered. Examples of similar existing entities include In-Q-Tel, DARPA, and the National Center for Missing & Exploited Children. These entities have shown that harnessing private sector innovation, independence, and trusting relationships with local-level organizations (respectively) are essential in tackling large, quickly changing problems.26 With a well-funded and broad mandate, this hypothetical entity could start by considering the following complementary approaches.

Conduct Digital Mobilization in the Medium-Term

Efforts to counter extremist messaging online, in the medium-term, should focus on “digital mobilization”: the act of using the Internet to organize individuals into a group that supports a common cause. Campaigns by the United States and its partners should be designed to:

1. Target in-group influencers;
2. Draw on content tailored to the target group (“narrowcasting”) using a variety of data sources, including big data, polling data (where available), information elicited through social engineering, and existing literature on the effectiveness of various types of content;
3. Leverage the digital medium’s utility for organization, user creativity, and fast communication;
4. Experiment and adapt to incorporate new modes of digital communication; and
5. Incorporate built-in feedback mechanisms.

Using credible voices to engage individuals over the Internet creates a counterbalance to the voices of adversaries who promote extremist messaging. As stated above, individuals do not change their behaviors or beliefs through passively consuming content. Instead, interaction and

conversation with a community is essential. Digital mobilization campaigns are one method to engage individuals who may be susceptible to extremist messaging.

Table 1 presents a sample campaign strategy framework with these characteristics to illustrate how such a campaign might look in practice, while Table 2 provides examples of in-depth measures of effectiveness for assessing the impact of digital mobilization campaigns.

Table 1: Example Framework for a Digital Mobilization Campaign

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Market Research</td>
<td>Layer existing research on vulnerable online populations with data from social listening tools</td>
<td>Identify in-group influencers and analyze behavior/preferences through big data collection and social engineering</td>
</tr>
<tr>
<td>2. Content Development</td>
<td>Content focused on motivating targeted individuals to join the digital fight against ISIS</td>
<td>Education on how to take over an ISIS chatroom; encouragement to create and spread counter-ISIS stories</td>
</tr>
<tr>
<td>3. Dissemination</td>
<td>Use a variety of mechanisms to get the content out</td>
<td>Click-bait; Google search strength; leveraging influential celebrities</td>
</tr>
<tr>
<td>4. Positive Feedback</td>
<td>Support good user-generated messages</td>
<td>Add “likes,” “shares,” etc.</td>
</tr>
<tr>
<td>5. Monitoring, Assessment, Adaptation</td>
<td>Develop rapid and flexible means to evaluate and tweak the approach</td>
<td>See Table 2</td>
</tr>
</tbody>
</table>
### Table 2: Example Measures of Effectiveness

<table>
<thead>
<tr>
<th>Activity</th>
<th>Timeframe (Quantitative)</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessing Disruption</td>
<td>Short-Term</td>
<td>Number of accounts suspended</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of chats interrupted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of pieces of content flagged for removal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of pieces of content removed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of followers before/after account suspension after reopening</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of recruiters identified</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of targets of recruitment identified</td>
</tr>
<tr>
<td></td>
<td>Short-Term (Qualitative)</td>
<td>Number of websites disrupted/taken down</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Indicators of linguistic sophistication in postings (e.g., number of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>languages posted in, fluency of multi-lingual media</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISIL presence on open web relative to presence on dark or deep webs</td>
</tr>
<tr>
<td>Assessing Expansion</td>
<td>Short-Term (Quantitative)</td>
<td>Number of individuals who access/share/generate/interact with content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ratios of access-to-share and access-to-generate (compared to other US/coalition efforts and compared to ISIL efforts)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total growth rates of the above two metrics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Duration of the lifecycle (i.e., how long individuals share and engage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with content relative to the lifecycle of a typical ISIL media campaign)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergence of spin-off efforts (i.e., an increase in non-ISIL and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>counter-ISIL engagement both in digital as well as non-virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td>communities)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Observed changes in ISIL behavior to counter the threat posed by these</td>
</tr>
<tr>
<td></td>
<td></td>
<td>efforts</td>
</tr>
<tr>
<td></td>
<td>Short-Term (Qualitative)</td>
<td>Text-block analysis of spread and evolution of content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Demographics of recruits by country of origin, nationality, language,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ethnicity, religion, and other factors</td>
</tr>
<tr>
<td></td>
<td>Long-Term (Qualitative)</td>
<td>Conduct long-term study of children</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Study the views about ISIL held by individuals who have never had any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>real-life experience the organization, and the relation of these</td>
</tr>
<tr>
<td></td>
<td></td>
<td>views to the level of exposure those individuals have had to counter-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>messaging</td>
</tr>
</tbody>
</table>

