

RELEASE IN FULL

September 11, 2016

SENSITIVE BUT UNCLASSIFIED

INFORMATION MEMORANDUM

TO: The Ambassador

THRU: A/DCM – Sue Niblock

FROM: PAO – Ragini Gupta

**SUBJECT: Counter-ISIL Messaging Effort and USG Interaction With Social Media Companies to Address Extremist Content**

Per your request, Public Affairs reached out to the Department for language on counter-messaging and an update on USG interactions with social media companies in regards to addressing extremist content online. This information memo contains Department-cleared language on both topics, provided by R staff, NEA, the CT Bureau and other stakeholders.

**1. Countering ISIL/Extremist Messaging (“Line of Effort 6”):**

Following are the points prepared for Under Secretary Stengel’s use when talking about counter-messaging efforts. They were passed to us by R staff.

Top Lines

- This is a long campaign and we are seeing progress.
- No question we all need to do more on foreign fighters and in countering ISIL messaging.
- We are working towards this and took a big step with the opening of the Sawab Center.

Coalition’s Progress

- Any time you talk about Coalition efforts to counter ISIL, you have to remember where we started. A year ago ISIL was barreling towards Baghdad and the country was in real danger of falling apart.

- The Coalition has come a long way in a very short period of time. The military effort in support of the Government of Iraq has proven decisive in a number of encounters with Daesh, such as Kobane, Tikrit, and Tel Abiyad, and will doubtless play a critical role in the liberation of Mosul. There has been notable progress in Coalition efforts to restrict the flow of foreign fighters and choking off sources of revenue for Daesh, as well.
- Elsewhere in Iraq, civilians are returning to Tikrit. In places like al-Baghdadi and Haditha, we have been able to organize the tribes and Iraqi forces, to take back territory and hold ground in the area.

#### Coalition Efforts in Communications Sphere

- In the communications sphere -- which the U.S. co-leads, along with Emirati and British partners -- we are assisting our Coalition partners to expose ISIL for what it really is. These efforts will counter Daesh's appeal to vulnerable and gullible youth. Of course we are constantly evaluating progress and plans with our partners.
- We have begun an aggressive campaign, led primarily by our partners in the Middle East region. We've seen fatwas issued from top religious leaders in Egypt and Saudi Arabia, declaring ISIL a direct threat to Islam. And we are working with coalition partners to establish communication centers to combat ISIL's social media presence and messaging campaign in real time.
- We have a large number of initiatives (spokesman and social media training, professional exchanges, information sharing, and more).
- **A new type of information battle:** The effort against ISIL is not a traditional information battle or campaign. In a traditional campaign, if your opponent has approval ratings in the single digits, such as ISIL has in much of the Muslim world, you would think that you are well-positioned. But ISIL is trying to appeal to the grievances of a small minority.
- **ISIL is overwhelmingly rejected:** The majority of 1.6 billion Muslims have rejected ISIL's tactics, but ISIL is able to draw from the

small percentage of people who may be susceptible to recruitment. And while this is a small percentage - perhaps less than one percent - in real numbers, it means it has been able to recruit tens of thousands of foreign fighters; this is unacceptable.

- **Addressing content imbalance:** While number indicate that ISIL produces tens of thousands of tweets daily, one study shows that it has 500-2,000 dedicated tweeters and that many tweets are sent out by bots into oblivion.
- Counter content is not as sensational as terrorist content and doesn't attract the same headlines. Most people dismiss it instead of replying.
- We are pleased that a number of governments, including Jordan, have approached us to see how they have might use our CSCC as a model for their efforts.
- From the U.S. Side we are:
  - Expanding our messaging efforts, including original content on social media platforms, in Arabic, Somali, Urdu, Hausa, and English, to amplify stories of ISIL defectors and former fighters, poor living conditions under ISIL, and ISIL atrocities, particularly against Muslims, who make up a vast majority of ISIL's victims.
  - Expanding partnerships with government and NGO partners to directly counter ISIL's messaging. They are the best messengers for counter-ISIL efforts.
  - Coordinating U.S. government and Coalition messaging by issuing daily and thematic guidance on counter-ISIL topics to nearly 3,000 U.S. government officials and Coalition partners.
- **Social Media platforms closing down ISIL accounts:** We are in touch with these companies on a regular basis and have a constant, constructive dialogue on the question of freedom of expression versus security and incitement. There are certain protocols and terms of agreement that codify the rules for removing site and content on the

internet and we are generally satisfied with how these companies comply with these procedures and with their willingness to discuss the matter with concerned parties.

