Addressing the Threat of American Jihadist Travelers

The challenges posed by American jihadist travelers are varied and complex. While the data and analysis provided in this study can help further our understanding, it is also important that they are applied to future policy and civil society efforts towards preventing jihadist travel. Despite the multifaceted nature of the issue, there are recurring themes and implications which can be useful in forming potential responses.

Although large-scale travel has now concluded, as the U.S. experience with jihadist travelers from the 1990s and 2000s suggests, there may be a future mobilization of travelers when new battlefields emerge. Policymakers must attain a solid understanding of the dynamics in jihadist travel that have developed across mobilizations so that the U.S. can respond adequately to future waves. To account for the complexity of the threat, the U.S. must develop multifaceted, innovative, and alternative approaches.

The risk that "homegrown" extremists will commit attacks on U.S. soil outweighs the risk of attacks from returning travelers.

Since 2011, there have been 22 jihadist attacks in the U.S. None of them were committed by a traveler who returned from Syria and Iraq. More to the point, only one of the 64 travelers is known to have returned to the U.S. for the purposes of committing an attack.

"The risk of attacks from returning travelers is overshadowed by jihadists who never leave the U.S."

This is not to say that travelers do not pose any threat, or that the current approach of monitoring their activities is flawed. Yet, the risk of attacks from returning travelers is overshadowed by jihadists who never leave the U.S. This comparison is not only supported by research on the traveler contingent in Syria and Iraq, but studies of other jihadist mobilizations of Americans.[1] However, there is evidence from previous periods of mobilization to suggest that returnees have assisted homegrown jihadists in attack planning and travel. Travelers who return from Syria and Iraq bring new contacts, skills, and status within jihadist movements. Policies must be supplemented with responses designed to prevent returning jihadists from facilitating the plots of others.

A multi-tier classification and review system is necessary to assess the threat posed by individual travelers.

Overall the U.S. utilizes a provisional, case-by-case approach to returning travelers. This allows for a degree of flexibility, but absent a framework for processing different types and categories of travelers, agencies default to prosecution. U.S. strategies should consider the differing risks, levels of disengagement, and appropriate responses to jihadist travelers.

This strategy should include tiered threat assessments, categorizations of travelers, and a variety of responses, spanning from traditional to non-traditional approaches. The appropriate responses to returning jihadist travelers should be determined by several factors, such as: age, background, personal connections to other jihadists, behavior prior to departing, their overseas activities, and their motivations for returning to the U.S.

In addition to these variables, this study's three categories of travelers can be instructive for authorities when determining responses to each case. Are they a pioneer or veteran of multiple conflicts? Have they built networks with like-minded supporters in the U.S. that may facilitate their re-entry into jihadist activity? Or are they loners who do not have the personal connections to reintegrate into jihadist networks? From such classifications, authorities could develop a range of policies and responses.

The most pressing question for U.S. officials is whether a traveler is returning for the purposes of conducting an attack. Approaches should include threat assessments of travelers from the intelligence community, combined with input from overseas allies and partners, to assess this probability.

When travelers who are planning to commit an attack do return, the response should be clear cut: prosecution. However, the challenge is in determining appropriate measures for cases in which returnees do not intend to plan terrorist attacks. Law enforcement must distinguish between individuals who have completely disengaged from jihadism, and those who have not. Some travelers will return after surrendering to U.S. forces or renouncing their jihadist groups. This class of returnees, if leveraged correctly, can be crucial human intelligence sources. They can provide a window into the operations of jihadist organizations and other Westerners fighting overseas. However, these travelers have their own incentives and disincentives for providing information. Notably, they may view cooperation as a ticket to a reduced jail sentence or other privileges. Nonetheless, a record of cooperation with federal authorities may decrease the risk of recidivism.

More perplexing cases involve individuals who disengaged from the battlefield in Syria and Iraq, but not from jihadism or their group. These are high-risk cases for facilitation and terrorist recidivism. Law enforcement faces a difficult challenge in assessing whether their disengagement is genuine and lasting.

The U.S government also needs a strategy to respond to travelers who held ostensibly non-combatant roles in jihadist groups. In the wave of IS-related mobilization, whole families traveled to the group's territory in Syria and Iraq. Returning women and children travelers possess unique experiences, and may have different reintegration needs than adult male travelers. However, authorities should not essentialize their roles.

Women returnees, like their male counterparts, may downplay their involvement in a ploy to receive favorable treatment in judicial proceedings. Despite this, American policymakers should understand that women travelers often play essential roles in the operation of jihadist organizations. They should not be exempt from criminal liability for their actions merely because they are women, or because they served in non-combat roles.[2]

The U.S. government must work with non-governmental partners (including, psychologists, sociologists, community leaders, and families) to prepare for the return of American children who were taken by their families or born in Syria and Iraq. While the U.S. has prosecuted individuals as young as 15, the Department of Justice may decline to press legal charges against returning minors. There is currently no system in place to address this issue. These minors have spent their formative years engrossed in a culture that values death and espouses hatred for the West. A process of disengagement, or even deradicalization, is required for these individuals.

