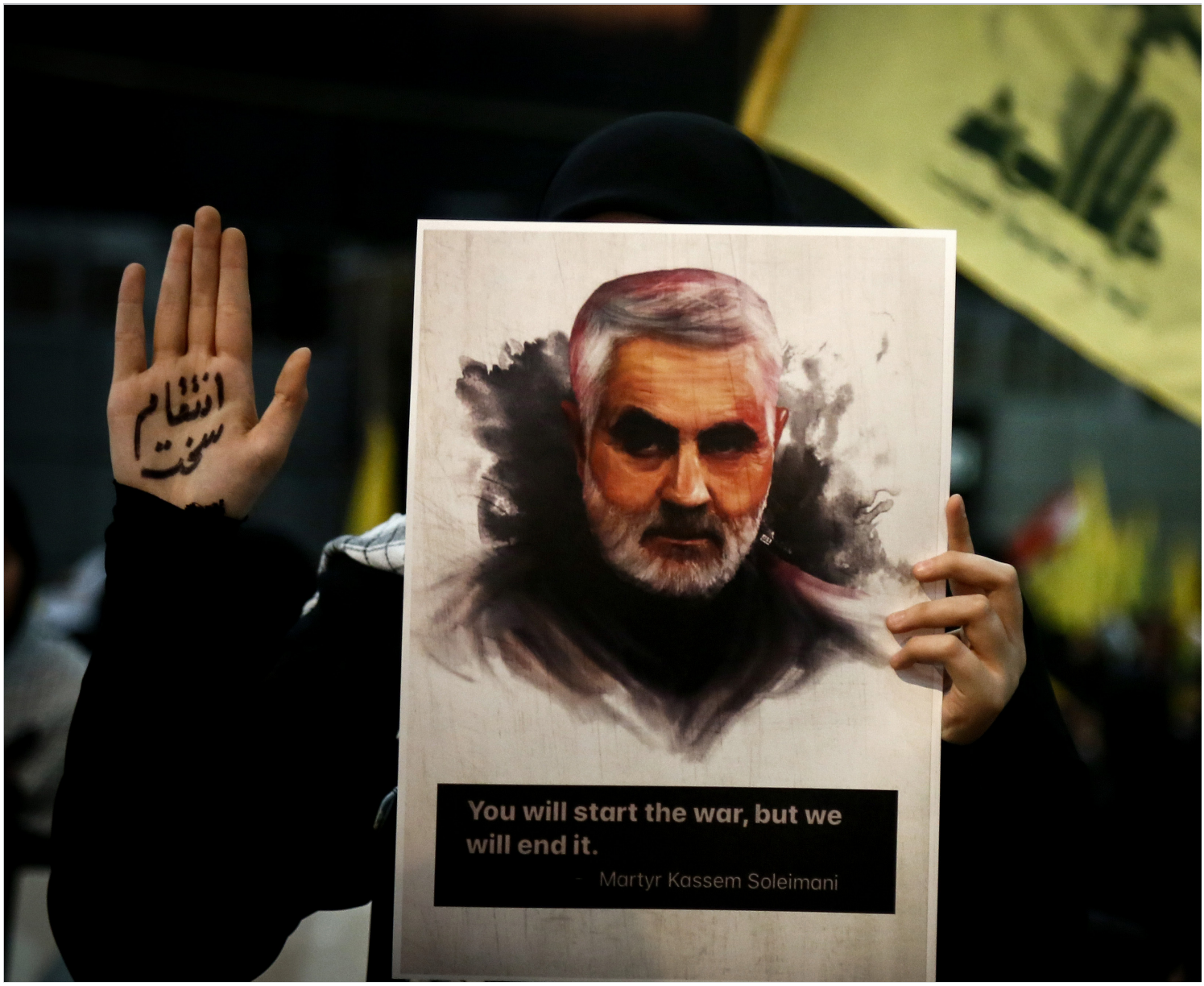
COMBATING TERRORISM CENTER AT WEST POINT

CTC SENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | FEBRUARY 2020 · VOLUME 13, ISSUE 2



FEATURE ARTICLE

Fighters Without Borders

Forecasting new trends in the Iran threat network foreign operations

MATTHEW LEVITT

A VIEW FROM THE CT FOXHOLE

Brigadier General Dagvin Anderson

COMMANDER, U.S. SPECIAL OPERATIONS COMMAND AFRICA

Contents

FROM THE EDITOR

Following the January 3, 2020, U.S. drone strike that killed Islamic Revolutionary Guard Corps Quds Force chief General Qassem Soleimani, there is significant concern that Iran may seek to retaliate against U.S. interests in the Middle East, and possibly even in the U.S. homeland. In our feature article, Matthew Levitt forecasts that "Iran and the foreign legion of Shi`a proxies at its disposal are likely to employ new types of operational tradecraft, including deploying cells comprised of operatives from various proxy groups and potentially even doing something authorities worry about but have never seen to date, namely encouraging Shi`a homegrown violent extremist terrorist attacks."

Annie Fixler assesses Iran will likely not order a major intensification of cyber operations against the United States to avenge Soleimani per se, because "claiming credit [to make clear any attack is in retaliation] also removes plausible deniability, which is one of the benefits of cyberattacks in the first place." Instead, she argues, the state-sponsored cyber threat from Iran will continue along its current elevated trajectory, driven to a significant degree by the Iranian regime's desire to hit back because of U.S. sanctions.

Our feature interview is with Brigadier General Dagvin Anderson, Commander of U.S. Special Operations Command Africa. In our second interview, conducted by Amarnath Amarasingam, an official at Europol's EU Internet Referral Unit outlines how in November 2019, the unit coordinated with messaging platforms, including Telegram, to carry out a major takedown of Islamic State channels online.

At a time of continued concern over the security risk posed by the thousands of Islamic State fighters detained in northern Syria, Bennett Clifford and Caleb Weiss assess the global threat posed by jihadi attacks on prisons and jihadi riots inside prisons. They document how from West Africa to Southeast Asia, targeting prisons systems in this way has continued to be a priority for the Islamic State and other jihadi groups. "In planning these types of attacks," they write, "jihadis are interested in restoring their force size, releasing incarcerated jihadi leaders or specialists, and/or creating a propaganda win."

Paul Cruickshank, *Editor in Chief*

CTCSENTINEL

Editor in Chief
Paul Cruickshank

Managing Editor
Kristina Hummel

CONTACT

Combating Terrorism Center
U.S. Military Academy
607 Cullum Road, Lincoln Hall
West Point, NY 10996
Phone: (845) 938-8495
Email: sentinel@westpoint.edu
Web: www.ctc.usma.edu/sentinel/

SUBMISSIONS

The *CTC Sentinel* welcomes submissions. Contact us at sentinel@westpoint.edu.

Cover: A supporter of Lebanon's Iran-allied Hezbollah movement with a Farsi inscription reading "Revenge Severely" written on her palm, holds a picture of Qassem Soleimani, commander of the Quds Force of the Iranian Revolutionary Guard, who was killed in a U.S. airstrike in Baghdad, as she attends a mass rally and a televised speech by Hezbollah Secretary-General Hassan Nasrallah. (Marwan Naamani/picture alliance via Getty Images)

"Fighters Without Borders"—Forecasting New Trends in Iran Threat Network Foreign Operations Tradecraft

By Matthew Levitt

The threats to U.S. interests in the Middle East, and possibly in the U.S. homeland, increased in the wake of the January 3, 2020, U.S. drone strike that killed Islamic Revolutionary Guard Corps Quds Force chief General Qassem Soleimani and Iraqi Shi`a militia commander Abu Mahdi al-Muhandis. While the primary overt objective of Iran and its proxies post-Soleimani will likely be to push all U.S. military forces out of Iraq and the region, they will undoubtedly also want to avenge Soleimani's death. And as Hezbollah leader Hassan Nasrallah has made clear, all Iranian proxy militant groups will be expected to play their parts in this campaign. When they do, Iran and the foreign legion of Shi`a proxies at its disposal are likely to employ new types of operational tradecraft, including deploying cells comprised of operatives from various proxy groups and potentially even doing something authorities worry about but have never seen to date, namely encouraging Shi`a homegrown violent extremist terrorist attacks.

Speaking in the wake of the January 3, 2020, U.S. drone strike in Baghdad that killed the commander of Iran's Quds Force, Major General Qassem Soleimani, Hezbollah Secretary-General Hassan Nasrallah made clear that the response to the Soleimani assassination would be carried out by the full range of Shi`a militant groups beholden to Iran far into the future.[1] In the post-Soleimani era, Nasrallah intimated, operations by Iran and its web of proxy groups would also deviate from traditional tactics. "Whoever thinks that this dear martyrdom will be forgotten is mistaken, and we are approaching a new era," he said.[2]

To be sure, much of the established *modus operandi* honed over years of training and practice by the Quds Force and Hezbollah will continue to feature prominently in Iranian and Iranian proxy operations.[3] But Nasrallah's vague pledge to modernize begs the question: What might be expected of a "new era" of international operations carried out by Iran and its proxy forces?

One difference from past operations is opportunistic—prioritizing the effort to push U.S. forces out of the Middle East. Iran will likely leverage Soleimani's assassination to achieve with his death what he aspired toward but failed to achieve in life. Another departure is more strategic— further solidifying the network of Shi`a militant groups Soleimani quilted together under the Quds Force. Iranian Supreme Leader Ali Khamenei has described the Quds Force as Tehran's "fighters without borders," but given the Quds Force's control of this network of Shi`a foreign fighters, the term more aptly applies to the Quds Force and the Shi`a militant networks under its control.[4] Hezbollah has already stepped in to help guide Iraq's various Shi`a militias, at least temporarily.[5] Other changes will likely be tactical, increasingly focused on trying to enhance operational security and the potential to carry out terrorist operations with reasonable deniability.

This article focuses on the areas of tactical adjustment that the Quds Force, Hezbollah, and other Shi`a militant groups might make to enhance their international terrorist attack capabilities. First, the article explains why U.S. authorities are so animated by the potential threat of a terrorist attack against U.S. interests, possibly in the homeland, following the Soleimani drone strike. Second, it forecasts and assesses in turn two specific lines of operational effort that authorities fear Iran and its proxies (led by the Quds Force and Hezbollah) are developing for future operations:

(a) Deploying teams including non-Iranian and non-Lebanese Shi`a militants from around the world and representing a variety of Iranian proxy groups to carry out international terror operations at Iran's behest; and

(b) Developing and encouraging a terrorist trend common in the world of Sunni extremism but not yet seen in the context of Shi`a extremism—Shi`a homegrown violent extremism (HVE).

The Threat to the United States

U.S. law enforcement and intelligence agencies long assessed that Iran and its proxy groups were unlikely to carry out an attack in the U.S. homeland, unless the United States took direct action undermining their interests.

For example, a 1994 FBI report, issued in the wake of the Hezbollah bombing targeting the AMIA Jewish community center in Buenos Aires a few months earlier, downplayed the likelihood of Hezbollah attacking U.S. interests, unless the United States took actions directly threatening Hezbollah. "The Hezbollah leadership, based in Beirut, Lebanon, would be reluctant to jeopardize the relatively safe environment its members enjoy in the United States by committing a terrorist act within the U.S. borders," it assessed. "However, such a decision could be initiated in reaction to a perceived threat from the United States or its allies against Hezbollah interests."[6]

In 2002, the FBI informed the Senate Select Committee on Intelligence that while "many Hezbollah subjects based in the United States have the capability to attempt terrorist attacks here should

Dr. Matthew Levitt is the Fromer-Wexler fellow and director of The Washington Institute's Reinhard Program on Counterterrorism and Intelligence. He has served as a counterterrorism official with the FBI and Treasury Department, and is the author of Hezbollah: The Global Footprint of Lebanon's Party of God. *He has written for* CTC Sentinel *since 2008. Follow @Levitt_Matt*

this be the desired objective of the group," Hezbollah had never carried out an attack in the United States and its extensive fundraising activities in the United States would likely serve as a disincentive for simultaneous operational activities.[7]

But over the past few years, well before the Soleimani hit, authorities disrupted Iranian and Hezbollah operations here in the United States that have forced them to reconsider longstanding assessments of the possibility that either a state or non-state group might seriously consider carrying out an attack in the homeland.[8]

In fact, in 2012, Iranian-American used car salesman Mansour Arbabsiar pleaded guilty to plotting the previous year with Iranian agents to assassinate the Saudi ambassador to the United States in Washington, D.C.[9] This was not the first time Iran plotted an attack in the United States, but it was the most spectacular and came at a time when few analysts assessed Iran would consider such an operation.[10] In the wake of that case, then Director of National Intelligence James Clapper testified before Congress that the plot "shows that some Iranian officials—probably including Supreme Leader Ali Khamenei—have changed their calculus and are now more willing to conduct an attack in the United States in response to real or perceived U.S. actions that threaten the regime."[11]

U.S. officials further worried that Hezbollah's calculus may have begun to shift in early 2015, when it became a matter of public record that the February 2008 assassination of Imad Mughniyeh, the founding leader of Hezbollah's Islamic Jihad Organization terrorist network, was a joint U.S.-Israeli operation.[12] Hezbollah printed a deck of playing cards featuring Israeli leaders it held responsible for Mughniyeh's death, which some described as a hit list.[13] Might Hezbollah now seek to avenge Mughniyeh's death by attacking American officials too? As Matthew Olsen, the director of the National Counterterrorism Center (NCTC) at the time, testified just five months before Mughniyeh was killed: "Lebanese Hezbollah remains committed to conducting terrorist activities worldwide. … We remain concerned the group's activities could either endanger or target U.S. and other Western interests."[14]

Then, in June 2017, the FBI arrested two alleged Hezbollah operatives, Ali Kourani and Samer El Debek, for carrying out surveillance of U.S. targets in the United States.[15] "While living in the United States, Kourani served as an operative of Hezbollah in order to help the foreign terrorist organization prepare for potential future attacks against the United States," U.S. Assistant Attorney General for National Security John C. Demers said. These included buildings housing the FBI and U.S. Secret Service in Manhattan, as well as New York's JFK airport and a U.S. Army Armory. Kourani was tried, convicted, and sentenced to 40 years.[16] El Debek has yet to stand trial.

Four months after the arrests, in October 2017, then director of NCTC Nicholas Rasmussen told reporters that Hezbollah was "determined to give itself a potential [U.S.] homeland option as a critical component of its terrorism playbook." "This is something that those of us in the counter-terrorism community take very, very seriously," he added.[17]

Kourani described himself as a Hezbollah sleeper agent. According to the FBI, Kourani informed that "there would be certain scenarios that would require action or conduct by those who belonged to the cell." Kourani reported Hezbollah operatives like him would be called upon to act in the event that the United States and Iran went to war, or if the United States were to take certain unnamed actions targeting Hezbollah, Nasrallah himself, or Iranian interests. Kourani added that "in those scenarios the sleeper cell would also be triggered into action."[18]

In September 2019, the FBI arrested Ali Saab, an alleged Hezbollah operative who underwent military and bomb-making training in Lebanon and later collected intelligence on potential targets in New York, Boston, and Washington, D.C. Saab allegedly provided details on targets including the United Nations headquarters, Statue of Liberty, and New York airports, tunnels, and bridges—including detailed photographs and notes on structural weaknesses and "soft spots" for potential Hezbollah targets "in order to determine how a future attack could cause the most destruction," according to the U.S. Department of Justice.[19] Saab has yet to stand trial.

The U.S. assassination of Soleimani and Abu Mahdi al-Muhandis (aka Jamal Jaafar Ibrahimi), the leader of the Iraqi Shi`a militant group Kata'ib Hezbollah who was with Soleimani at the time, appears to meet the standard Kourani described for potential Hezbollah terrorist action, namely U.S. action directly targeting a senior Iranian official, according to the assessment of this author. As such, it is not surprising that in the wake of the Soleimani assassination, Hezbollah's threat rhetoric took a sudden and sharp shift away from focusing primarily on Israeli targets. "America is the number one threat," Nasrallah announced after the drone strike that killed Soleimani, adding that "Israel is just a military tool or base."[20]

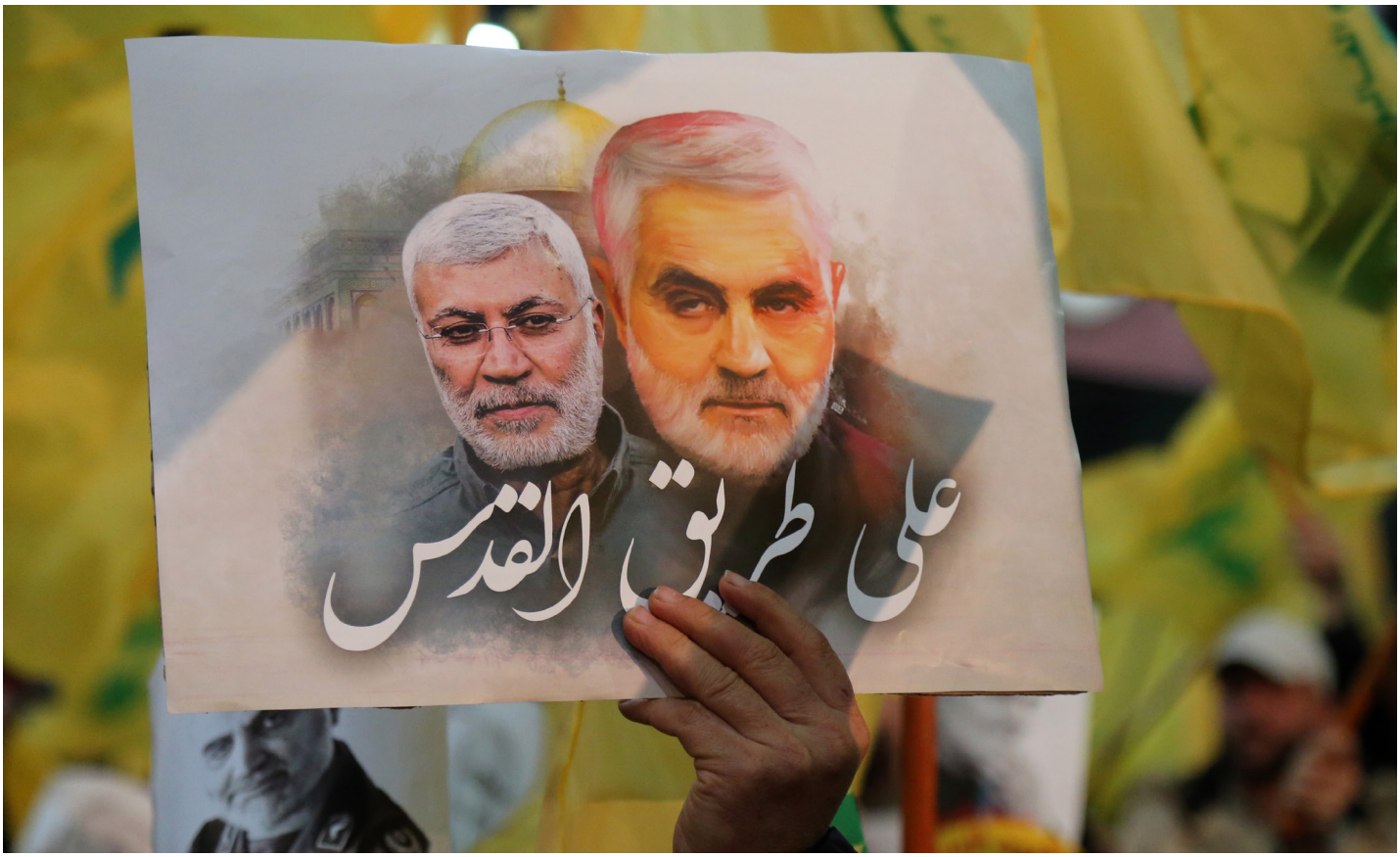
It seems clear that the primary overt objective of Iran and its proxies post-Soleimani will be to push all U.S. military forces out of Iraq and out of the Middle East. Nasrallah made this clear, warning that this included "the U.S. military bases, the U.S. warships, every single U.S. officer and soldier in our region, in our countries and on our territories."[21] And he intimated at how Hezbollah could help evict U.S. forces from the region, boasting that "[t]he suicide attackers who forced the Americans to leave from our region in the past are still here and their numbers have increased."[22]

While stating that his threats did not apply to American civilians in the region, Nasrallah warned that when it came to U.S. soldiers and officials, "the only alternative for them to be leaving horizontally [in coffins] is for them to leave vertically, on their own."[23]

Iran and its proxies will also want to avenge Soleimani's death, possibly by targeting a senior U.S. official in response to the assassination of one of their own (an option Nasrallah has publicly downplayed)[24] or by executing some other type of reasonably deniable asymmetric attack.

Indeed, deniability is also important politically. Iran and its proxies will want to be especially careful not to be tied to any action that might stem the flow of anti-American momentum Tehran feels it has at its back, in Iraq in particular, following the Soleimani strike. Neither Iran nor Hezbollah wants direct conflict with the United States,[a] and in the wake of the Soleimani hit, they have to take seriously U.S. threats to retaliate harshly for any attack on

a In the September 2019 issue of this publication, then Acting Director of National Intelligence Joseph Maguire stated, "We assess that Iran will do everything they can not to go into a conventional conflict with the United States because they realize they cannot match the United States in its conventional capability." Paul Cruickshank and Brian Dodwell, "A View from the CT Foxhole: Joseph Maguire, Acting Director of National Intelligence," *CTC Sentinel* 12:8 (2019).



A Hezbollah supporter holds a picture of Qassem Soleimani, the Iranian IRGC commander killed in a U.S. drone strike, right, as Hassan Nasrallah, leader of Hezbollah, delivers a televised speech, in Beirut, Lebanon, on January 5, 2020. (Hasan Shaaban/Bloomberg via Getty Images)

American citizens.[b]

U.S. law enforcement and intelligence fear Iran and its proxies may well decide to carry out a terrorist attack to avenge the Soleimani strike, a fact which explains why the day after the strike, the U.S. Department of Homeland Security (DHS) issued a bulletin under its National Terrorism Advisory System warning that "Iran likely views terrorist activities as an option to deter or retaliate against its perceived adversaries. In many instances, Iran has targeted United States interests through its partners such as Hezbollah."[25] Following the January 8, 2020, Iranian missile attack on military bases used by U.S. forces in Iraq, former FBI deputy director Andrew McCabe warned of the potential for terrorist attacks by Iran and its proxies—even in the U.S. homeland—in a *Washington Post* editorial entitled "If you think Iran is done retaliating, think again."[26]

One consequence of the Soleimani assassination may be a weakening of Iranian command and control over its various proxies, which were never a uniform bloc of groups equally committed to taking orders from Tehran to begin with.[27] But even among those groups most closely aligned with the Quds Force, like Lebanese Hezbollah and Kata'ib Hezbollah in Iraq, the loss of Soleimani—a charismatic leader beloved by Shi`a militia foot soldiers and commanders alike—means the Quds Force is now likely to be run by committee with a few more senior commanders and experienced managers collectively trying to take on the many roles previously filled singularly by Soleimani.[28] Soleimani played a hands-on role, involving himself personally in key operations, building rapport and personal bonds with militia commanders, and mediating disputes over prestige or money when those arose among Khamenei's fighters without borders.[29] Lacking the personal touch Soleimani contributed to the command and control of these groups, it is not clear that even if Iran wanted to stop one of its proxy groups from carrying out a terrorist attack it would be in a position to do so. Kata'ib Hezbollah, in particular, is likely to seek vengeance for the assassination of its leader, Abu Mahdi al-Muhandis, whose intimate ties to the Quds Force and Hezbollah go back decades.[30]

The International Terror Threat from Iran's Shi`a Liberation Army

All this begs the question: what might a "new era" of international terror operations carried out by Iran's "fighters without borders" look like?

A series of arrests of Hezbollah operatives around the world over the past few years—including the three U.S. cases noted above and others in Cyprus, Thailand, France, and Peru—collectively exposed a significant amount of information on the *modus operandi*

b On January 4, 2020, President Trump tweeted that the United States would target 52 Iranian sites if Tehran struck any American or American assets. See Donald J. Trump, "....targeted 52 Iranian sites (representing the 52 American hostages taken by Iran many years ago) ..." Twitter, January 4, 2020.

of Hezbollah's covert operations.[31] But these cases, some of which only came to light recently, are most revealing about how Hezbollah operated a decade ago, when the operational activities largely took place.

Iranian agents and Hezbollah operatives will undoubtedly play central roles in this new strategy, but they will not, according to the aspirations of Hezbollah's leader, be acting alone. "Meting out the appropriate punishment to these criminal assassins … will be the responsibility and task of all resistance fighters worldwide," Nasrallah said on January 3, 2020, shortly after the Soleimani strike. "We will carry a flag on all battlefields and all fronts and we will step up the victories of the axis of resistance with the blessing of his [Soleimani's] pure blood," he added.[32]

One option law enforcement officials assess the Quds Force, Hezbollah, and other elements of Iran's threat network could employ would be to draw upon the deep bench of Shi`a militants across the spectrum of Iran's Shi`a proxy groups to carry out terrorist operations. There is ample literature discussing Iran's ability to deploy Shi`a militia fighters to other battlefields in the region,[33] but this new concern focuses on Iran's ability to deploy select Shi`a militia operatives not to fight in other regional conflicts but to carry out acts of international terrorism.

In a Joint Intelligence Bulletin issued days after Soleimani was killed, the U.S. intelligence community warned that if Iran decided to carry out a retaliatory attack in the United States, it "could act directly *or enlist the cooperation of proxies and partners* [emphasis added by the author], such as Lebanese Hezbollah."[34]

Security officials worry that the next "Hezbollah" attack in the West, or infiltration across Israel's northern border, could be carried out by non-Iranian, non-Lebanese operatives within these proxy and partners groups from Iraq, Afghanistan, Pakistan, the Gulf States, or elsewhere. As Nasrallah himself said in a speech following Soleimani's death, "the rest of the Axis of Resistance must begin operations," implying that the burden of exacting a price for the Soleimani assassination cannot be carried by Hezbollah alone.[35]

Hezbollah trained many of these Shi`a militants in the first place, typically in training sessions lasting 20-45 days (though some received additional specialized training), and then fought with them on the battlefield in Syria.[36] The Quds Force and Hezbollah are well-placed to spot exceptional candidates, provide them specialized training in terrorist tactics and operational security, and dispatch them to carry out attacks in an effort to hide their own ties to such actions. This may create dangers for Americans on U.S. soil and overseas. The NCTC reported in October 2019, "Iran and Hezbollah's ongoing efforts to expand their already robust global networks also threaten the homeland."[37] Outside the United States, through the Quds Force and Ministry of Intelligence and Security (MOIS), Iran also "maintains links to terrorist operatives and networks in Europe, Asia and Africa that could be called upon to target U.S. or allied personnel."[38]

In 2016, an IRGC general first used the term "Shi`a Liberation Army" in reference to the Fatemiyoun brigade of Afghan Shi`a militants fighting on Iran's behalf in Syria. "The upside of the recent [conflicts] has been the mobilization of a force of nearly 200,000 armed youths in different countries in the region," the commander of the IRGC said that same year.[39] Soleimani invested much time and effort building up and coordinating the mix of Shi`a violent extremist groups, which, despite having their own identities and local grievances, have bonded together in an informal web of relationships serving as proxy agents for Iran. U.S. officials often refer to this as the Iran Threat Network, or ITN.

