Countering and Exposing Terrorist Propaganda and Disinformation

Daniel Kimmage
Principal Deputy Coordinator, State Department Global Engagement Center

Transcript
The Washington Institute for Near East Policy Counterterrorism Lecture Series

February 17, 2021

Thank you Matt, and thank you to all of the viewers and listeners out there in the virtual world. So the Global Engagement Center, in its current form, was created by the 2017 National Defense Authorization Act. It was created to coordinate the efforts of the U.S. government to counter foreign state and nonstate propaganda and disinformation that aims to undermine the interests of the United States, our allies, and partners. This builds on two earlier efforts, both of which focused on counterterrorism, and both of which were created by executive orders. Matt mentioned one when he went through my bio: the Center for Strategic Counterterrorism Communications. The second was an earlier version of the Global Engagement Center, created by a 2016 executive order and focused on countering ISIS.

But in 2017, Congress recognized an urgent national security imperative and expanded the Global Engagement Center's mission. Today, the GEC at the State Department not only focuses on terrorist propaganda, but also on disinformation and propaganda spread by adversarial state actors to undermine U.S. security, policy, and those of our partners and allies. So let me talk broadly at the outset about four major GEC milestones in the recent past.

The first is our analytic work. As we have built up the GEC, one of our key goals has been to make sure that it is driven by data and analysis. To do that, we have created a team of more than thirty data scientists who analyze open-source developments in the information space. That team is producing analysis that informs actions by our State Department colleagues and our interagency partners. Also, they lead collaboration with a range of other U.S. government and international partners.

Secondly, we know that we cannot do this alone. However much the Global Engagement Center expands, it needs to be at the hub of a much larger effort. As we have built up our own capabilities, we have also established and strengthened government-to-government partnerships that enable us to coordinate our analysis and, more importantly, our actions, over the long term.

Third, we are taking proactive action globally. We are executing campaigns, programs, and initiatives to reduce the space available to bad actors for nefarious influence activities.

Finally, because we understand that technology is woven into virtually every aspect of this problem, we are trying to stay ahead of that curve as well. We have launched a comprehensive framework to drive U.S. and international coordination on technology and, specifically, on counter-disinformation technologies and their implementation. This framework was recently highlighted, favorably, by the National Security Commission on Artificial Intelligence, and I will talk about its components a little bit later. So the bottom line is that we have established a level of coordination that did not previously exist in the U.S. government.

Let me talk now about some of our organizational components. First among those are our threat teams. We have teams focused on Russia, China, Iran, and counterterrorism. They conduct specific operations and they also carry out interagency coordination to counter propaganda and disinformation from those threat actors.

Second are our functional teams. These include our analytics and research team, which I spoke about above in the context of its analysis, and our technology and engagement team, which I will [detail] a bit more later on.

Third, we have an interagency and international coordination cell, which—because government loves acronyms—we call the I2C2. It is comprised of liaison officers from departments and agencies, and in the case of the Department of Defense, from Combatant Commands, so that we are connected, as we need to be, with those partners to coordinate.

Now, let me talk a bit more about our analytic support. To counter adversarial propaganda and disinformation, we really need the best possible understanding of the information environment, and we need to share that understanding with our partners both within the U.S. government and internationally. Over the past year, we have conducted analysis touching on at least seventy-seven countries.

We tailor our analytic products to the needs of our consumers, who are typically an embassy, a State Department bureau, or one of our international partners. These reports are designed to be actionable and unclassified. There is a growing demand for open-source data and research. We do this so when we put this in the hands of, for example, an embassy on a Tuesday morning, they can go and do something with it almost as quickly as possible, whether that is writing talking points or reallocating resources to a program that they are supporting. What we want to do is tell the embassy what is happening in a quantifiable and a data-driven matter, whether or not some propaganda or disinformation event is prevalent in the information space, whether or not it is coordinated by a threat actor, whether it dovetails with prevailing sentiment among a target audience, and what can be done. We also benefit, of course, from feedback from our colleagues in the field, who have a fantastic grasp of local dynamics, politics, culture, and history. That is an iterative cycle.

Let me talk about our work in the context of the COVID crisis. In January 2020, we already began to look at propaganda and disinformation in this context. It rapidly became clear that this would be an issue of global consequence, not simply in the scope of the crisis, but also in our area of propaganda and disinformation. We saw Russia pushing conspiracy theories. We saw the People's Republic of China suggesting various false and nefarious narratives about the origin of the virus. So we began to see a certain narrative convergence between the Chinese and Russian efforts. These were not the only countries to push these false narratives, but they have very well-developed mechanisms and ecosystems to spread their messages to audiences around the world on a variety of platforms. We took a multifaceted approach in our efforts to counter this wave of COVID-related disinformation and propaganda.

First, we tracked all of it, beginning in January 2020. We released reports. One of our first reports looked at Russia's disinformation campaign on the virus, and how it spread through their ecosystem. Secondly, building on this analysis, we worked to expose these disinformation efforts. Here, I would flag for everyone: while most of our reports are for internal use, we do public products as well. Last year, we released a major report on the pillars of the Russian disinformation ecosystem, which highlights the proxy news outlets and websites that they use, but also focuses on the role of that ecosystem in spreading COVID-related propaganda and disinformation. Third, we worked with the media to inform the public, for example, about Beijing's propaganda and disinformation campaigns on the [pandemic]. Finally, we provided rapid-response grants to local organizations on the frontlines fighting the adversarial narratives of the COVID "info-demic" as some have called it.

Now let me talk a little bit more about our threat teams. Our Russia team, it leads and coordinates U.S. interagency and global partner efforts to understand, expose, counter, and to build resiliency to Russian malign influence that aims to undermine democratic systems.

