Vigilance and COLLABORATION

Governments must broaden the gathering and sharing of ISIS intelligence

By **JAMES HOWCROFT**, Director, Marshall Center Program on Terrorism and Security Studies

PHOTOS BY THE ASSOCIATED PRESS

Three years after declaring itself a caliphate, ISIS, as an organization that governs territory, is in a death spiral. Its adversaries have slowly but surely squeezed and demolished its economic underpinnings, even as its own simultaneously quixotic and brutal governance attempts in Syria and Iraq have unraveled, as did al-Qaida's in Iraq. The cumulative coalition air campaign, the capture of the iconic town of Dabiq, and now the fall of Mosul have vitiated the core ISIS tenet of "remaining and expanding," crushing its image of surging victory. ISIS can no longer effectively recruit or pay even the few wild-eyed latecomers who may show up.

But even when ISIS' caliphate is extinguished, the problem it represents will not be. It will retain a capability to launch attacks around the world from other sites. The world's security services failed to effectively monitor, record or interdict the travel of their citizens to Iraq and Syria. We should not be caught similarly unaware when ISIS' former fighters come home — as some are already doing. Now is the time to establish a network of measures to record, monitor and, when there is a legal basis, interdict foreign terrorist fighters on their return. The foundation of these measures is accurate, actionable intelligence shared internationally and put into the hands of front-line security first responders.

U.S. Secretary of State Rex Tillerson, center, talks with British Foreign Minister Boris Johnson, right, and Iraqi Foreign Minister Ibrahim Jafari during the Meeting of the Ministers of the Global Coalition on the Defeat of ISIS in March 2017 in Washington, D.C. Political will is necessary to break the bureaucratic inertia that hinders effective intelligence sharing.

We are already well aware that foreign fighters returning from Syria and Iraq constitute a domestic security threat. The size of this diaspora is difficult to predict. Many who went have died and some will stay, at least for a while, or go to other Muslim-majority countries. Some who return will have never had combat experience or military training. Some will return to family and social networks that will constrain any impetus to violence — at least for a time. But we do not know these numbers, meaning that the number of genuinely dangerous returnees is also unknown.

For example, European Union Security Commissioner Sir Julian King recently estimated that there are 2,500 European foreign terrorist fighters in the combat zone.

Iraqi Army soldiers celebrate a victory during a military operation to regain control of a village outside Mosul in November 2016. As ISIS loses more ground on the battlefield, returning fighters pose a terrorism threat to Western countries.

He was at a loss to guess how many dangerous returnees there might be. The total number of foreign terrorist fighters who traveled to Iraq and Syria ranges from 30,000 to 40,000, most of them from the Middle East and North Africa. Of the fighters who have returned, some are known to their governments. But many returned undetected. The challenge of tracking returnees is about to grow sharply with ISIS' last urban havens of Mosul and Raqqa disappearing. What should we do?

Three main obstacles must be overcome if the United States and allied governments are to effectively use intelligence to protect citizens against the returnee threat. The first challenge is to fuse the intelligence information we have to produce a single useful file, or target package, on each foreign terrorist fighter. The second challenge is to greatly improve file sharing among global partners. The third challenge is to get these packages into the hands of those who need them most — front-line security professionals at borders and transport hubs. None of these obstacles is insurmountable; nor do they require new or large amounts of money. What we need is political will and leadership to overcome outdated thinking and inappropriate prohibitions limiting sharing and implementation.

Depending on their capabilities and the perceived threat to their nations, most intelligence services have been collecting data to identify fighters and their networks. Most national intelligence services have some capability to intercept foreign terrorist fighters' email and phone conversations. Social media posts by fighters who are proud of their efforts and anxious to recruit others and demonstrate fidelity to the cause, are invaluable sources for identifying terrorist locations, actions and networks. Interrogations and debriefings of returned foreign fighters sometimes yield valuable information. It is not uncommon for families to contact the authorities with information to help bring their relatives home safely. Photographs, fingerprints and in some cases DNA on identified foreign terrorist fighters reside in government databases if the individuals applied for a driver's license, received social benefit payments, or were ever arrested or convicted of a crime.

Unfortunately, this wealth of information is rarely integrated, connected or coordinated — even within Europe. For example, phone and email intercepts are kept by the organization that does intelligence collection and are classified at a high level, limiting access by others for fear of compromising collection techniques. Debriefings of returning foreign fighters are handled by the ministries or organizations that deal with human intelligence and are highly classified to protect the human sources, again limiting access by other agencies. Social media collection is classified at a lower level, and thus is frequently done by yet another department or agency. Justice ministries or their equivalent, not intelligence services, hold information on people who have been in the domestic criminal justice system. Photographs and fingerprints of those who applied for licenses or benefits are held at the local governmental level, or by a state's domestic social welfare ministry.