**Televise Counter-Messaging Campaigns for the Long-Term**

Efforts to counter extremist messaging in the long-term should focus on televised counter-messaging campaigns because increased exposure to television can change people’s
perceptions of reality. The USG should maximize the effectiveness of televised counter-messaging by:

- Incorporating counter-messaging into children’s television shows because televised messages have the strongest influence on children;
- Refining counter-messages and increase their credibility by gaining a better understanding of how other cultures perceive Americans through American television shows;
- Using televised counter-messaging to shape the radicalization narrative; and
- Implementing a multi-sector approach and partnering with Hollywood to design credible televised counter-messages.

One example of US-funded television production in Afghanistan is “Eagle Four.” Such efforts are not always successful, but there is an earlier body of work from which to draw. For more information on TV propaganda in Afghanistan, see: Nordland, “On TV, an Afghan Unit Tackles the Taliban”; Abi-Habib, “U.S. Courts Afghans Through Television”; and Tierney, “Making Soapies in Kabul.”
Understanding the Adversary: ISIL Case Study

To understand how a digital influencing campaign can be carried out, this task force conducted an analysis of American competition for influence with ISIL in the digital space. This case study provides insights that can be immediately helpful in combating that adversary. In recent years, an increasing number of extremist groups have begun to use the digital world to further their goals and spread their messages through email, chatrooms, e-groups, forums, virtual message boards, YouTube, Google Earth, social media, and other outlets. Groups have used the Internet to conduct psychological warfare, spread propaganda, recruit and mobilize members, mine data, raise funds, and plan and coordinate attacks. To understand the threats posed by such groups and to explore potential solutions for countering extremist groups’ digital influence, this report examined ISIL’s digital presence through the lens of a case study.

ISIL’s Digital Influence Strategy

To increase the organization’s digital influence, ISIL’s digital propaganda utilizes “narrowcasting,” the dissemination of propaganda to specific audiences, to communicate with a wide range of demographics on an individual level. ISIL has been successful at targeting a variety of demographics, including people of varying ages, gender, socio-economic backgrounds, religions, and nationalities. ISIL’s propaganda often contains two main components: “depicting the caliphate as a peaceful and idyllic domain” and depicting “a society awash in apocalyptic violence.” While ISIL’s violent beheading videos are meant to strike fear into Western audiences, they are also meant to inspire individuals to “leap into the Islamist fray.” Seemingly in contrast to this messaging, ISIL attempts to depict their territory as being a “livable destination,” a place where their target audiences throughout the world can move and enjoy life. Despite the contrast in these types of messaging, both the idyllic caliphate propaganda and

---

29 Ibid., 53.
30 Bergen et al., “ISIS in the West: The Western Militant Flow to Syria and Iraq.”
31 Miller and Mekhennet, “Inside the Surreal World of the Islamic State’s Propaganda Machine.”
32 Ibid.
33 Ibid.
apocalyptic violence propaganda are meant to speak to the needs of their varying audiences and the reasons each audience may feel drawn to ISIL.