#### ISIL's Endgame/U.S. Reaction

- It's going to take time, but with the coalition we are working on the different elements of a strategy that will push back ISIL and help Iraq recover from the devastation ISIL is leaving behind. As the President said, "ISIL will lose" because they don't have anything to offer except for "misery and death and destruction."
- **Coalition broadening campaign against ISIL beyond Iraq and Syria:** We have seen increasing claims of ISIL-affiliated terrorist groups in the region, though we are still assessing the extent of operational and tactical linkages. There's no denying that ISIL seeks to extend its control in the Middle East and beyond, and that's something we are concerned about. They are attempting to do this even as ISIL-held territory in Iraq is shrinking and they are suffering battlefield losses.

#### **Coalition Counter-Messaging Working Group Activities**

(SBU) U/S Stengel launched the first meeting of the Coalition Communications Working Group in Kuwait in October 2014. In January, after the London Small Group meeting, a counter-messaging working group was formed. The United Kingdom is serving as the "Secretariat." The Working Group should enable the coalition to swiftly develop responses and proactive communication campaigns to contest Daesh's narrative. We are not there yet. In response to this, we are intensifying our engagement with key Coalition partners – particularly the front line states of Iraq, Jordan, Lebanon, Kuwait and Egypt – to increase the group's productivity. Jordan has been invited to participate in these meetings; their participation is sporadic, at best.

Thus far, the working group has agreed to the following actions:

- **Alignment of messaging / Counter-messaging** – coordination among spokespersons via regular teleconferences; development and sharing of communication products through a cloud-based database; sharing best

practices in government communications; and sharing target audience analysis. Examples include the current government ministry spokesperson's teleconference and the Sawab Center.

- **Social media engagement** – coordination of government activities in the digital space; amplification of content developed by our partners; engagement with social media technology companies. Examples include anti-Daesh social media workshops conducted by private sector technology companies and technology skills building workshops.
- **Amplification of credible voices/ partnerships** – media campaigns and outreach programs to support other Coalition lines of effort. These could focus on strengthening the effective use of tools and opportunities by legitimate religious and community leaders. Examples of this include recent people to people exchanges and faith-based engagement conferences/summits facilitated by Coalition governments.

## **2. USG Policy and Efforts With Social Media Companies:**

The following material is provided by NEA and the CT Bureau. The first section is the USG policy on countering use of the internet by extremists and terrorist groups; following that are the key messages on the topic, as cleared by the Department.

(SBU) The use of the Internet, including social media, for terrorist purposes is a significant and growing counterterrorism and foreign policy concern for the U.S. government. At issue is, first, when and how the U.S. government should take action to counter the use of the Internet for terrorist purposes in accordance with U.S. laws and international obligations and, second, how we describe U.S. policy in international settings. This complex and cross-cutting issue must be addressed through a consistent and consistently articulated approach, based on guiding principles and best practices. U.S. policy to counter the use of the Internet for terrorist purposes should also be aligned to and integrated with U.S. cyber policy and Internet governance policy discussions, as appropriate. While the U.S. position and guiding principles on this issue are understood by many in the U.S. government and have been stated publicly in remarks, in bilateral engagements and in multilateral fora, there is no formal document outlining this policy.

**(U) Background and Guiding Principles**

(SBU) The increasing urgency of countering the use of the Internet for terrorist purposes (also referred to as “terrorist use of the Internet” or “cyberterrorism”) is reflected in the growing interest in this topic domestically and internationally, including in multilateral fora. This debate also is being used for other purposes, such as to promote control of content in cyberspace. Some governments have different definitions of, and approaches to, terrorism and therefore have different approaches to the use of the Internet for terrorist purposes. These differing definitions and approaches often result in fundamental disagreements over the appropriateness of strategies or approaches for addressing certain types of content in cyberspace between the U.S. government – which broadly protects freedom of expression and the free flow of information – and other governments – which vary in how broadly they protect speech and how much they live up to their international obligations and commitments in this respect.

U.S. policy to counter the use of the Internet for terrorist purposes complements other U.S. government procedures, guidelines and authorities. Although the use of the Internet for terrorist purposes can intersect with other cybercrime and transnational threats and many of the tools to combat these threats are the same, there are additional political and policy issues to consider in addressing the use of the Internet by alleged terrorists, such as whether the actors are actually terrorists (versus political dissidents).

**U.S. Policy to Counter the Use of the Internet for Terrorist Purposes**

The U.S. government is concerned with a number of different possible terrorist uses of the Internet. These include, for example, using the Internet and social media to disseminate propaganda, promote radicalization to violence, and facilitate recruitment, training, planning and coordination of attacks. Another example is use of the Internet to facilitate terrorist finance, particularly through Internet or mobile telephone payment systems. The U.S. government also is concerned with terrorists using the Internet to launch cyber attacks, although there have been no cyber attacks clearly attributable to terrorists to date.