Syria served not only as an operational training ground but as a finishing school for operational tradecraft for this Shi`a foreign legion, providing Iran a deep bench of experienced militants from among whom it could spot potential candidates for terrorist operations training. Even just a few years ago, until the wars in Syria and Iraq, Iran had no such option. As Colin Clarke and Phillip Smyth noted in November 2017:

> *The wars in Syria and Iraq have given Iran the opportunity to formalize and expand networks of Shi`a foreign fighters throughout the region. Units of Shi`a militants from Syria, Lebanon, and Iraq are undergoing a transformation into a "Hezbollah"-style organization that is loyal to Iran and willing to fight alongside Iranian troops and advisers. Meanwhile, Afghan and Pakistani Khomeinist networks have been reformed to supply thousands of fighters who can be used as shock troops on battlefields stretching from the Middle East to South Asia.*[40]

To be sure, the U.S. intelligence community has given considerable attention to Iran's proxy relationships. In November 2019, for example, the Defense Intelligence Agency (DIA) released a report entitled *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance*. According to the report,

> *Through the IRGC-QF, Iran provides its partners, proxies, and affiliates with varying levels of financial assistance, training and materiel support. Iran uses these groups to further its national security objectives while obfuscating Iranian involvement in foreign conflicts. Tehran also relies on them as a means to carry out retaliatory attacks on its adversaries. Most of these groups share similar religious and ideological values with Iran, particularly devotion to Shia Islam and, in some cases, adherence to velayat-e faqih* [Rule of the Jurisprudent].[41]

The support Tehran provides these groups includes "facilitating terrorist attacks," the DIA reported. "These partner and proxy groups provide Iran with a degree of plausible deniability, and their demonstrated capabilities and willingness to attack Iran's enemies serve as an additional deterrent."[42] The DIA assessed in late 2019 that "Tehran is likely to continue using these fighters in Syria," but added that "it remains unclear if there are plans to deploy them to other locations."[43]

Whether or not Iran decides to dispatch Afghan Fatemiyoun, Pakistani Zainabiyoun, or Iraqi Heidariyun Shi`a militants[c] to other regional battlefronts such as Israel's norther border or Yemen, it could select the *crème de la crème* from these militias for specialized terrorist operations training, much as Hezbollah has hand-

c Heidariyun is an umbrella term used to connote Shi`a militants from Iraq employed by Iran to support its operations in Syria. The U.S. Treasury Department describes the Fatemiyun as "an IRGC-QF-led militia that preys on the millions of undocumented Afghan migrants and refugees in Iran, coercing them to fight in Syria under threat of arrest or deportation." It describes Zeinabiyun as "Syria-based, IRGC-QF-led militia, composed of Pakistani fighters mainly recruited from among undocumented and impoverished Pakistani Shiite immigrants living in Iran." See *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance* (Washington, D.C.: Defense Intelligence Agency, November 2019), p. 61, and "Treasury Designates Iran's Foreign Fighter Militias in Syria along with a Civilian Airline Ferrying Weapons to Syria," U.S. Treasury Department, January 24, 2019.

picked militia fighters for its Islamic Jihad Organization terrorist operations.[44] As a report by the International Institute for Strategic Studies in London noted, "an essential function that Hizballah has performed on behalf of Iran in the management and mentoring of many of Tehran's Arab partners. Indeed, the organization has become a central interlocutor for an array of Arab militias and political parties that have sectarian and ideological, or simply opportunistic, ties to Tehran."[45] Today, Hezbollah performs such a function for a wider spectrum of Shi`a militant groups beholden to Iran, such as the Shi`a militia groups in Iraq.[46] [d]

To a significant degree, deploying terrorist attack cells with personnel drawn from various components of Iran's network of proxies would mark a return to old tradecraft. Consider, for example, the Iranian-directed plots targeting Kuwait in the mid-1980s. The first in this string of attacks were the December 12, 1983, bombings at the American and French embassies in Kuwait, at the Kuwaiti airport, near the American Raytheon Corporation's grounds, at a Kuwait National Petroleum Company oil rig, and at a government-owned power-station. A seventh bomb, outside a post office, was diffused.[47] Six people were killed, and some 87 were injured in the attacks.[48] The string of well-coordinated bombings, which occurred within a span of two hours, were executed at Iran's behest by Lebanese and Iraqi Shi`a militants—including Lebanese Hezbollah's Mustapha Badreddine and Abu Mahdi al-Muhandis, then of the Iraqi Dawa Party[e] (who, according to the United States and Kuwait, helped plan the Kuwait attacks[49] and, as already outlined, was killed in January 2020 alongside Soleimani). The nature of the attack provided Iran grounds for plausible deniability. Iran denied any involvement in the plots, insisting that "attribution of these attacks to Iran is part and parcel of a comprehensive plot by the United States of America and its agents against the Islamic revolution."[50]

Iran has already found creative new ways to use its Shi`a militia proxies for unorthodox purposes, such as deploying Shi`a fighters to break up anti-regime demonstrations in Iran in November 2019.[51] The month before, Iran-backed militia snipers were deployed to Baghdad during anti-government protests there.[52]

And there is already evidence that Iran and Hezbollah have been moving in this direction. For several years now, Hezbollah has been actively recruiting and deploying dual-nationals—from the United States, Canada, France, Sweden, Great Britain, and Australia, among other countries—who are able to travel for operational purposes on their non-Lebanese passports.[53] For example, Ali Kourani traveled from New York to China on his U.S. passport to negotiate a deal to buy ammonium-nitrate ice packs of the kind Hezbollah uses to construct bombs.[54] And Samer El Debek allegedly traveled to Thailand to remove explosive precursor materials from a compromised Hezbollah safe house, and to Panama where he allegedly conducted preoperational surveillance of American, Israeli, and Panamanian targets.[55]

More recently, an article in *Le Figaro* reported that Hezbollah has begun recruiting operatives with non-Lebanese profiles in the wake of exposures of its Lebanese operatives traveling on non-Lebanese passports. According to this report, in August 2019, a Pakistani suspected of being a Hezbollah operative was questioned by authorities in Thailand. Dozens of operatives with non-Lebanese profiles, including Shi`a from Pakistan and Afghanistan, have been recruited by Hezbollah for foreign operations, and are often deployed using cover stories as tourists, the report stated.[56] Another cover involves recruiting Lebanese who have lived somewhere abroad for a long time. In July 2019, Ugandan authorities arrested a Lebanese national who had lived in the country since 2010 on suspicion of being an undercover Hezbollah agent.[57]

Again, there is precedent for Hezbollah recruiting non-Lebanese operatives. According to a 1994 FBI report, "an Iraqi-born Shia cleric, who is based in Texas, has positioned himself in a leadership role of Hezbollah in the United States."[58]

The Quds Force has also begun to recruit non-Iranian Shi`a operatives for espionage and terrorist missions abroad. In January 2019, German authorities arrested a dual Afghan-German citizen, who worked as a translator and advisor for the German army, on charges of spying for Iran.[59] In another case, Dutch authorities accused Iran of hiring local criminals to assassinate Iranian dissidents in the Netherlands.[60] And in December 2019, a Swedish court convicted an Iraqi man on charges of spying for Iran, including "gathering information on Iranian refugees in Sweden, Denmark, Belgium and the Netherlands."[61] Iran recruited an African rebel to build up pro-Iranian terror cells in Central Africa,[62] and in June 2019, Israeli authorities arrested a Jordanian national on espionage charges for trying to recruit people in the West Bank to spy on Israel for Iran.[63]

By deploying members of its foreign legion of proxy groups, its "fighters without borders," Iran (and Hezbollah) seeks "to anonymize its action in order to conduct its operations without being directly implicated."[64] To that end, authorities are concerned about another possible new trend in Iran Threat Network mobilization—one that to date has never occurred, but nonetheless has the attention of U.S. officials.

Inspiring Lone Offenders: Shi`a HVE?

Testifying before the House Judiciary Committee on February 5, 2020, FBI Director Christopher Wray underscored that the international terrorist threat to the United States had "expanded from sophisticated, externally directed FTO [foreign terrorist organization] plots to include individual attacks carried out by HVE [homegrown violent extremists] who are inspired by designated terrorist organizations."[65] These lone offenders present unique challenges to law enforcement, due to their lack of ties to known terrorists, easy access to extremist material online, ability to radicalize and mobilize to violence quickly, and use of everyday communication platforms that utilize end-to-end encryption. While Director Wray highlighted the particular success the Islamic State has demonstrated in leveraging digital communications to draw lone offenders to

d As a point of comparison, two key things that led to the development and rise of al-Qa`ida were the experience its recruits gained in an active combat zone (i.e., Afghanistan) and the group's ability to offer broad and specialized training at scale. The specialized training also created an opportunity for al-Qa`ida to talent spot. Today, a similar dynamic can be seen in the context of Iran's IRGC, Hezbollah, and related Shi`a militant proxies, specifically experience in a conflict zone, large numbers, and robust training infrastructure.

e Founded in the 1950s, the Iraqi Dawa Party opposed the Baathist regime that came to power in 1968, and after 1979 Iranian revolution, a faction of the party formed a military wing based in Iran to target the Iraqi regime. This wing, tied to the Supreme Council for the Islamic Revolution in Iran (SCIRI), subscribed to the Khomeinist ideology of waliyat-e-faqih, and formed close ties to Lebanese Hezbollah. After the fall of the Saddam regime, the Dawa Party entered the Iraqi political scene. See Joel Wing, "A History of Iraq's Islamic Dawa Party, Interview With Lowy Inst. for Intl. Policy's Dr. Rodger Shanahan," Musings on Iraq, August 13, 2012, and Ali Latif, "The Da'wa Party's Eventful Past and Tentative Future in Iraq," Carnegie Endowment for International Peace, August 19, 2008.

its ideology, he noted that many other terrorist organizations reach out to people who may be "susceptible and sympathetic to violent terrorist messages." In fact, law enforcement agencies are confronting "a surge in terrorist propaganda and training available via the Internet and social media."[66]

Today, Iran's Quds Force and other Shi`a extremist terrorist groups are disseminating extremist material online. This trend has the attention of U.S. law enforcement and intelligence officials, who have warned that one possible "catalyzing event" for Shi`a HVE plotting in the United States would be if "radicalizing enablers" began actively "amplifying anti-US and pro-Shia rhetoric among audiences in the US."[67]

Indeed, within 24 hours of the Soleimani drone strike, DHS released a bulletin under its National Terrorism Advisory System warning of potential Iranian or Iranian-inspired plots against the homeland. The bulletin stressed the Department had no information regarding any specific, credible threat to the homeland, but advised that "Homegrown Violent Extremists could capitalize on the heightened tensions to launch individual attacks," adding that "an attack in the homeland may come with little or no warning."[68]

A few days later, DHS, FBI, and NCTC released a joint intelligence bulletin advising federal, state, local, and other counterterrorism and law enforcement officials and private sector partners "to remain vigilant in the event of a potential [Government of Iran] GOI-directed *or violent extremist GOI supporter threat* to US-based individuals, facilities, and [computer] networks" [emphasis added by the author].[69] The report warned not only of Iranian-directed plots—including both lethal attacks and cyber operations—but also of attacks by supporters of Iran inspired to carry out attacks on their own.

Concern within the U.S. counterterrorism community over the prospect of Shi`a HVE attacks predates the Soleimani strike. The intelligence community has given the prospect of Shi`a HVE violence some thought, and NCTC defines Shi`a HVEs as "individuals who are inspired or influenced by state actors such as Iran, foreign terrorist organizations such as Hezbollah, or Shia militant groups but who do not belong to these groups and are not directed by them."[70]

In an October 2018 analytical report, the product of a structured analytic brainstorming session, entitled "Envisioning the Emergence of Shia HVE Plotters in the US," NCTC explained that although there have been no confirmed cases of Shi`a HVE plotting attacks in the United States, analysts identified several enabling factors that would increase the likelihood of Shi`a HVEs mobilizing to violence.[71] The first is the occurrence of a "catalyzing event" such as "direct U.S. military action in Iran, sustained U.S. operations against Hezbollah in Lebanon or Syria, or the assassination of a senior Iranian or Hezbollah leader perceived to have U.S. involvement." These events would be sufficiently significant, the analysts assessed, to "push some U.S. Shia to radicalize and consider retaliatory violence." Such a scenario may have been theoretical conjecture at the time, but the assassinations of Soleimani and al-Muhandis surely, in this author's assessment, meet this bar.[72]

For Shi`a HVE mobilization in the United States to occur, the U.S. intelligence analysts assessed, some combination of a series of other boxes would also have to be checked. Some of these boxes have been checked in the past without Shi`a HVE mobilization, but the analysts noted that "repeat occurrences of such incidents could contribute to or spark radicalization." The analysts added that these include catalyzing events other than U.S. military action, such as Shi`a leaders and clerics calling for violence in the United States; Israeli or Sunni Arab government lethal operations targeting Iran, Hezbollah, or other Shi`a; or anti-Shi`a activity in the United States.[73]

The potential for Shi`a HVE mobilization to violence increases, the report continued, if the catalyzing event occurred in conjunction with "radicalization enablers." Such enablers could include, for example, charismatic U.S.-based radicalizers, perhaps people who have fought with Hezbollah or other Shi`a militant groups overseas, promoting Shi`a grievances and advocating attacks. Alternatively, social-media influencers tied to Iran or Hezbollah or independent Shi`a websites promoting Shi`a grievances could conduct influence operations intended to sow discord among Shi`a in the United States and mobilize them to violence. The NCTC report notes, for example, the pro-Hezbollah "Electronic Resistance" social media outfit, which supports Hezbollah but is not controlled by it and which spreads Shi`a extremist material online. NCTC refers to these as "Shi`a cyber actors."[74] If Shi`a media, which is dominated by Iran and its proxies, began to open sanction retaliatory violence, that too, according to the NCTC report, would serve as an enabling factor for Shi`a HVE mobilization.

As it happens, Iran runs extensive digital influence operations, including using Instagram accounts to spam the White House and Trump family after the Soleimani assassination with images of coffins draped in U.S. flags with the caption "prepare the coffins."[75] Iran's IRGC also disseminates its ideological training materials online in Farsi. A new study by the Tony Blair Institute for Global Change details how IRGC ideological training documents "propagate the idea that there is an existential threat to Shiism and Shia Muslims from a '[Sunni] Arab-Zionist-Western axis.'" Among the report's key findings is that the worldview within which the IRGC ideological training is framed is extremist and violence. "It identifies enemies—from the West to Christians and Jews, to Iranians who oppose the regime—and advocates supranational jihad in the name of exporting Iran's Islamic Revolution."[76]

And there are signs that Shi`a militia groups themselves are producing material on social media aimed at radicalizing Shi`a and mobilizing them to violence. A tweet by a Kata'ib Hezbollah spokesperson on January 3, 2020, right after the Soleimani hit, encourages volunteers to undertake "martyrdom operations against invading Crusader foreign forces" by noting that the first to register would be the first to be martyred.[77] A post on Twitter dated February 5, 2020, shows a photograph of what it says is Kata'ib Hezbollah's registration form for those interested in carrying out suicide operations targeting U.S. forces in Iraq.[78]

A variety of factors inhibit the emergence of Shi`a HVE activity in the United States—not a single case of Shi`a HVE activity has been reported to date—including the fact that Shiism is hierarchical, and there is therefore an inherent disincentive to carrying out truly inspired, lone-offender attacks absent direction from senior Iranian, Hezbollah, or other authority figures. But in the event that radicalization enablers follow one or more catalyzing events, NCTC argued, these would "probably increase the number of Shia HVEs or accelerate their mobilization to violence by amplifying anti-US and pro-Shia rhetoric among Shia audiences in the US."[79]

In another scenario, Shi`a HVE mobilization would not necessarily have to start from zero. A case could be envisioned in which a member of the Shi`a community in the United States is self-rad-

icalized with the help of online extremist Shi`a messaging, but still more likely is that someone already involved with a Shi`a extremist group is mobilized to action on their own, independent of the organization.

Such concerns warrant attention, especially in light of the historical precedent. In August 1989, a Hezbollah operative died while preparing an explosive device in a London hotel.[80] Mustafa Mahmoud Mazeh intended to assassinate Salman Rushdie, the author whose 1988 publication, *The Satanic Verses*, prompted Ayatollah Khomeini to issue a *fatwa* condemning him to death.

A Lebanese citizen born in Guinea, Mazeh joined Hezbollah as a teenager. He visited the family village in Lebanon before making his way to England via The Netherlands. Later, in the context of discussing Khomeini's Rushdie *fatwa*, a Hezbollah commander told an interviewer that "one member of the Islamic Resistance, Mustafa Mazeh, had been martyred in London."[81] According to a 1992 CIA assessment, attacks on the book's Italian, Norwegian, and Japanese translators in July 1991 suggested "that Iran has shifted from attacking organizations affiliated with the novel—publishing houses and bookstores—to individuals involved in its publication, as called for in the original *fatwa*."[82] A shrine dedicated to Mazeh was erected in Tehran's Behesht Zahra cemetery with the inscription: "The first martyr to die on a mission to kill Salman Rushdie."[83]

Conclusion

Speaking at a ceremony marking the 40th day since Soleimani was killed, IRGC Commander Major General Hossein Salami warned both Israel and the United States, "If you make the slightest error, we will hit both of you."[84] A day earlier, Iran's foreign ministry released a statement—on February 12, 2020, the anniversary of Imad Mughniyeh's death—warning that "the Islamic Republic of Iran will give a crushing response that will cause regret to any kind of aggression or stupid action from this regime [Israel] against our country's interests in Syria and the region."[85]

In fact, it is likely that any Iranian international terror campaign in response to real or perceived action against its interests—be it the assassination of Qassem Soleimani in Iraq or airstrikes in Syria targeting Shi`a militias or weapons transfers destined for Hezbollah—would include actions taken by Shi`a militants of varying nationalities operating at Iran's behest. Under Soleimani, the Quds Force built up its Shi`a militant foreign legion, and as a consequence of their shared experience fighting in Syria and Iraq, these proxy groups are both battle-hardened and strongly committed to Iran. For many, fighting in Iran's foreign legion is all they have known for the past several years. It only makes sense for Iran to deploy these fighters to new theaters, be they battlefronts or terror networks. Doing so provides Iran with reasonable deniability, and enlisting operatives traveling on a variety of non-Lebanese and non-Iranian passports may allow them to fly under the radar of law enforcement and intelligence services. Indeed, as noted in this piece, both Hezbollah and Iran have already started using these kinds of operatives for terrorist missions, so there is every reason to think they will continue to do so. Hezbollah has groomed Shi`a militants from a wide range of groups, and law enforcement authorities now worry Iran may be actively pursuing a strategy of radicalizing and mobilizing lone offenders to carry out attacks of their own out of solidarity with, but without explicit foreign direction from Iran or Hezbollah.

But the most likely scenarios for near-term ITN operations targeting the United States or its allies involve attacks on U.S. and other forces in the region and a wide range of cyberattacks.[86] Iran and its proxies will undoubtedly look for opportunities to avenge the assassination of Qassem Soleimani. As counterterrorism officials try to forecast what new trends in Iranian and Hezbollah operational *modus operandi* might look like, they are increasingly focused on Iran's Shi`a Liberation Army, its "fighters without borders," and potentially seeking to radicalize lone actors—Shi`a HVEs—as tools Tehran could use to hide its fingerprints in any future attack on U.S. interests, in the region, or in the homeland. CTC

Citations

1 Sara Taha Moughnieh, "Sayyed Nasrallah: Suleimani Revenge is Long Track, Trump Biggest Liar in History of US Presidency," Al-Manar, January 14, 2020.
2 Ibid.
3 Matthew Levitt, "Hezbollah Isn't Just in Beirut. It's in New York, Too," *Foreign Policy*, June 14, 2019.
4 Maryam Sinaiee, "New Vice-Commander of Iran's Qods Force Signifies Khamenei's Message of 'Fighters without Borders,'" Radio Farda, January 20, 2020.
5 "Tehran-Backed Hezbollah Steps in to Guide Iraqi Militias in Soleimani's Wake," Reuters, February 11, 2020.
6 "International Radical Fundamentalism: An Analytical Overview of Groups and Trends," Terrorist Research and Analytical Center, Federal Bureau of Investigation, Department of Justice, November 1994, declassified on November 20, 2008.
7 "Answers to Questions for the Record from Assistant Attorney General Daniel J. Bryant to Senators Bob Graham and Richard Shelby," U.S. Senate Select Committee on Intelligence, July 26, 2002, Marked SSCI # 2002-3253; appended to printed edition of "Current and Projected National Security Threats to the United States," Hearing before the Select Committee on Intelligence of the United States Senate, 107th Congress, Second Session, February 6, 2002, p. 339.
8 Matthew Levitt, "Why Iran Wants to Attack the United States, *Foreign Policy*, October 29, 2012.
9 "Man Pleads Guilty in New York to Conspiring with Iranian Military Officials to Assassinate Saudi Arabian Ambassador to the United States," Department of Justice, October 17, 2012.
10 Matthew Levitt, "Tehran's Unlikely Assassins," *Weekly Standard*, August 20, 2012.
11 James R. Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," Hearing before the Senate Select Committee on Intelligence, National Counterterrorism Center, Office of the Director of National Intelligence, January 31, 2012, p. 5.
12 Adam Goldman and Ellen Nakashima, "CIA and Mossad Killed Senior Hezbollah Figure in Car Bombing," *Washington Post*, January 30, 2015.
13 Roee Nahmias, "Hezbollah Prepares Hit List to Avenge Mughniyeh Killing," Ynet News, September 15, 2010.
14 Matthew G. Olsen, "Worldwide Threats to the Homeland," Testimony before the House Committee on Homeland Security, September 17, 2014.
15 "Bronx Man and Michigan Man Arrested for Terrorist Activities on Behalf of Hizballah's Islamic Jihad Organization," U.S. Attorney's Office, Southern District of New York, U.S. Department of Justice, June 8, 2017.
16 "Hizballah Operative Sentenced to 40 Years in Prison for Covert Terrorist Activities on Behalf of Hizballah's Islamic Jihad Organization," U.S. Attorney's Office, Southern District of New York, U.S. Department of Justice, December 3, 2019.
17 Elise Labott and Laura Koran, "US officials warn of potential Hezbollah

threat to US homeland," CNN, October 11, 2017.
18 U.S. v Ali Kourani, U.S. District Court, Southern District of New York, Testimony of FBI Special Agent Keri Shannon, May 8, 2019, p. 236 of trial transcript.
19 "Manhattan U.S. Attorney Announces Indictment of New Jersey Man for Terrorist Activities on Behalf of Hizballah's Islamic Jihad Organization," U.S. Attorney's Office, Southern District of New York, U.S. Department of Justice, September 19, 2019.
20 Moughnieh.
21 Ibid.
22 Qasim Abdul-Zahra and Bassem Mrou, "Iraq Vote, Hezbollah Threat Leveled at US Troops in Mideast," Associated Press, January 5, 2020.
23 Moughnieh.
24 "Sayyed Nasrallah: Qassem Suleimani's Shoe is Worth Trumps Head (Video)," Al-Manar, January 6, 2020.
25 "Summary of Terrorism Threat to the U.S. Homeland," National Terrorism Advisory System Bulletin, U.S. Department of Homeland Security, January 4, 2020.
26 Andrew McCabe, "If You Think Iran is Done Retaliating, Think Again," *Washington Post*, January 9, 2020.
27 Becca Wasser and Ariane Tabatabai, "Iran's Network of Fighters in the Middle East Aren't Always Loyal to Iran," *Washington Post*, May 21, 2019.
28 Matthew Levitt, "The New Iranian General to Watch," Politico, January 23, 2020.
29 Ibid.; Ali Soufan, "Qassem Soleimani and Iran's Unique Regional Strategy," *CTC Sentinel* 11:10 (2018).
30 For background on Jamal Jaafar Ibrahimi, aka Abu Mahdi al-Muhandis, see "Jamal Jaafar Ibrahimi a.k.a. Abu Mahdi al-Mohandes," Counter Extremism Project.
31 See, for example, Matthew Levitt, "Hizb Allah Resurrected: The Party of God's Return to Tradecraft," *CTC Sentinel* 6:4 (2013) and Matthew Levitt, "Hezbollah Isn't Just in Beirut. It's in New York, Too," *Foreign Policy*, June 14, 2019.
32 "Hizbullah: Avenging Soleimani Responsibility of Resistance Worldwide," Naharnet, January 3, 2020.
33 Hanin Ghaddar ed., *Iran's Foreign Legion: The Impact of Shia Militias on U.S. Foreign Policy*, Policy Note 46, Washington Institute for Near East Policy, February 2018; Colin Clarke and Phillip Smyth, "The Implications of Iran's Expanding Shi'a Foreign Fighter Network," *CTC Sentinel* 10:10 (2017).
34 "Escalating Tensions Between the United States and Iran Pose Potential Threats to the Homeland," Joint Intelligence Bulletin, DHS, FBI, NCTC, January 8, 2020, at https://cdn.ymaws.com/members.iamu.org/resource/resmgr/informer_2019/JIB_Iran_1-8-20.pdf
35 Moughnieh.
36 *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance* (Washington, D.C.: Defense Intelligence Agency, November 2019), p. 61.
37 Acting NCTC Director Russell Travers, "Global Terrorism: Threats to the Homeland," Hearing before the House Committee on Homeland Security, National Counterterrorism Center, Office of the Director of National Intelligence, October 30, 2019.
38 Ibid.
39 For both quotes, see Nader Uskawi, "Examining Iran's Global Terrorism Network," Testimony submitted to the House Homeland Security Subcommittee on Counterterrorism and Intelligence, April 17, 2018.
40 Clarke and Smyth.
41 *Iran Military Power*, p. 33.
42 Ibid., p. 57.
43 Ibid., p. 61.
44 Matthew Levitt, "Hizballah and the Qods Force in Iran's Shadow War with the West," *Policy Focus* 123 (2013): p. 3.
45 "Iran's Networks of Influence in the Middle East, an IISS Strategic Dossier," International Institute for Strategic Studies, November 2019, p. 67.
46 "Tehran-Backed Hezbollah Steps in to Guide Iraqi Militias in Soleimani's Wake."
47 Haim Shaked and Daniel Dishon eds., *Middle East Contemporary Survey, vol III: 1983-84* (Boulder, CO: Westview Press, 1986), p. 405.
48 Ibid.; Judith Miller, "Driver in Embassy Bombing Identified as Pro-Iranian Iraqi," *New York Times*, December 17, 1983.
49 James Glanz and Marc Santora, "Iraqi Lawmaker was Convicted in 1983 Bombings in Kuwait that Killed 5," *New York Times*, February 7, 2007; Matthew S. Schwartz, Who Was The Iraqi Commander Also Killed In The Baghdad Drone Strike?, NPR, January 4, 2020.
50 "Iran Denies Kuwait Blast Role," *New York Times*, December 14, 1983.
51 "Iran-Backed Fighters Claim They Were Deployed Against Protestors in November," Radio Farda, February 4, 2020.
52 "Exclusive-Iran-Backed Militias Deployed Snipers in Iraq Protests-Sources," Reuters, October 17, 2019.
53 Matthew Levitt, "Hezbollah's Criminal and Terrorist Operations in Europe," AJC, September 2, 2018.
54 "USA v Ali Kourani, Complaint," Southern District of New York, Department of Justice, May 31, 2017.
55 "USA v Samer el Debek, Complaint," Southern District of New York, Department of Justice, May 31, 2017.
56 Nicolas Barotte, "Le Hezbollah cheche a constituer de nouvelle cellules dormantes a l'etranger," *Le Figaro*, January 23, 2020.
57 "Exclusive: Ugandan and Israeli Intelligence Unmask International Terrorist Plot in Uganda," Kampala Post, July 22, 2019.
58 "International Radical Fundamentalism: An Analytical Overview of Groups and Trends."
59 "Germany Charges Man with Spying for Iran," Associated Press, August 16, 2019.
60 Raf Sanchez, "Iran Hired Criminals to Assassinate Dissidents in the Netherlands, Dutch Government Claims," *Telegraph*, January 8, 2019.
61 David Keyton, "Sweden Sentences Iraqi Man of Spying for Iran," Associated Press, December 20, 2019.
62 Jack Losh, "Revealed: How Iran Tried to Set Up Terror Cells in Central Africa," *Telegraph*, January 11, 2020.
63 Judah Ari Gross, "Israel Says it Nabbed Iranian Spy in West Bank Trying to Build Espionage Network," *Times of Israel*, June 20, 2019.
64 Barotte.
65 Christopher Wray, "FBI Oversight," Testimony before the House Judiciary Committee, February 5, 2020.
66 Ibid.
67 "Envisioning the Emergence of Shia HVE Plotters in the US," NCTC Current, National Counterterrorism Center, October 16, 2018, at https://www.infragard-la.org/wp-content/uploads/2018/11/NCTC-U-FOUO-Envisioning-the-Emergence-of-Shia-HVE-Plotters-in-the-US.pdf
68 "Summary of Terrorism Threat to the U.S. Homeland."
69 "Escalating Tensions Between the United States and Iran Pose Potential Threats to the Homeland."
70 "Envisioning the Emergence of Shia HVE Plotters in the US."
71 Ibid.
72 Ibid.
73 Ibid.
74 Ibid.
75 Emerson T. Brooking and Suzanne Kianpour, "Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century," Atlantic Council, February 11, 2020.
76 Kasra Aarabi, "Beyond Borders: The Expansionist Ideology of Iran's Islamic Revolutionary Guard Corps," Tony Blair Institute for Global Change, February 4, 2020.
77 Abu Ali al-Askari, "Bring lightness and gravity, and put your money and yourselves …," Twitter, January 3, 2020, courtesy of Phillip Smyth.
78 Ali al-Iraqi, "In the name of Allah the Merciful, the architecture of the Elamam State …," Twitter, February 5, 2020, courtesy of Phillip Smyth.
79 "Envisioning the Emergence of Shia HVE Plotters in the US."
80 Anthony Loyd, "Tomb of the unknown assassin reveals mission to kill Rushdie," *Times* (London), June 8, 2005.
81 H. E. Chehabi and Rula Jurdi Abisaab, *Distant Relations: Iran and Lebanon in the Last 500 Years* (New York: St. Martin's Press, 2006), pp. 292-293.
82 "Iran: Enhanced Terrorist Capabilities and Expanding Target Selection," Central Intelligence Agency, April 1, 1992.
83 Loyd.
84 "Iran Says it Will Strike U.S. and Israel if They Make the 'Slightest Error,'" Reuters, February 13, 2020.
85 "Iran Vows 'Crushing Response' to Any Israeli Action against Regional Interests," Reuters, February 12, 2020.
86 Mark Mazzetti, Ronen Bergman, and Farnaz Fassihi, "How Months of Miscalculation Led the U.S. and Iran to the Brink of War," *New York Times*, February 13, 2020.