**Target Audiences of ISIL’s Digital Influence**

Just as there is no single terrorist psychology, there is no single psychological profile or demographic specifically drawn to terrorist organizations. However, there are general target audiences that are both drawn to and targeted by specific terrorist organizations. The target audiences discussed in this paper are not meant to describe the “cookie cutter” ISIL recruit. Instead, these categories are meant to give an example of how ISIL utilizes “narrowcasting” to increase their digital influence. Any single ISIL recruitment target may fall into multiple target audiences (and potentially none at all). The motivation to join a terrorist organization can be based upon several reasons, including political, social, economic, and personal factors—ultimately, it varies with each individual.

Like other terrorist organizations, ISIL has specifically targeted disenfranchised individuals in the West. This includes those who feel of isolated, sad, angry, or those who have suffered a negative life event. Many of these individuals are drawn online out of a desire to find a sense of belonging. There, some encounter radical ideologies, like that of ISIL, which provide them with a new social identity. Two groups of disenfranchised individuals ISIL targets using narrowcasting are women and children.

**Women**

ISIL’s use of narrowcasting on women primarily emphasizes the “idyllic caliphate” motif. By portraying the ideal life lived by female members of ISIL, recruiters exploit the desire of many recruited women who seek a sense of belonging, a community, and a purpose, whether through “building a caliphate or being a part of a larger sisterhood.” Many women who are attracted to ISIL have a “romanticized notion about what the caliphate is.” Therefore, a common theme of ISIL’s online propaganda for women focuses on the selling of a “fantasy

---

34 Bouzar, Caupenne, and Valsan, “CPDSI Report on the Recruitment and Indoctrination by Radical Islamic Sects.”
35 Bergen et al., “ISIS in the West: The Western Militant Flow to Syria and Iraq.”
36 Women In The World Staff, “Women a ‘Mainstay’ of ISIS Propaganda and Recruitment.”
37 Fenton, “Why Women Are Leaving The U.S. & Europe To Join ISIS — & What Can Be Done.”
escape” to women, particularly women in the West. Recruitment videos targeted at women depict smiling children, an attempt to show that women who join ISIL can raise happy and healthy families; many of the ISIL Twitter accounts aimed towards women are run by female ISIL members. Those ISIL members post pictures of beautiful scenery in ISIL territory and write captions about how wonderful their lives are as ISIL women.

Children

Rather than focusing upon messages emphasizing the idyllic caliphate, ISIL’s use of narrowcasting on children focuses largely upon propaganda emphasizing apocalyptic violence. Violent propaganda is appealing to numerous children because they are often drawn by the organization’s depictions of violence, excitement, and adventure. According to Daniel Koehler, Director of the German Institute on Radicalization and Deradicalization Studies, “The amount of Islamic State videos and propaganda aimed at children has really jumped...We haven’t seen anything quite like this, not on this scale and of this quality. They know that in the West, you don’t expect a 10-year-old to be a terror suspect.” To emphasize this apocalyptic violence, ISIL uses children in a number of their violent propaganda videos. In some cases, children participate in beheadings and firing squads. ISIL’s propaganda for children also includes alphabet learning apps with militaristic terminology, including “gun,” “tank,” and “rocket,” geared to 3–4 year-olds, as well as violent video games for older children.

---

38 Ferran and Kreider, “Selling the ‘Fantasy’: Why Young Western Women Would Join ISIS.”
39 Ibid.
41 Faiola and Mekhennet, “What's Happening to Our Children?”
42 Ibid.
44 Engel, “ISIS Has Released a New Android App Aimed at Children.”
Best Practices in Counter-Messaging Campaigns Against ISIL

While there is no single approach that will defeat ISIL in the digital space, this report has identified technologies and methodologies that are assessed to be particularly effective in the short-, medium-, and long-term. Digital disruption of the adversary has the most immediate effect. In the medium-term, efforts should be focused to increase the effectiveness of counter-ISIL messaging by mobilizing online communities to generate their own content. Long-term efforts aim to influence the next generation.

