JUST SECURITY
A FORUM ON LAW, RIGHTS, AND U.S. NATIONAL SECURITY

America's Muddled Approach to Fighting ISIS

Patrick Eddington

January 28, 2016

Last month, the *Los Angeles Times* ran a story that helped highlight one facet of the muddled thinking afflicting the US government's campaign against ISIS: While the military wants to sabotage the group's cyber propaganda and recruitment capabilities, FBI and intelligence officials argue doing so would close a critical window into its operations and ability to detect domestic terrorist plots. Even as it stands on verge of acting, the government is fighting with itself (both in the press and presumably behind closed doors) and implementing contradictory policies. A better course of action would be acknowledging that it has struggled to find ways to weaken the organization, and refocusing the government's resources and attention on the real problem (ISIS), rather than pursuing counterproductive policies at home.

These kinds of bureaucratic and mission turf wars are nothing new; they figured prominently in the 9/11 Commission's hearings and in its final report. What the apparent bickering between the FBI and military officials underscores is that the 9/11 Commission's recommendations — virtually all of which have been implemented, including the creation of a Director of National Intelligence to help mitigate such bureaucratic turf wars — have done nothing to solve this age-old problem.

Left unaddressed in the *LAT* piece is the larger historical parallel between the federal government's overblown and counterproductive responses to past alleged pan-nationalist threats in the 20th century and its response to militant Salafism today.

For example, during the "Red Scare" that started during the First World War and ran largely unbroken throughout the Cold War, the federal response included efforts to subvert the primary means of communication at the time — through telephone taps, the interception of telegrams, and censoring the mail. In the undeclared war against alleged or potential ISIS adherents in America, federal authorities have returned to that playbook, updated to account for the advances in technology.

In a pattern that has recurred almost weekly for the last two years, a government official has repeated the canard that ISIS's use of encryption technologies is making it impossible to track:

> But there are apparently limits to U.S. cyber capabilities. Speaking to reporters Dec. 9, Rep. Michael McCaul (R-Texas), chairman of the House Homeland Security Committee, said Islamic State hackers "have developed an encrypted app and can communicate anywhere in the world

from an iPhone without any ability for us to pick up those communications. … They have mastered this dark space."

Like the overwhelming majority of members of Congress, McCaul lacks sufficient technological literacy or even a cursory familiarity with the most current literature on exactly how maladroit ISIS truly is in cyber operations. As one prominent cyber expert recently noted, ISIS appears to lack personnel with even modest cyber skills:

From their dwindling talent pool of low grade hackers, to their limited cyber operations and their poor training regime, it is clear that ISIS do not pose a credible cyber threat to anyone. While this may change in the future (anything's possible), it seems very unlikely that they will possess the capability to do any damage to anyone. ISIS simply are not a serious cyber threat actor.

Even so, McCaul has proposed an "encryption commission" to study how to cut the digital Gordian knot of protecting user privacy and still giving law enforcement what it allegedly needs to track and thwart terrorist plots. The fact that virtually every reputable crypto expert in the world has dismissed such an idea as dangerous and unworkable has had no effect in curtailing law enforcement's requests for an impossible solution. Moreover, even a complete private crypto ban would not stop ISIS-inspired "lone wolf" attacks like the one in Chattanooga last year. And in a body-blow to the FBI's position on the issue, NSA Director Admiral Mike Rogers made it clear during a talk at the Atlantic Council that trying to ban public key encryption is "a waste of time."

The persistent belief in the possibility of creating "good guys-only" crypto "backdoors" evinced by FBI Director James Comey and other federal officials is a form of magical thinking. It's an intellectual dodge that helps them ignore the government's own failures to penetrate ISIS in the Middle East and Europe — the single best way to take down the organization's members.

And questionable anti-ISIS legislative proposals are not confined to the technological arena.

Another Texas House delegation member who is usually quite good on First Amendment issues, Rep. Ted Poe, has strayed from the path of wisdom by joining those who believe that Twitter and Facebook can somehow magically banish ISIS and its supporters from social media platforms.

In December 2015, the House passed Poe's Combat Terrorist Use of Social Media Act (HR 3654) on a voice vote. The bill would mandate a report from the administration on how it will combat ISIS's use of social media, including (in the words of the bill summary) the development of a "policy that enhances the exchange of information and dialogue between the federal government and social media companies as it relates to the use of social media platforms by terrorists."

As the long list of DOJ indictments against ISIS supporters and would-be recruits over the last two years shows, the Patriot Act and related statutes have provided the FBI with ample authorities to get the data they need from social media companies to make cases against alleged terrorist plotters. What Poe's bill has done is provide ammunition for a civil lawsuit against Twitter for allegedly indirectly playing a role in the death of an American killed in a salafist-inspired attack in Jordan in November 2015.