The seriousness of the returnee threat is a compelling reason to break down organizational and international barriers to focus efforts on better fusing and then sharing intelligence. We need to make the intelligence "actionable" — meaning precise enough to be used to take concrete steps to protect citizens. And we need to make it available in a usable format for those who need it most: first-line security and law enforcement personnel who will encounter returning fighters as they move across borders, pass through transport hubs or are stopped for routine traffic offenses. To do this, the intelligence packages must be rendered unclassified so they can be put into the hands of a border guard, customs official or traffic patrolman who doesn't have a security clearance or access to classified information.

Obviously, the various classifications of intelligence sources by different agencies (and sometimes within the same agency) complicate any effort to make a product that can be widely shared. Generally, when different classifications of intelligence are fused into a single product, the entire package assumes the highest, most restrictive classification level. This is unacceptable given the threat posed by foreign terrorist fighters. If leadership insists, analysts can make packages that strip out the specifics of sources and methods while still maintaining the vital, precise identification data first responders need.

Once allied governments overcome their internal challenges, the second step is for these packages to be shared among as many responsible governments as possible. Of course, there is some risk that certain governments might accidentally leak information. But wide sharing is worth the modest risk. Interpol is uniquely positioned to serve as the global clearinghouse to push these packages to and from its 190 member nations. Interpol routinely coordinates informational exchanges, but it is dependent on member nations to voluntarily provide data on their citizens. According to Interpol, it has only about 8,000 records on foreign terrorist fighters, out of the 30,000 to 40,000 fighters estimated to exist.

Once these packages are received by the relevant government agencies, they must be relayed expeditiously with actionable details to front-line security professionals. The outdated 20th-century methodology of matching names on identity documents to watch lists is ineffective — lists of transliterated names or aliases aren't reliably useful. We can do better: Retina and iris scans, DNA, fingerprints, signature matches and facial recognition software are the 21st-century identification tools of the trade. We must develop and field the capability for an official in the field to quickly match the biometric physical attributes of the person standing in front of him with those in his package.

There are, of course, impediments to this approach. As noted, the first hurdle is to render this data unclassified. The second hurdle is to field simple, rugged, low-bandwidth systems that can access a centralized national database from a hand-held device in the field. With today's technology, this goal is achievable. If average citizens can access networks from a hand-held device to securely book flights and purchase airline tickets, then it is hardly unreasonable to insist that government officials have the means to access a foreign terrorist fighter database in real time via similar devices.

The hardware and networking hurdles can be surmounted with leadership, but the lack thereof has been precisely the problem. Political leaders and their appointees are usually men and women who are academics or commentators with little experience in running large organizations. They are inexperienced with two truths: First, organizations are extremely conservative and bureaucratic and can be counted upon to resist change; and second, it is extremely difficult to get existing organizations to qualitatively adjust their standard operating procedures to do new things.

Change of this magnitude calls for expedited authority and processes to break through bureaucratic inertia and inaction. For that reason and others, an interagency arrangement needs to be set up, a process that is directive, not built on consensus or lowest-common-denominator outcomes. Given the urgency and high priority of the issue, the president's office is probably the only place where such an effort can be effectively sited. Our processes must be simple, straightforward and applicable to as many international partners as possible. It won't do us much good if the U.S. government manages to get over the bar, but most of our allies and regional partners do not.

An interagency effort, beyond the intelligence community, must in the U.S. include the Justice Department because some of the impediments to effective new protocols are legal. Leaders must drive the effort to permit the sharing of personal information on a limited number of their citizens with other governments. There are legitimate privacy issues and human rights concerns. During this particular window of vulnerability, leaders must acknowledge these concerns but drive the effort to fuse intelligence and share it with partners anyway. One way to address valid privacy concerns could be to designate a temporary "state of heightened security measures," with a specified temporary period of application explicitly indicated, during which international information sharing would supersede privacy concerns. Congress would need to approve; this sort of thing ought not be done by executive order alone, if possible.

There are risks in such an approach, but these need to be weighed against the risks of the status quo. When the next terrorist attack conducted by a returned terrorist fighter or someone influenced by one occurs, the U.S. government and other governments must face their citizens and be able to say with honesty and conviction, "we did all we possibly could" to protect them. At this point, that would be a lie. □

This is an abbreviated version of an article published in *The American Interest* magazine. To read the original article, visit www.the-american-interest.com/2016/12/01/dare-to-share/.