



01

# COUNTERING EXTREMISM ONLINE

## Lessons Learned for U.S. Strategic Counter-ISIS Radicalization Programs.

BY CAPTAIN DEVIN QUINN

### INTRODUCTION

The Islamic State of Iraq and Syria burst onto the scene in 2014 with its blitzkrieg campaign across northern Syria and Iraq. Analysts were shocked by ISIS's ability to seize and hold large swaths of territory. However, lightning campaigns across the open desert and holding seized territory requires a large number of soldiers. To acquire these soldiers ISIS turned to a developing technology on the internet; social media. Terrorist groups have always used the internet for recruitment and communications but ISIS industrialized its use. At its height ISIS had over 75,000 active supporters on Twitter.<sup>01</sup> These supporters were able to radicalize and inspire over 30,000 foreign recruits to join ISIS and travel to its newly established Caliphate.<sup>02</sup> When the ISIS Caliphate began to collapse, it used its online radicalization network to inspire attacks in the West, like the 2015 shooting in San Bernardino that left 14 dead.<sup>03</sup>

To counter this online radicalization the Obama Administration turned to the Department of State. In 2016 President Obama issued Executive Order 13721 which established the Global Engagement Center. The GEC is a DoS entity whose primary mission is to:

*“lead the coordination, integration, and synchronization of Government-wide communications activities directed at foreign audiences abroad in order to*

*counter the messaging and diminish the influence of international terrorist organizations, including the Islamic State of Iraq and the Levant (ISIL).”<sup>04</sup>*

To achieve this mission the GEC was given a budget of \$80 million, \$60 million of which was transferred from the Department of Defense. The GEC was established to replace the Obama Administration's previous attempt at strategic counter-radicalization, the Center for Strategic Counterterrorism Communications, which had been widely criticized as being ineffective.

In this paper I analyze the U.S. Government's counter-radicalization programs against ISIS. In the first part of this paper I review the relevant literature on the subject and identify seven key themes that are critical to the proper execution of a strategic counter-radicalization program against ISIS. In the second part of this paper I use these key themes to conduct a comparative analysis of the counter-radicalization programs employed by the CSCC and the GEC. I conclude this paper with policy recommendations on how the U.S. Government can improve its counter-radicalization programs.

### LITERATURE REVIEW

For this literature review I critically examined 13 relevant sources pertaining to the U.S. government's strategic efforts towards counter-radicalization. From this analysis I was able to identify seven key themes pertaining to the U.S. Government's counter ISIS radicalization programs. The following lists and explains each of these key themes.

#### ■ 1) The U.S. Government is not an appropriate messenger for counter ISIS radicalization.

This theme was common across nine of the 13 sources I examined for this literature review. The Office of the

01 A U.S. Department of State video depicts a young Muslim being targeted by terrorists and questioning their morality. The video is part of an online campaign to target audiences most vulnerable to recruitment by the Islamic State.

SCREEN CAPTURE  
U.S. DEPARTMENT  
OF STATE VIDEO

Director of National Intelligence noted in a 2016 report that the U.S. Government lacks credibility in the Muslim world due to several unfavorable foreign policy blunders, the greatest one being the Iraq War. McFadden adds that unfavorable statements from U.S. officials, like President Bush referring to the War on Terror as a crusade, can further diminish the credibility of the U.S. Government.<sup>05</sup> Most ISIS supporters have a low, if not hostile, opinion towards the U.S. Government and U.S. attributed counter-radicalization messages will most likely not resonate with them. Most of the sources I examined expressed the need for a source more credible than the U.S. Government to disseminate counter-radicalization messages. One source I examined did refute this theme. Alberto Fernandez, the former head of the CSCC, called the idea of a credible counter-ISIS messenger “a myth” and explained that even Al-Qaeda had renounced ISIS.<sup>06</sup> Fernandez insisted there was still a need for the U.S. Government to create and openly disseminate counter-radicalization products.<sup>07</sup>