Our China team focuses on three priority lines of effort. The first is to puncture PRC propaganda narratives through high-quality open-source research. The second is to build resilience among civil society and the media. Third is to carry out strategic communications campaigns in reducing space for Beijing's whole-of-government influence campaigns, propaganda, and disinformation to thrive.

Our Iran team works to deny Iran use of disinformation that undermines US policy. To this end, the GEC educates and informs global partners on the threat of Iranian disinformation, including its manipulation of outcomes around elections and other international events.

In the counterterrorism realm, our counterterrorism team understands that they are dealing with a fluid information environment and seeks to be agile, analytic, and proactive in countering the threats that face our homeland. Terrorist organizations seek to leverage the online space, combining their online and offline propaganda activities to multiply the impact of their operations and build a perception that they are growing and successful movements, because those are the movements that can pull in funding and draw recruits. Our job, of course, is to prevent this at every stage of the way in the area of propaganda and disinformation, so that they can't do this. I would note in the counterterrorism context an increasing focus on racially and ethnically motivated violent extremism (REMVE). That comes in addition to our existing experience countering propaganda and disinformation by groups like ISIS and al-Qaeda.

Specifically, the Global Engagement Center is a co-chair of the Communications Working Group within the Global Coalition to Defeat ISIS. The GEC led the development in supporting the implementation of the de-ISIS resiliency counter-propaganda and disinformation campaign framework. This campaign takes a population-centric approach, building resiliency among audiences in Iraq and Syria that are the most vulnerable to ISIS ideology and coercion. The Global Engagement Center's Coordinator and Special Envoy serves as one of the three co-leads along with the UK and the UAE in the [coalition's] Communications Working Group, which today brings together more than fifty organizations and nations. In this role, the GEC has led discussions with Communications Working Group partners on how ISIS is exploiting the COVID-19 crisis and its propaganda, and we've explored new ways to counter the group's narratives. Our UK co-leads on the Communications Working Group are amplifying and providing analysis of the coalition's communications activities through the counter-Daesh communications cell in London, and challenging and degrading the legitimacy of ISIS globally. Through this overarching framework, members of the coalition are able to conduct activities independently of each other without fear of contradicting or duplicating the efforts of other partners.

Let me talk a little bit about some of our efforts in East Africa. Globally, we focus on building resiliency to terrorist propaganda through working with local, national, and regional partners. Specifically, we are doing this in several East African countries. We're training teachers, youth, and community leaders to detect and respond to signs of radicalization in their communities.

One program we're very proud of is called "Somali Voices," where we partner with local implementers who built websites and social media platforms focused on countering messaging from extremist organizations. They have produced thirty radio programs that were broadcast nationally on a major Somali language station. This product had very high levels of engagement on its social media platforms, with 4.8 million people reached through Facebook and a 16 percent engagement rate, and 307,000 persons on Twitter with a 36 percent engagement rate.

As I mentioned before, we are also increasingly focused on REMVE. Specifically, we are working with the U.S. Institute of Peace on a year-long research program in partnership with the RESOLVE academic network. This focuses on foreign, online REMVE communications, information ecosystems, and audiences, with a particular emphasis on Europe and Australia.

Last but certainly not least, let me talk a little bit more about our technology engagement. Our incorporation assessment of technologies to counter propaganda and disinformation starts by understanding the methods and capabilities the threat actors employ. This threat actor toolkit is a continually evolving set of technologies and tactics that enable the adversary to conduct propaganda and disinformation campaigns at scale. Understanding how our adversaries are seeking to promote disinformation helps us in advancing tactics and concerns, of course, to counter them. So we are looking at all of the latest techniques to, for example, uncover fake accounts and messages pushed out by bots and trolls.

As technology continues to advance, the adversarial capabilities will be augmented by technology, but we of course can also identify and put technology in the service of our partners. We have a number of specific programs here.

Tech Demos are biweekly and are held to provide a forum for private-sector companies to demonstrate technologies applicable to the disinformation challenge. They present these to U.S. government stakeholders. We've conducted forty-nine demos of ninety-one technologies over the last two years.

We also hold Tech Challenges. These are international events that provide a forum for foreign companies to demonstrate technologies that can help with the disinformation challenge in that country and can help some of our stakeholders there. We've had two of these already, one in the United Kingdom and one in Taiwan, and we have three scheduled for 2021. The GEC provides a certain amount of funding to the winner of the challenge for local implementation.

Third, we maintain a Technology Testbed. This is for the use of all U.S. departments and agencies to test the operational use of promising technologies that we identify through our Tech Demos. To date, we have tested twenty-five tools, and eight of them have been integrated into U.S. government use.

To further increase connectivity among this community of interest for the U.S. government, foreign partners, industry, and academia, we maintain an online platform called Disinfo Cloud that shares findings and information on disinformation-related challenges. This platform today has almost 1,200 members and has assessed seventy tools. We work very closely with our interagency partners, such as the Department of Defense, on counter-disinformation technologies and things that can enable them. We have established a liaison in Silicon Valley with the purpose of sharing lessons learned and developing two-way communications about foreign disinformation and propaganda with our partners in the technology industry.

To summarize, the GEC today is providing significant analytic support to the interagency and to U.S. embassies globally, to inform their actions in the information space. The GEC is operating over 100 programs in 120 countries. It is leading U.S. and international coordination on technology implementation through our Tech

Demos, our Tech Challenges, and our Testbed. We are supporting multiple international coordination mechanisms to provide a framework for coordination that can be sustained and can endure over the long term. So with that I'll pause, and I look forward to your questions.