A View from the CT Foxhole: Brigadier General Dagvin R.M. Anderson, Commander, U.S. Special Operations Command Africa

By Jason Warner

Brigadier General Dagvin R.M. Anderson is the Commander, Special Operations Command Africa, headquartered at Kelley Barracks in Stuttgart, Germany, and is responsible for the full spectrum of special operations activities conducted throughout Africa. He leads more than 1,700 U.S. military, interagency, and international military personnel operating throughout Africa and Europe.

Brig. Gen. Anderson has participated in several contingencies to include Operations Provide Comfort, Deny Flight, Deliberate Guard, Allied Force, Enduring Freedom, and Iraqi Freedom.

Brig. Gen. Anderson holds a master's degree in International Public Policy from the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University. He was a Fellow at the Weatherhead Center for International Affairs, Harvard University, and was an Olmsted Scholar in the Czech Republic.

CTC: You previously served as the deputy director of operations for U.S. Indo-Pacific Command at Fort H.M. Smith in Hawaii, where, obviously, the focus was not on Africa. To what extent has your background and career, particularly your Special Operations career, informed how you approach this new geographic command?

Anderson: I spent three years in the Pacific—one year in Korea and then two years up at INDOPACOM—and that was quite valuable for me to see the other side of the world, literally. Fifty-two percent of the world is under INDOPACOM's AOR [area of responsibility]. To understand what we're up against when it comes to China, China's very much a threat to our way of life. I think that they are working very diligently to undermine the U.S.-led system, the Western way, including the economic system. They're looking to undermine that, to undo that system and replace it with an alternative that is very much in their favor. One of the things that the United States points to with great pride is that we have ensured peace and stability throughout the Indo-Pacific for over 70 years since World War II and created an environment that has allowed all nations in that region, including China, to prosper and to benefit.

That system being open and fair has allowed many nations to improve their positions in life, as they have economic growth: you can see it in Japan and Korea, and in China. Well, what that perspective gave me was that China is very much trying to undo that for their own gain. They try to break our alliances, break our partnerships in order to then leverage the partners individually, and the reason why that's important to what I'm doing now is that I see that model very much being exported into Africa. China's very good about getting into the international systems, using their leverage there to peel a few countries away to paralyze that international system, and then work very methodically in bilateral engagement, primarily through economic engagement, to then leverage those bilateral relationships to their advantage.

The PRC [People's Republic of China] has chosen to compete for natural resources, and to extract those resources for their own value. Obviously, there's lots of oil and natural gas; there's rare earth minerals that are vital to our technology sector on the continent; there's precious metals. These are things the other powers—China and Russia—are trying to corner the market on or to gain access [to]. There's also, if you look at the African continent, no matter which way you go, key passages that are important for our national security to ensure that we have, and that the world has, free access to—whether that's coming through the Straits of Gibraltar by Morocco, going through the Mediterranean down through the Suez Canal, or through the Red Sea out through the Bab al Mandab straits by Somalia. All of that is key terrain on key waterways. And then to go around the other way, the long way around Africa—obviously, a huge land mass—and being able to have the key ports where you can have your port calls for refueling, refitting, etc., are absolutely vital.

Africa sits on key terrain, and it's important that we engage. What I've seen is that all of these nations, pretty much every nation in Africa, has a concern about violent extremism and terrorism. And we bring great credibility and great value—Special Operations—to help them address that security concern. Being able to partner with them and address that security concern gives us access, gives us engagement opportunity and influence in order to then compete with these other global powers—China and Russia—to ensure we have access and the world has access to these resources as well that are vital to our economies.

CTC: Thinking about the general role of SOCAF on the continent, how do U.S. Special Operations work to uniquely meet the challenges that the United States and our partners face in Africa? To that end, what is your assessment of what African partners' special operations capabilities are and what needs they have?

Anderson: It varies. Africa is not monolithic. It's a single continent, but it's composed of multiple countries, multiple cultures, and multiple tribes with different ethnicities, so there's no blanket statement you could make that covers all of Africa, by any means. So I'll answer that by talking about a couple key partners that are, I think, exemplary of how the U.S. engages and what they need. I'll start in the east and talk about Kenya.

Kenya's been a very good partner for several years, a very competent country that is developing a capable military intelligence capability in order to counter a very existential threat right on their border, which is al-Shabaab. Obviously, Kenya is very interested in the stability of Somalia; that stability hinges on Somali ability

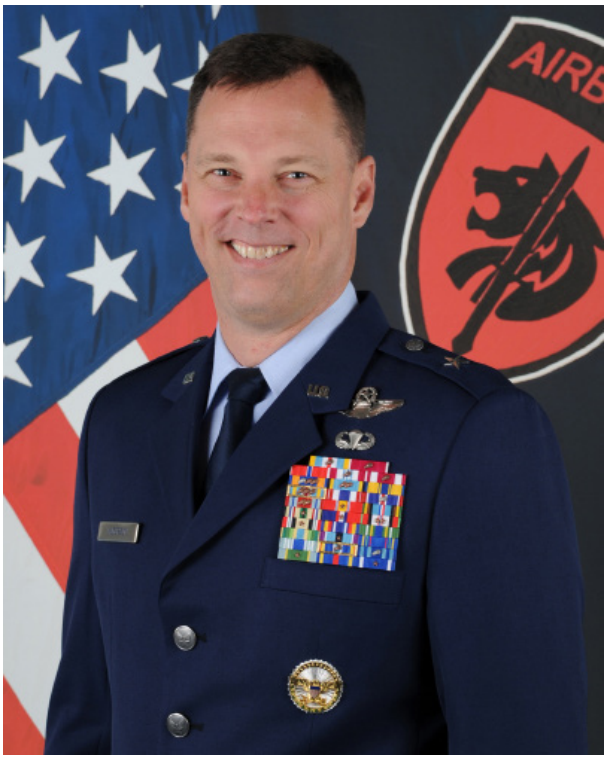
to deal with and contain and disrupt and degrade al-Shabaab. So what the Kenyans have done over time is they have built a capable military force to address that. They're also developing a border patrol capability that's coming on line and becoming more capable. They've really invested in intel fusion capability, and all that speaks to their will to engage and to improve. I think one of things it speaks of the most is that Kenya has been one of our most introspective partners, and they've actually taken a look at some of their mistakes—from Westgate through the [Garissa University College] attack they had a couple years later to the Dusit [D]2 [attack][1]—that Kenya has been willing to look at that and identify mistakes that they made or errors or gaps that they've had in their security capability, and then they've actually gone out and addressed [them].

That includes their integration between their military, civil, law enforcement, and their first responders, working with their medical response, because they understand that they have to be able to have a coherent, whole-of-government response to a terrorist attack and to prevent terrorist activity. They've done a lot of reflection on where they've made mistakes. They've been open, to some extent, to talking with other partners [about] where they could improve, and then making those improvements. Now, they've been incremental, but I think the Kenyans have done a very good job of doing that. Not many partners are willing to be that self-reflective. Kenya has really looked at how to improve the Kenya Ranger Regiment, how to improve their intelligence community, how to create a fusion cell. They developed an exploitation cell that is now becoming a highlight of their intelligence capability; they can actually take exploitable material off the battlefield and analyze that and turn that back into actionable intelligence and get that back to whether its border patrol, the police, or the military, to then take action on it.

To go back out to the west, I would say Niger is an example of a very willing partner. Niger is an incredibly poor country, a country that faces many challenges, a landlocked country that has a small economy, but what we see in Niger is a sense of pride in Niger, a national identity that transcends some of the tribal differences and grievances. They're able to come together, and we see a very willing partner when it comes to the CT fight. And while a great amount of illiteracy—around 70 percent of their population is illiterate—what we do see with their soldiers is they're very competent and capable, and while they may be illiterate, once you show them and teach them something, they retain it, they implement it, and they improve upon it so that we don't have to go back and retrain the unit skills we've taught. When we reengage with them, we can build on what they've already learned, and they quickly go out and apply that in the field. They're very aggressive about engaging in the CT fight, and they're very willing. And so again, I think Kenya and Niger are two good examples of where we see that will to actually go out and engage and then improve their forces, improve their capabilities.

I think the other piece is when you look at other partners, we bring that premium brand. The U.S. is the premier counterterrorism force. We've been doing this for several years, and we've perfected a lot of capabilities. We work with our partners to help them realize that it's more than just having a capable finish force that goes out and executes. It's also developing the intelligence capability as an interagency piece and the networking behind it that makes finish operations effective.

And regarding partners, we can't apply our standards to them. But when we give them key enablement and key training in some of these areas, we see results and we see them improve their ability.



Brigadier General Dagvin Anderson

I think one of the areas where we see that is Burkino Faso right now, where for a while they denied that they had a problem, but now as the northern province is collapsing and they are under great pressure, they've come to the realization that they need assistance. They've asked the United States, they've asked their Western partners, they've asked France, for assistance. And so we're doing some analysis on what we could do at a low level to enable them to be more effective and enable the European partners to engage and help assist the Burkinabe.

CTC: You gave some good examples of partners that are moving in the right direction, that have admirable outcomes. There's no need to single a particular country out, but are there particular areas that many countries in Africa need to improve on? Are there specific omissions or places for improvement that you see consistently needing work on across the continent?

Anderson: Where we see that countries have struggled is just identifying the threat, identifying they have a problem, and being able to articulate that. A lot of times, they're not willing to identify that problem because they see it as a weakness or they believe if they highlight that, that will reflect negatively on the government. Another issue that we see in many countries is they struggle with internal dynamics. This is what the VEOs [violent extremist organizations] often prey upon, the divisions within their cultures or within their nation. That could be tribal grievances that go back several years or issues between ethnicities or between the farmers and the herdsmen.

The same things are troublesome for the central government—are they able to provide government services to the different ethnicities so they feel part of that government? Or do they feel that the government is not taking care of them so they become vulnerable to the VEOs? We see that many of these countries are unable to

provide services outside the immediate surroundings of the capital and therefore they don't have legitimacy in the eyes of people in the farther regions of their country. That's true in many countries across the continent. Sometimes they have to work on those basic developmental issues and provide the government services—legitimacy of the government in the eyes of the people. I think the other area where we see problems with some countries is that they see the threat and they react—and then overreact. They become heavy-handed in their reaction. They don't necessarily discern where the violence is coming from, and so they take action against large swaths of the population. This can create human rights violations and issues where we can't work with them.

So we, on the defense side, need to work very closely with USAID, OTI [Office of Transition Initiatives], and State Department on the development side and on the diplomatic side. Very much across Africa, we see those three Ds [defense, diplomacy, and development] coming together very closely, where defense provides the security that enables the development. At the same time, the development provides the ability for the diplomacy to then engage to get the central government out to provide legitimacy, which then facilitates host-nation security forces. So there's this circle of events that takes place, and those three Ds come together closer in Africa than any place I've worked before.

CTC: As much as any other world region right now, the African continent is beset by dozens of jihadi terrorist groups—some allied to al-Qa`ida and others allied to the Islamic State. When you look very bluntly at the African security landscape, how would you compare the relative threat posed by AQ in Africa as opposed to the Islamic State? How do you conceptualize the two main parent groups? Are there particular similarities between them or differences? Are they just two sides of the same coin, to some extent?

Anderson: ISIS grabbed the world's attention with what they were able to do in Syria, and they've gained prominence and they're at the forefront of what people think about when it comes to global terrorism. And they're active in Africa. I think they're much more blunt in their methodology [than al-Qa`ida]. They're much more brutal. They tend to be more violent. And because of that, they sometimes run into issues of gaining legitimacy with segments of the population. The ISIS brand, if you want to call it that, is similar to any other global brand that everyone recognizes, so there are extreme groups on the continent that just want to be affiliated with that [brand] for recognition. Part of our effort is to discern what organizations are true believers, which ones truly follow the ISIS ideology, and which ones are just clinging to that name or trying to get affiliation for credibility or notoriety.

That said, though, we are seeing ISIS making inroads in different places. While they have a small footprint in Somalia, that footprint in Somalia [has led to] engagements in other parts of the continent—such as in the border region between DRC, Mozambique, and Tanzania. Again, we're not sure how ISIS is exactly exploiting those grievances, but we know that there's interest in them becoming more engaged. We also see that ISIS is in West Africa—both ISIS West Africa in Nigeria as well as in Mali with ISIS Greater Sahara. Those are slightly different affiliations, and they're not as responsive to ISIS Core direction. In some ways, since al-Baghdadi's death, what we see is ISIS public affairs publicizing the success of these western Africa affiliates primarily because I think ISIS is struggling for some identity and struggling for some success and these two affiliates have shown some success, so ISIS is latching onto them. We don't necessarily see them being responsive in return, though.

Now, having talked about ISIS, al-Qa`ida is our deeper concern on the continent, and I think long-term, al-Qa`ida poses a greater threat to the West and to U.S. interests. That's two-fold. One is a little bit in the east with their affiliation with al-Shabaab. I don't want to overplay that. There is an affiliation between al-Shabaab and al-Qa`ida; we've seen al-Shabaab respond to some al-Qa`ida taskings. Al-Shabaab is very much its own Somali organization and effort, but there are ties to al-Qa`ida. There's some troublesome concerns there that al-Shabaab is looking to do more external operations. And then will that relationship with al-Qa`ida grow or not? That's something we have to continue to watch. The deeper concern, though, for me is looking at how al-Qa`ida is engaging in the west, particularly through JNIM [Jama'at Nasr al-Islam wal Muslimin] and through AQIM [al-Qa`ida in the Islamic Maghreb], we know that [Abdelmalek] Droukdel is part of the senior leadership of al-Qa`ida; he operates out of Algeria. We know that he has great influence in AQIM.

We also know that JNIM, an affiliate of al-Qa`ida, is responding to their direction, and what we see in West Africa is al-Qa`ida is establishing themselves in the Azawad area of northern Mali. They're quietly establishing their connections and their relationships there. We've seen them intermarry into the local tribes. We've seen them become very entrenched in local politics and do this very quietly. And their goal, in my opinion, is that they want to establish a safe haven to operate from. They want to eventually establish a caliphate, but they know if they're too public about their intentions or if they raise the flag over some city, that will draw the attention of the West. And so they quietly continue to entrench themselves and develop their network with the local tribes to continue to build this safe haven. And then, we see they're expanding south out of Mali; they're doing it in a very deliberate fashion.

As I talked about earlier with Burkina Faso, we saw the security situation in the northern province of Burkina Faso deteriorate extremely rapidly, in literally a few months. Early in 2019, there were some initial attacks in the northern areas that we thought was extremism spilling over across the border. But now in hindsight, we look at that, and they were probably initial probing attacks to test the resolve and capabilities of the Burkinabe. Because we then saw, in the July-August time frame, this very deliberate attack on infrastructure, particularly bridges. JNIM attacked these key bridges that started to isolate the northern province from key Burkinabe outposts and the capital city. And then shortly after that, we saw complex attacks, sometimes on multiple Burkinabe outposts, that essentially overran a few of the Burkinabe forward operating bases. That left the Burkinabe concerned about their ability to support and resupply these bases after the lines of communications and the bridges were cut. After the security forces were removed, there was a very deliberate campaign against the leadership that was most visibly highlighted by the assassination of the mayor of Djibo, who spoke at our exercise Flintlock last year and who was an outspoken and capable leader in the community. He [was] also a member of parliament. He was intercepted on the road to Ouagadougou, dragged from his car, and he and his entourage were publicly executed on the side of the road. And so that was a very public move,

and as they start to eliminate and remove the leadership of the region, they're starting to consolidate their efforts.

They haven't taken control of any of the cities such as Djibo. I don't think they want to be burdened with that level of responsibility of providing services. But they do control the movement and the economics in the area, and what we saw them do in [the] October-November [2019] timeframe was expand east and west along the lines of communication. But they're now isolating key economic centers and the key markets. They then destroy or damage the bridges and then establish checkpoints so that anyone [looking] to get to market in order to sell their goods has to pass these checkpoints. Then we've seen them destroy crops, making the local populace more dependent on them, forcing them further under their control. What we've seen is at least 400,000 internally displaced [at the time of the interview, now more than 500,000], which is creating a huge problem for the government of Burkina Faso to try to deal with. Extremists then invite people to come back to their homes and say, "all you have to do is accept sharia law; you're welcome back," which is, when you look at it, a brilliant strategy. Now they're forcing those people to make a mental shift and acceptance of that extremist governance in order to return home. And those people now come home, they acquiesce to JNIM or ISIS Greater Sahara. And now they control that population while creating a dilemma for the Burkinabe government with the displaced people.

At the same time, now they have consolidated that area, we see them conducting strikes farther south, and they're publicizing those very much in the information space, saying that they're threatening the key population centers—particularly Kaya. We see them very deliberately moving south. We see a very deliberate effort along the borders with criminal activity to try and control the economic trade route there that are worth not just millions but billions of dollars of illicit trade. They're also getting down into the gold mining areas of Burkina Faso to try to get into these small artisanal mines. The gold is obviously a very easily transportable material. We also see the violence has gone down in northern Mali because they've consolidated much of their control there and they're starting to push south. And we feel that they're looking at a lot of this for economic gain to control these economic trade routes in order to provide some sort of steady revenue.

So this is why we are concerned about what al-Qa`ida is doing because we don't believe it's just criminality. We don't think it's just local grievances. We think al-Qa`ida's oversight and leadership has galvanized these grievances into something deeper that's starting to take hold. This is more than just five separate extremist organizations[a] or tribes. They have come together for a common purpose. And what we see also is that JNIM and ISIS are cooperating in this region. There are many reasons why they're cooperating in this region. JNIM provides unity of purpose, unity of effort but not necessarily unity of command. JNIM and ISIS-GS operate together and even coordinate attacks together. They're less concerned about who has complete control locally, focusing instead on propagating their extremist ideology and working toward the greater cause of establishing an Islamic state. I don't want to overstate this cooperation as a merging of the larger organizations as this is very much a local phenomenon. There are obviously historical ties between these groups that span clans, span tribes, and go from the leadership all the way down to the local fighters. This allows the ISIS and al Qa`ida affiliates here [to] cooperate in way we don't see anywhere else.

So all of that, to me, combines to be a very nasty situation developing in West Africa. We don't assess that it poses a direct threat to the U.S. and the U.S. homeland, but I can see over time that it very well could develop into a threat to the homeland as they gain control over economic centers and trade routes, consolidate their gains in the Azawad area, and have the time and space to plan operations outside of the region. It's difficult to say how fast this will develop, but we know they have the stated desire to develop these capabilities to attack the homeland.

CTC: The G5 Sahel[b] and Operation Barkhane[c] have faced challenges. From your perspective, what are their inefficiencies, and where are they succeeding? Where might they improve? And where might SOCAF fit into that broader puzzle?

Anderson: For this effort, the French very much have the lead for the European/Western nation effort here. They've been involved for several years and are very committed to this fight. This is a complex fight. When you look at the amount of French forces there, they've got about 5,000 French troops from their general purpose forces all the way to their elite taskforce that are operating across the Sahel. When you look at the size of that Sahel, 5,000 people is stretched thin very quickly. I know a lot of people underestimate the size of this AOR, the size of the area that they're being asked to engage in, and the complexity of the battlespace. Just within that area of Mali, there's multiple ethnicities, multiple tribes, not to mention the tri-border area between Mali, Burkina Faso, and Niger that complicates the international effort to work across borders.

So it's not, by any means, an easy task. But I think the French have been fighting admirably, and they've been working to address the fight. And I think that our limited support to them has been effective. Our goal, though, is how do we enable the French to continue to take the lead, how do we enable other European partners to engage? I know there's some interest; there's discussions about bringing other European partners into the fight. I think that would be very beneficial to everyone. Getting the Europeans engaged in a constructive manner and helping them work with the partners and train the partners would be a very valuable step forward, and we should continue to encourage this effort.

One view of extremist groups in the Sahel has been that they are a loose conglomeration of tribes that have their own grievances that were being held together maybe by a small group of charismatic leaders, that if we eliminated that leadership, then these tribes, this coalition would crumble and they'd go back to tribal grievances. I think that we at SOCAFRICA disagree with that assessment to some extent. While we agree with that foundation—that's how JNIM came together and was formed—we believe that it's evolved

a Editor's note: These are AQIM-Sahara, Ansar Dine, Macina Liberation Front, Al-Mourabitoun, and JNIM.

b Initiated in February 2017, the G-5 Sahel is an alliance between five Sahelian countries—Burkina Faso, Mali, Mauritania, Niger, and Chad—to address common transborder security challenges, including terrorism.

c Initiated in August 2014, Operation Barkhane is a 4,500-person strong French force primarily intended to deal with terrorism in the Sahel, which generally spans the breadth of the G-5 countries: Burkina Faso, Mali, Mauritania, Niger, and Chad.

beyond just that charismatic leader with Ag Ghaly.[d] They've elevated key leaders from various ethnicities, which gives them legitimacy in the eyes of many of these marginalized groups. We think there's a deeper ideology that's starting to take hold, and that is allowing them to propagate and develop in ways we didn't anticipate. It makes it a harder fight to address.

The other piece of this is how do we work effectively with our partners in the region? Mali has to have the will in order to develop their military and then we have to have partners that help engage and train them effectively and go out and advise them as well. We've got many international efforts that are working within Mali, including MINUSMA [United Nations Multidimensional Integrated Stabilization Mission in Mali], that's working with one of the most deadly peacekeeping missions on the continent. We've got the European training mission that's out there training forces, but they train them and put them out, they don't advise them, and so what we're missing [is] the operationalization of these forces. Then we need help [to] develop the leadership. What it takes is two-fold. It takes the will of the Malians to invest in their leadership and invest in their forces to equip them and train them. But it also takes an investment in the partner from the international community. How do we partner and how do we, meaning the Europeans as well—and this is really a European-led initiative here—how do we then invest appropriately to train the Malian forces so that they are credible forces and that they have competent leadership? Where we've seen some recent Malian defeats, it wasn't because the Malians couldn't fight. It's because they lacked some training, they lacked a little bit of equipment, but they really lacked the leadership to stand and fight from some very defensible locations. And so how do we engage with them appropriately to give them the confidence that they can defend themselves and that they then have the proper leadership to take the right actions to prepare their defenses, to prepare their locations, and actually defend.

And where we have seen much success for the U.S. piece of this effort is where we're engaged, albeit in a small way, in Niger where we have worked with the BSI [Special Intervention Battalion], which is their Special Operations equivalent, to create a very capable fighting force that has taken on the lessons that we have been able to teach. They've built upon our efforts, and they've become an effective force. When we have invested in a willing partner, they have been able to produce results.

So how do we work with our European partners, how do we enable them to come in here and create a force that can then be engaged with the partners and create a credible defense? And then how do we work with and how do we have the French take the lead and continue to take the fight to the enemy? Obviously, the French very much want to lead this effort. They're very invested in the region, and I think the international community needs to support that effort so that they can continue to be effective.

The G5 Sahel hasn't really performed because they haven't been operationalized. The G5 Sahel was set up to secure the borders between the five Sahel nations, but they've been unevenly resourced from the different nations—some nations have not given fully equipped or fully manned units to do that; some of the countries as they've come under threat have withdrawn their forces from the G5 Sahel—so the G5 Sahel has never been fully developed in order to execute. I've painted a picture of all these international efforts out there, one of the things we lack is really unity of effort amongst all of them. That's where the international community needs to step forward and corral these efforts in order to really gain traction and be more effective. And just that unity of effort would go a long way, I think, in realizing more gains within the Sahel.