### 2) The volume and timeliness of ISIS messages on social media far exceeded the efforts of the U.S. Government.

Nine of the 13 sources examined found that this was a major issue hampering U.S. Government counter-radicalization efforts. Stengel noted that at its height ISIS supporters were able to produce 90,000 pieces of online content per day while the entire U.S. Government counter-ISIS effort was only able to produce 350.<sup>08</sup> The volume of online content can be attributed to the fact that ISIS supporters tend to be more active on social media and manage multiple accounts. Two American ISIS supporters managed 57 and 97 Twitter accounts respectively.<sup>09</sup> On social media, volume matters because it creates and echo chamber, increases credibility, and drowns out any dissent.<sup>10</sup> The sources evaluated cited lack of funding and personnel, and the bureaucratic process for developing and disseminating messages as reasons the U.S. Government could not keep up with the volume of ISIS messages. At the height of ISIS messaging in 2015 the CSCC only had a staff of 12 and a budget of \$6 million which severely limited its capabilities.<sup>11</sup>

### 3) Disrupting ISIS messaging is more effective than trying to match ISIS volume.

Several sources, including Greenberg, Kean & Hamilton, and Fernandez, argued that disruption of ISIS content is a sufficient way to cut down on its volume. Kean & Hamilton noted that from 2015-2016 Twitter removed 125,000 ISIS accounts for promoting terrorism in violation of Twitter’s user agreement.<sup>12</sup> This approach requires a strong relationship between the U.S. Government and the tech industry as social media companies bear the responsibility of barring accounts from their platforms. Some analysts believe that removing terrorists from

mainstream social media will drive them to the dark web where they can’t easily be monitored however, Greenberg argues this is beneficial because there is a smaller audience on the dark web to radicalize.<sup>13</sup>

### 4) Analysis and performance measurement of counter-radicalization campaigns is important for developing the right counternarrative.

Five of the sources analyzed, including Greenberg, ODNI, Bing, McFadden, and Katz, argued there is a need for data-driven analysis and performance measurement of both radicalization and counter-radicalization campaigns online. Katz noted that in order to counter a problem you must first study and understand the problem.<sup>14</sup> Early efforts by the CSCC lacked analysis and led to a counter-radicalization strategy that was ambiguous and misleading.<sup>15</sup> Greenberg argues for the use of data-analytics to measure the performance of counter-radicalization campaigns so that they can be adjusted if they are not working.<sup>16</sup> The ODNI noted that data-driven target audience analysis can help to target messaging more efficiently.<sup>17</sup>

### 5) Targeted messaging is more effective than broad messaging.

Five sources; Greenberg, Williams, ODNI, Kean & Hamilton, and Fernandez, all observed that targeted messaging is far more effective at counter-radicalization than broad messaging. Kean & Hamilton note that the reasons for radicalization vary with each individual, making broad counter-radicalization ineffective.<sup>18</sup> Fernandez notes that the most effective counter-radicalization messaging is personalized.<sup>19</sup> An example of personalized counter-radicalization occurred at West Point where students posed as ISIS members online to lure potential recruits away from the organization.<sup>20</sup> By analyzing different demographics, messages can be developed to target the specific vulnerabilities and grievances that lead to radicalization.

### 6) The content of the counter-radicalization message matters.

Crafting counter-radicalization messages with the right content is critical to their effectiveness. Greenberg and Williams noted that the most effective counter-radicalization narratives included testimony from ISIS defectors who were disillusioned by their experiences. Another effective technique observed by Williams and Fernandez was to highlight discrepancies in ISIS’s own radicalization narratives. Additionally, Greenberg and Fernandez both proposed that any effective counter-narrative needs to be fact based. Finally, Greenberg and McFadden noted it is important to incorporate alternative narratives rather than only offering negative messages that tell potential recruits not to join ISIS, but offer no alternatives.