*Digital Disruption in the Short-Term (1–5 Years)*

Technical collection and disruption operations are essential to identifying and countering ISIL online activity. By degrading the ability of ISIL leaders and its members to reach a broad audience, the USG will decrease the access potential recruits may have to ISIL information, as well as provide more opportunities for effective USG counter-messaging. Different actors have specific capabilities and strengths—broadly speaking, the government has large amounts of money and manpower, while firms in the private sector are generally more nimble and innovative.\[^{45}\] Due to the varying strengths of the different actors, coordination is necessary for success.

If the USG can identify key online figures in ISIL (those producing propaganda, those posting it, and those actively encouraging pro-ISIL conversations) and reduce their voices by limiting their online presence (through attacks, removal from social sites, and other related methods), ISIL’s more easily-accessible spaces are reduced. Given that ISIL has lost significant territory in the last year and that it aims to continue to expand its reach, increased online operations are one logical step for ISIL to take.\[^{46}\] For that reason, the USG should explore ways to establish systems to keep ISIL propaganda out of reach of curious potential radicals.

*Digital Mobilization in the Medium-Term (5–10 Years)*

The United States and its partners can make changes to increase the short- and medium-term effectiveness of digital engagement with communities that may be vulnerable to ISIL

\[^{45}\] World Bank Group, “Government Objectives: Benefits and Risks of PPPs.”

\[^{46}\] Blanchard and Humud, “The Islamic State and U.S. Policy.”
propaganda and recruitment campaigns. Specifically, the USG needs to encourage the creation of organic content by a community of online users. This would constitute a kind of “digital mobilization”—an effort to mobilize digital communities of users to generate and spread counter-extremist messaging. A digital mobilization campaign carried out over the medium-term to counter ISIL’s online influence should:

1. Target in-group influencers—individuals who are the trendsetters and strongest voices within the group;
2. Tailor content at the individual level (narrowcasting);
3. Move away from one-way communication and instead use the digital medium’s utility for organization and user-generated storytelling;
4. Follow a model of experimentation and adaptation; and
5. Have built-in feedback mechanisms.

Current efforts like State Department’s Peer-2-Peer (P2P) and the World Organization for Resource Development and Education (WORDE) that encourage communities to create their own messages are a good start. More attention can be focused on identifying and enabling key in-group influencers to mobilize organic, grassroots movements. Counterterrorism expert Basia Spalek states, “The focus on connectors rather than communities helps understand the role that key actors play in counterterrorism, whether these are police officers, youth workers, or community members.” Local connecting partners are critical to individualizing counter-messaging campaigns and can directly engage in promising peer-to-peer efforts.

The following analysis draws applicable lessons from four case studies of successful efforts to change the beliefs and behavior of a target group. The case studies represent a variety of contexts: the first two are specific to extremism; the second two are specific to the digital realm.

---

47 Lessons are distilled from the four case studies analyzed later in this section.
48 Harte and Volz, “U.S. Looks to Facebook, Private Groups to Battle Online Extremism.”
49 Ibid.
50 Ibid.
#1: ISIL’s Tailored Interventions

ISIL uses “tailored interventions” in which susceptible individuals are identified and then digitally surrounded by a community of ISIL supporters who maintain high levels of contact and communication with the target. This TTP provides four important lessons. First, the use of such a resource-intensive TTP suggests that ISIL finds its own passive propaganda insufficient to radicalize and recruit at a pace and scale that meet its objectives. Therefore, there is no reason to expect passive counter-ISIL messaging to be any more effective. Second, it suggests the value of integrating messaging and organizing efforts. Third, it highlights the value of individualized and tailored targeting. Fourth, while some individuals conducting the interventions are ISIL members, others are volunteers. This might serve as a model for creating and mobilizing an online community of digital activists. This would not only accelerate the spread of the counter-ISIL message, but would also satisfy the need for personal significance—a contributing factor to radicalization.

