GlobalResearch
Center for Research on Globalization

# ISIS Online: A Pretext for Cyber COINTELPRO?

By Eric Draitser
Global Research, February 27, 2015
CounterPunch 26 February 2015

Region: Middle East & North Africa, USA
Theme: Intelligence, Terrorism

*In its ever expanding war against Syria, now under the broader pretext of "fighting ISIS," the US Government has employed a variety of tactics. From arming terrorists whom it dishonestly labels "moderates," to encouraging Turkey and Jordan to host jihadi training centers, to the CIA working with the Muslim Brotherhood to funnel weapons and fighters into Syria, the US and its allies have demonstrated the multi-faceted approach they're taking to fighting ISIS, extremism, and the Syrian Government.*

The war, once believed to be relegated solely to Syria and Iraq, has now been broadened to a regional, and indeed, a global war with no geographical boundaries or time limits. And now, the Obama administration has announced that its war will also be waged in cyberspace. As the NY Times reported:

> At the heart of the plan is expanding a tiny State Department agency, the Center for Strategic Counterterrorism Communications, to harness all the existing attempts at countermessaging by much larger federal departments, including the Pentagon, Homeland Security and intelligence agencies. The center would also coordinate and amplify similar messaging by foreign allies and nongovernment agencies, as well as by prominent Muslim academics, community leaders and religious scholars who oppose the Islamic State.

While the use of social media and other online platforms is nothing new, the coordinated nature of the program demonstrates the broader capacity the US State Department and intelligence agencies are going to employ in penetrating cyberspace to, in theory, counter ISIS and other extremists groups' propaganda. But is this all they'll be doing? There is good reason to doubt the seemingly innocuous sounding mission of the Center for Strategic Counterterrorism Communications (CSCC).

Countermessaging or Counterintelligence?

It is clear that the US Government is actively going to expand its social media and cyberspace presence vis-à-vis online extremism. According to the expressly stated goal, the CSCC is intended to:

> ...coordinate, orient, and inform government-wide foreign communications activities targeted against terrorism and violent extremism... CSCC is comprised of three interactive components. The integrated analysis component leverages the Intelligence Community and other substantive experts to ensure CSCC communicators benefit from the best information and analysis available. The plans and operations component draws on this input to devise effective ways to counter the terrorist narrative. The Digital Outreach Team actively and openly engages in Arabic, Urdu, Punjabi, and Somali.

Although the description makes the program seem harmless enough, a close reading should raise very serious questions about just what exactly the CSCC will be involved in. The so called "integrated analysis" and "plans and operations" components provide an ambiguously worded description of collaboration with US intelligence agencies – CIA, DIA, DHS, and NSA undoubtedly among them. These agencies, aside from gathering intelligence and performing surveillance in every corner of the globe, are also involved in everything from espionage to "black ops" and "dirty ops" and other shadowy activities.

In effect, the CSCC will act in concert with these agencies both in the realm of information and activity. Does anyone seriously doubt, especially in light of the Snowden revelations about the all-encompassing nature of US surveillance and counterintelligence capabilities, that ultimately part of the CSCC's responsibilities will be to act as a de facto arm of US intelligence in the cyberspace realm, with specific attention to global hotspots such as Syria, Iran, Pakistan, Libya etc.?

As for the so called "Digital Outreach Team," it could rightly be described as a cyberwar unit, one that will be able to operate both openly and anonymously in a variety of capacities online. And therein lay the danger. As Richard Stengel, Under Secretary of State for Public Diplomacy and Public Affairs told the Times, "[CSCC] would use more than 350 State Department Twitter accounts, combining embassies, consulates, media hubs, bureaus and individuals, as well as similar accounts operated by the Pentagon, the Homeland Security Department and foreign allies." Now of course, if this much has been admitted publicly, there is undoubtedly a much larger cyber capacity being developed covertly. The question then becomes: how will this capacity be used?

If history is any indicator, then activists, political radicals, dissidents, and many others will be targeted online. The revelations about COINTELPRO documented by the Church Committee demonstrated the way in which "intelligence gathering" becomes counterintelligence with all the attendant repression, subversion, entrapment, and more. As William C. Sullivan, former head of the FBI's intelligence operations was quoted in the Church Committee report:

> This is a rough, tough, dirty business, and dangerous. It was dangerous at times. No holds were barred… We have used [these techniques] against Soviet agents. They have used [them] against us… [The same methods were] brought home against any organization against which we were targeted. We did not differentiate. This is a rough, tough business.