CTC: Turning to various jihadi hotspots, the Islamic State in Libya was at its pinnacle from 2014-2016, but after it was ousted from Sirte, the group has sort of gone into the desert. How do you view its strength today? There is also concern about what's going on with the Islamic State Central African Province, or in other words, the cells in DRC and Mozambique. And then on the al-Qa`ida side, there is the enduring challenge posed by al-Shabaab. What needs to improve in the efforts against that group?

Anderson: I'll start with what you talked about with Libya, and I would say, one, it's hard for us to really say because of the continued civil war that's ongoing there and the hostilities. We don't have anybody on the ground to provide good assessments of that. So because of that, it's hard for us to fully understand the situation. That being said, we monitor where we can. As has been out in the press recently, there's been some efforts to disrupt their leadership,[2] and I know those have been effective in keeping ISIS Libya off balance. These strikes against their leadership have been critical to keep them from being able to fully reconstitute and pose a greater threat. As of right now, that's what we've been able to do: monitor and then disrupt effectively to keep them from gaining a solid foothold.

You talked about ISIS and Central African Republic and Mozambique. That's a concern to us as we watch it develop, but again, as I mentioned earlier, we don't fully understand what's driving it. We know in northern Mozambique, there are local grievances that ISIS is [exploiting]. At least one faction has grabbed onto the ISIS brand. We're trying to look at the situation and understand deeper what exactly does that mean and is that truly ISIS-driven or is it just a local grievance that's using ISIS for notoriety. We're watching that carefully. Obviously, we're interested in this situation because the U.S. has interests in developing the gas fields off the coast there. So there's U.S. interest in that area, but we're still trying to assess how strong ISIS' foothold and influence is there. And I'd say that's pretty similar for the DRC and the eastern part of the Central African state. How strong is that ISIS connection? And have they just raised the flag for notoriety? We have to continue to try to determine that, but these are very remote areas and they're difficult for us to get in to monitor and we don't have a presence there to really engage. So I would say, right now, we're monitoring the situation to see how the intelligence develops on those affiliates.

And the last one I think you had was al-Shabaab. That's been going on for a while. One of the things we have seen in the Lower Shabelle[e] is that the Somalis have been engaged in a successful, if very incremental offensive. They have very incrementally been able to expand their control; they've been able to take key villages along the Lower Shabelle River. They've been able to then secure and

d Editor's note: Iyad Ag Ghaly is the overall leader of JNIM. Previously, he was the leader of the now-defunct militant group Ansar Dine, which operated mostly in Mali. In 2017, Ansar Dine merged with Jama'at Nasr al-Islam wal Muslimin (JNIM).

e Editor's note: The Lower Shabelle is an administrative region in southern Somalia that abuts the capital, Mogadishu.

hold those areas. It's not been a rapid movement. It hasn't been large gains of territory, but their ability to gain influence and gain control of those key towns has provided an additional layer of security for Mogadishu and along its key lines of communication into the city. I don't want to overstate the success by any means, but the fact that the Somalis are leading this effort and they are holding is a positive development, that we are continuing to encourage that and to encourage them to invest in their force generation and the development of their security forces and to continue to build their more elite fighting force, the Danab.

We've seen the credibility of the Danab go up over the last year in their engagements as being a credible fighting force, as able to go out and secure these locations. That's built some faith within the Somali populace in the areas where they're operating that they are a capable security force. But there's still a long ways to go. There's still a long ways to go to get after where al-Shabaab has found a de facto safe haven down in the Jilib corridor along the Juba River valley and how are we able to disrupt this activity here. And that's really going to be how do we work with AMISOM, the Ethiopians, and the Kenyans who obviously share an interest in that security as al-Shabaab's a threat to both of those nations' security as well. How do we continue to encourage those countries to engage and apply pressure to al-Shabaab and to deny them that safe haven and apply pressure on al-Shabaab leadership that's down in that area?

It's in everyone's interest to have a stable Somalia. There are large U.S. economic interests along the eastern seaboard of Africa. Kenya's a key country in that, and supporting our partner there is key for U.S. investment. Prime Minister Abiy of Ethiopia, who was recently awarded the Nobel Peace Prize, has reached out to the United States and looked for greater support. How do we engage with him and continue to provide him and Ethiopia the support going forward for their reforms? I think those are all in the U.S.' interests. Partnering with these two countries is key to creating stability and fostering development in Somalia. It's not by any means an easy feat, but we've seen some very incremental successes and we want to continue to build on those.

CTC: What do you wish the American public knew about U.S. national security interests in Africa today? And as you look to the future, is there one particular threat or development that really keeps you up at night?

Anderson: For the American public, I think [it's] to have a better understanding of why Africa matters to the United States and why U.S. interests in Africa matter. If you just look at the access to rare earth minerals, that's key to our technology sector and making sure that those aren't exploited by other nations or that that market isn't cornered and we become beholden to someone else for access to those key minerals. I think they [our adversaries] understand the strategic geography that Africa has. North Africa is the southern flank of NATO and Europe. The key straits of the Middle East are key transits for economic but also key to our own national security. It is important that we stay engaged in Africa. I think I would ask that the American public understand this is important and our engagement here does matter.

The other piece of it is that there may be a misperception over what the future holds in Africa. I think we work with some very good partners here and that there is development, there is progress in Africa, that this is not the same Africa of 50 years ago, and that there have been some significant changes here. But we only hear about Africa in the United States, it seems, when there's something negative or something bad happens. We don't hear about the positive. That's unfortunate because there is a lot of positive that comes out of Africa. There's a lot of potential. In the just six short months of being here and six different trips to the continent and being able to engage and talk with folks there, there is a lot of positive energy. They're facing some real threats that are existential to some of these countries, but they are digging deep, being resilient, and addressing them. They just need a little assistance. That little bit of assistance we provide goes a long way. It provides, I think, large returns on the dollar for what little we spend here.

I also think that it does matter when it comes to China and Russia and how we compete. Those two countries have chosen to be here because there's economic interests here, and if we choose not to compete here, then we abdicate all of these resources, all this capability, all of this future potential to our adversaries. That would not be in our interest. I think it's in our interest to stay engaged on the continent. The world's a very small place. When it comes down to it, we all live on this same planet, and our futures and our interests are interconnected. Sometimes, it's hard to see that when your home's in middle America, but I don't think it takes much to draw those lines and connect the dots to see where it does matter to our future. Also, there are threats that are emanating out of this area that if we don't continue to watch, if we don't continue our vigilance, they could be concerning to ourselves, the United States, and to Europe. Europe is realizing this. They are engaging, especially in the Sahel. But those threats are not just to European interests but to U.S. interests.

[On] what keeps me up at night, if you want to say that, I'm not sure. I sleep pretty well overall because I think we as a country are still a force to be reckoned with, that we make a difference in the world. But if there's a concern I have, [it] is that we take our eye off the threat. We can't understand what we can't see. We don't have good visibility in these areas, and there are folks that wish to do us, especially the United States, harm. If we don't continue to monitor that, we could give them a pass to develop a capability to attack us, we could once again be surprised. That would be a concern. We have to be vigilant in order to preserve our own liberty. CTC

Citations

1 Editor's note: For more on the Dusit D2 attack, see Matt Bryden and Premdeep Bahra, "East Africa's Terrorist Triple Helix: The Dusit Hotel Attack and the Historical Evolution of the Jihadi Threat," *CTC Sentinel* 12:6 (2019).

2 Editor's note: See, for example, "U.S. Africa Command airstrike targets ISIS-Libya," U.S. Africa Command Public Affairs, September 30, 2019; "U.S. Africa Command airstrike targets ISIS-Libya," U.S. Africa Command Public Affairs, September 27, 2019; and "U.S. Africa Command airstrike targets terrorist fighters," U.S. Africa Command Public Affairs, September 25, 2019.

A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit

By Amarnath Amarasingam

On November 21-22, 2019, the EU Internet Referral Unit (EU IRU)—a team inside the European Union's law enforcement agency, Europol—and Telegram engaged in a serious disruption campaign against the Islamic State's channels and groups on the platform.[1] While there had been similar 'days of action' in the past, the campaign of November 2019 was far greater in scope and impact.[2] Hundreds of channels associated with the Islamic State-affiliated Nashir News Agency disappeared and have yet to recover.[3] In this interview, which was conducted on December 11, 2019, via Skype, CTC talks with a member of the EU IRU about this campaign, about the ongoing relationship with social media companies, and the continued challenge of combating terrorist content online. The official requested anonymity. Europol has reviewed this interview and approved its publication.

CTC: What exactly is Europol's EU Internet Referral Unit? When was it founded? Was there an immediate cause that led to its founding?

Europol EU IRU Official: We set up the unit in July 2015. Within Europol, within the European Counter-Terrorism Centre (ECTC) of Europol, there was a capacity to monitor and analyze terrorist propaganda, meaning jihadist propaganda, since 2007. The scope was major jihadist groups, designated terrorist organizations. The reason for that was to have a better understanding of the threat picture, especially when it comes to the threat posed to Europe and European interests outside of Europe from these designated terrorist organizations. This was the case for some years, but then it became increasingly evident that we needed to build this capacity and also have a mandate for supporting member states with online investigations in the context of counterterrorism, plus engaging with online service providers in order to help them build their resilience against the dissemination of terrorist propaganda. So, this was the reason that the IRU was set up in 2015. And since day one, we started engaging with online service providers to flag terrorist content to them and find solutions on how to disrupt the dissemination of terrorist content online.

CTC: Were there certain social media platforms or companies that were more open to working with you from the beginning, and why do you think that was?

Europol EU IRU Official: Yeah, at that time, I recall that the bulk of the propaganda was on mainstream social media such as Twitter or Facebook. We prioritized these types of platforms to work together, and their response was very positive. We based this on a voluntary approach. So basically, we started our operations for monitoring terrorist content—meaning content that is branded, that is produced and disseminated by designated terrorist organizations—and by tracing this content across the internet, we were in a position to also flag [it] to online service providers. So, we started flagging this type of content to the social media companies, and we engaged in a discussion with them on how we can help them improve their internal operations so they can build some measures internally to prevent the exploitation of their platforms by terrorist organizations.

CTC: Were you asking them for anything in terms of help from their side, or was it mostly you providing information to them?

Europol EU IRU Official: Our starting point is a particular media file. We don't look into particular accounts; we don't look into profiles on Facebook or Twitter accounts. We start by detecting a new media file that is put on the internet by a designated terrorist organization, and whenever we are in a position to detect and collect this content, we collect the URLs and flag the URLs to the specific post to the social media companies. Another way we help them is to share some of our experiences in, let's say, collecting visuals, logos, or markers that are used by designated terrorist organizations. We share these types of packages with them to help them understand how terrorist organizations use branding to become visible and spread their message to wider audiences.

CTC: Can you describe what a typical day looks like at the EU IRU?

Europol EU IRU Official: We are a team with people of many different backgrounds. We have the counterterrorism investigators; we have IT experts, communication experts, researchers with expertise in Islamic jurisprudence, and also in area studies. We also have linguists; we cover most of the European languages plus Arabic, Russian, and Turkish. So, we try to combine this set of skills in order to understand both the content of the message and the dissemination of the propaganda. We collect and analyze this information. There are then two lines of work. First, we support member states in their online investigations, so it's like police work, it's law enforcement work. Second, we also flag the content to the online service providers, with a request not to take down content but to review the content against their own terms of reference. Then it's up to them to make the decision whether they act upon it or not.

CTC: A number of these companies weren't always so open to acting. Why do you think there has been such a shift in culture in these social media companies more recently?[4]

Europol EU IRU Official: It was not just a shift in the understanding of social media companies, but it was a shift in the understanding of the whole international community looking at this specific issue that we cannot allow terrorist organizations to exploit publicly accessible social media and online service providers in order to promote their message, to plan their operations, to reach out to people for recruiting and financing purposes. This was crucial because we really tried to engage with the whole of the international community, not just the social media companies in doing our job. We did that in the framework of the EU Internet Forum, which was set up by the European Commission in late 2015 to facilitate this type of engagement. If I go back to this period that you mention, I can say that we have achieved at least the primary objective of restricting public access to this type of content. It's increasingly more difficult for the average user to stumble upon terrorist content as they go [about] their day-to-day browsing of the internet. Back then, a Twitter user might have been following a popular hashtag and in his Twitter feed terrorist content popped up. We thought that this was problematic, and in our discussions with social media companies, everyone agreed.

Moving forward to today, terrorist content is, of course, still accessible on the internet. We never claimed that our job is to clean the internet of terrorist content, but our job is to try to identify who is behind that, to attribute the terrorist offenses to those who are behind the screens, and also to protect the general public.

CTC: So, on the social media side you're concerned with limiting visibility. On the law enforcement side, do you only help with cases that member states come to you with, or do you proactively point them toward citizens or somebody who's in their country that they should be looking at?

Europol EU IRU Official: When it comes to investigations, we support member states with publicly available information. We don't have access to closed information. Member states need to use their legal instruments in order to request access to this type of information from the social media companies. So basically, if there's an open investigation by member states and they get access to this type of content, they can come to us for further analysis. But we don't have the legal basis to request social media companies to disclose any non-publicly available data to us.

CTC: So you're collecting data, and if law enforcement of a member state comes to you through legitimate channels, you then have the ability to help.

Europol EU IRU Official: Exactly.

CTC: How do you deal with the support network or the 'fanboys' who are very much online? Do you see official releases and supporter releases as kind of the same thing as long as they're branded, or do you deal with them differently?

Europol EU IRU Official: As long as it is branded, it is part of our concern, but of course we make a clear distinction because you cannot weigh an official statement or piece of propaganda the same way with a banner or something that is produced by a fanboy, which is not connected to jihadist media outlets. But we see this as a joint effort that has to be done by other stakeholders, by other participants in this work against terrorist content. So, we engage also with researchers; we have set up an advisor network. We try to share our experience but also to integrate the results of their research, and these discussions about how we deal with supporter-generated content is a critical issue because we see that sometimes content that is produced by just fanboys might hit the headlines, might be reproduced, and this distorts the terrorist threat assessment. It might be reproduced by people who inadvertently want to report on this content, but at the same time, they help in amplifying this content.

So, we work together with institutions, researchers, in order to raise awareness about these issues. For example, when we see that some journalists or researchers use the same hashtags [created by jihadi media outlets to promote their content] or part of a terrorist video clip to report on the terrorist content, we can see this as problematic because at the same time, you reproduce or you further spread this message. The point here is that unedited content or content that re-mediatizes the brand of the terrorist organization should not be circulated. Most professionals take a nuanced approach, but this is not always the case. So again, we have an extended network of stakeholders; we work with European institutions, with European Strategic Communication Network (ESCN), with the Radicalization Awareness Network (RAN), with the global research network that was set up by the Global Internet Forum to Counter Terrorism (GIFCT).

CTC: What surprised you most about how the Islamic State has used the internet as compared to other terrorist groups?

Europol EU IRU Official: The first thing that comes to my mind is their branding, how they were able to promote and maintain their branding. From a researcher's point of view, from someone who is engaging with terrorist content, you see that IS had to put up with changes many times in the past. They had to change their narrative from the apocalyptic discourse, Dabiq and the end of days battle, and "remaining and expanding." Then they lose territory, but still they remain relevant by continuously changing their narrative. They ask their supporters to remain steadfast and so on. For me, there were many missed opportunities. I would have expected the impact of them having to change the discourse so many times to have been more negative than it was. Because they were able to maintain the branding and basically create an online environment that took on its own life and was somehow disconnected from the reality on the ground, this was something that in my view was problematic and this is where we need to focus more.

CTC: When the Islamic State started to move to Telegram in late 2015, how did that impact your work?[5]

Europol EU IRU Official: As I said, we start our observations from tracing content. So, when they moved to Telegram, we tried to reach out to Telegram and explain the situation. We started flagging terrorist content to Telegram, and gradually we established a channel of communication and cooperation with Telegram. For tech companies, when they set up their own business, they don't think about the exploitation of their platform by terrorists. So for many companies, not just for Telegram, the first step is to raise awareness about what's happening on their platform and then start building trust with them. This is important, and that's why we highlight the importance of voluntary cooperation, the importance of the public/

private partnership. If I'm being honest, some of the online service providers that we try to engage with, their first reaction is why is a law enforcement agency asking me to review this type of content? What is behind that? Do you come with a legal mandate? Are you going to ask for more information? We [Europol] don't have any enforcement powers there. Our legal mandate is to flag the content and then work together with them [social media companies] to raise awareness. Then it's their own decision. This is also how it worked with Telegram.

CTC: There is a perception that Telegram was slow in the beginning to come to the table. What do you think the reason for that was?[6]

Europol EU IRU Official: I cannot say whether it was slow or fast, but it takes time until tech companies understand what the problem is. What is important is for us to maintain this type of communication, to establish regular communication, and try to engage and give the right answers to these companies. Not everyone wants to engage; in some cases, they're not interested and then they don't engage.

CTC: Why do you think that kind of shift happened for Telegram?

Europol EU IRU Official: I think it's partly that they realized that they don't need to put up anymore with this type of activity. No online service provider would have ever liked to put up with this type of activity. And if you see the joint press release that we have published on our website, in the aftermath of the Europol campaign, there's also a quote from Telegram saying basically that enough is enough.[7] They see this as their responsibility, to have a platform that is free of terrorist abuse.

CTC: Can you describe the November 2019 operation Europol coordinated with online communication platforms such as Telegram to take down Islamic State content?[8]

Europol EU IRU Official: This was part of our standard procedure in engaging with online service providers. We had already done a couple of, let's say, actions together with Telegram in the past. We cover a large number of online service providers, not just Telegram. But at some point last year, we took some time to specifically look at Telegram. We did a joint action, and then we started building from that point on into trying to work closer together to map the network of core disseminators, so to speak, propagandists whose main business it is to disseminate this type of content. And this cooperation culminated with this type of action, but at the same time, we have been working together with law enforcement in member states in order to disrupt the internet operations of the Islamic state. In the past, we did some investigative work, and together with the prosecutors, we managed to cease some of the web assets (e.g., servers) that the Islamic State propagandists were using to store content [and] to communicate.

And these actions we saw as opportune [in their] timing. We did not merge the two actions, but wanted to have an impact by using the time factor there. So the prosecutors, member state investigators working on the investigative part, and then also content specialists, referral specialists, working with Telegram and other platforms to refer this type of content. This was a planned action, and we knew that if this went well, it would shake up the community of jihadist propagandists on Telegram.

And by disrupting their operations on Telegram, you create new opportunities [for those working on counterterrorism]. I mean, it was not that difficult to guess what they would try next. Of course, we don't know everything, but there were already some indications from 2018 that they were willing to experiment with certain platforms. It was not a big surprise that they tried to go back and use some of these platforms. They, of course, experimented with some new platforms, but this creates a lot of opportunities [for those working on counterterrorism]. First of all, this creates a lot of disruption. Then it has an impact on the branding, because nobody's sure who is creating the new channels, the new Nashir channels, the new Amaq channels, on each new platform. What is the message? We see now many messages that caution protagonists or sympathizers from using this or the other platform or using or following this or the other media outlet. So, there's a clear impact on brand, and there's also an opportunity to create new investigative leads.

So, what I'm saying here is that in the past, we worked on both the investigation/attribution and the referral aspects. But now we try to bridge the gap there. So, this is not the end of the story. This is the beginning of the story, and that's why we really want to engage with the international community to put all of our efforts together to work both on prevention and attribution. By disrupting the jihadist networks on the internet, you contribute to prevention. This is what we're trying to do here by doing referrals; by flagging this content in a timely manner to online service providers and by helping member states to investigate these networks, we try to bridge the gap that we've seen in the past between prevention and investigative work.

CTC: That part of it is especially interesting. Are you seeing social media companies being open to working with member states, and are you trying to serve as the bridge between those two?

Europol EU IRU Official: Yes, absolutely. And as I already mentioned, there's now an understanding among social media companies that they shouldn't put up with this type of exploitation. Again, this depends on the platform and on their relationship with investigators and prosecutors in member states. We see that some platforms are more willing than others to share additional information. This has nothing to do with freedom of speech. We are, of course, for the protection of freedom of speech and fundamental rights and the digital rights of citizens, but our focus is very targeted. And we see that companies start seeing this as another type of crime around which they have already been working with law enforcement, like banking fraud or child sexual exploitation. They're willing to share more data because they see a benefit from disrupting these networks and bringing these people to justice.

CTC: The Europol press release mentioned that the November 2019 operation "was led by the Belgian Investigating Counter Terrorism Judge and the Belgian Federal Prosecutor's Office, together with the Belgian Federal Judicial Police of East-Flanders." And there is mention of "an arrest in Spain of an individual suspected of being part of the core disseminators of IS terrorist propaganda online."[9] What is the significance of men-

tioning these law enforcement agencies in the press release?

Europol EU IRU Official: This is related to the operational work. Member states were working together with us to seize some of the assets and create some investigative leads. This phase of the operation—I'm talking about the investigative part, not the referral part—was led by the Belgian prosecuting authorities, and the Belgian and the Spanish colleagues wanted to present a strong message that this is the way forward. All of us getting together, working together in order to attribute terrorist offenses to the perpetrators.

CTC: Some people say that what you and others are doing is basically just a game of cat and mouse—just chasing terrorists around the internet. They say that this is not a good use of law enforcement time and energy. How do you respond to that?

Europol EU IRU Official: I would like to go a few years back and compare the situation today with the situation back in 2014, 2015. I think it's unfair to say that there's no progress made in this respect. Now, I see that the focus is on this whack-a-mole game, but we're talking about a steep decrease in terrorist propaganda output, especially high-profile items coming from the officially endorsed media outlets. Today, we're talking about some networks of people who really want to exploit small- and medium-sized enterprises online to disseminate terrorist content and especially supporter-generated content. But this is limited. This is more limited than it used to be back in 2015, 2016. So, if we want to be fair, I think we have to give some credit to this effort, to the public/private partnership that has been put forward since that time and recognize that now we're dealing with a different kind of problem. Of course, some people are dedicated disseminators and supporters of these organizations. The internet is an enabler; it's not the root cause of terrorism. But we need to take some action because otherwise you just leave it open to whoever wants to exploit the situation.

CTC: Can you talk a little bit about the Islamic State media structure, what you noticed with their presence in Syria and Iraq versus Europe or North America? Were there core individuals everywhere, or was it centered in Syria and Iraq? And relatedly, how did the destruction of the physical caliphate impact the media environment and structure?

Europol EU IRU Official: This is a very difficult question. What I can say is that we think that there are different layers of the structure they have put forward to produce and disseminate content. At the peak of their activity, they have styled Amaq as like an independent news agency to report on the evolution on the ground in real time. At the same time, they had the officially endorsed media outlets. Then there was another layer of supporting media outlets; some of them pre-dated the advent of the Islamic state, and they pledged allegiance to the Islamic State. Some others were created to support the work of the Islamic State, but they, at the same time, produced their own content and disseminated their own content. And then in the third layer, there were sympathizers who were willing to create the supporter-generated content and disseminate it. So, we give different weights to these layers.

Also, at the peak of their activity, they used to have a very sophisticated campaign on the internet starting from sending out teasers about new releases, like about the magazines they were going to put out. This was what we thought of as the "seeding phase." Then there was the "launch phase," and then they had the "echo phase" in which they re-mediatized content in large volumes. This was a sophisticated campaign on their side when it comes to strategic communications, and this has also been the target of our operations. By doing that, and working together with member states and law enforcement, you come across valuable information, and I think that over the past years, member states, law enforcement, and judicial services have managed to disrupt part of this network and bring these people to justice. This is a continuous effort, a work in progress.

CTC: I've observed in my research how university students have helped translate material for the Islamic State and build banners and so on. To what degree are younger people joining the media apparatus post 2018/2019?[10]

Europol EU IRU Official: I'm afraid I cannot talk about the demographics because we don't have any specific analysis on that. But, for us, it's important to continue working with law enforcement and member states. They're responsible for the investigations, and they're responsible for dealing with those joining the terrorist organization in their effort to propagate their narratives. We also want to share our experience with other institutions. I mentioned, for example, the Radicalization Awareness Network because prevention is equally important. We are a counterterrorism center and we deal with counterterrorism, but I think that our experience is valuable for others who work on the prevention side. So, we try to engage, we try to share our experience and our knowledge, and we hope that the root causes of terrorism are addressed and that preventive work is done to stop people from resorting to this type of activity.

CTC: Is your team involved on the far-right side of things as well? There's a lot of far-right activity on Telegram and other platforms. Are you also looking at that and other kind of ideologically inspired terrorist violence, or is it mostly focused on jihadi material?

Europol EU IRU Official: So far it has been mostly focused on jihadi terrorist propaganda. In some cases, we also supported member states in far-right terrorist cases. This is basically under discussion currently to see how Europol can further support this effort in other fields. Of course, there's some similarities but also some differences when we talk about right-wing terrorist groups. So, we're currently looking into that, to assess how we can better contribute to this effort. CTC

Citations

1 "Europol and Telegram Take on Terrorist Propaganda Online," Europol, November 25, 2019.
2 "Europol disrupts Islamic State propaganda machine," BBC Monitoring, November 25, 2019.
3 Ibid. See also "Jihadists Presence Online Decentralizes After Telegram Ban," Flashpoint, January 17, 2020; tracking of Islamic State-associated online content by the author (Amarnath Amarasingam).
4 Jessica Stern and J.M. Berger, *ISIS: The State of Terror* (New York: Harper Collins, 2015), p. 134.
5 "Jihadis Shift to Using Secure Communication App Telegram's Channel Service," MEMRI, October 29, 2015.
6 For analysis of the Islamic State's previous presence on Telegram, see Bennett Clifford, "'Trucks, Knives, Bombs, Whatever': Exploring Pro-Islamic State Instructional Material on Telegram," *CTC Sentinel* 11:5 (2018); Bennett Clifford and Helen Powell, "Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram," George Washington University's Program on Extremism, June 2019; Laurence Binder, "Wilayat Internet: ISIS's Resilience Across the Internet and Social Media," Bellingcat, September 1, 2017.
7 Editor's note: "Europol and Telegram Take on Terrorist Propaganda Online."
8 Ibid.; Paolo Zialcita, "Islamic State's 'Not Present on the Internet Anymore' Following European Operation," NPR, November 25, 2019.
9 "EU Law Enforcement and Judicial Authorities Join Forces to Disrupt Terrorist Propaganda Online," Europol, November 25, 2010.
10 Amarnath Amarasingam, "Telegram Deplatforming ISIS Has Given Them Something to Fight For," Vice Motherboard, December 5, 2019.