**AT ITS HEIGHT ISIS SUPPORTERS WERE ABLE TO PRODUCE 90,000 PIECES OF ONLINE CONTENT PER DAY WHILE THE ENTIRE U.S. GOVERNMENT COUNTER-ISIS EFFORT WAS ONLY ABLE TO PRODUCE 350.**



01

### 7) Partnering with industry and allies will boost counter-radicalization messaging

Eight of the 13 sources analyzed called for the U.S. Government to integrate and coordinate with both industry and allies. Parker & Roger note that any form of counter-radicalization communication requires support from non-security stakeholders including companies and private citizens.<sup>21</sup> Bing observes that partnering with technologies companies can help the U.S. Government develop better tools for countering radicalization online.<sup>22</sup> In 2015 the DoS and Department of Homeland Security partnered with Facebook to launch the Peer to Peer: Challenging Extremism program which crowd sourced novel counter-radicalization techniques from colleges and universities around the world.<sup>23</sup> The U.S. Government Accountability Office praised government efforts to collaborate with middle eastern allies and train partner militaries in counter-radicalization techniques.<sup>24</sup> As someone who has trained partner militaries in these techniques I can attest that it is a much more viable and enduring option than U.S. Government direct counter-radicalization messaging.

## COMPARATIVE ANALYSIS

In 2011 President Obama issued Executive Order 13584 which established the Center for Strategic Counterterrorism Communications. In 2013 the CSCC's Digital Outreach Team launched its U.S. Government attributed Twitter account as a platform to disseminate counter ISIS radicalization material and directly engage with ISIS sympathizers and supporters.<sup>25</sup> The CSCC used this platform to launch its "Think Again, Turn Away," counter-radicalization campaign which was aimed at

discouraging potential recruits from joining ISIS.<sup>26</sup> The campaign sent tweets like "ISIS recruits order book Islam for dummies," and "Drugs in ISIS HQ," in an attempt to show discrepancies in ISIS's narrative.<sup>27</sup> The campaign was broad, U.S. attributed, and failed to demonstrate any analysis or understanding of the target audience or its own messaging. The CSCC also attempted to use its Twitter account to conduct more targeted messaging by engaging in snarky banter with ISIS supporters. This technique was widely criticized because it gave obscure ISIS supporters more clout by allowing them to engage in verbal combat with the U.S. Government.<sup>28</sup> Additionally, the CSCC account could not match ISIS's volume on Twitter as it only sent an average of six to seven tweets per day to its 7,300 followers while some pro-ISIS accounts sent as many as 125 tweets per day.<sup>29</sup>

The biggest CSCC gaff came in 2014 when it released the video "Welcome to ISIS land."<sup>30</sup> This product was a mock recruiting video that encouraged its watchers to "Run, don't walk to ISIS land."<sup>31</sup> Although the video was widely circulated, receiving over 900,000 views, it was also heavily criticized by Western journalists for its sarcastic nature.<sup>32</sup> The video showed the CSCC had no comprehension of how Westerners were recruited into ISIS.<sup>33</sup> The CSCC attempts at counter-radicalization violated nearly every key theme identified in the literature review. The CSCC used a U.S. Government attributed platform, could not keep up with ISIS's volume, inadvertently promoted rather than disrupted ISIS messaging, was too broad, lacked analysis, and had poor content. As a result, the CSCC was widely seen as a failure.

The failure of the CSCC prompted President Obama to issue Executive Order 13721 in 2016 which established the Global Engagement Center. President Obama sought to correct the failures of the CSCC by ensuring the GEC


01  
A U.S. Department of State video depicts a young Muslim being targeted by terrorists and questioning their morality. The video is part of an online campaign to target audiences most vulnerable to recruitment by the Islamic State.  
SCREEN CAPTURE  
U.S. DEPARTMENT  
OF STATE VIDEO

would coordinate interagency support, build partner capacity, and develop analytical models to assess its performance.<sup>34</sup> With a budget and staff ten times the size of the CSCC the GEC hired tech companies to develop tools to ensure it engaged in counter-radicalization programs that were driven by analysis.<sup>35</sup> A good example of this new analytical based approach is a recent counter-radicalization program the GEC ran in North Africa. Using the “Redirect Method” developed by Google’s Jigsaw the GEC purchased Facebook ads that targeted young men in Tunisia and Morocco who frequently searched for terrorist propaganda online.<sup>36</sup> The Facebook ads included a video of an ISIS recruit who quickly becomes disillusioned with his experiences on the frontlines.<sup>37</sup> This new method allows the GEC to only target those most vulnerable to recruitment and adjust the narrative based on feedback from different demographics.<sup>38</sup>