Sullivan quite bluntly explained how the line between foreign and domestic counterintelligence became completely blurred as the repression of political radicals became equated with fighting the Cold War. Of course, anyone seriously examining today's world cannot help but draw parallels between the aggressive rhetoric about the Soviet threat during the Cold War, and that around the "terrorist threat" of "radical Islam" today. It would be folly to think that, in light of the exponentially more powerful and all-encompassing surveillance architecture (to say nothing of the draconian laws such as the PATRIOT Act, National Defense Authorization Act, etc.), the government would not employ similar, and perhaps more severe and repressive, tactics today against any individuals and groups challenging dominant narratives, organizing antiwar/anti-imperialist activities, building economic and political alternatives, and much more.

It's Happened Before, It'll Happen Again

It should come as no surprise that there is a voluminous documented record of online information manipulation and propaganda designed to achieve political ends. Recent examples specific to the war on Syria are endlessly instructive about some of the tactics one should be prepared for.

A recent example of the sort of social media disinformation that has been (and will continue to be) employed in the war on Syria/ISIS came in December 2014 when a prominent "ISIS twitter propagandist" known as Shami Witness (@ShamiWitness) was exposed as a man named "Mehdi," described as "an advertising executive" based in Bangalore, India. @ShamiWitness had been cited as an authoritative source – a veritable "wealth of information" – about ISIS and Syria by corporate media outfits, as well as ostensibly "reliable and independent" bloggers such as the ubiquitous Eliot Higgins (aka Brown Moses) who cited Shami repeatedly. Conveniently enough, once exposed, Mehdi's identity has been withheld from investigators, and he has since disappeared from public view. While it is impossible to say for certain exactly who Mehdi is, the significant point here is that this is a prime example of how social media is used to manipulate and frame false narratives, and to bolster threats and propaganda that serves particular interests.

In early 2011, as the war on Syria was just beginning, and many in the West especially were still harboring the delusion of an "Arab Spring uprising," a blogger then known only as the "Gay Girl in Damascus" rose to prominence as a key source of information and analysis about the situation in Syria. Corporate news outlets such as The Guardian lauded her as "an unlikely hero of revolt" who "is capturing the imagination of the Syrian opposition with a blog that has shot to prominence as the protest movement struggles in the face of a brutal government crackdown." However, by June of 2011, the "brutally honest Gay Girl" was exposed as a hoax, a complete fabrication concocted by one Tom MacMaster. Naturally, the same outlets that had been touting the "Gay Girl" as a legitimate source of information on Syria immediately backtracked and disavowed the blog. However, the one-sided narrative of brutal and criminal repression of peace-loving activists in Syria stuck. While the source was discredited, the narrative remained entrenched.

There are many other examples specific to the war in Syria, as was the case in Libya where dozens of twitter accounts purportedly from anti-Gaddafi Libyans mysteriously emerged in the lead-up to the war that toppled the Libyan government, providing much of the "intelligence" relayed on western media including CNN, NBC, and all the rest. It was at precisely that same moment (February 2011) that PC World ran a story headlined "Army of Fake Social Media Friends to Promote Propaganda" which noted that:

> ...the U.S. government contracted HBGary Federal for the development of software which could create multiple fake social media profiles to manipulate and sway public opinion on controversial issues by promoting propaganda. It could also be used as surveillance to find public opinions with points of view the powers-that-be didn't like. It could then potentially have their "fake" people run smear campaigns against those "real" people.

Of course, if the story had already been broken by that point, one could rest assured that such programs were already long since being employed by US and other intelligence agencies for the purposes of achieving precisely what they achieved in Libya: the dissemination of disinformation for the purposes of constructing a false narrative to sway

public opinion to support Washington's agenda.

So, we know that US intelligence has the ability to create an endless supply of Facebook, Twitter, and other social media accounts. In light of this information, it is not terribly difficult to see the danger of allowing a centralized, intergovernmental "counterterrorism center" from engaging in an online spook war with the alleged threat of ISIS online. It is entirely plausible that this is yet another manufactured pretext for still further penetration of social media by US intelligence for the purposes of infiltrating and subverting online activists, independent journalists, and others.