The Cyber Threat from Iran after the Death of Soleimani

By Annie Fixler

Following the U.S. drone strike that killed Iranian commander Qassem Soleimani, the U.S. government has issued repeated warnings to be vigilant against cyberattacks from Iran. In the immediate aftermath, Iranian social media disinformation operations, website defacements, phishing attempts, and network probing emanating from Iran spiked. Iranian hackers of all skill levels—from amateurs to professionals—appear to be taking the initiative to launch attacks they believe the regime would want them to undertake, whether or not they have received direct orders or requests from the government to launch these operations. Public reporting indicates that the Iranian regime itself has yet to retaliate for the commander's death with a destructive cyberattack. Based on past behavior and the regime's use of cyber as a tool in its asymmetric arsenal, it is likely that state-backed hackers will attempt to conduct significantly damaging cyber operations in the future. Soleimani's death itself, however, is unlikely to significantly alter the trajectory of the cyber threat from Iran. State-sponsored Iranian cyber operations are likely to continue, either in direct response to Soleimani's death, in reaction to U.S. economic pressure, or in pursuit of other regime interests.

Tensions between the United States and Iran have been escalating since the Trump administration came into office in January 2017[1] and withdrew from—and in November 2018 began reimposing sanctions lifted pursuant to—the 2015 nuclear agreement, formally known as the Joint Comprehensive Plan of Action (JCPOA).[2] Washington has further escalated sanctions since then, and Iran has responded with violence and destabilizing activities across multiple domains.[3] In total, U.S. sanctions have cost Iran $200 billion in investment and oil revenue, according to President Hassan Rouhani.[4] Inflation is rampant,[5] foreign exchange reserves are rapidly shrinking, and the country has entered a deep recession.[6]

In response, the regime and its Islamic Revolutionary Guard Corps (IRGC) have harassed and even bombed vessels traveling through the Persian Gulf,[7] and downed a U.S. drone in international airspace.[8] State-backed hackers have, among other things, increased targeted phishing attempts[a] against private industry in the United States and around the world[9] and against journalists and activists.[10] Tehran also stands accused of launching drone and missile attacks on Saudi oil giant Saudi Aramco.[b]

While the Trump administration reportedly launched cyberattacks on Iran following the downing of the U.S. drone,[11] the president ordered but then canceled military strikes minutes before their execution.[12] After the Aramco attack, the Trump administration reportedly again used exclusively U.S. cyber tools, this time conducting an attack aimed at degrading Iran's propaganda capabilities.[13] As a result, the U.S. strike that killed General Qassem Soleimani, commander of the IRGC Quds Force, took the world by surprise.

The January 3, 2020, drone strike that killed Soleimani and Abu Mahdi al-Muhandis, commander of the Iranian-backed, U.S.-designated terrorist organization Kata'ib Hezbollah (KH),[14] came in response to rocket attacks by KH that killed a U.S. contractor working on a military base in northern Iraq.[15] The U.S. military first responded with airstrikes on KH targets in Iraq and Syria.[16] Pro-Iranian protestors then attacked the U.S. embassy in Baghdad.[17] A day later, the U.S. military launched its drone strike.

Commentators on both sides of the political spectrum fretted that the United States was on the "brink of war,"[18] but the tensions that threatened to boil over have since returned to a simmer. Even as the Iranian regime responded to Soleimani's killing by launching a barrage of missiles at U.S. military bases in Iraq, President Trump proclaimed that Iran "appears to be standing down."[19] Foreign Minister Javad Zarif similarly tweeted that the regime "concluded proportionate measures," indicating that no further escalation was forthcoming.[20]

And yet, the threat that the Islamic Republic poses in cyberspace has not abated. Just as the regime is unlikely to cease its support for terrorism, pursuit of nuclear-capable intercontinental ballistic missiles, and aggressive behavior toward its neighbors,[21] it is unlikely to cease its malicious cyber operations. Indeed, nearly three weeks after Soleimani's death, the FBI urged businesses to remain on alert and review warnings about the conduct of pro-regime cyber

Annie Fixler is the deputy director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, a Washington-based, nonpartisan research institute focusing on national security and foreign policy. Follow @afixler

a When conducting a phishing attack, hackers send fraudulent emails impersonating another individual or company to convince the recipient to click on a malicious link, download a piece of malware, or enter credentials on fake websites.

b While Houthi militants in Yemen have claimed responsibility, the Trump administration has dismissed these statements and blamed the Islamic Republic of Iran. The public evidence supports the administration's assertion but is not definitive. David D. Kirkpatrick, Christoph Koettl, Allison McCann, Eric Schmitt, Anjali Singhvi, and Gus Wezerek, "Who Was Behind the Saudi Oil Attack? What the Evidence Shows," *New York Times*, September 16, 2019; "Special Report: 'Time to take out our swords' - Inside Iran's plot to attack Saudi Arabia," Reuters, November 25, 2019; Erin Cunningham, "Iran's gamble: Analysts say brazen attack aimed to pressure U.S. with little fear of reprisal," *Washington Post*, September 20, 2019.

operators.[22]

It is well understood that cyber can be an effective asymmetric tool for causing damage to more militarily powerful adversaries, particularly when deployed against the private sector. The U.S. intelligence community assesses that the Iranian regime is "capable of causing localized, temporary disruptive effects" and is constantly preparing cyberattacks against the United States and its allies.[23] There is no indication that Soleimani's death will fundamentally alter the regime's regional ambitions or its *modus operandi* in the physical and cyber domains. Statements from both Iran's Supreme Leader Ali Khamenei and from Soleimani's successor, Esmail Qaani, have emphasized the continuity of Iranian policy despite the change of leadership.[24]

While Iran is generally considered a less sophisticated cyber actor than other U.S. adversaries, the regime and its hackers tend to be much less risk-averse.[25] A common view held by researchers who follow the activity of Iranian hackers is that they are more likely to engage in destructive or disruptive attacks whereas their counterparts in other countries might be more inclined to quietly collect valuable data and intelligence.[26] c

Kiersten Todt, the executive director of the Commission on Enhancing National Cybersecurity under President Barack Obama, explained, "Iran is dangerous because they have the intent, motivation and capabilities. While their cyber capabilities are not on par with Russia and China, they are innovative and can cause both physical and psychological disruption."[27]

This article examines Iran's cyber strategy, including by analyzing two significant operations in order to understand how the regime uses cyber as part of its asymmetric arsenal. The article then examines the malicious cyber activity emanating from Iran since Soleimani's death and the overall cyber threat landscape with regard to Iran to begin to anticipate the type of state-backed, Iranian cyber operations that may occur in the short and medium term. This analysis leads to the conclusion that while the Iranian cyber threat is significant and persistent, Soleimani's death may have little impact on the trajectory.

The Islamic Republic's Cyber Strategy

Cyber operations are a key pillar of Iran's strategy, which relies on asymmetric capabilities to battle its more powerful adversaries.[28] Following the killing of Soleimani, retired Lieutenant General Vincent Stewart, former deputy commander at U.S. Cyber Command, testified before Congress that the regime views its cyber capabilities as a "vital tool of statecraft and internal security" and a "low cost" way to retaliate against its enemies.[29]

Like many nation states, Iran uses cyber operations to collect intelligence and conduct espionage, and like all authoritarian governments, the regime uses cyber to "silence and weaken" its internal opposition, according to a 2018 U.S. State Department report.[30] In fact, most victims of regime cyber operations are Iranian citizens and expatriates, scholars Collin Anderson and Karim Sadjadpour have noted.[31]

When targeting the United States and its allies, the Iranian regime often directs its cyber operations against private industry, which is generally less well defended than U.S. government networks. As a result, Tehran is able to target the soft underbelly of its more powerful foes. These cyber-enabled economic warfare operations appear to be Iran's attempts to warn its adversaries that just as the United States can cause economic damage to its enemies by using financial sanctions, Tehran can undermine the strategic capabilities of its enemies by targeting their economies with cyberattacks.[32]

Externally, Saudi Arabia has borne the brunt of Iranian malicious cyber operations in recent years. Even when Iranian operatives target numerous government and private entities over the course of a campaign, private cybersecurity firms consistently find that the plurality of victims are Saudi.[33] This is likely because the two states are bitter regional rivals and because Saudi cyber defenses are weaker than those of Iran's other primary foes, Israel and the United States.[34] For example, after Israel's Cyber Defense Directorate detected an Iranian attempt in 2017 to infiltrate and possibly corrupt its home front missile alert system, the division was able to quickly excise the hackers, assess what they had accessed, and reinforce network defenses.[35]

In contrast, despite suffering substantial losses when the Shamoon computer virus hit state-owned oil company Saudi Aramco in 2012 (discussed later), Riyadh's systems were insufficiently reinforced such that four years later, hackers working on behalf of the Iranian regime were able to use a new variation of the virus to corrupt computers at more than a dozen Saudi government agencies and businesses.[36]

There are two other explanations related to the comparative weakness of Riyadh's defenses that are worth mentioning. Iranian hackers may be practicing against an easier target to hone their skills before pivoting to attacking the United States or Israel. Or, these hackers may be attempting to attack the United States, Israel, and Saudi Arabia with the same frequency but because U.S. and Israeli defenses are stronger, these two nations are able to suppress threats quickly and quietly whereas attacks on Saudi Arabia are more likely to be reported.

To understand how cyber capabilities fit into Tehran's asymmetric toolbox, it is worth examining two of the regime's first forays into offensive cyber operations: the regime's 2012 attack against Saudi Aramco and 2011-2013 distributed denial of service (DDoS) attacks against U.S. financial institutions. Iranian hackers have since conducted numerous campaigns, in particular since the Trump administration came into office. (See Table 1.) In more recent campaigns, hackers have targeted dozens or hundreds of companies and individuals, not always for the same reason. For example, cybersecurity firm FireEye found that one Iranian Advance Persistent Threat (APT) group targeted aviation and energy companies in Saudi Arabia, South Korea, and the United States. FireEye hypothesized that "the targeting of the Saudi organization may have been an attempt

c There is also some evidence suggesting that Iranian hackers may also be more likely than their counterparts to launch operations where they cannot predict the precise real-world effects or the victim's response. For example, an Iranian hacker affiliated with the IRGC infiltrated the Bowman Dam in Rye, New York, between August 28 and September 18, 2013. It is unclear why a hacker would target this 20-foot dam. It is possible that the hack was a dry run for a more spectacular operation or that the hacker got the dam mixed up with a much larger facility with the same name. If the latter, and if analysts are correct that the hacker intended to take over the dam's functions, did this hacker and the Iranian government understand the full implication of causing a physically destructive cyberattack against U.S. critical infrastructure? "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," U.S. Department of Justice, March 24, 2016; Joseph Berger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *New York Times*, March 25, 2016.

to gain insight into regional rivals, while the targeting of South Korean companies may be due to South Korea's recent partnerships with Iran's petrochemical industry as well as South Korea's relationships with Saudi petrochemical companies."[37] In contrast, the two early cases have discrete targets attacked over a limited timeframe, and therefore it is easier to extrapolate the regime's motivations and goals as a way to understand the regime's strategy more generally. These two cases are also well-documented in the public space by multiple sources rather than relying exclusively on the reporting of one or two private cybersecurity firms.

Table 1: Notable Examples of Iranian Cyber Operations Since January 2017

Date	*Event*
Jan. 2017 - Jan. 2019	Global DNS Spoofing campaign[38]
2017	Israel thwarts Iranian cyberattack of Iron Dome[39]
2017 - 2018	Cyber infiltration against governments and businesses in the Middle East[40]
2017 - 2019	Infiltration of more than 200 businesses and governments around the world[41]
Mid-2017 - 2019	Very targeted malware campaign against energy firms in the Middle East, Asia, and United States. According to multinational cybersecurity and defense company Trend Micro, these operations "likely resulted in concrete infections in the oil industry."[42]
June 22, 2019	The U.S. Department of Homeland Security warns of a "rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies."[43]
Aug. - Sept. 2019	Attempts to compromise accounts belonging to 241 presidential campaign staffers, current and former U.S. government officials, journalists, and prominent Iranian expats[44]
Fall 2019	Broad efforts to infiltrate U.S. electric utilities[45]
Mid/Late 2019	Targeted ("not opportunistic") wiper (destructive) attacks on organizations in the energy and industrial sectors in the Middle East[46]
Oct. - Nov. 2019	Attacks begin to target a narrower list of organizations and shift from attacks on IT systems to attacks against industrial control systems, according to analysis by Microsoft security researchers.[47]

Wiper Attack on Saudi Aramco

In August 2012, the Iranian regime launched its first destructive cyberattack against a foreign adversary.[d] A hacker group calling itself the Cutting Sword of Justice[e] infiltrated the networks of Saudi Aramco and unleashed a virus dubbed Shamoon.[f] The malware moved quickly within the network, destroying data and rendering 35,000 computers inoperable.[48] While Shamoon did not affect Aramco's oil production, it disrupted a majority of the company's business processes, including its supply management, shipping, and contract management.[49] As this author explained in a previous study of Iranian cyber-enabled economic warfare strategy and capabilities, overnight, the Shamoon virus forced the company "to revert to faxes, inter-office mail, and typewriters. It reportedly took approximately five months to get all of the company's systems back online."[50]

That prior study also pointed out that "at the time, Iran's oil exports were dropping rapidly as the United States increased its sanctions on Iran's energy and financial sectors and as the EU imposed a ban on imports of Iranian crude. Thus, it is possible that Tehran hoped its cyberattacks would drive up energy prices so that Iran's limited exports would bring in more revenue."[51][g] If this were the hackers' motivation, it would indicate that Iranian operations are more likely to target companies and industries where Tehran can reap an indirect economic benefit from the attacks.

It is also possible that Shamoon was to a small or large degree retaliation for U.S. sanctions on Iran's energy sector. Military scholar Michael Eisenstadt concludes that "Iran has traditionally taken a tit-for-tat approach to actions by its adversaries."[52] Thus, it may be the case that targets of Iranian cyber operations are likely to mirror industries against which Washington has levied sanctions.[h]

Finally, Tehran may have targeted Aramco because oil is Saudi Arabia's most important economic asset. In this case, Tehran anticipated that causing significant harm to a major source of Saudi revenue (and perhaps even undermining the global market's faith in Saudi Arabia as a major oil producer) would weaken the Kingdom. From its founding, the Islamic Republic has conceptualized its own economy as providing the means to fortify the revolution at home and export it abroad,[i] and thus the regime recognizes the impact

d The Islamic Republic of Iran has continued to deny its responsibility for this attack, but it is commonly accepted that this was a state-backed operation.

e The Iranian hacker group Cutting Sword of Justice claimed responsibility for the Aramco hack on this message board: Statement, "Untitled," Pastebin, Cutting Sword of Justice, August 15, 2012.

f The virus also appears to have struck Qatari natural gas producer RasGas, although much less is known publicly about this case including the overall damage inflicted. Much of the public reporting at the time linked RasGas and Aramco but did not provide evidence (technical data, company statements, or other documentation) beyond the coincidence of timing and roughly similar outages at both companies to support this assertion. See, for example, Camilla Hall and Javier Blas, "Qatar group falls victim to virus attack," *Financial Times*, August 30, 2012, and Kim Zetter, "Qatari Gas Company Hit With Virus in Wave of Attacks on Energy Companies," *Wired*, August 30, 2012.

g If this were indeed the hackers' motivations, they failed to achieve their objectives. While global prices were elevated at the time, they did not spike after the attacks. "2012 Brief: Average 2012 crude oil prices remain near 2011 levels," U.S. Energy Information Administration, January 10, 2013.

h Some analysts also believe that Shamoon was retaliation for a cyberattack on Iran's own energy sector. Author interview, cybersecurity analyst, October 2018; "Suspected cyber attack hits Iran oil industry," Reuters, April 23, 2012.

i The Iranian constitution states that the economy "is a means that is not expected to do anything except better facilitate reaching the goal [of advancing the Islamic revolution]." Constitution of the Islamic Republic of Iran 1979 (as last amended on July 28, 1989), Preamble.

A sign indicates Saudi Aramco in front of the company's offices in Riyadh, Saudi Arabia, on December 5, 2019. (Fayez Nureldine/ AFP via Getty Images)

that cyber-enabled economic warfare can have. If this were Tehran's motive, then its adversaries' strategically significant industries will likely be among Iran's future cyber-targets.

Operation Ababil: DDoS Attacks on U.S. Banks

Operation Ababil involved a series of DDoS campaigns against the U.S. financial sector beginning in December 2011 and continuing into mid-2013.[53] The attacks occurred only intermittently for the first 10 months and then escalated to a near-weekly basis starting in September 2012, targeting 46 banks and financial institutions, according to a U.S. Department of Justice indictment.[54]

While DDoS attacks are relatively blunt and unsophisticated operations compared to covert infiltrations of a company's networks, the attacks forced banks to spend tens of millions of dollars in remediation.[55] One of the security researchers responsible for responding to the attack commented to *The New York Times* that "the scale, the scope and the effectiveness of these attacks have been unprecedented."[56] The attack primarily prevented customers from accessing mobile banking, but the fallout could have quickly spiraled had consumers begun to worry if their money was still safe in the bank. Financial institutions themselves recognized the significance of their cyber risk, and over the next two years, more than 4,000 institutions joined the Financial Sector Information Sharing and Analysis Center, an industry organization for sharing cyber threat information among financial institutions.[57]

In 2016, the Justice Department formally accused Tehran of sponsoring the attack, stating that the hackers were working "on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps."[58] As this campaign coincided with the last major recession Iran faced,[59] U.S. officials and cybersecurity experts believe that operation was likely retaliation for U.S. economic sanctions.[60] The period of time when the attacks occurred—late 2011 to early 2013—coincided with unprecedented U.S. sanctions against the Iranian financial sector, including designating the entire sector as a "jurisdiction of primary money laundering concern" under U.S. law, targeting the Iranian central bank with sanctions, and forcing the international, financial messaging system SWIFT to remove Iranian banks from its network.[61] Like the Aramco attack, Operation Ababil appears to have been a cyber-enabled economic warfare campaign designed to send a message that just as the United States can impose financial sanctions on Iran, Iranian hackers can cause economic damage as well.

In both of these cases, hacker groups professing independence from the Iranian government claimed responsibility,[j] but the U.S. government has attributed the attacks to the Iranian government.[62] This is consistent with how the regime engages with its hacker community. In Iran, there are individuals and groups of hackers who simultaneously engage in criminal activity, legitimate software development, and regime-sponsored operations.[63] For example, when the U.S. Justice Department indicted Behzad Mesri for hacking and extorting HBO, the press statements and indictment itself did not indicate that this operation was at all directed by the regime in Iran.[64] This same alleged hacker, however, was indicted less than 18 months later for conspiracy, espionage, and cyberattacks on behalf of the Islamic Republic.[65]

Cyber threat intelligence firm Recorded Future calls this a "contractor" model, in which the government and the IRGC work with trusted middlemen who "translate intelligence priorities into segmented cyber tasks."[66] Groups and individuals then vie for these contracts.[67] In essence, in this system, the Iranian regime may not tell the contracted hackers precisely how and when to hit a target. Rather, the government lays out its priorities and what it wants to accomplish, and the middlemen and the hackers figure out how to best to achieve these objectives.[68] In this system, hackers work on behalf of the Iranian regime when "under contract" but also freelance and work on their own projects at the same time, some of which align with regime interests and some of which are purely criminal or commercial operations.[69] While there are numerous government and IRGC bodies responsible for cyber policy (including items such as censorship and infrastructure investment) and defending the regime's own networks and there are even regime-affiliated research institutions that recruit and train would-be hackers, it appears that Iran's offensive cyber operations are committed by individuals and groups working under government contract.[70]

Will Iran Retaliate for Soleimani's Death with Cyberattacks?

The U.S. government, private sector, and allied governments therefore can anticipate that the Islamic Republic will continue to lash out in the cyber domain. Regardless of the motivation behind the attacks—whether to retaliate for the killing of Soleimani or to try to persuade Washington to relieve economic pressure from sanctions—the real-world effects may be the same: disruptive and destructive cyberattack on U.S. interests.

Indeed, prior to Soleimani's death, the U.S. government and private cybersecurity firms were already warning of heightened Iranian cyber activity.[71] Some of these warnings even predate the reported June 2019 U.S. cyberattacks on the Islamic Republic following the downing of the U.S. drone. Days prior to that U.S. operation, cybersecurity firm FireEye noted that it had already observed a

j The Iranian hacker group Cutting Sword of Justice claimed responsibility for the Aramco hack on this message board: Statement, "Untitled," Pastebin, Cutting Sword of Justice, August 15, 2012. See also Thomas Brewster, "U.S. Accuses 7 Iranians Of Cyberattacks On Banks And Dam," *Forbes*, March 24, 2016. The hacker group Izz ad-Din al-Qassam claimed responsibility for the DDoS attacks. See Rym Momtaz and Lee Ferran, "US Bank Cyber Attackers Deny Iran Connection," ABC News, November 12, 2012.

widespread Iranian phishing campaign against U.S. and European governments and companies.[72] According to Israeli cybersecurity firm Check Point, following Washington's imposition of additional oil sanctions on Iran in May 2019 and through the end of the year, Iranian cyberattacks on U.S. entities doubled in comparison to the first half of 2019.[73] Dragos, a cybersecurity firm specializing in industrial control systems (ICS), also observed that throughout the fall of 2019, one APT group was engaged in a broad campaign attempting to infiltrate U.S. electric utilities.[74]

In the weeks following the killing of Qassem Soleimani, the U.S. government issued repeated warnings to the private sector to be vigilant against Iranian cyberattacks.[75] Hours after the strike, Chris Krebs, director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), tweeted the same statement the Department had issued in June 2019 on Iranian cyber threats and reiterated, "time to brush up on Iranian TTPs and pay close attention to your critical systems, particularly ICS. Make sure you're also watching third party accesses!"[76]

Days later, CISA issued guidance to network defenders with a series of standard cyber hygiene reminders, noting that "Iran and its proxies and sympathizers have a history of leveraging cyber and physical tactics to pursue national interests, both regionally and here in the United States."[77] DHS also issued a National Terrorism Advisory System bulletin warning that, among other threats, Iran's cyber capabilities are sophisticated enough to cause temporary disruptions to U.S. critical infrastructure.[78] While the bulletin and subsequent statement in mid-January 2020 from Acting Secretary of DHS Chad Wolf emphasized that the United States had no information indicating a specific, credible threat to the homeland,[79] the FBI also issued an advisory to U.S. companies warning that Iranian hackers have increased their probing and reconnaissance activities.[80]

Cybersecurity firms similarly warned that companies should assume that Tehran will launch a cyberattack in response to Soleimani's killing: John Hultquist of FireEye predicted an increase in cyber espionage against government systems in an attempt to gather intelligence and understand the United States' likely next moves.[81] His colleague Lee Foster and other analysts also warned of likely disinformation operations promoting regime propaganda.[82] Robert Lee of Dragos cautioned against overreaction but urged security professionals to "proactively hunt for threats" on their networks.[83] The chief information and security officer at digital risk firm Digital Shadows also urged companies to review their business continuity and recovery plans.[84] And Kiersten Todt, who previously led the Commission on Enhancing National Cybersecurity, warned that Iranian hackers are likely to attempt to infiltrate the computer networks that run the physical equipment of U.S. critical infrastructure:

> *We should certainly expect an Iranian attempt against our infrastructure; our Industrial Control Systems are particularly vulnerable. Iranian hacking groups like APT33 (also known as Refined Kitten) [are] looking for points of ingress into the U.S. Government (Dept. of Energy, including National Labs) for disruption or espionage; [they are] also looking at how to sabotage ICS by gaining access to networks of ICS suppliers/supply chain security; [there are] reported attempts to create malware for types of ICS used in U.S. power grids and water systems.*[85]

Credit rating agency Moody's concluded simply that "there would likely be a wide range of potential targets."[86]

Most of these warnings recognize that cyberattacks carry inherent advantages for Tehran because the regime can "cause damage without casualties."[87] Stewart Baker, former general counsel at the National Security Agency, explained that the regime is likely seeking "ways to cause pain in the United States without provoking a severe counterattack." Dmitri Alperovitch of CrowdStrike similarly noted that the Islamic Republic perceives cyber operations as "below the thresholds likely to trigger a U.S. retaliation."[88]

If Tehran decides to launch a retaliatory cyber operation, the regime will likely want to conduct an attack that does not provoke the United States to escalate, but rather keeps U.S.-Iran tensions below the threshold of traditional military confrontation. This was the conventional wisdom after the missile attack on the U.S. bases in Iraq. The attack occurred in the middle of the night, and Iran reportedly provided Iraq with advance warning.[89] Coupled with President Trump's statement and Foreign Minister Zarif's tweet,[90] it appears that the regime wanted to conduct a flashy operation while simultaneously minimizing injury, damage, and loss of life. It is worth noting, however, that this conventional wisdom may be wrong. A U.S. commander on the ground stated that Iran's actions were intended to inflict casualties.[91] And as of about a month after the missile strikes, the Pentagon has confirmed more than 100 cases of concussions and traumatic brain injury.[92] This divergence of opinions on Iranian intentions may have parallels in a future cyber confrontation with Iran. If Washington misinterprets Tehran's intentions in an attempted or successful cyberattack, it could result in either a non-response that emboldens the regime to engage in even more provocative cyberattacks or an overreaction by the United States.

Had Iran wanted to respond immediately using its cyber capabilities, it likely would have had to pre-position the capabilities. In short, most types of cyberattacks cannot happen without pre-planning: it often takes a while to scout a network to understand its vulnerabilities and develop malware that can exploit them. Only then can an actor launch a cyber operation. Indeed, Melissa Hathaway, a senior cyber advisor to Presidents Obama and George W. Bush, has stated that likely targets of Iranian operations are systems they have already "mapped."[93] And while Iranian hackers have reportedly been attempting to breach the U.S. electric grid since at least 2015,[94] Tehran either did not have the right pre-positioned assets in place or could not (or chose not to) use them at this time.

While it is possible that Tehran attempted to use its pre-positioned assets but was quickly thwarted (similar to the Israeli Cyber Defense Directorate's response in 2017), the U.S. government's public statements indicate this was not the case. CISA Director Krebs put it this way:

> *"The truth here is that if the Iranians were going to do something, they would probably – it was already too late. If they were going to do something cyber – cybery – they would probably already be in a position and take the shot. We saw that they really didn't. … [They] "didn't have time to strategically position against energy or natural gas."*[95]

Taking Director Krebs' comments at face-value, either Tehran did not have pre-positioned assets that it could deploy or the regime had assets in other sectors besides energy but decided for whatever reason not to "take the shot" at this time. Still, it is this author's assessment that the primary concern for both the private sector and the U.S. government should be that over the medium term, Iranian hackers could increase their probing of networks in order be able to launch cyberattacks in the future at a time of the regime's choosing.