#2: Lessons from De-radicalization Programs

Successful collective de-radicalization in the non-virtual world “begins as an elite-level process among one or several key individuals” who then influence their followers to shift their beliefs and behavior. While ISIL’s interventions target vulnerable individuals, it may be more helpful for counter-ISIL efforts to target individuals who can influence their peers. The value of using the digital realm to achieve this effect is supported by studies demonstrating that peer pressure and social networks are key factors in successful collective de-radicalization. It is also important to note that de-radicalization requires two-way communication at a minimum: extremists do not change their beliefs or behavior by passively ingesting information, but from actively communicating and participating in the process. This underscores the limitations of a strategy that focuses on propaganda and excludes engagement. While the content of outreach efforts is outside the scope of this report, the body of work analyzing which techniques move

---

52 Ibid.
53 Kruglanski, “Psychology Not Theology: Overcoming ISIS’ Secret Appeal.”
54 Rabasa et al., Deradicalizing Islamist Extremists.
55 Ibid.
56 Ibid.
Islamic extremist influencers to de-radicalize in the non-virtual world may be useful for developing digital content. There is also valuable literature explaining how choices can be framed to produce the selection of a desired outcome. Studies have shown that the voices and perspectives of de-radicalized terrorists are particularly effective in non-virtual de-radicalization. As a result, it may be valuable to include such individuals in all phases of the planning and execution of the digital mobilization effort.

#3: Recent Presidential Campaigns in the United States and Narrowcasting

In the last decade political campaigns, especially presidential campaigns, have been refined their messaging through narrowcasting based on extensive polling data, big data analytics, and effective feedback mechanisms that enabled rapid adaptation and message refinement. The campaign also created new digital tools for organizing and engagement, reinforcing the importance of leveraging the digital medium’s power for communication as well as organization.

#4: Digital Marketing and Social Listening

Narrowcasting has become a crucial element in marketing and brand-awareness efforts. Sophistication is increasing with the development of “social listening” tools that can identify and characterize influencers within the group, analyze sentiment, analyze digital community demographics, and provide a host of other relevant services. These services emphasize the rapid changes in the digital landscape and offer to inform adaptation. The literature on interactive advertising is an area where further lessons could be drawn for digital influencing efforts to counter violent extremism.

Effective Counter-Messaging in the Long Term (10+ Years)

This report recommends the use of counter-messaging in television shows as an effective long-term strategy based on an idea called “cultivation theory.” Cultivation theory, also known as

57 Kahneman, Thinking, Fast and Slow.
58 Rabasa et al., Deradicalizing Islamist Extremists.
59 Issenberg, “How Obama’s Team Used Big Data to Rally Voters.”
60 Marvin, “The Best Social Listening and Influencer Identification Tools of 2017.”
cultivation analysis, is “designed to assess the contributions television viewing makes to people’s conceptions of social reality.” Television has become the world’s storyteller, replacing parents, peers, schools, and religious institutions. As a result, television is “our most common and constant learning environment, one that very few can or even want to escape.” Cultivation research suggests “the mass media—especially television—exert a small but statistically significant impact on people’s views of social reality.”

According to cultivation theory, viewers may either develop new perspectives on social reality or maintain their existing perspectives as a result of the long-term exposure to television. As childhood and adolescence are significant time periods for the creation of mental and cultural models, televised messages that are viewed during those time periods may influence the formation of mental and cultural models, which may affect social reality beliefs in adulthood. Television represents America’s melting pot, as attitudes or behaviors that are commonly associated with social or political components can be reduced or become non-existent amongst individuals who watch more television. Television also has the strongest centering effect amongst groups whose opinions need to change the most to align with the mainstream.

Multiple studies suggest that American TV might have a very powerful impact on individuals’ perceptions of the United States in other countries, even if it has no influence on how they perceive their own societies. However, American TV can also influence how people