The GEC’s new approach seems to have remedied the deficiencies of the CSCC and meets the key themes identified in the literature review. The new Facebook ads bear no U.S. logo and although the GEC continued to operate an attributed Twitter account until October 2019 the new head of the GEC, Lea Gabrielle, has shifted the priorities of the GEC away from attributed messaging.<sup>39</sup> The GEC no longer tries to compete with ISIS’s volume and instead focuses on targeted messages. The GEC has heavily invested in analytic technology and trains other U.S. agencies and allies how to use it. The GEC uses this analysis to create content that is pertinent and persuasive. The GEC has received some criticism for losing talent and being too bureaucratic but it is a vast improvement over the CSCC.<sup>40</sup>

## CONCLUSION

Since the creation of the GEC in 2017, new threats have emerged. The National Defense Authorization Act of 2019 broadened the GEC’s mission to include identifying and countering state and non-state actor influence operations and today nearly 75 percent of the GEC’s budget is spent countering Russian misinformation.<sup>41</sup> Psychological Operations professional should understand, appreciate, and leverage other organizations throughout the U.S. Government who are conducting influence operations. To that end, U.S. Army Psychological Operations needs a seat at the GEC table as it is the closest thing the U.S. Government has to a strategic influence entity. Ideally, PSYOP should establish a permanent working group within the GEC that is staffed with representatives from each PSYOP battalion. This will ensure that PSYOP is integrated into the interagency coordination on influence that the GEC facilitates. Additionally, the rise of Great Power Competition has revealed that our greatest competitors operate across all Geographic Combatant Commands. A working group comprised of PSYOP professionals from each GCC can ensure that opportunities to counter Chinese and Russian influence are coordinated globally. Positioning this working group within the GEC ensures that PSYOP professionals have immediate access to interagency partners which can amplify PSYOP effects. Finally, all PSYOP professionals can benefit from the key themes for online counter-radicalization

identified in this paper. As new programs and authorities emerge that shift PSYOP professionals focus online these themes can be applied broadly to any online PSYOP activity. Applying the lessons learned here to future operations can help to ensure mission success. 

## ABOUT THE AUTHOR

**CPT Devin Quinn** is a Psychological Operations Officer serving in 6th Psychological Operations Battalion 4th Psychological Operation Group. CPT Quinn previously served in 8th Psychological Operations Battalion and in July 2018 deployed to Syria as a Tactical Psychological Operations Detachment Commander. While deployed CPT Quinn witnessed and contributed to the fall of ISIS’s physical caliphate. CPT Quinn is a graduate of Dickinson College and a current graduate student at Penn State University.