Used exclusively as a retaliatory tool, however, a cyberattack may not provide the regime with the kind of propaganda win that it would be seeking. The U.S. State Department has concluded that "similar to the regime's support for proxies, the Islamic Republic prioritizes plausible deniability for its malicious cyber activities."[96] In a retaliatory action, however, the regime would likely want to send a message that it can do damage to the United States and that Washington "can't do a damn thing" to Iran, as regime leaders often boast.[97] If the regime in Iran launches a cyberattack but does not claim responsibility, it loses the propaganda win. Even if the U.S. government knows the origin of the attacks, unless the regime claims credit, it cannot boast of its successes against "the Great Satan."[98] Claiming credit, however, heightens the likelihood that the United States will counter-strike at least in part to warn Iran and other cyber adversaries that there are consequences to attacks on the U.S. homeland or assets abroad.[k] Claiming credit also removes plausible deniability, which is one of the benefits of cyberattacks in the first place. Thus, the advantages of cyber operations and the goals of a retaliatory action are likely to run contrary, and thus of all of the types of responses Iran can conduct, a cyber operation may be the least advantageous from the regime's perspective.[l]

Regardless of what the regime itself decides to do, Iranian hackers not affiliated or only loosely affiliated with the Iranian government have already begun taking the initiative to launch low-level, unsophisticated cyberattacks. Soon after the drone strike, attempted attacks against U.S. federal, state, and local government websites originating from Iranian IP addresses jumped 50 percent, according to website security firm Cloudflare.[99] Pro-regime hackers successfully defaced websites belonging to the Federal Depository Library Program,[100] the Texas Department of Agriculture,[101] and an Alabama veterans organization.[102] This type of defacement is very simplistic and therefore likely conducted by pro-regime hacktivists looking for the least secure .gov and other websites to score propaganda victories rather than hackers contracted by the Iranian government to conduct a meaningful cyber operation to damage the United States and its allies.

In the days following Soleimani's death, pro-regime, pro-Soleimani, and anti-American messages also exploded on Twitter.[103] Broadly speaking, in recent years, the Islamic Republic has expanded its influence and disinformation operations from traditional state-owned media outlets to social media as well.[104] Researchers assessed that the latest campaign was likely a coordinated effort given how rapidly the hashtag #HardRevenge spread and the fact that the accounts amplified the same messages and were all created within the past few months.[105] It is not clear, however, if the regime was behind the coordination or if merely regime-aligned activists were involved.

There is likely to be a proliferation of attacks aligned with the regime's interests but not necessarily directed by Tehran because of the "contractor" nature of the Iranian hacker community, as discussed earlier. Iranian hackers of varying skill levels may take the initiative to launch attacks they believe the regime would want them to undertake, even when they do not receive direct orders or requests from the government to launch these operations. And because hackers vie for government contracts awarded by middlemen, amateurs may have an incentive to engage in flashy cyber operations at least in part as a way to gain the attention of the middlemen who can award them contracts in the future.

All hackers—ranging from both more professional groups that have conducted government operations in the past to amateur hacktivists—are likely to continue and indeed proliferate their cyber operations. It is difficult to predict, however, if the regime itself will respond to Soleimani's death by commissioning new cyber operations. And yet, it is safe to assume based on past activities that the regime will continue to launch cyber operations as a response to U.S. economic sanctions and other pressure. In short, cyberattacks by Iranians are likely to escalate because hackers believe they are doing what the regime wants them to do, even though they may not receive direct instructions. Meanwhile, the Iranian regime is likely to continue to commission cyberattacks as a response to U.S. economic pressure. These two factors indicate that the Iranian cyber threat will not decrease following Soleimani's death and may in fact increase because of the operations of independent hackers. But, at the same time, the regime may not issue new contracts for cyber operatives to take new actions as a retaliation for Soleimani's death, and thus, his death may also not cause a step-change in the cyber threat that the Iranian regime itself poses. From a U.S. intelligence perspective, these distinctions are important. However, for the victims of Iranian cyber operations, whether the motivation is retaliation for Soleimani's death or a reaction to U.S. sanctions matters little. The real-world effects are similar.

Tehran is likely to focus these cyberattacks on the U.S. private sector rather than direct attacks on the more fortified U.S. government systems for a couple of reasons: 1) The private sector is a 'soft' target, which tends to be what the hackers working on behalf of the regime hit;[106] and 2) there have been no publicly reported instances of the U.S. military responding to a cyberattack on private industry with traditional military strikes. (These attacks can do damage with a low risk of provoking a military counter-response.) Examining past Iranian attacks offers some indication of the specific industries that Iranian hackers will attempt to target. Iranian hackers are likely to hit sectors of the U.S. industry 1) that mirror those Iranian economic sectors targeted under U.S. sanctions and/or 2) that Tehran deems strategically significant to the U.S. economy and national power.

Washington's ability to wield financial power in the form of sanctions is largely the result of the size of the U.S. economy and the dominant role of the dollar in global trade.[107] Targeting the U.S. financial sector (similar to Operation Ababil but perhaps using very different attack vectors) would thus both attack the power Washington uses to apply sanctions on Iran as well as mirror the fact Wash-

k Iranian state-backed hackers have conducted numerous cyberattacks on U.S. interests around the world, including attacks on U.S. allies. Based on public information, none of these has prompted a U.S. military response. If, however, the Iranian regime is responsible for a direct cyber attack on the U.S. homeland or U.S. troops, embassies, or other assets—not U.S. allies or interests, but on Americans—Washington is much more likely to respond with force. This distinction may also explain why the drone and missile attacks on Saudi Arabia did not prompt a U.S. military response but the death of a U.S. contractor and the subsequent attacks on the U.S. embassy in Baghdad prompted military strikes, including the drone strike that killed Soleimani.

l Jan Kallberg, a research scientist at the Army Cyber Institute at West Point and assistant professor at the U.S. Military Academy, has argued that a counter cyber strike on Iran is particularly dangerous for the Islamic Republic because of the instability and internal opposition to the government. Jan Kallberg, "Why Iran would avoid a major cyberwar," Fifth Domain, January 17, 2020. For additional analysis on why Tehran may not find cyberattacks an attractive retaliatory measure, see Jackie Schneider, "Iran can use cyberattacks against the U.S. That's not nearly as bad as it sounds," *Washington Post*, January 6, 2020.

ington has sanctioned the Iranian financial sector.[108] Commercial banks have hardened their systems since 2013, but hackers could still hit the U.S. financial system by targeting companies that facilitate transactions, payments, and trading, as explained recently by financial fraud and data breach analyst Al Pascual.[109] "I would imagine that U.S. organizations that are critical to facilitating financial transactions, like consumer or commercial payments and trading activity, will be at the top of Iran's hit list," he said.[110]

These attacks could be significant. CISA Director Chris Krebs has warned that "Iran has the capability and the tendency to launch destructive attacks."[111] The U.S. intelligence community's annual Worldwide Threat Assessment noted that Tehran is "capable of causing localized, temporary disruptive effects,"[112] and as noted earlier, the Dragos report warned that an APT group has been attempting to infiltrate the U.S. electric grid.[113] Microsoft's security experts observed similar activities and speculated that if successful, Iranian hackers might use their ICS access to launch attacks with disruptive or destructive effects in the physical world.[114]

While Iranian hackers cannot affect the entire grid system, they could disrupt electricity at a local level.[115] And if the Islamic Republic believes that the U.S. government will not respond militarily, the regime may be more likely to unleash its hackers to conduct a risky operation like temporarily disrupting the electric grid in a localized area either to try to coerce the U.S. government into relieving economic pressure, to demonstrate the sophistication of its cyber capabilities, to simply embarrass the United States, or to achieve other regime objectives.

Finally, Iranian hackers could also use their demonstrated capabilities in new ways. For example, Iranian hackers were responsible for the SamSam ransomware attacks on major U.S. cities and healthcare-related companies.[116] SamSam disrupted municipal functions but primarily from a billing and paperwork perspective. Could similar attacks instead be directed in such a way to affect not utility bills but the utilities themselves, particularly the delivery of lifeline services like water and sewage?

The situation could quickly escalate due to Iranian miscalculation or purposeful risky behavior. Suzanne Spaulding, former chief cyber official at DHS during the Obama administration, noted that the regime has "a high tolerance for escalating risk," pointing in particular to the 2011 plot to assassinate the Saudi ambassador to the United States at a popular Washington, D.C., restaurant.[117] The "current risk of escalatory action by Iran is particularly high, given that the 'red lines' are not clearly defined in cyberspace," she explained.[118]

Conclusion

While the United States has yet to suffer a debilitating cyberattack at the hands of the Islamic Republic, the threat has not diminished, and continued vigilance by the U.S. government and private sector is critical. Whether as a retaliatory strike for the killing of Qassem Soleimani or as part of its campaign to pressure the United States to lift economic sanctions, Tehran is likely plotting its next move in cyberspace.

In fact, Soleimani's death may have little impact on the cyber threat posed by the Iranian government. Based on statements from Iranian government officials[119] as well as the structure of Iran's military forces and trend lines of its recent operations,[120] the killing of Soleimani is unlikely to have reduced the regime's appetite for dangerous and aggressive behavior, and thus Tehran is likely to continue its malign activity in cyberspace. As discussed, regime-sponsored attacks were already ongoing prior to the January 2020 drone strike and have continued since at least in part because of the damage that U.S. sanctions are imposing on Iran. And while hackers appear to be taking their own initiative to launch cyber operations in retaliation for the killing of Soleimani, based on public information, there is no evidence at this point that the regime itself has issued new directions to middlemen to contract out new cyber operations to retaliate for the U.S. killing of General Soleimani.

Over the longer term, it will be important to assess how much control the regime has over its contractors, specifically related to the question of whether and what might happen if contractors engage in riskier and more destructive attacks than the regime wants. Might this situation force the regime to exert greater control over its hacker community? And how would this change the U.S. intelligence community's assessment of the Iranian cyber threat? At the same time, however, the contractor model and plausible deniability may enable or encourage the regime to take greater risks in the future—something which must also be factored into U.S. threat assessments.

For now, however, even as the Defense Department has announced a new cyber strategy focused on engaging the adversary in cyberspace outside of U.S. government networks and potentially on the adversary's own networks to "to disrupt or halt malicious cyber activity at its source"[121]– a policy known as "defend forward"[m] – the U.S. government more broadly has continued to rely on law enforcement and financial sanctions tools to combat malicious cyber activities.[122] Yet these actions seem to have failed to deter Iranian hackers. For example, after the Department of Justice indicted nine state-sponsored Iranian hackers engaged in a massive cyber theft operation against universities in the United States and around the world,[123] the same hackers resumed their activities only months later.[124] The indictment has no real-world impact because the U.S. government simply cannot extradite these hackers, and the Iranian government appears not to have rescinded their 'contract' as a result of them getting caught.

Thus, rather than focusing on deterrence through punishment (particularly if the punishment is confined to actions that amount to naming and shaming hackers), the United States may be more successful at preventing or at a minimum thwarting Iranian cyber operations by focusing on deterrence through denial—that is, by preventing the Islamic Republic from achieving its desired outcomes in cyberspace. Regardless of the regime's motives, the United States is more likely to be able to prevent attacks by ensuring the targets of Iranian malicious cyber operations have the specific information they need to defend themselves or remediate and recover quickly in the event of an attack. For example, in the days following Soleimani's death, the New York Department of Financial Services (DFS) not only provided general cyber hygiene recommendations to all regulated entities, but also warned these companies that "Ira-

m As Robert Chesney, associate dean at the University of Texas Law School, explains, "defense forward entails operations that are intended to have a disruptive or even destructive effect on an external network: either the adversary's own system or, more likely, a midpoint system in a third country that the adversary has employed or is planning to employ for a hostile action." Robert Chesney, "The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes," Lawfare, September 25, 2018.

nian hackers are known to prefer attacking over the weekends and at night precisely because they know that weekday staff may not be available to respond immediately." DFS then reminded these companies to ensure that their alert systems respond quickly "even outside of regular business hours."[125]

While examining prior Iranian cyber operations provides insights into possible future targets, to be best prepared to thwart Iranian cyber operations, it is necessary to understand what Tehran views as the industries that are critical to U.S. power. This type of assessment, paired with the analysis of regular chatter on hacker forums and other intelligence, may illuminate a list of possible future targets of Iranian cyber operations. These future targets would thus be the priority list for U.S. government engagement with the private sector on cyber defense. If the partnership between government and industry can reduce the effects of the Islamic Republic's cyber operations, the United States will have weakened a key pillar of Tehran's asymmetric strategy. CTC

Citations

1 Behnam Ben Taleblu, "Making sense of Iranian escalation," FDD's Long War Journal, May 20, 2019.
2 "Remarks by President Trump on the Joint Comprehensive Plan of Action," White House, May 8, 2018; Michael R. Pompeo and Steven T. Mnuchin, "Update on Iran Policy and Sanctions," briefing at the Foreign Press Center, November 5, 2018.
3 Mark Mazzetti, Ronen Bergman, and Farnaz Fassihi, "How Months of Miscalculation Led the U.S. and Iran to the Brink of War," *New York Times*, February 13, 2020.
4 Amy Teibel, "Iran's Rouhani Says U.S. Sanctions Cost Country $200 Billion," Bloomberg, December 31, 2019.
5 Saeed Ghasseminejad, "Inflation in Iran Reaches 23-year Peak," Foundation for Defense of Democracies, August 13, 2019.
6 Davide Barbuscia, "Iran recession to deepen, reserves to fall to $73 billion by March: IIF," Reuters, January 15, 2020.
7 David D. Kirkpatrick, Richard Pérez-Peña, and Stanley Reed, "Tankers Are Attacked in Mideast, and U.S. Says Video Shows Iran Was Involved," *New York Times*, June 13, 2019.
8 Joshua Berlinger, Mohammed Tawfeeq, Barbara Starr, Shirzad Bozorgmehr, and Frederik Pleitgen, "Iran shoots down US drone aircraft, raising tensions further in Strait of Hormuz," CNN, June 20, 2019.
9 Andy Greenberg, "Iranian Hackers Launch a New US-Targeted Campaign as Tensions Mount," *Wired*, June 20, 2019.
10 Raphael Satter and Christopher Bing, "Exclusive: Iran-linked hackers pose as journalists in email scam," Reuters, February 5, 2020; "Fake Interview: The New Activity of Charming Kitten," Certfa Lab, February 5, 2020.
11 Julian E. Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyberattacks on Iran," *New York Times*, June 22, 2019; Ellen Nakashima and Paul Sonne, "U.S. military carried out secret cyberstrike on Iran to prevent it from interfering with shipping," *Washington Post*, August 28, 2019.
12 Allison Quinn and Jamie Ross, "Trump: We Were 'Cocked & Loaded' Before I Scuttled Iran Strike," Daily Beast, June 21, 2019.
13 Idrees Ali and Phil Stewart, "Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials," Reuters, October 16, 2019.
14 "Treasury Designates Individual, Entity Posing Threat to Stability in Iraq," U.S. Department of the Treasury, July 2, 2009; "The Foreign Terrorist Organization List," Congressional Research Service, updated January 15, 2019.
15 Julian E. Barnes, "American Contractor Killed in Rocket Attack in Iraq," *New York Times*, December 27, 2019.
16 Nicole Darrah, "US conducts airstrikes in Iraq, Syria after contractor killed, American troops injured in rocket attack," Fox News, December 30, 2019.
17 Saphora Smith, "Iraqi protesters withdraw from perimeter of U.S. Embassy, building now secured," NBC News, January 1, 2020.
18 Clifford D. May, "Iranian regime's 'gray-zone' war tactics are the new norm," *Washington Times*, January 21, 2020.
19 Alex Leary, Nancy A. Youssef, Aresu Eqbali, and Sune Engel Rasmussen, "U.S. and Iran Back Away From Open Conflict," *Wall Street Journal*, January 9, 2020.
20 Javad Zarif, "Iran took & concluded proportionate measures in self-defense under Article 51 of UN Charter …," Twitter, January 7, 2020.
21 Jonathan Schanzer and Behnam Ben Taleblu, "Where the US-Iran shadow war goes from here," *Washington Examiner*, January 9, 2020.
22 Tim Starks, "FBI stresses vigilance against pro-Iranian hackers," Politico, January 30, 2020.
23 Daniel R. Coats, Statement for the Record, "Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, January 29, 2019, p. 6.
24 Rebecca Klar, "Soleimani successor vows revenge for US strike," Hill, January 6, 2020; "Soleimani successor: continuity figure in uncertain times," Agence France-Presse, January 8, 2020.
25 Sam Jones, "Cyber warfare: Iran opens a new front," *Financial Times*, April 26, 2016.

26 Ibid.
27 Joseph Marks, "The Cybersecurity 202: Get ready for serious cyberattacks from Iran, experts say," *Washington Post*, January 13, 2020.
28 Annie Fixler and Frank Cilluffo, *Evolving Menace: Iran's Use of Cyber-Enabled Economic Warfare* (Washington, D.C.: Foundation for Defense of Democracies, 2018). For an in depth look at the Islamic Republic of Iran's concepts and doctrines of warfare, see J. Matthew McInnis, *Iranian Concepts of Warfare: Understanding Tehran's Evolving Military Doctrines* (Washington, D.C.: American Enterprise Institute, February 2017).
29 Testimony, Lt. Gen. (ret) Vincent Stewart, "U.S.-Iran Tensions: Implications for Homeland Security," House Committee on Homeland Security, January 15, 2020.
30 Iran Action Group, *Outlaw Regime: A Chronicle Of Iran's Destructive Activities* (Washington, D.C.: U.S. Department of State, 2018), p. 32.
31 Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge* (Washington, D.C.: Carnegie Endowment for International Peace, 2018), p. 6.
32 Fixler and Cilluffo.
33 "Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions," Symantec, July 25, 2018; "Rocket Kitten: A Campaign with 9 Lives," Check Point, 2015; Robert Falcone and Bryan Lee, "The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor," Palo Alto Networks, May 26, 2016.
34 Anderson and Sadjadpour, pp. 34-35; "The Iranian-Saudi Conflict and Its Cyber Outlet," Recorded Future, June 26, 2015.
35 Yoav Limor, "Cyber Defense Head: Iranians Attempt to Disrupt Home Front Command," Israel Hayom, February 8, 2018; Gwen Ackerman, "Iranian Hackers Drew Worryingly Close to Israel's Missile Alarm," Bloomberg, February 24, 2019.
36 Ms. Smith, "Saudi Arabia again hit with disk-wiping malware Shamoon 2," CSO, January 24, 2017; "Shamoon 2 Malware," IBM X-Force Exchange, accessed February 5, 2020; "Shamoon: Multi-staged destructive attacks limited to specific targets," Symantec, January 27, 2017.
37 Jacqueline O'Leary, Josiah Kimble, Kelli Vanderlee, and Nalani Fraser, "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware," FireEye, September 20, 2017.
38 Muks Hirani, Sarah Jones, and Ben Read, "Global DNS Hijacking Campaign: DNS Record Manipulation at Scale" FireEye, January 9, 2019. The FireEye report coincided with a DHS emergency directive about DNS spoofing, although it is unclear if these were the same or different campaigns. "Mitigate DNS Infrastructure Tampering," Emergency Directive 19-01, U.S. Department of Homeland Security, January 22, 2019.
39 Ackerman.
40 "Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions."
41 Robert McMillan, "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years," *Wall Street Journal*, March 6, 2019.
42 Feike Hacquebord, Cedric Pernet, and Kenney Lu, "More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting," Trend Micro, December 12, 2019.
43 "CISA Statement on Iranian Cybersecurity Threats," U.S. Department of Homeland Security, June 22, 2019.
44 Tom Burt, "Recent cyberattacks require us all to be vigilant," Microsoft, October 4, 2019.
45 Andy Greenberg, "Iranian Hackers Have Been 'Password-Spraying' the US Grid," *Wired*, January 9, 2020; *North American Electric Cyber Threat Perspective* (Hanover, MD: Dragos, 2020), pp. 1, 4, 6, and 10.
46 Limor Kessem and X-Force IRIS, "New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East," IBM Security Intelligence, December 4, 2019.
47 Andy Greenberg, "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems," *Wired*, November 20, 2019.
48 Jose Pagliery, "The inside story of the biggest hack in history," CNN Money, August 5, 2015; Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012.
49 Pagliery.
50 Fixler and Cilluffo.
51 Ibid.
52 Michael Eisenstadt, *Iran's Lengthening Cyber Shadow* (Washington, D.C.: The Washington Institute for Near East Policy, 2016), p. 6.
53 Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times*, January 8, 2013.
54 "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," U.S. Department of Justice, March 24, 2016; Indictment, United States of America v. Ahmad Fathi et al, 16 Cr. (S.D.N.Y filed March 16, 2016).
55 "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged."
56 Perlroth and Hardy.
57 Cyber-enabled economic warfare tabletop exercise, not-for-attribution remarks, hosted by the Foundation for Defense of Democracies, Washington, D.C., October 2018.
58 Indictment, *United States of America v. Ahmad Fathi et al*.
59 Mark Dubowitz and Rachel Ziemba, "When Will Iran Run Out of Money?" Foundation for Defense of Democracies and Roubini Global Economics, October 1, 2013; Mark Dubowitz, Jennifer Hsieh, and Rachel Ziemba, "Iran's Economy Will Slow But Continue To Grow Under Cheaper Oil and Current Sanctions," Foundation for Defense of Democracies and Roubini Global Economics, February 4, 2015.
60 Perlroth and Hardy. See also Fixler and Cilluffo.
61 Mark Dubowitz and Annie Fixler, *'SWIFT' Warfare: Power, Blowback, and Hardening American Defenses* (Washington, D.C.: Foundation for Defense of Democracies, 2015), pp. 8-16.
62 "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged;" Dante D'Orazio, "US officials claim Iran behind cyberattack on Saudi oil firm, suggest it's a retaliation," Verge, October 24, 2012.
63 Anderson and Sadjadpour, pp. 18, 23-25.
64 "Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO," U.S. Department of Justice, November 21, 2017.
65 "Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues," U.S. Department of Justice, February 13, 2019.
66 Levi Gundert, Sanil Chohan, and Greg Lesnewich, *Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations* (Somerville, MA: Recorded Future, 2018).
67 For more information on how and why this system developed, see Fixler and Cilluffo.
68 For comparison, Russia tends to "piggy back" on criminal hackers when conducting its operations while China relies on hackers employed directly by the government. Boris Zilberman, *Kaspersky and Beyond Understanding Russia's Approach to Cyber-Enabled Economic Warfare* (Washington, D.C.: Foundation for Defense of Democracies, 2018), pp. 13-15; Zack Cooper, *Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare* (Washington, D.C.: Foundation for Defense of Democracies, 2018), pp. 13-16.
69 For additional analysis of the Iranian regime's relationship with hackers and its historical reliance on proxies, see Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York: Cambridge University Press: 2018), Chapter 5, "Cyber Proxies on a Loose Leash: Iran and Syria."
70 See section on "Architecture of Cyber Warfare" in Fixler and Cilluffo.
71 Annie Fixler, "Iran Escalates Cyber Operations Targeting U.S.," Foundation for Defense of Democracies, July 8, 2019.
72 Greenberg, "Iranian Hackers Launch a New US-Targeted Campaign as Tensions Mount."
73 Mazzetti, Bergman, and Fassihi.
74 Greenberg, "Iranian Hackers Have Been 'Password-Spraying' the US Grid;" *North American Electric Cyber Threat Perspective*, pp. 1, 4, 6, and 10.
75 For example, U.S. Department of Homeland Security, "Increased Geopolitical Tensions and Threats," CISA Insights, January 6, 2020.
76 Chris Krebs, "Given recent developments, re-upping our statement from the summer ..." Twitter, January 2, 2020.
77 "Increased Geopolitical Tensions and Threats."
78 U.S. Department of Homeland Security, "Summary Of Terrorism Threat To The U.S. Homeland," National Terrorism Advisory System Bulletin, January 4, 2020.
79 Charlie Mitchell, "DHS chief Wolf expounds on efforts to counter cyber, other threats from China, Russia and Iran," Inside Cybersecurity, January 17, 2020.
80 Sean Lyngaas, "FBI says Iranian hackers have stepped up reconnaissance since Soleimani killing," CyberScoop, January 10, 2020.
81 Sean Lyngaas and Shannon Vavra, "After U.S. kills Iranian general, an-

alysts warn of Tehran's ability to retaliate in cyberspace," CyberScoop, January 3, 2020.
82 Eduard Kovacs, "Iran May Respond With Cyberattacks to Killing of Qassem Soleimani," Security Week, January 3, 2020; Tony Romm, Isaac Stanley-Becker, and Craig Timberg, "'A cyberattack should be expected': U.S. strike on Iranian leader sparks fears of major digital disruption," *Washington Post*, January 3, 2020.
83 Lyngaas and Vavra.
84 Kovacs.
85 Charlie Mitchell, "Industrial operators on notice about enhanced Iranian cyber threat," Inside Cybersecurity, January 7, 2020.
86 Michael B. Farrell, "Signs of hacking in Georgia prior to 2016 vote," Politico, January 17, 2020.
87 Marks.
88 Ibid.
89 Martin Chulov, "Dialled down: Iran's phoned-in attack just enough to ease tensions," *Guardian*, January 8, 2020; Howard Altman, Aaron Mehta, Shawn Snow, and Meghann Myers, "Iran didn't kill anyone in missile attack, spurring hopes for de-escalation," *Military Times*, January 8, 2020.
90 Leary, Youssef, Eqbali, and Rasmussen; Zarif.
91 Louisa Loveluck, "U.S. commanders at al-Asad base believe Iranian missile barrage was designed to kill," *Washington Post*, January 13, 2020.
92 Barbara Starr, "Over 100 US troops have been diagnosed with traumatic brain injuries following Iran strike," CNN, February 10, 2020.
93 Charlie Mitchell, "Heightened U.S.-Iran tensions may bring 'national reckoning' in cyberspace," Inside Cybersecurity, January 6, 2020.
94 Garance Burke, "AP Investigation: US power grid vulnerable to foreign hacks," Associated Press, December 21, 2015.
95 Andrew Eversden, "Top DHS cyber official discusses when Iran may retaliate in cyberspace," Fifth Domain, January 17, 2020.
96 *Outlaw Regime*, p. 31.
97 "US embassy attack: Trump threatens Iran over violent protest in Iraq," BBC, January 1, 2020. "
98 See David Brennan, "Trump's Treatment Of Iran Will Ensure America Remains The 'Great Satan' For Decades To Come," *Newsweek*, November 5, 2019.
99 Brian Fung, "Hacking attempts originating in Iran nearly triple following Soleimani strike, researchers say," CNN Business, January 8, 2020.
100 Allyson Chiu, "A government website was 'defaced' with pro-Iran messaging and an image of a bloodied Trump. Hackers claimed responsibility," *Washington Post*, January 6, 2020.
101 Benjamin Freed, "Texas government website defaced with pro-Iran message," StateScoop, January 7, 2020.
102 Joseph Cox, "Iranian Hackers Claim Defacement of Texas Government and Alabama Veterans Websites," VICE, January 7, 2020.
103 Jeff Stone, "Pro-Soleimani messaging immediately floods Twitter following general's death in drone strike," CyberScoop, January 3, 2020.
104 Patrick Tucker, "Iran Is Expanding Its Online Disinformation Operations," Defense One, January 9, 2020. See also Adam Rawnsley, "New York Post Reporter's Identity Hijacked to Spread Pro-Iran Propaganda," Daily Beast, January 8, 2020.
105 Stone.
106 *Outlaw Regime*, p. 31.
107 Juan Zarate, Testimony, "Sanctions and Financial Pressure: Major National Security Tools," House Foreign Affairs Committee, January 10, 2018, p. 5; Eric B. Lorber, *Securing American Interests: A New Era of Economic Power* (Washington, D.C.: Foundation for Defense of Democracies, 2017), p. 11. For an in-depth analysis of U.S. economic power and the use of sanctions, see Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: PublicAffairs, 2013).
108 See, for example, David Cohen, Testimony, "Negotiations on Iran's Nuclear Program," Senate Committee on Foreign Relations, February 4, 2014; and Dubowitz and Fixler, pp. 8-16.
109 Penny Crosman, "Should banks expect cyberattacks from Iran?" *American Banker*, January 7, 2020.
110 Ibid.
111 Zolan Kanno-Youngs and Nicole Perlroth, "Iran's Military Response May Be 'Concluded,' but Cyberwarfare Threat Grows," *New York Times*, January 8, 2020.
112 Coats, p. 6.
113 *North American Electric Cyber Threat Perspective*, pp. 1, 4, 6, and 10.
114 Dorothy Denning, "Explainer: How Iran's military outsources its cyberwarfare forces," *Navy Times*, January 23, 2020.
115 Marks.
116 "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," U.S. Department of Justice, November 28, 2018.
117 Kovacs.
118 Ibid.
119 Klar; "Soleimani successor: continuity figure in uncertain times."
120 Behnam Ben Taleblu, "Remember, Iran's Terror Network Is Global," Radio Farda, February 8, 2020; Behnam Ben Taleblu, "Iran is increasingly using missiles in its military operations — that's a problem," Hill, January 21, 2020.
121 "Summary of Department of Defense Cyber Strategy," U.S. Department of Defense, September 2018.
122 Annie Fixler and David Maxwell, "Midterm Assessment: Cyber," Foundation for Defense of Democracies, January 31, 2019.
123 "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps," U.S. Department of Justice, March 23, 2018.
124 Charlie Osborne, "Iranian hackers target 70 universities worldwide to steal research," ZDNet, August 24, 2018; Danny Palmer, "Iranian hackers resume credential-stealing phishing attacks against universities around the world," ZDNet, September 11, 2019; Sean Lyngaas, "'Cobalt Dickens' group is phishing universities at scale again, researchers say," CyberScoop, September 11, 2019.
125 "Department of Financial Services Issues Alert to Regulated Entities Concerning Heightened Risk of Cyber Attacks," New York State Department of Financial Services, January 4, 2020.