---

62 Ibid.
63 Riddle, “Developing a Lifetime Television Exposure Scale: The Importance of Television Viewing Habits During Childhood,” in Morgan, Shanahan, and Signorielli, Living with Television Now, 286.
64 Signorielli, “Cultivation theory.”
66 Signorielli, “Cultivation theory.”
67 Ibid., 104. Gerbner et al (1982), Gross (1984), Singorielli (1989), and Shanahan and Morgan (1999) all found that heavy television viewers were “significantly more likely to self-identify as holding moderate political views.” However, while television had a general centering political effect, heavy viewers were in fact expressing more conservative views on many social issues, an influence that was strongest in geographic areas with high liberal bias. Glynn et al (1999) found that exposure to daytime talk shows increased viewers’ support of government involvement in social issues, an effect that was strongest among conservatives.
68 Van den Bulck, “International Cultivation” in Morgan, Shanahan, and Signorielli, Living with Television Now: Advances in Cultivation Theory & Research, 240; For example, Tan et al. found that “the top five characteristics of Americans, as perceived by 788 adult Chinese respondents in Taiwan, were individualistic, conceited, practical, athletic, and ambitious” (Van den Bulck 2012, 242). In another study, the same authors found that 150 Mexican college students thought of Americans as “materialistic, ambitious, artistic, practical, and industrious.” Exposure to the TV shows Dallas and Dynasty correlated with individuals’ perceptions of Americans in both studies.
in other countries view their own social realities. When people watch fiction TV, they make repeated reality judgments. When those viewers encounter what they previously only knew as televised reality for the first time, their expectations of it are influenced by the TV images they determined as probable. If all of their knowledge consists of American TV, televised images no longer represent reality as it probably is in the United States, but reality as it probably is everywhere. For example, a Belgian study has shown that Belgians who faced incarceration for the first time in their lives had clear expectations of how a prison in Belgium would look like. Their source of knowledge was the way American TV shows and films depicted life in prison.

#1: Counter-messaging is Most Likely to Create a Cultural Change in the Long-term When Incorporated into Children’s TV Shows

Based on the research that shows childhood is a crucial age for developing cultural models, this report suggests that counter-messaging likely has the largest long-term impact when children consume it. Popular television shows can be used to shape children’s values and beliefs, especially when it comes to realities they have never experienced before. While this recommendation may sound simplistic, cultivation research has shown that attitudes or behaviors that are commonly associated with social or political components can be reduced or become non-existent amongst individuals who have a higher exposure to television.

#2: Counter-messaging Campaigns Have the Potential to Shape the Radicalization Narrative

Due to its global reach, American television also influences how individuals perceive social realities that they have never encountered before. In the context of counter-messaging, American television shows can influence the radicalization narrative and negatively portray the process and outcomes of online radicalization. Portraying ISIL’s digital platform or the physical caliphate negatively through a television show has the potential to create negative expectations.

---

69 Signorielli, “Cultivation theory,” 245.
70 Ibid.
71 Ibid., 246.
72 Riddle, “Developing a Lifetime Television Exposure Scale: The Importance of Television Viewing Habits During Childhood” in Morgan, Shanahan, and Signorielli, Living with Television Now.
73 Nancy Signorielli, “Cultivation Theory.”
74 Van den Bulck, “International Cultivation.”
for individuals all over the world about ISIL and life in the caliphate. However, as mentioned before, such messages must be credible to be effective. To increase the chances of credibility, the USG should take a multi-sector approach when creating televised counter-messages.

#3: A Multi-sector Approach: A USG Entity Should Partner with Hollywood and Television Networks to Design Credible Popular Culture Counter-messaging

While the USG may wish to convey specific counter-messages to individuals vulnerable to online radicalization, it should not design those messages alone. Creating popular culture products requires expertise. The USG should discreetly communicate with television producers, screenwriters, and network officials to ensure that counter-messaging is incorporated into popular television culture. Otherwise, counter-messages will not reach as broad an audience, or worse, they will be quickly dismissed and lose relevance.
VII. FUTURE RESEARCH

This report provides key recommendations to improve the effectiveness of USG efforts to influence non-state extremist adversaries in the digital space. The research upon which these recommendations is based also suggests the value of further study on several related topics.