The U.S. approach to the use of the Internet for terrorist purposes focuses primarily on evaluating after the fact whether terrorists’ online

communications violate the law rather than on a prescriptive approach that blocks or filters communications. Therefore, the U.S. government is concerned with two key categories of the use of the Internet for terrorist purposes, each of which require different approaches: 1) *countering terrorists' illegal activities in cyberspace*; and 2) *countering violent extremists' non-illegal activities on the Internet, including social media*.

#### Countering Terrorists' Illegal Activities in Cyberspace

- (SBU) Cybercrimes, like intrusion into or otherwise damaging computer systems or data, as well as use of the Internet to facilitate terrorism, such as attack planning and coordination and fundraising, can be pursued through traditional law enforcement channels. Investigation of alleged crimes on the Internet shall comport with human rights obligations, only occur for proper purposes, only perform authorized actions, and never occur based solely on activities protected by the First Amendment.
- (SBU) Countering some illegal online communication by terrorists can be challenging. The line between illicit speech that provides material support to designated terrorists or incites imminent violence and expression that is protected by the First Amendment is not always clear. Remedies must also be appropriately tailored, as shutting down websites or social media accounts that are owned, operated, or used for illicit speech may also have the effect of limiting some protected expression and be inconsistent with U.S. and international human rights law.

#### Countering Violent Extremists' Non-Illegal Activities on the Internet, including Social Media

- (U) For violent extremists' online activity that does not meet the threshold of incitement to imminent violence, the primary U.S. approach is counter-messaging or competitive messaging, as the U.S. government believes that alternative viewpoints are a more effective response to objectionable speech than attempted suppression of that speech.
- (SBU) Finally, it is worth noting that, on their own initiative, service providers may remove terrorist websites or social media accounts with content that violates their user service agreements, or they may do so at the request of users, advocacy groups, or governments that flag

objectionable content. In certain circumstances, the U.S. government may wish to alert providers of content that may violate such user agreements for the providers' own consideration. These circumstances should be narrowly defined and the process for coordinating such outreach should be clearly established and regularly reviewed.

**Key Messages:**

**The use of the Internet, including social media, and the use of information technology in furtherance of terrorism and other crimes must be addressed by all lawful means, while respecting international obligations and commitments regarding human rights, including freedom of expression, the free flow of information, and a free and open Internet.** Even in the case of the most vitriolic websites and social media accounts in the United States, much of their content is protected by our Constitution. Whether online content is of the sort that could be restricted or for which individuals could be penalized (e.g., it reaches the level of incitement to imminent violence or material support for terrorism) is heavily fact dependent and decided on a case-by-case basis consistent with U.S. law.

**Therefore, our efforts to counter terrorism in cyberspace focus on criminal activities that facilitate terrorism,** such as illicit financing through money transfers, attack planning and coordination and other crimes committed online, rather than on constraints on expressive content, no matter how repugnant or inimical to our core values.

**Terrorist organizations use the Internet to raise money, recruit, and radicalize individuals to violence, and the United States remains committed to taking appropriate steps to ensure that U.S.- and United Nations-designated terrorist groups cannot support their operations by raising money in the United States.** The United States takes its international obligations very seriously and will, as appropriate, take action against sanctioned entities to freeze assets.

**Although the Internet provides a medium both to spread messages that attempt to justify violence and to sustain the morale of those already committed to violence, the Internet is but one tool of many that terrorists use to recruit.** Most recruitment and radicalization to violence continues to occur through person-to-person interaction. Therefore, our efforts to counter radicalization to violence must continue to focus on

engagement with those who may be targeted by violent extremists and the social, physical networks that influence them.

**In general, alternative viewpoints are a more effective response to objectionable speech than suppression of that speech.** We can most effectively counter violent extremists' propaganda on the Internet by contesting terrorist narratives and worldviews through competitive or alternative messages, including directly contesting terrorists' messages, particularly where terrorist recruiters are trying to win new adherents. In the United States, the interagency Center for Strategic Counterterrorism Communications (CSCC) housed in the Department of State engages terrorists directly online with counterarguments and audiovisual materials to challenge and disrupt the terrorist narrative. CSCC also promotes alternative viewpoints using the same tools, seeking to reach those individuals who may be looking for a substitute for terrorist narratives. CSCC's online activities are open and attributed to the Department of State.

**We must work with international partners to build partnerships that include the private sector, civil society, and all levels of government to counter the threats from the use of the Internet for terrorist purposes.** States should work cooperatively to ensure that they protect their networks, share best practices, and communicate regarding threats, investigations and prosecutions. In addition, private companies may choose to remove terrorist websites or social media accounts with content that violates their user service agreements.

|          |     |                  |    |
|----------|-----|------------------|----|
| Drafted: | AIO | JGiordono-Scholz |    |
| Cleared: | PAO | RGupta           | ok |
|          | IO  | EBarbee          | ok |