Indeed, such activities would fit perfectly into the broader strategic imperative infamously articulated by Obama confidant, friend, and former head of the Office of Information and Regulatory Affairs, Cass Sunstein. As Glenn Greenwald wrote in 2010:

> [Sunstein] is responsible for "overseeing policies relating to privacy, information quality [emphasis original], and statistical programs." In 2008, while at Harvard Law School, Sunstein co-wrote a truly pernicious paper proposing that the U.S. Government employ teams of covert agents and pseudo-"independent" advocates to "cognitively infiltrate" [emphasis original] online groups and websites... Sunstein advocates that the Government's stealth infiltration should be accomplished by sending covert agents into "chat rooms, online social networks, or even real-space groups." He also proposes that the Government make secret payments to so-called "independent" credible voices to bolster the Government's messaging.

This sort of "cognitive infiltration" is undoubtedly happening in myriad ways that still remain largely unknown. What can be said for certain though is that US intelligence agencies have both the tools and strategic vision to manufacture online threats such as the meme of "ISIS social media recruiting" in order to bolster their failing propaganda war, and to justify yet another unpopular war to the American people.

This wouldn't be the first time that intelligence and law enforcement agencies have manufactured threats and/or entrapped alleged "terrorists" for the purposes of justifying the repressive apparatus of the police state, not to mention their own jobs.

State Sponsored Terror At Home

Just looking at the recent historical record, one begins to see an unmistakable pattern of terror plots concocted by the FBI and other agencies which they then portray themselves as having thwarted. In September 2011, the FBI allegedly foiled an "aerial bombing plot and attempts to deliver bomb-making materials for use against US troops in Iraq." However, as the AFP article casually noted:

> During the alleged plot, undercover FBI agents posed as accomplices who supplied Ferdaus with one remote-controlled plane, C4 explosives, and small arms that he allegedly envisioned using in a simultaneous ground assault in Washington. However, "the public was never in danger from the explosive devices, which were controlled by undercover FBI employees," the FBI said. Ferdaus was arrested in Framingham, near Boston, immediately after putting the newly delivered weapons into a storage container, the FBI said.

So, this alleged "terrorist" had neither the means nor the opportunity to carry out any plot

at all, until the FBI became involved, supplying him with everything he needed, including actual explosives. They then high-fived each other for a job well done, foiling this dastardly plot. It would be comical if it weren't so utterly repugnant.

Similarly, in 2010 the FBI claimed to have stopped a terrorist operation in Oregon – the insidious "Christmas Tree Bomber" – who likewise was supplied with the explosives, not to mention training, by the FBI themselves. In 2012, the FBI claimed to have thwarted a suicide bomb attack on the US Capitol. Conveniently buried in the story however is the fact that the explosives and technical expertise were all provided by the bureau's undercover operatives.

There are literally a dozen or more other incidents that one could point to where US Government agencies have been intimately involved in planning, and then "foiling," terrorist operations. The point is not to allege some grand conspiracy, but rather to illustrate the documented history of manipulation and fabrication of threats – both real and imagined – for the purposes of justifying the military-industrial-intelligence-surveillance complex.

If such agencies have proven countless times that they have the wherewithal and determination to carry out such operations, why should we believe that today is any different?

It is clear that the government has hyped threats against the US for a variety of reasons. So too is this story of ISIS and social media being hyped for a specific agenda – to legitimize the creation of yet another shadowy COINTELPRO-style interagency unit that will further entrench US intelligence in cyberspace, especially in social media.

How will you know if that Instagram picture of an ISIS member holding a cute kitten is authentic, or is simply a government-controlled troll, a fake identity created by some guy in a room in Virgina? How will you know if those young British-Saudis holding jars of Nutella in front of an ISIS flag are who they are alleged to be? How will you know if any of what you're seeing on Twitter, Facebook, or anywhere else is real at all?

You won't know for sure. And that is precisely the point.

*Eric Draitser is the founder of StopImperialism.org. He is an independent geopolitical analyst based in New York City. You can reach him at ericdraitser@gmail.com.*



---