Prosecutions are a necessary, but insufficient strategy to respond to American jihadist travelers. In addition to convictions, the U.S. government must develop alternative responses, especially in the U.S. prison and parole systems.

The diverse nature of American travelers and returnees demonstrates that in most cases, criminal prosecution is warranted. However, it is not always the appropriate response. Article III criminal prosecution has heralded significant successes in the response to returning travelers. For instance, Abdirahman Sheik Mohamud received a 22-year sentence, the longest for any returnee from Syria or Iraq. Yet, these cases are exceptions to the norm. Strikingly, the prison sentence for convicted, successful travelers is, on average, four years less than the average sentence for individuals who attempted to travel but were apprehended.

Returning travelers have been convicted for several offenses. However, if a material support case cannot be established, remaining offenses usually carry much shorter prison sentences. Travelers' activities in Syria and Iraq are disguised by the "fog of war," and evidence from the battlefield may not be admissible in court. Thus, law enforcement is forced to pursue lesser charges as a fallback. In November 2017, NCTC Deputy Director

Russell Travers addressed the potential downside of this approach: "if [travelers] are arrested and put in jail, the chances are that the sentences will be relatively light in some cases, and they will be out on the streets in a few years … this is going to be recurring threat."[3]

It is worth considering the costs and benefits of this approach. The amount of time that travelers convicted of a lesser offense spend in prison may be relatively negligible. Travelers also have the potential to build networks within the prison system, and have few incentives to disengage from jihadism while incarcerated.

To date, two individuals who were convicted of offenses related to their participation in jihadist groups in Syria and Iraq have already completed their sentences. Within the next five years, at least three more are scheduled for release. Currently, there are no deradicalization and disengagement programs targeted towards incarcerated terrorists in the U.S. federal prison system. In this regard, the U.S. lags behind many Western nations and must make such programs a priority. The alternative—allowing individuals convicted of terrorism-related offenses to serve out sentences without any deradicalization programming—is a band-aid solution that relies solely on the deterrent effect of prison sentences.

U.S. Bureau of Prisons officials have expressed concerns that individuals convicted of terrorism offenses may build support networks within prison and attempt to radicalize other inmates.[4] European countries have had an especially difficult lesson to learn regarding terrorist networks that were partially or wholly facilitated in their prison systems. For instance, several members of the cell responsible for the 2015 Paris attacks and the 2016 bombings had previously been incarcerated, and two of them initially met one another in the same prison.[5]

Yet, perhaps in response to these failures in traditional criminal justice approaches, some European countries have developed innovative strategies aimed towards deradicalizing and re-integrating travelers.[6] An instructive example is Denmark's Aarhus model. This program developed a four-stage process for returning travelers to utilize counseling services provided by a consortium of community leaders, psychologists, sociologists, former travelers, and their families.[7]

Another alternative option relies on the use of disengaged and deradicalized returnees in targeted interventions. This approach has been implemented in several European countries using former members of various types of extremist groups (including far-right extremists, white nationalists, criminal gang members, and jihadists).[8] These options, due to the personnel they require, can fail without strict program guidelines, clear metrics of success, and careful risk assessments.

Some American returnees have expressed disillusionment with the false utopian vision offered by jihadist groups. The U.S. should consider leveraging these individuals in a more comprehensive way. In a very select number of cases, law enforcement should discreetly consider pursuing alternatives to prosecution for returning travelers who can use their experience to discourage future recruits. Prior to this decision, a comprehensive review of their intent and disillusionment with jihadism must be implemented.

Targeted intervention programs, including those that utilize returnees, have not been attempted on a large scale in the U.S. However, small-scale programs are underway to develop innovative approaches to address returnees and prevent future recruitment. Policymakers may consider scaling up these programs as part of a coherent national strategy. For example, an American returnee is currently involved in an experimental intervention program aimed towards deradicalizing other would-be travelers.[9] The returnee has thus far succeeded in using the credibility gained from their experience to dissuade at least one other American from making similar mistakes. This program is not yet part of any national strategy, and the dedicated local officials who implement this program receive little federal support.

However, just like criminal prosecution, such alternative approaches should not be considered silver bullets. They are designed to augment the criminal justice process, not replace it. High-risk cases of travelers for whom alternative

programs are not appropriate will certainly exist. For others, however, they may be worth considering.

Regulating online services (e.g. censorship, content and account deletion, restricting or banning privacy-maximizing tools) may have limited utility in countering jihadist travel-facilitation networks.