- NOTES** **01.** Elizabeth Bodine-Baron et al. “Examining ISIS Support and Opposition Networks on Twitter,” Rand Corporation. (2016). Retrieved from [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1300/RR1328/RAND\\_RR1328.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1328/RAND_RR1328.pdf). **02.** K. Greenberg, Counter-Radicalization via the Internet. *The Annals of the American Academy*. (2016). DOI: 10.1177/0002716216672635. **03.** Chris Bing, “Inside the tech being used to combat ISIL online,” *Fedscoop*. (2016). Retrieved from <https://www.fedscoop.com/isis-state-department-twitter-global-engagement-center-data-analytics-2016/>. **04.** Barack Obama, Executive Order 13721: Developing an Integrated Global Engagement Center to Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584. Office of the President of the United States. (2016). Retrieved from <https://www.hsd.org/?view&did=791347>. **05.** Crystal McFadden, “Strategic Communications: The State Department Versus The Islamic State,” Thesis. Naval Post Graduate School. (2017) Retrieved from <https://www.hsd.org/?view&did=813341>. **06.** Alberto Fernandez, “Here to stay and growing: Combating ISIS propaganda networks,” Center for Middle East Policy at Brookings Institute. Washington, DC. (2015). Retrieved from [https://www.brookings.edu/wp-content/uploads/2016/06/IS-Propaganda\\_Web\\_English.pdf](https://www.brookings.edu/wp-content/uploads/2016/06/IS-Propaganda_Web_English.pdf). **07.** Ibid. **08.** Richard Stengel, *Information Wars*. Atlantic Monthly Press. (2019). New York, NY. **09.** Thomas Kean and Lee H. Hamilton, “Digital Counterterrorism: Fighting Jihadists Online,” Task Force on Terrorism and Ideology. Bipartisan Policy Center. (2017). Retrieved from <https://bipartisanpolicy.org/wp-content/uploads/2019/03/BPC-National-Security-Digital-Counterterrorism.pdf>. **10.** Fernandez, “Here to stay and growing.” **11.** Haroro Ingram, “Persuade or Perish: Addressing Gaps in the U.S. Posture to Confront Propaganda and Disinformation Threats,” Program on Extremism. George Washington University. (2020) Retrieved from <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Ingram%20Persuade%20or%20Perish.pdf>. **12.** Kean and Hamilton, “Digital Counterterrorism.” **13.** Greenberg, “Counter-radicalization via the Internet.” **14.** Rita Katz, “The State Department’s Twitter War With ISIS Is Embarrassing,” *Time*. September 16, 2014 Retrieved from <https://time.com/3387065/isis-twitter-war-state-department/>. **15.** McFadden, “Strategic Communications.” **16.** Greenberg, “Counter-radicalization via the Internet.” **17.** Office of the Director of National Intelligence (ODNI), “Applying Private Sector Media Strategies to Fight Terrorism,” (2016) Retrieved from <https://www.odni.gov/files/PE/Documents/Media-Strategies.pdf>. **18.** Kean and Hamilton, “Digital Counterterrorism.” **19.** Fernandez, “Here to stay and growing.” **20.** Greenberg, “Counter-radicalization via the Internet.” **21.** Pearce D. Parker and M. B. Roger, *Challenges for Effective Counterterrorism Communication: Practitioner Insights and Policy Implications for Preventing Radicalization, Disrupting Attack Planning, and Mitigating Terrorist Attacks*. Studies in Conflict & Terrorism. (2017). 42:3. 264-291, DOI: 10.1080/1057610X.2017.1373427. **22.** Bing, “Inside the tech being used to counter ISIL online.” **23.** Greenberg, “Counter-radicalization via the Internet.” **24.** United States Government Accountability Office (GAO). 2017. “Countering Isis And Its Effects: Key Issues for Oversight,” Washington, DC. Retrieved from <https://www.gao.gov/assets/690/685908.pdf>. **25.** McFadden, “Strategic Communications.” **26.** Ibid. **27.** Andrew Kaczynski, “Here’s How The State Department Trolls Terrorists On Social Media,” *Buzzfeed*. (2014). Retrieved from <https://www.buzzfeednews.com/article/andrewkaczynski/heres-how-the-state-department-trolls-terrorists-on-social-m>. **28.** Ibid. **29.** Katz, “The State Department’s Twitter War With ISIS Is Embarrassing.” **30.** Ibid. **31.** Stengel, *Information Wars*. **32.** Fernandez, “Here to stay and growing.” **33.** Katz, “The State Department’s Twitter War With ISIS Is Embarrassing.” **34.** Obama, Executive Order 13721. **35.** McFadden, “Strategic Communications.” **36.** Joby Warrick, “How a U.S. team uses Facebook, guerrilla marketing to peel off potential ISIS recruits,” *Washington Post*. (2017). Retrieved from [https://www.washingtonpost.com/world/national-security/bait-and-flip-us-team-uses-facebook-guerrilla-marketing-to-peel-off-potential-isis-recruits/2017/02/03/431e19ba-e4e4-11e6-a547-5fb9411d332c\\_story.html](https://www.washingtonpost.com/world/national-security/bait-and-flip-us-team-uses-facebook-guerrilla-marketing-to-peel-off-potential-isis-recruits/2017/02/03/431e19ba-e4e4-11e6-a547-5fb9411d332c_story.html). **37.** Ibid. **38.** Ibid. **39.** Ingram, “Persuade or Perish.” **40.** Patrick Tucker, “Analysts Are Quitting the State Department’s Anti-Propaganda Team,” *Defense One*. (2017). Retrieved from <https://www.defenseone.com/technology/2017/09/analysts-are-quitting-state-departments-anti-propaganda-team/140936/>. **41.** Stengel, *Information Wars*