By the logic of the plaintiffs in that case, the manufacturers of the guns used in the San Bernardino attack could also be held civilly liable, as could the manufacturers of the pressure cookers used to make the improvised explosive devices employed in the Boston Marathon bombing, and so on. If the suit succeeds, it won't just be social media companies that are put at financial risk from future terrorism-related lawsuits. Any company whose products or services contributed even indirectly to a terrorist act against an American could face civil liability for the misuse of their products or services.

Just as with the government's misdirected focus on encryption apps and services, the civil liability focus of such suits takes the spotlight off of the real criminals — ISIS — and the federal government's own role in creating and furthering the expansion of salafist groups like al Qaeda and ISIS by invading Iraq and Libya.

Congressional calls for banning certain forms of speech or censoring publications are nothing new. They began within a decade of the ratification of the Constitution and have, unfortunately, continued into the modern era. After the post-WWI Red Scare in 1919–20, a Senate committee called for a ban on foreign language publications that allegedly carried "un-American" ideas on their pages. The Overman Committee helped fuel an anti-foreigner and anti-communist hysteria that would ultimately give rise to the House Unamerican Activities Committee, Senator Joseph McCarthy, and a poisonous domestic political climate that would lead to the surveillance and persecution of hundreds of thousands of Americans in the 20th century. Current federal counterterrorism policies have the nation on the path to repeating the same mistakes in the 21st century.

The government's current "countering violent extremism" (CVE) policies already have undercurrents that mimic the Red Scare era. These include the creation of a "domestic counter terrorism counsel" within DOJ, the establishment in DHS of the euphemistically named "Office of Community Partnerships" (which is exclusively focused on extremism in Arab- and Muslim-American communities), the FBI's development of a school-based CVE program that would effectively pit teachers against their Arab- and Muslim-American students and propagate false and misleading information about Islam, and legislation to make at least some of these programs permanent fixtures of the federal government.

Each of these actions puts the focus — and by extension, the blame — for domestic terrorist acts committed by individual Muslims on Arab- and Muslim-American communities as a whole. No such federal efforts were initiated among the white, Protestant community as a whole after episodes involving the Covenant, Sword and Arm of the Lord, the siege at Ruby Ridge, the storming of the Branch Davidian compound, theOklahoma City Federal Building bombing, or the recent racially and politically motivated murder of nine African-Americans at a Charleston, South Carolina church. The contrast is as stark as it is hypocritical.

Indeed, the government's CVE programs are echoes of failed efforts to ferret out "disloyal" Americans during both World War II and the Cold War — from the use of dubious "loyalty oaths" to the Smith Act to the internment of Japanese-Americans to the McCarran Internal Security Act and the Attorney General's List of Subversive Organizations. But we continue to forget the lessons we learned from those failed policies and programs.

Indeed, the history of the List of Subversive Organizations should be a reminder and a warning about how easily federal agencies can go down the road of grouping domestic organizations into "loyal" or "subversive" categories. The recent IRS scandal involving the targeting of right-of-center anti-federal government groups only underscores the fact that the threat of such discriminatory treatment is real. It's rather easy to imagine something similar happening to Arab- or Muslim-American groups based on their level of cooperation with or resistance to these CVE programs.

The current GOP presidential front-runner has called for the creation of federal databasesto track not only Arab/Muslim refugees from the Middle East, but also potentially Arab- and Muslim-American citizens as well, in addition to an outright ban on Arab/Muslim immigration to the United States. If he were elected and ordered federal agencies to take such actions, would career civil servants at DHS and DOJ have the courage to defy Mr. Trump and refuse to implement such proposals? If the recent history of America's political, legal, and moral devolution into the use of torture is any guide, the more likely outcome would be agency compliance with the wishes and direction provided by the President.

And these CVE-related actions have something else in common: They shift the blame away from the federal government for its role in helping create and sustain ISIS — first by invading and destabilizing Iraq and Libya, and second by doubling-down on a failed security-centric approach to counterterrorism in the Arab and Muslim world. That disastrously overly-militarized approach to militant salafism, combined with federal support for de facto anti-Arab and anti-Muslim CVE programs at home, only help groups like ISIS make the case that America is, contrary to all public statements to the contrary, at war with Islam.

Our self-imposed counterterrorism schizophrenia comes at a high cost for all of us, just as our anti-communist hysteria led us into the quagmire that was the Vietnam War. In his veto message on the original Internal Security Act, President Truman spoke words of wisdom that we would do well to heed today:

> Our position in the vanguard of freedom rests largely on our demonstration that the free expression of opinion, coupled with government by popular consent, leads to national strength and human advancement. Let us not, in cowering and foolish fear, throw away the ideals which are the fundamental basis of our free society.

Amen.

Patrick Eddington is a Policy Analyst in Homeland Security and Civil Liberties at the Cato Institute.