"Breaking the Walls" Goes Global: The Evolving Threat of Jihadi Prison Assaults and Riots

By Bennett Clifford and Caleb Weiss

Assaulting prisons and inciting prison riots are cornerstones of jihadi operational strategy. Jihadi groups target prisons as sites for attacks to free operatives and leaders from detention, and to create propaganda wins against their adversaries. While jihadi attacks on prisons and prison riots have been frequently employed by the jihadi movement, during the past few years, a new string of these incidents have affected prison systems in the Sahel, Southeast Asia, and Central Asia. In each case, severe deficits in basic prison security mechanisms provided opportunities for jihadis to exploit, allowing them to launch successful attacks on prison facilities and orchestrate prison riots that escalated into mass violence.

Many counterterrorism analysts and practitioners view jihadi-inspired attacks targeting prisons as both short-term and longer-term security risks.[1] In many countries' prison systems, the numbers of individuals incarcerated for supporting the Islamic State and other jihadi groups has risen to a historically unprecedented level during the past few years.[2] With the cessation of territorial control of the Islamic State inside Iraq and Syria, many of its onetime combatants are currently detained in prisons and camps throughout the Levant. The most infamous facility is the Syrian Democratic Forces (SDF)-administered al-Hol camp, which currently houses over 60,000 people, of which approximately 9,000 are foreign (non-Syrian and non-Iraqi) citizens.[3a] Since the fall of the Islamic State's territorial caliphate, the group frequently incites its supporters in the region to free its affiliates who are held in facilities in Syria and Iraq.[4] A report submitted by U.N. monitors in December 2019 to the United Nations Security Council noted that the Islamic State was "calling and planning for the breakout of ISIL fighters in detention facilities" and noted the "precariousness of the holding arrangements of local authorities and non-State armed groups for displaced persons and detainees."[5]

The Islamic State and other jihadi groups have also incited attacks and riots outside of the Levant. With the large number of detained jihadis worldwide, the fear is that the groups to which they belong may either target prisons for attacks with the aim of releasing them or the incarcerated jihadis will spark riots and assault staff. During the past three years, several notable examples of both types of attacks occurred in several prison systems around the globe. In many instances, mostly within prisons in Western Europe and North America, a single inmate or small group of jihadi inmates carried out small-scale attacks against correctional staff or other inmates.[6] These incidents largely did not escalate into mass violence, and the perpetrators are usually detained swiftly before casualties mounted. In contrast, a number of assaults by jihadi groups and in-prison riots involving large groups of perpetrators mobilized by detained jihadis took place, mostly in prison systems outside the West.[b] These incidents escalated into mass violence between the attackers and correctional staff, law enforcement, or military special response teams.

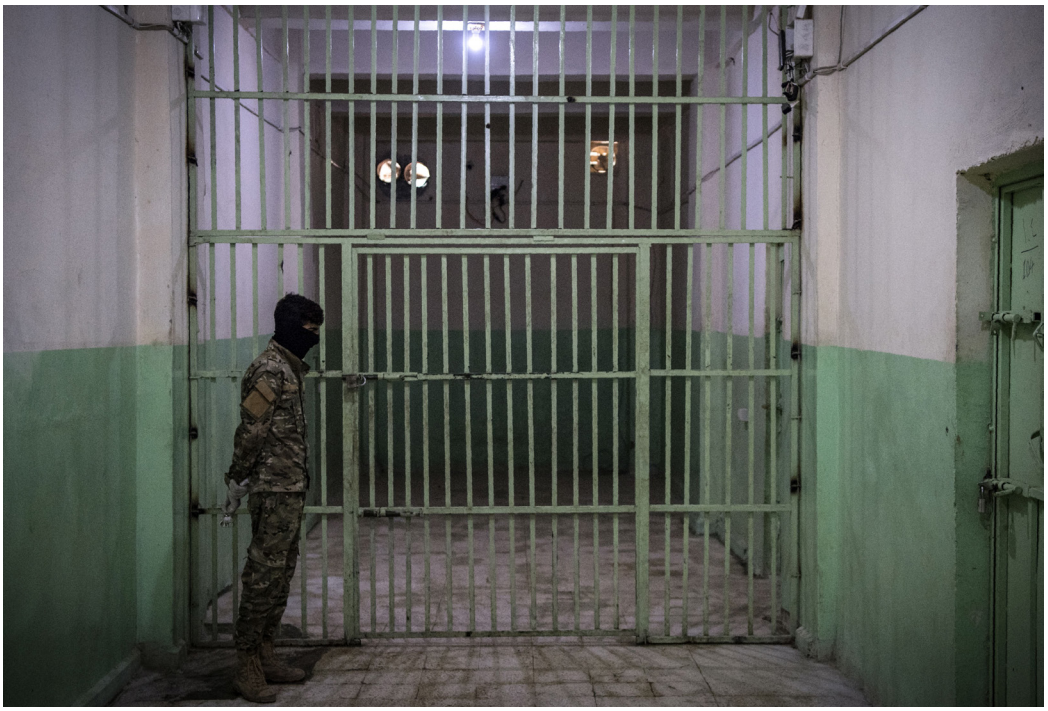
This article focuses mainly on the second type of jihadi prison attacks and riots, which resulted in either substantial casualty figures or mass escapes. To understand this phenomenon and assess its threat, this article reviews both jihadi attacks on prison facilities and mass riots sparked by Islamic State-affiliated prisoners during

Bennett Clifford is a research fellow at the Program on Extremism at George Washington University and a Master of Arts in Law and Diplomacy candidate at The Fletcher School at Tufts University. Follow @_bCliff

Caleb Weiss is a research analyst and contributor to FDD's Long War Journal, where he focuses on political violence and jihadism in the Middle East and Africa, and a Master of Arts in Law and Diplomacy candidate at The Fletcher School at Tufts University. Follow @Weissenberg7

a Recent estimates of the total population and the number of Islamic State fighters held in northeastern Syria vary. In December 2019, one United Nations member state reported that in the al-Hol camp alone, the total population exceeded 100,000 people, 10,000 of whom were male Islamic State fighters. The number of foreign (non-Syrian and non-Iraqi) Islamic State fighters in the camp was reported by this member state to be approximately 2,000. Outside of al-Hol, the SDF has been reported to hold thousands more in various other detention facilities. For example, as of January 2020, the SDF was reportedly holding 4,000 Islamic State prisoners in northeastern Syria. If the numbers of 2,000 in al-Hol are accurate, then it is likely the other 2,000 reported prisoners are outside of al-Hol. See "Twenty-fifth report of the Analytical Support and Sanctions Monitoring Team concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities," United Nations, December 27, 2019, and Jeff Seldin, "In Syria, Captured Islamic State Fighters, Followers Going Home," Voice of America, January 23, 2020.

b For example, this article analyzes a May 2018 jihadi prison riot in Indonesia and two jihadi prison riots in Tajikistan, in November 2018 and May 2019, respectively.



A member of the Syrian Democratic Forces stands guard in a prison where men suspected of being affiliated with the Islamic State are jailed in Hasakeh, Syria, on October 26, 2019. (Fadel Senna/AFP via Getty Images)

the past few years, with the hopes of situating these incidents within the recent history of prison attacks. The authors' findings are twofold. First, drawing on previous literature, historical attacks, and the current reemergence of jihadi groups' attempts to target prison systems, the authors find that three considerations drive jihadi prison assaults and riots. In planning these types of attacks, jihadis are interested in restoring their force size, releasing incarcerated jihadi leaders or specialists, and/or creating a propaganda win.

Second, prison assaults and riots are opportunistic. Jihadis exploit profound weaknesses in prison system management, resources, intelligence, and wherewithal in order to conduct attacks. The authors analyze a string of highly successful raids on prisons by Sahelian jihadi groups during the past five years, as well as prison riots in Indonesia and Tajikistan perpetrated by Islamic State supporters. Specifically, several of the prison facilities examined in the article faced one or more of these problems: severe overcrowding, a lack of basic security infrastructure and effective management regimes for terrorist offenders, and/or recent facility conversion into prison wings for terrorist offenders. In the Sahel, Indonesia, and Tajikistan, jihadi perpetrators took advantage of these opportunities, and disturbances were able to escalate into successful attacks and riots.

After an explanation of the recent historical incidences of prison assaults and riots perpetrated by jihadi groups, this article places recent cases in the Sahel, Indonesia, and Tajikistan in the broader strategy and history of these types of attacks. In examining these cases, the assessments demonstrate that jihadi groups were able to exploit a lack of basic security infrastructure within the prison systems that they targeted. The last part of this article looks at possible future trends. Due to the continued strategic importance of prison assaults and riots, the increasing number of jihadi detainees worldwide, and permissive environments in prison systems, jihadi groups are likely to continue their campaigns of targeting prisons and jails.

The Recent History and Strategy of Prison Assaults and Riots

To answer the question of the strategy behind why a jihadi group might execute or even prioritize attacks on or inside prisons, the authors postulate three possible scenarios: 1) force regeneration; 2) freeing high-value individuals; and 3) propaganda value. The first possible scenario, force regeneration, is perhaps the most prominent. Following sustained military operations against it, the jihadi group may stand to regenerate some of its lost manpower by conducting assaults on prisons. As Trevor Cloen, Yelena Biberman, and Farhan Zahid found, these types of assaults in places with weak central authorities have been "low cost, high reward" operations for these groups.[7]

This logic is exemplified by the Islamic State of Iraq's "Breaking the Walls" campaign from 2012-2013, which as Aki Peritz described "enabled the Caliphate's rise" by freeing hundreds of fighters from prisons across Iraq.[8] As part of this campaign, the Islamic State of Iraq targeted prisons in Kirkuk, Tikrit, Taji, Abu Ghraib, and other facilities, resulting in "at least eight separate jailbreaks in Iraq that freed hundreds of senior- and mid-level ISIS militants."[9] By the end of the "Breaking the Walls" campaign, the Islamic State of Iraq had restored its ranks with hundreds of previously detained, skilled operatives, setting the stage for its resurgence and the transition into the Islamic State of Iraq and Syria. Due to its success and strategic importance, the Islamic State's jailbreak strategy can now be considered part of the group's organizational fabric.[10] As Craig Whiteside, Ian Rice, and Daniele Raineri astutely argued in 2019, "prisons, and the valuable human capital they contain, will be the key to any future resurgence of the group."[11]

However, this dynamic is not exclusive to Iraq or the Islamic

State. The Movement of the Taliban in Pakistan (or the Pakistani Taliban, TTP) conducted at least two large-scale prison assaults in 2012-2013, which also freed hundreds of fellow jihadis from Pakistani prisons.[12] Meanwhile, in Afghanistan, Taliban prison breaks in 2008,[13] 2011,[14] and 2015[15] freed almost 2,000 fighters combined. In each case, these operations have undoubtedly impacted these groups' longevity and overall operational capacity.

Looking at the authors' second scenario, the freeing of high-value individuals, this also stands to have severe long-term consequences for jihadi groups. For instance, in 2006, Nasir al-Wuhayshi and 22 other al-Qa`ida members escaped from a prison in Sana'a, Yemen.[16] These individuals would provide the nexus of the first generation of leadership for what would become al-Qa`ida in the Arabian Peninsula (AQAP).[17] While al-Wuhayshi would become AQAP's first emir, he would also eventually, before his death, become the "general manager" of al-Qa`ida's overall global network.[18] Al-Wuhayshi's successor as the second AQAP emir, Qasim al-Raymi, another jihadi veteran, also escaped from the Sana'a prison alongside al-Wuhayshi.[19]

More recently, in 2014, AQAP launched a massive operation against Sana'a's central prison.[20] Utilizing suicide bombers and an assault team, the group was able to free at least 29 fellow jihadis, including several key operatives.[21] A year later, AQAP launched an assault on Mukallah's central prison, which freed over 300 jihadis including Khalid Batarfi.[22] Batarfi, an important AQAP commander prior to his arrest in 2011, resumed his role as a senior AQAP leader upon being freed.[23] Following the January 2020 death of Qasim al-Raymi,[24] Batarfi was selected as the new AQAP emir.[25] And much like al-Wuhayshi, FDD's Long War Journal has assessed that Batarfi likely plays a key role in al-Qa`ida's global leadership.[26] Batarfi's appointment also means that all three emirs of AQAP have been prison escapees.

Lastly, the authors posit that the propaganda value of prison breaks or assaults on/in prisons is twofold. First, the individual groups can message to its supporters or allies that it does not forget its imprisoned members, akin to the "leave no man behind" mantra. Secondly, these operations can send a powerful message to the outside world about the lack of state capacity and the exploitation thereof.

Though virtue signaling about freeing prisoners to a group's supporters or allies is a common theme in jihadi propaganda, it is a core part of their strategy.[27] For instance, in his final message as the leader of the Islamic State in September 2019, Abu Bakr al-Baghdadi told his followers to "do your utmost to rescue your brothers and sisters and break down the walls that imprison them."[28] This notion was repeated by Abu Hamza al-Quraishi, the Islamic State's current spokesman, when he announced the deaths of both al-Baghdadi and former spokesman Abul Hassan al-Muhajir. In that message, al-Quraishi repeated al-Baghdadi's appeal to "set free the captive Muslims from their prisons [and] remove unjust from the oppressed."[29] A January 2020 report to the United Nations Security Council notes that due to the continuity in the Islamic State's messaging about freeing detained fighters before and after al-Baghdadi's death, "the plight of ISIL detainees and refugees" will continue to be "the worst and most important matter" for the group.[30]

In Pakistan, the TTP and the Islamic Movement of Uzbekistan (IMU) even formed an entire unit dedicated to freeing jihadi prisoners in 2013.[31] That unit, Ansar al Aseer (Helpers of the Prisoners), was likely responsible for at least one prison assault in Pakistan's Khyber Pakhtunkhwa, which freed at least 200 inmates.[32] In its inaugural video in January 2013, a Russian-speaking member of IMU's contingent to the unit noted that "our beloved brothers and sisters have had to live in captivity, when they spit, they spit blood."[33] Making a call to action to the entire Muslim world, he also added, "yet this 1.5 billion-strong Ummah [worldwide Islamic community] is doing nothing about it."[c]

On social media, jihadis have established at least two recent campaigns on the online messaging platform Telegram dedicated to the issue of jihadi prisoners.[d] The Islamic State-oriented Kafel[34] and the pro-al-Qa`ida Fukku al Asirat (Free the Female Prisoners)[35] channels have posted in support of jihadi prisoners held in makeshift camps and prisons in northern Syria. In addition to propaganda regarding the freeing of jihadi prisoners, Kafel has even posted photos of Islamic State-loyal women inside these camps—often depicting the women pleading for outside help.[36] Fukku al Asirat, on the other hand, has allegedly helped with the smuggling of female jihadi prisoners out of these camps.[37]

The need to free well-known prisoners is also a staple of jihadi propaganda. For example, al-Qa`ida propaganda routinely discusses the freeing of Aafia Siddiqui, colloquially known as "Lady al-Qa'ida," from her cell in a Texas prison.[38] Prior to her arrest in 2008, Siddiqui was alleged by U.S. officials to have been involved in the plotting of several attacks inside the United States.[e] Since then, she has become a common talking point of al-Qa`ida and its various branches around the world. In 2015, her plight became the subject of a high-profile terrorism case in the United States. A year earlier, Abdirahman Sheik Mohamud, a U.S. citizen, traveled to Syria to fight with Jabhat al-Nusra, then al-Qa`ida's branch in Syria.[39]

According to the court documents, Mohamud was instructed by al-Nusra to return to the United States to conduct an attack.[40] As a result, Mohamud plotted to target the Federal Medical Center, Carswell in Fort Worth, Texas, where Siddiqui is held, before his arrest.[41] During Mohamud's sentencing, the presiding judge stated that Mohamud's goal was to free Siddiqui from the prison.[42]

Another common jihadi cause was that of freeing Omar Abdel Rahman, or "The Blind Sheikh." Prior to his death in a North Car-

c Interestingly, that Russian-speaking jihadi, Abdul Hakim al-Tatari, would defect to the Islamic State with most of the IMU in early 2015. He would then join the Islamic State's Wilayat Khorasan before migrating to Iraq. He was killed in action near Baiji, Iraq, in late 2015 and later eulogized by the Islamic State. See Caleb Weiss, "Islamic State eulogizes former Islamic Movement of Uzbekistan figure killed in Iraq," FDD's Long War Journal, November 8, 2017.

d In late November 2019, Telegram undertook a massive purge of Islamic State-affiliated accounts on its platform. While not all were taken down, as the authors still maintain access to several Islamic State channels that were not removed, and some accounts remain active today unscathed, Kafel was among those channels taken down by the platform. For more on the purge, see Max Bernhard, "Telegram App Tackles Islamic State Online Propaganda," *Wall Street Journal*, November 26, 2019.

e Siddiqui was convicted on two charges of attempted murder, armed assault, using and carrying a firearm, and assault of U.S. officers and employees. Following her arrest in Afghanistan in 2008, she reportedly opened fire on a group of U.S. personnel who were interrogating her after grabbing one of the soldiers' weapons. See Ed Pilkington, "Pakistani scientist found guilty of attempted murder of US agents," *Guardian*, February 3, 2010.

olina prison,[f] Abdel-Rahman was a common propaganda point for various al-Qa`ida branches and affiliates around the world. For instance, "The Blind Sheikh" was mentioned in Usama bin Ladin's original declaration of war against the United States in 1996.[43] In 2013 during the In Amenas, Algeria, hostage crisis, veteran jihadi Mokhtar Belmokhtar, who led the attack, demanded Abdel-Rahman's release.[44][g] Three years later, Hamza bin Ladin would go on to include Abdel Rahman's plight in a 2016 speech.[45] Even after his death, the "Blind Sheikh" continues to be a staple of al-Qa`ida propaganda.[46]

Several terrorist attacks have also been launched in the pursuit of freeing the "Blind Sheikh." For instance, the November 1997 Luxor massacre, which was perpetrated by Abdel Rahman's group al-Gama'a al-Islamiyah, was reportedly conducted in order to free the Sheikh.[47] Pamphlets found at the scene also noted the group referred to itself as "Omar Abdel Rahman's Squadron of Death of Destruction."[48] And the September 2012 storming of the U.S. Embassy in Cairo, Egypt, was also reportedly partly inspired by the plight of the Sheikh.[49] Several protestors were also filmed outside the embassy before the attack calling for the release of Abdel Rahman.[50]

Showcasing weak state capacity or control over prisons can also be an effective tool for propaganda.[51] In Sudan, this can clearly be seen when four members of the al-Qa`ida-linked Ansar al Tawhid managed to escape from the Kober prison in Khartoum in 2010.[52][h] Almost two years later, an al-Qa`ida-linked media organization released a video of the escape.[53] The video demonstrates the intricate planning of the prison break, as well as the massive tunnel the jihadis were able to construct leading out of the prison.[54] In releasing the video, the jihadis were able to effectively highlight exploitable structural flaws even within the police state of dictator Omar al-Bashir.

In current discussions about attacks on prisons or prison breaks, the majority of the focus is on the makeshift prisons in northern Syria currently holding thousands of Islamic State militants.[55] Female detainees have been reported as "imposing their own caliphate" in the al-Hol camp in northeastern Syria through a series of attacks on other prisoners and facility staff.[56] Several women were also responsible for an attack on Kurdish security guards within the camp last October.[57] That same month, hundreds of Islamic State members were able to break out of Kurdish-held prisons in northern Syria following the Turkish incursion into the region.[58] A mass Islamic State jailbreak attempt also occurred in northern Syria's Al Malikiya (also known as Derik in Kurdish) in April 2019.[59]

However, as the following section demonstrates, jihadi efforts to assault prisons is not limited to Syria. The bulk of the attacks on prison facilities by jihadi groups in the past few years has instead occurred in countries of the Sahel, where the ongoing destabilization of the overall security environment and immense structural weaknesses in prisons housing large numbers of jihadi operatives[60] led to significant opportunities for jihadi attacks. These attacks have the potential to further strengthen the array of jihadi groups operating in the region, as with many of these assaults, jihadi groups successfully freed dozens of skilled operatives.

Jihadis Assaults on Prisons: 'Breaking the Walls' in the Sahel

In the Sahel, both al-Qa`ida and Islamic State-loyal groups have routinely launched attacks on prisons in Mali, Burkina Faso, and Niger over the last few years. In 2013, gunmen believed to be members of the al-Qa`ida-linked Movement for Oneness and Jihad in West Africa (MUJAO)[i] launched a coordinated assault on the Niamey, Niger, prison. That attack began when a Sudanese MUJAO member detained at the prison stole a gun and opened fire on security guards. Meanwhile, MUJAO fighters positioned outside the facility launched their own assault, freeing at least 22 jihadi prisoners.[61] In October 2016, Nigerien security forces were able to repel an Islamic State attack on the Koutoukalé prison outside of Niamey.[62]

A month later, one of al-Qa`ida's Malian affiliates, Ansar Dine, took responsibility for a prison assault in the central Malian town of Banamba.[63] Following this attack, a statement from the group was published in AQAP's Al Masra newspaper threatening more prison assaults to "liberate all prisoners in Mali."[64] Ansar Dine made significant progress on this threat in December 2016 when its men freed 93 fellow jihadis from another prison in central Mali.[65]

Tracking with the rapid deterioration in security in the Sahel over the last three years,[66] these types of operations have grown in frequency. In many respects, the Sahel is also currently witnessing its own version of the "Breaking the Walls" campaign seen in Iraq. While jihadi attacks on prisons in the Sahel have occurred in the past, the region is currently witnessing a relative spike in this phenomenon.[67][j]

For example, in October 2018, jihadis targeted a Burkinabe gendarmerie-run prison near the town of Djibo close to the borders with Mali.[68] A few months later, in May 2019, Islamic State gunmen targeted the Koutoukalé prison outside of Niamey, Niger.[69] While Nigerien authorities have claimed that the attack was quickly repelled,[70] an Islamic State video detailing the assault paints a different picture. The video, which was released in January 2020,

f Abdel Rahman died in 2017 in the North Carolina-based Federal Medical Center, Butner, where he was serving a life sentence for his role in the 1993 World Trade Center bombing. See Julia Preston, "Omar Abdel Rahman, Blind Cleric Found Guilty of Plot to Wage 'War of Urban Terrorism,' Dies at 78," *New York Times*, February 18, 2017.

g The group responsible for the In Amenas attack, Al-Moulathimin, would go on to form one of the backbones of al Qa`ida's branch in the Sahel.

h After the prison break, one individual, Abdul Raouf Abu Zeid Muhammad Hamza, was recaptured shortly thereafter. Two other individuals, Mohammad Makkawi and Mohannad Osman Youssef, went to Somalia and joined al-Qa`ida's affiliate al-Shabaab. Youssef was killed in Somalia sometime before the release of the video, while Makkawi became a commander within the group. He would later defect to the Islamic State before being assassinated by al-Shabaab gunmen in December 2015. The whereabouts or condition of the fourth individual, Abdel-Basit Haj al-Hassan, is currently unknown, although the U.S. government believes he is also in Somalia. See "Sudanese jihadist media front releases video detailing prison escape of convicted militants," FDD's Long War Journal, December 30, 2012, and "Abdelbasit Alhaj Alhassan Haj Hamad," Rewards for Justice.

i Formed in 2011 as an offshoot of al-Qa`ida in the Islamic Maghreb (AQIM), MUJAO ceased to exist after it merged with another AQIM splinter, al-Moulathimin, to form al-Murabitoon, an al-Qa'ida loyal entity, in August 2013. See Bill Roggio, "Al Qaeda group led by Belmokhtar, MUJAO unite to form al-Murabitoon," FDD's Long War Journal, August 22, 2013.

j For instance, since November 2019, there have been three major successful or attempted jihadi assaults on prisons in Mali and Burkina Faso with two occurring in the December 2019-January 2020 timeframe. The only similar rate at which this occurred was between October to December 2016 in which there were three other major successful or attempted jihadi assaults on prisons in Mali and Niger.

shows the jihadis clearly breaching the prison's perimeter.[71] Nigerien officials later stated that one soldier was indeed killed during the prison assault.[72]

In November 2019, the Group for Support of Islam and Muslims (JNIM), al-Qa`ida's branch in the Sahel,[k] claimed an attack on the Diré prison south of Timbuktu, Mali.[73] In keeping in line with jihadi messaging on these operations, JNIM warned of further prison breaks by stating that "we renew our promise with our imprisoned brothers and we say to them that we have not forgotten you and we will not forget you."[74]

On December 31, 2019, another Burkinabe gendarmerie-run prison near the town of Djibo was targeted by jihadis.[75] According to local officials, the jihadi gunmen were able to free "several" inmates from the prison.[76] Two days later, a Malian prison in Niono was also attacked by gunmen from JNIM, though Malian officials have claimed the assault was repelled.[77]

JNIM's operations against prisons have been featured in al-Qa`ida propaganda. On January 18, 2020, al-Qa`ida's General Command (AQGC) released a statement praising JNIM's activities in the Sahel.[78] In the statement, the leadership commended the jihadi group for its "success in liberating the prisoners from the prisons of the oppressors."[79] AQGC added, "your jihad is a glad tiding for the Islamic Maghreb and the entire Ummah."[80]

Worsening jihadi violence coupled with the lack of strong state capacity in the Sahelian states does not bode well for the future of the region. As regional and international states struggle to contain the spread and scale of the violence, it is likely that this growing trend of prison assaults in the region will continue. Already, states are struggling to contain the spread of a surging Islamic State branch in the region.[81][l] In just over one month, for instance, Niger has lost at least 174 soldiers to the jihadi group in just three separate attacks in late December 2019 to January 2020.[82] It is unlikely that state security in Niger, Burkina Faso, or Mali will be able to stave off any coordinated jihadi strategy around assaults on prisons.