#1: Understanding and Shaping ISIL’s Future

As ISIL loses physical territory, there is a great deal of uncertainty regarding what the organization might do in the digital realm. It is possible that losses of territory will motivate the group to move towards an even stronger and more consolidated digital presence. Alternatively, ISIL may evolve into a fractured, decentralized network of multiple digital groups with varied or limited centralized control. Numerous possible outcomes exist, and each presents unique opportunities and risks for the United States that should be proactively studied to adequately prepare for ISIL’s future. Future research should:

- Outline likely possibilities;
- Identify the most preferred and least preferred outcomes; and
- Provide recommendations for a strategy aimed at influencing the group in a desired direction.

Such studies may be crucial to inform American strategy moving forward. For example, a campaign to sow mistrust among various ISIL leadership elements might be useful if the USG desired to decentralize or fracture the group, but could be ill advised if the desired outcome was consolidation. Outlining the plausible future paths of digital presence for groups like ISIL may thus aid not only in the presentation of clear options to policymakers, but also in the selection of policies which could best achieve US strategic interests vis-à-vis digital extremism.

---

75 For contrasting views of the future of ISIL, see: Ingram and Whiteside, “In Search of the Virtual Caliphate: Convenient Fallacy, Dangerous Distraction”; Votel et al., “#Virtual Caliphate: Defeating ISIL on the Physical Battlefield Is Not Enough.”
#2: Considering the Broader Applications of Countering Digital Extremist Influencing

Although this report has focused heavily on aspects of counter-messaging that might be used against digital extremism by armed non-state groups, the United States faces significant threats from a wide variety of state and non-state actors seeking to use the digital space for influence operations. Analysis of Chinese, Russian, and Iranian strategy indicates that these states place high importance on digital influence operations, the tactics and strategies of which may share core elements with the messaging strategies of extremist groups like ISIL. Further research is needed to assess the nature of these threats and develop appropriate responses. Future research may thus significantly contribute to policy discussions by:

- Determining which lessons from the United States’ current counter-ISIL campaign can be used; and
- Identifying what gaps still exist in our understanding of how to address these emerging threats.

---

BIBLIOGRAPHY


Judge Advocate General Subject Matter Expert. Interview by Georgetown University National


Kruglanski, Arie W. “Psychology Not Theology: Overcoming ISIS’ Secret Appeal.” *E-
not-theology-overcoming-isis-secret-appeal/.

Lee, Timothy B. “The NSA Is Trying to Have It Both Ways on Its Domestic Spying
https://www.washingtonpost.com/news/the-switch/wp/2013/12/22/the-nsa-is-trying-to-
have-it-both-ways-on-its-domestic-spying-programs/.

Magazine, July 19, 2017. https://www.pcmag.com/roundup/342728/the-

Mazzetti, Mark, and Michael R. Gordon. “ISIS Is Winning the Social Media War, U.S.
https://www.nytimes.com/2015/06/13/world/middleeast/isis-is-winning-message-war-
us-concludes.html.

Miller, Greg, and Scott Higham. “In a Propaganda War against ISIS, the U.S. Tried to Play by
https://www.washingtonpost.com/world/national-security/in-a-propaganda-war-us-
tried-to-play-by-the-enemy-s-rules/2015/05/08/6eb6b732-e52f-11e4-81ea-
0649268729e_story.html.

Miller, Greg, and Souad Mekhennet. “Inside the Surreal World of the Islamic State’s
https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-
propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92dd2b_story.html.

Molzahn, Wendy. “The CIA’s In-Q-Tel Model: It’s Applicability.” *Acquisition Review Quarterly*


Nakashima, Ellen. “U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated
https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-
to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html.

Nordland, Rod. “On TV, an Afghan Unit Tackles the Taliban.” New York Times, November 20,

O’Flynn, Janine, Deborah Blackman, and John Halligan, eds. *Crossing Boundaries in Public

O’Flynn, Janine, Deborah Blackman, and John Halligan, eds. *Crossing Boundaries in Public

Protecting America’s Youth: An Update from the National Center for Missing and Exploited Children,
Before the Comm. on Education and the Workforce, 113th Cong. 7–8 (2002) (statement of