Many governments are still struggling to adapt to the dynamic role of digital communications technologies in terrorist recruitment. Identifying and monitoring travelers was considerably simpler when they used open platforms to plan their travel arrangements. In many ways, the blatant openness of their support provided opportunities for surveillance and a window for law enforcement to interject through arrests. Recently, supporters of jihadist groups have primarily transitioned to online platforms that offer privacy-maximizing services (such as secure browsers, virtual private networks, protected email services, mobile security applications, and encrypted messengers).[10]

"While...ease of access to jihadist propaganda online was a factor in many cases analyzed in this report, there is little evidence to suggest that this was the primary motivation for their travel."

The U.S. government has repeatedly raised this concern. Authorities claim that as a result of terrorist supporters "going dark," law enforcement is less likely to prevent individuals from traveling to conflict zones or planning attacks. Acting Deputy Attorney General Rod Rosenstein argued that "'going dark' threatens to disable law enforcement and enable criminals and terrorists to operate with impunity. When police cannot access evidence, crime cannot be solved. Criminals cannot be stopped and punished."[11] Some European countries have taken a more robust stance. For example, in October 2017 UK Home Secretary Amber Rudd introduced a plan to criminalize accessing and viewing jihadist material online.[12] UK Prime Minister Theresa May and French President Emmanuel Macron have also considered laws to make social media service providers liable for failing to remove jihadist content from their platforms.[13]

These tougher stances were developed mainly in response to recent homegrown terrorist attacks in Western countries, and were adopted well after the peak of jihadist travel to Syria and Iraq. There is evidence that many travelers utilized digital communications technologies to help facilitate their journey. While some requests for regulations on these services have merit and may assist in reducing terrorist recruitment, they face multiple obstacles.

The impulse to ramp up online censorship by taking down social media accounts and content is understandable given the success of jihadist groups in the online environment. Removing jihadist supporters and propaganda from Twitter, Facebook or YouTube, now standard practice for these companies, helps to diminish the group's presence on open platforms. In the cases of budding jihadist sympathizers with no real-world connections to the group, censorship may ensure that IS propaganda and recruiters are now harder (albeit still possible) to access and contact.

However, while there is no doubt that ease of access to jihadist propaganda online was a factor in many cases analyzed in this report, there is little evidence to suggest that this was the primary motivation for their travel. In most cases, a range of factors, online and offline, pushed individuals to make their journeys. Even when travelers went online, they displayed an active understanding of how to circumvent existing censorship measures by using lesser-known social media platforms. On these alternative platforms, propaganda, content, and facilitators remained easily (if not equally) accessible.

Thus, while censorship efforts will continue, they should be done with an acknowledgement that the approach has several limitations. American jihadists who migrated to

lesser-known social media platforms found a similar amount of jihadist material and access to recruiters.

Mohamad Khweis' case indicates the full spectrum of measures that travelers have taken to not only evade online censorship and account deletion, but also mask both their online activities and international travel. FBI investigators found no less than four secure calling platforms, three end-to-end encrypted messaging applications, three VPN services, an anonymous browser, and a video downloading application on Khweis' mobile devices.[14]

Attempts to counter terrorist use of privacy- maximizing tools face even greater hurdles than online censorship. In December 2015, then-FBI director James Comey expressed his frustration that the Bureau was unable to access 109 encrypted messages between Garland attacker Elton Simpson and an "overseas terrorist."[15] The issue has also become more pressing in Europe, with demands from politicians that popular applications which offer encryption, like WhatsApp and Telegram, cooperate more with authorities.[16] In response, certain countries have requested "backdoor" access to encrypted messages.[17]

There is no doubt that these emerging communication tools are of immense benefit to terrorists. Encryption and government access, therefore, is likely to be the most complex and long-running of all the debates surrounding extremist use of the internet. With this in mind, encryption must also be understood outside of the narrow context of terrorism and counter-terrorism. Countless people use encryption and other privacy-maximizing services every day, mostly for benign reasons, and it is often an invaluable tool for dissidents living under oppressive regimes.

Even if it was beneficial to do so, it is likely too late to limit access to end-to-end encryption.[18] Encryption is the future of digital communications. The technology is readily available, and new applications offering encryption are regularly developed. While possible technical solutions—including specific backdoor access to archived chats rather than live encrypted conversations—are beyond the scope of this report, there are many issues which must be considered if governments plan to regulate, weaken or ban these tools.

For instance, some companies offering privacy-maximizing services will refuse to acquiesce to government requests. One notable example is Telegram, which claimed in a March 2017 statement that "Telegram has disclosed zero bytes of user data to third parties, including governments" and claimed that it has no intention of cooperating with any government requests for data.[19] Moreover, the incentives and disincentives that help convince major technology companies to remove content or share data with governments may not apply to smaller social media providers. To counter terrorists' use of the internet in a rapidly-shifting online environment, the U.S. government must learn how to engage smaller (and more ideologically driven) companies.