The aforementioned Islamic State video of its assault on the Koutoukalé prison outside of Niamey, Niger, highlights this problem well. That facility, like many others in the Sahel, was shown to be both poorly equipped and defended and prone to attacks.[m] While Nigerien security might have been successful in fending off that particular raid, without proper defenses, funding, and equipment, it is unclear how well those security forces can continue to adequately defend the prison from further jihadi assaults. That said, it is worth noting that with the rampant corruption in the Sahelian states, it is possible that even with these things, jihadis could exploit the systemic corruption to still conduct successful attacks on prisons.[83] Given the lack of state capacity throughout the region, this scenario plays out in many other prisons and makeshift detention facilities in Mali, Burkina Faso, and Niger. And much like other regions in which jihadis are actively engaged in combat with state authorities, operations against prisons will only serve to further prolong and exacerbate the conflict.

Jihadi Prison Riots: Indonesia and Tajikistan

In addition to externally coordinated attacks on prisons, incarcerated supporters of jihadi groups have also launched prison riots. In some cases, it is easier for jihadi groups to instigate prison riots from outside the prison walls than conducting external attacks. Additionally, in the wake of jihadi prison riots that do not involve external planning, organizations can claim responsibility for the attacks through media releases.

Jihadi prison riots seem to follow some of the objectives of externally coordinated attacks: jihadis attempt to free prisoners, disturb the institutional security of the correctional facility, and create propaganda victories for jihadi groups. Yet, incarcerated jihadis may also spark riots to wound or kill other inmates over ideological or other disputes, or simply to heighten the state of chaos within a prison and lessen the perception that the correctional staff control an institution.

In the United States and Western Europe, several notable attacks on correctional staff by individual jihadis occurred during the past few years. The most recent example is the January 2019 attack on prison guards by two jihadi prisoners at HMP Whitemoor in the United Kingdom. On the morning of January 9, 2019, two inmates at the high-security prison staged an attack on correctional staff using makeshift knives and imitation suicide belts.[84] Fortunately, prison staff quickly detained the two perpetrators of the attack, but five prison guards suffered injuries.[85] Due to the circumstances of the assault, the Metropolitan Police Service's Counter Terrorism Command treated the incident as a terrorist attack.[86] One of the reported perpetrators, Brusthom Ziamani, was serving a 22-year sentence for preparing a jihadi-inspired assault on a U.K. military base.[87] As Robin Simcox notes, the United States and France have also experienced these types of attacks in their prison systems in increasing frequency.[88]

While these examples represent significant threats to security within Western prisons, they did not escalate into full-blown riots. In comparison, the jihadi prison riots described below caught

k Formed in March 2017, JNIM includes several former al-Qa`ida affiliates in the region, including Ansar Dine, Katibat Macina, al-Qa`ida in the Islamic Maghreb's (AQIM) Sahara Emirate, and Al-Murabitoon. It is led by former Ansar Dine emir Iyad Ag Ghaly and has sworn allegiance to Abdelmalek Droukdel, the emir of AQIM; Ayman al-Zawahiri; and Hibatullah Akhundzada, the emir of the Afghan Taliban. See Thomas Joscelyn, "Analysis: Al Qaeda groups reorganize in West Africa," FDD's Long War Journal, March 13, 2017.

l Formed in 2015 and colloquially known as the "Islamic State in the Greater Sahara (ISGS)," the group has operated under the Islamic State's West Africa Province (ISWAP) moniker since early 2019. However, the leadership hierarchy between Islamic State commanders in Nigeria, where ISWAP is headquartered, and ISGS commanders in the Sahel is currently unknown. The United Nations has found that though ISGS and ISWAP "have joint facilitators," ISGS is currently "operationally independent" from ISWAP. "Twenty-fifth report of the Analytical Support and Sanctions Monitoring Team," p. 11.

m The prison facility, as shown in the Islamic State video, lacked proper defensive fortifications and was poorly staffed. The video also detailed how the jihadi gunmen were able to easily breach the perimeter of the prison, further highlighting its structural flaws. This is not unlike other prisons or makeshift detention centers in the Sahel. For an example of a poorly defended gendarmerie station in the Sahel, which often house jihadi detainees in makeshift prisons, see Menastream, "#Niger: On October 21, 2017, #ISGS militants attacked the gendarmerie in Ayorou, #Tillabery Region …" Twitter, March 31, 2018.

momentum, involved larger groupings of prisoners, and eventually metastasized into mass violence in prisons, resulting in dozens of casualties. Since 2018, three notable jihadi prison riots claimed by the Islamic State—in Indonesia and Tajikistan, respectively—resulted in institutional breakdowns and mass casualties.

Indonesia: Mako Brimob Riot

During the past three years, one incident that exemplified the continued relevance of jihadi prison riots was an uprising launched by supporters of the Islamic State at the Indonesian National Police's Mobile Brigade Corps' (Mako Brimob) detention unit in the West Javan town of Depok.[89] On May 8, 2018, over 150 prisoners in a section of the detention center holding terrorist offenders broke out of their holding cells, overpowered prison guards, and seized dozens of weapons.[90] The situation quickly devolved into a hostage crisis, as the inmates held six prison guards hostage for nearly 24 hours.[91] During the hostage crisis, official Islamic State propaganda channels began circulating footage and photos, apparently taken from within the prison, of the hostage-takers with the Islamic State's black flags and weapons.[92] On the first full day of the hostage crisis, the Islamic State's Amaq News Agency claimed that the perpetrators of the riot were Islamic State fighters.[93] Several rounds of communications between the hostage-takers and the Indonesian police failed to resolve the situation, and by the time that the police declared the negotiations to be a failure, the perpetrators had already killed five of the six hostages.[94] On May 9, 2018, Indonesia's counterterrorism unit Densus 88 stormed the prison and shut down the riot using tear gas; in total, five prison guards and one inmate died during the raid.[95]

Tajikistan: Khujand and Vakhdat Riots

Indonesia's prison system was not the only one to face mass rioting by jihadi prisoners in recent years. Late on November 7, 2018, a riot erupted in High Security Prison 3/3 in Khujand, Tajikistan, started by several inmates affiliated with the Islamic State.[96] The riots reportedly began when an inmate attacked a guard and seized control of his rifle, turning it on other guards and freeing other prisoners to join the riot.[97] In the aftermath, estimates of the numbers of rioters and the casualty figures varied widely between media and official accounts. The government of Tajikistan claims that the perpetrators included 12 individuals who previously fought in Syria for the Islamic State and returned to Tajikistan, alongside several members of other extremist groups.[98] Officials reported 25 casualties as a result of the November 2018 Khujand riot; independent media claims that as many as 50 people died.[99] A day after the attack, Amaq News Agency claimed responsibility for the riot on behalf of the Islamic State.[100]

On May 19, 2019, another prison riot broke out in Tajikistan involving Islamic State affiliates, this time at the maximum-security Kirpichniy prison in Vakhdat.[101] Tajik authorities claim that the riot began when four prisoners, incarcerated on charges of supporting the Islamic State, used homemade knives to stab three prison guards to death.[102] The Islamic State-affiliated perpetrators in Vakhdat were reportedly led by 20-year-old Behruz Gulmurod, the son of former Tajik police colonel and Islamic State minister of war Gulmurod Halimov.[103][n] In 2017, Behruz Gulmurod had been arrested in Tajikistan after planning to travel to Iraq to join his father.[104] Following the attack on the prison guards, these inmates allegedly freed two dozen other prisoners tied to other Islamist groups banned in Tajikistan.[o] In tandem, the individuals involved in the riot attacked guards and other prisoners and burned down a prison medical facility before Tajik special police (OMON) intervened.[105] A list published by the Ministry of Internal Affairs of Tajikistan reports 29 prisoner casualties in addition to three guards slain during the attack.[106] The Ministry of Internal Affairs claimed that the initial group of four rioters were responsible for five of the deaths—three guards and two prisoners—while 25 other inmates died during the effort to "neutralize" the inmates involved in the riot.[107]

The Future of Jihadi Prison Assaults and Riots

Attacks on prisons and prison riots can be considered an essential objective of the strategic and operational planning for global jihadi groups. The 2019 addresses by former Islamic State leader Abu Bakr al-Baghdadi and current spokesperson Abu Hamza al-Qurashi underscore the critical relevance of this type of tactic for jihadi groups moving forward.[108] A successful raid or mass prison break by jihadi operatives is rife with advantages for the organizations that they represent. As both historical and more recent incidents prove, given certain conditions a strike team of jihadis can free large numbers of operatives in a matter of hours. In certain cases, incarcerated jihadis possess significant prior experience in jihadi groups, including essential training and skills. As opposed to attempts to free jihadi prisoners, training non-incarcerated supporters to reach the same status and skill-level may take years. Moreover, raids to free prisoners and prison breaks are imbued with historical and ideological significance for the jihadi movement. By using successful assaults and riots in propaganda releases, jihadis signal to their followers that their adversaries' attempts to subdue the movement through arrests and prosecution is a band-aid solution, while simultaneously challenging the authority and governance of the states that oppose them.

n The other perpetrators of the riot in Vakhdat (Fathiddin Gulov, Mahmadullo Sharipov, and Ruhullo Hasanov) were listed by the Ministry of Internal Affairs as Islamic State supporters, although their roles and activities on behalf of the group are unknown. "[List: Convicted persons who were neutralized or died as a result of the riot at High Security Prison 3/2 on May 19th and 20th, 2019]," Ministry of Internal Affairs of Tajikistan, May 20, 2019.

o According to the list of prisoner casualties during the Vakhdat riot published by the Ministry of Internal Affairs of Tajikistan, casualties included inmates affiliated with the Islamic State; Hizb-ut-Tahrir, the banned salafi group "Ansarulloh;" and the former Islamist opposition party Islamic Renaissance Party of Tajikistan (IRPT). Among the dead were senior IRPT members Sattor Karimov (Makhsumi Sattor), Qiyomiddin Ghozi, and Jomahmad Boev, regarded by external watchdog groups as political prisoners. Tajik religious figure Saidmakhdikhon Sattorov (also known as Sheikh Temur), convicted of fraud and leading a cult after he declared himself to be the Mahdi in 2012, was also killed during the riot. Accounts vary as to whether the Islamic State-linked perpetrators of the riot or the prison guards that responded to it were responsible for the deaths of the non-Islamic State inmates killed at the Kirpichniy prison. "[List: Convicted persons who were neutralized or died as a result of the riot at High Security Prison 3/2 on May 19th and 20th, 2019];" "Tajik Opposition Party Accuses Authorities Of Concealing Truth About Deadly Prison Riot," Radio Free Europe/Radio Liberty, May 21, 2019; "[Prison riot: 32 killed, 35 detained. Among the casualties—"Sheikh Temur," Makhsumi Sattor and Qiyomiddin Ghozi]," Radioi Ozodi, May 21, 2019.

Jihadi groups' continual targeting of prisons and jails entails significant implications for improving the resilience of prison systems across the world against terrorist attacks. Recent cases from the Sahel, Indonesia and Tajikistan demonstrate that prison systems in which jihadi external assaults and riots bore the most success for the perpetrators had basic security deficits. The United Nations Office on Drugs and Crime found that "the credibility of any prison system rests on its ability to keep prisoners in custody safely and securely—in other words, to prevent violence or harm within the prison setting and to prevent escapes."[109]

In the incidents discussed above, jihadi groups exploited gaps in security infrastructure within prisons, leading to the success of assaults on prisons or the escalation of riots. Infrastructure and capacity deficits are particularly prominent in the Sahel, where the average national prison overcrowding rate is over 230 percent of capacity—among the highest in the world.[110] A fact-finding mission by the United Nations found that "in the Sahel region, high overcrowding rates, poor infrastructure and precarious detention conditions increase the likelihood of violence and related security incidents in prison settings."[111] The threats posed by overcrowding and lack of infrastructure were found to be "further aggravated by the increasing presence of high risk detainees suspected of being extremist terrorists in penitentiary institutions throughout the region."[112] These same factors are present, albeit to a lesser extent, in Indonesia and Tajikistan.[113] In these instances, it is worth noting that all three prison riots examined in detail in this article involved prisons (Mako Brimob in Indonesia; Khujand and Vakhdat in Tajikistan), which were converted from prison camps or detention units into high- or maximum-security prisons for extremist offenders. However, prison authorities did not develop the infrastructure that typifies high-security facilities, such as individual cells, sufficient staff power, or security controls.[p] The 'maximum-security' component of all three prisons consisted of only a few armed guards and designated wings for extremist offenders.[114] In the Mako Brimob facility, as many as 10 inmates shared individual cells within a 156-person prison block, while both of the Tajik prison units were large barracks that fit 200 inmates in a single hall with several rows of bunk beds.[115]

One or more of the following factors—overcrowding, ill-equipped facilities, and co-location of extremist inmates—were precursors to many of the security breaches discussed in this article. Co-location is one management approach to violent extremist prisoners, wherein terrorist offenders are separated from other inmates and placed into a single prison or unit within a prison.[116] Its benefits are preventing inmates with terrorist affiliations from radicalizing or recruiting others, and when effectively implemented, can isolate security risks posed by terrorist offenders and prevent them from spilling over into the rest of the prison. However, in systems where basic capacities are missing, co-location may pose additional risks.[117] Overcrowded "extremist prisons" or "extremist prison wings" without adequate security infrastructure potentially allows inmates with affiliations to terrorist groups to easily communicate, form groupings, develop critical mass to overpower prison staff, and spark riots.[118] It could also assist terrorist groups seeking to assault prisons in limiting their targets to particular prisons or particular wings, if they know a large quantity of their operatives are being held there.

Developing prison system resilience is important because jihadi groups are likely to attempt additional attacks and spark riots in the near-term. A significant number of jihadis are currently incarcerated across the globe, and many prison systems are structurally unprepared to deal with large numbers of extremists held in their facilities. The Islamic State and various al-Qa`ida affiliates are encouraging and directing operatives to assault prisons and praising the perpetrators of prison riots. If history is a guide, supporters of jihadi groups typically respond to leadership focus on prison systems by perpetrating attacks and riots, most clearly exemplified by the "Breaking the Walls" campaign in Iraq during the early 2010s. With these new calls to action, continued jihadi attacks on prisons and riots by incarcerated jihadis is a very likely possibility. CTC

p Security controls for prisons include, but are not limited to, centralized locking mechanisms for jail cells, surveillance equipment, alarm systems, detection equipment (metal detectors, x-ray machines, etc.) physical security instruments and aids (e.g., handcuffs, shackles, and/or fetters), and physical infrastructure (walls, fences, watchtowers, etc.). "Handbook on Dynamic Security and Prison Intelligence," United Nations Office on Drugs and Crime, 2015.

Citations

1 Aki Peritz, "The Coming ISIS Jailbreak," *Foreign Affairs*, October 23, 2019.
2 Lorenzo Vidino and Bennett Clifford, "A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism," Europol, July 12, 2019; "Handbook on the Management of Violent Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons," United Nations Office on Drugs and Crime, October 2016; "EU Terrorism Situation and Trend Report (TE-SAT) 2019," Europol, June 27, 2019.
3 "North East Syria: Al-Hol Camp," United Nations Office for the Coordination of Humanitarian Affairs, January 13, 2020; Louisa Loveluck and Souad Mekhennet, "At a sprawling tent camp in Syria, ISIS women impose a brutal rule," *Washington Post*, September 3, 2019.
4 "Twenty-fifth report of the Analytical Support and Sanctions Monitoring Team concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities," United Nations, December 27, 2019.
5 Ibid., pp. 3, 5.
6 Vidino and Clifford.
7 Trevor Cloen, Yelena Biberman, and Farhan Zahid, "Terrorist Prison Breaks," *Perspectives on Terrorism* 12:1 (2018): pp. 59-68.
8 Peritz.
9 Ibid.
10 See Ibid.; Ellen Ioanes, "Donald Trump's abrupt withdrawal from Syria may allow ISIS to come back with a vengeance — using the group's time-tested strategy," *Business Insider*, October 10, 2019; Tim Arango and Eric Schmitt, "Escaped Inmates From Iraq Fuel Syrian Insurgency," *New York Times*, February 12, 2014; and "Twenty-fifth report of the Analytical Support and Sanctions Monitoring Team," p. 6.
11 Craig Whiteside, Ian Rice, and Daniele Raineri, "Black Ops: Islamic State and Innovation in Irregular Warfare," *Studies in Conflict & Terrorism* (2019).

12 Bill Roggio, "Pakistani Taliban assault prison, free nearly 400 inmates," FDD's Long War Journal, April 15, 2012; Bill Roggio, "Pakistani Taliban assault prison, free hundreds of inmates," FDD's Long War Journal, July 30, 2013.
13 "Prison break may cause problems in field: general," CTV News, June 14, 2008.
14 Bill Roggio, "More than 450 Taliban leaders, fighters escape from Kandahar jail," FDD's Long War Journal, April 25, 2011.
15 Bill Roggio, "Taliban suicide assault team overruns prison, frees hundreds," FDD's Long War Journal, September 14, 2015.
16 "Yemen foils al-Qaeda prison break," Al Jazeera, October 23, 2013.
17 Thomas Joscelyn and Bill Roggio, "AQAP's emir also serves as al Qaeda's general manager," FDD's Long War Journal, August 6, 2013.
18 Ibid.
19 "Profile: Al-Qaeda in the Arabian Peninsula," BBC News, June 16, 2015.
20 Bill Roggio, "AQAP storms prison in Yemen's capital, frees al Qaeda operatives," FDD's Long War Journal, February 13, 2014.
21 Ibid.
22 Oren Adaki, "AQAP storms Yemeni prison, frees jihadist leader," FDD's Long War Journal, April 2, 2015.
23 Thomas Joscelyn, "Senior AQAP leader added to US terror list by State Department," FDD's Long War Journal, January 23, 2018.
24 "Al-Qaeda confirms death of AQAP leader Qassim Al-Raymi: Site Intelligence Group," Reuters, February 23, 2020.
25 "Al Qaeda confirms death of leader, appoints successor," DW, February 23, 2020.
26 Joscelyn, "Senior AQAP leader added to US terror list by State Department."
27 "Twenty-fifth report of the Analytical Support and Sanctions Monitoring Team," p. 3.
28 Richard Spencer, "Isis leader Baghdadi calls for prison camp raids in Syria and Iraq," *Times*, September 17, 2019.
29 Thomas Joscelyn, "Islamic State confirms Baghdadi's death, names new 'Emir of the Faithful,'" FDD's Long War Journal, November 1, 2019.
30 Letter dated 20 January 2020 from the Chair of the Security Council Committee, p. 6.
31 Bill Roggio, "Taliban, IMU form Ansar al Aseer to free jihadist prisoners," FDD's Long War Journal, February 5, 2013.
32 Roggio, "Pakistani Taliban assault prison, free hundreds of inmates."
33 Roggio, "Taliban, IMU form Ansar al Aseer to free jihadist prisoners."
34 John Dunford and Brandon Wallace, "ISIS Prepares for Breakout in Prisons and Camps," Institute for the Study of War, September 23, 2019.
35 Aymenn al-Tamimi, "'Free the Female Prisoners': A Campaign to Free Women Held in SDF Camps," aymennjawad.org, October 15, 2019.
36 Jihadoscope, "Islamic State supporters launch English language Telegram channel relaying messages …," Twitter, August 8, 2019; Dunford and Wallace.
37 Al-Tamimi.
38 Thomas Joscelyn, "Analysis: 'Lady al Qaeda' in propaganda," FDD's Long War Journal, December 16, 2010.
39 Thomas Joscelyn, "US citizen pleaded guilty to training with al Qaeda in Syria, plotting attack," FDD's Long War Journal, July 5, 2017.
40 Ibid.
41 Ibid.
42 Andrew Welsh-Huggins, "Man apologizes, sentenced to 22 years for US terrorism plot," Associated Press, January 21, 2018.
43 Thomas Joscelyn, "Al Qaeda often agitated for Omar Abdel Rahman's release from US prison," FDD's Long War Journal, February 19, 2017.
44 Thomas Joscelyn, "Report: Al Qaeda group demands release of 2 well-known jihadists," FDD's Long War Journal, January 18, 2013.
45 Thomas Joscelyn, "Osama bin Laden's son says al Qaeda has grown despite 15 years of war," FDD's Long War Journal, July 10, 2016.
46 Thomas Joscelyn, "Shabaab's jihad against the 'leaders of disbelief,'" FDD's Long War Journal, August 14, 2019.
47 "Luxor massacre group offers Mubarak `truce'," *Irish Times*, November 21, 1997.
48 John Daniszewski, "Terrorists Kill 60 Tourists in Attack at Egyptian Temple," *Los Angeles Times*, November 18, 1997.
49 Sara Lynch and Oren Dorell, "Deadly embassy attacks were days in the making," *USA Today*, September 12, 2012; Thomas Joscelyn, "In Service of the Blind Sheikh?" Foundation for Defense of Democracies, September 13, 2012; Thomas Joscelyn, "Al Qaeda-linked jihadists helped incite 9/11 Cairo protest," FDD's Long War Journal, October 26, 2012.
50 "Egyptian Salafists Call for Release of Sheik Omar Abd Al-Rahman from US Prison, Chant Antisemitic Slogans," MEMRI, September 11, 2012.
51 Cloen, Biberman, and Zahid.
52 "Shawshank Redemption-style prison breakout in Sudan raises eyebrows," *Sudan Tribune*, June 12, 2010.
53 "Sudanese jihadist media front releases video detailing prison escape of convicted militants," FDD's Long War Journal, December 30, 2012.
54 Ibid.
55 Brian Michael Jenkins, "Options for Dealing with Islamic State Foreign Fighters Currently Detained in Syria," *CTC Sentinel* 12:5 (2019).
56 Natalia Sancha, "ISIS women impose their own caliphate in Syria's Al Hol camp," *El Pais*, October 25, 2019.
57 "Islamic State women attack security at Syria camp: SDF," Reuters, October 11, 2019.
58 Samuel Osborne, "Isis militants break out of prison in Syria after bombing by Turkey," *Independent*, October 11, 2019; Bethan McKernan, "At least 750 Isis affiliates escape Syria camp after Turkish shelling," *Guardian*, October 13, 2019; "Twenty-fifth report of the Analytical Support and Sanctions Monitoring Team," p. 5.
59 "US-led coalition says allies in Syria foil Islamic State prison break," Associated Press, April 6, 2019.
60 "Niger - Prisoner De-radicalization and Reintegration: UNODC promotes deradicalization and reintegration for high risk detainees and suspected terrorists," United Nations Office on Drugs and Crime; "Note d'information de l'ISSAT sur La réforme du secteur de la sécurité au Niger," International Security Sector Advisory Team; Diana Goff and Erwin van Veen, "A Crisis of Confidence, Competence, and Capacity: Programming Advice for Strengthening Mali's Penal Chain," International Development Law Organization, November 2015.
61 "Niamey prison break: Niger confirms 22 escaped," BBC, June 2, 2013.
62 Caleb Weiss, "Niger thwarts jihadist prison break attempt," FDD's Long War Journal, October 17, 2016.
63 Caleb Weiss, "Ansar Dine claims string of attacks across Mali," FDD's Long War Journal, November 7, 2016.
64 See Caleb Weiss, "Suspected jihadists launch jailbreak in southern Mali," FDD's Long War Journal, December 7, 2016, and "Al-Qa'ida in the Arabian Peninsula," Al Masra, issue 29, available at Jihadology.
65 "Suspected Islamist militants free 93 prisoners from Mali jail," Reuters, December 6, 2016.
66 See, for example, "'Unprecedented terrorist violence' in West Africa, Sahel region," UN News, January 8, 2020; "Atrocities by Armed Islamists and Security Forces in Burkina Faso's Sahel Region," Human Rights Watch, March 22, 2019; "Jihadist violence putting 'generation at risk' in Africa's Sahel: WFP," Reuters, November 19, 2019; and "Mali: Militias, Armed Islamists Ravage Central Mali," Human Rights Watch, February 10, 2020. This is also based on author Caleb Weiss' tracking of the Sahel for FDD's Long War Journal.
67 Based on author Caleb Weiss' tracking of jihadi attacks in the Sahel for FDD's Long War Journal.
68 "Attaque d'une gendarmerie dans le nord du Burkina Faso," VOA Afrique, October 19, 2018.
69 "'Terrorist' attack on Niger high-security Koutoukalé prison foiled," Defense Post, May 13, 2019.
70 Ibid.
71 Caleb Weiss, "Islamic State video details operations across the Sahel," FDD's Long War Journal, January 10, 2020.
72 "Communiqué du Ministère de l'Intérieur relatif à l'attaque de la prison de Koutoukalé," Markmg.227 News, via Facebook, May 15, 2019.
73 Caleb Weiss, "JNIM claims prison break in Mali," FDD's Long War Journal, November 16, 2019.
74 Ibid.
75 "Burkina Faso : La Gendarmerie De Djibo Attaquée Et Plusieurs Détenus Libérés," Newland Info, January 1, 2020.
76 Ibid.
77 "Mali: un assaillant abattu dans l'attaque de la prison de Niono," Sahelien, January 2, 2020. For JNIM's claim, see Wassim Nasr, "#Mali #JNIM #AQMI #AlQaeda revendique plusieurs ops & dans le pays …," Twitter, January 16, 2020.
78 Caleb Weiss, "1. Al Qaeda's General Command released a statement today praising JNIM's operations …," Twitter, January 19, 2020.
79 Thomas Joscelyn, "Al-Qaeda's senior leadership praises jihadists in Mali and Somalia," FDD's Long War Journal, January 20, 2020.
80 Ibid.
81 Weiss, "Islamic State video details operations across the Sahel;" Caleb Weiss, "Islamic State kills almost 100 soldiers in Niger," FDD's Long War

Journal, January 14, 2020; "IntelBrief: France Reconsiders Force Posture in Sahel Amid Surging Violence," Soufan Center, February 11, 2020.
82 Weiss, "Islamic State kills almost 100 soldiers in Niger."
83 "Sahel Programme Progress Report," United Nations Office on Drugs and Crime, June 2017.
84 "HMP Whitemoor Incident," Counter Terrorism Policing, Metropolitan Police Service, January 10, 2020.
85 Ibid.
86 Ibid.
87 "HMP Whitemoor prison stabbings classed as 'terrorist attack,'" BBC, January 10, 2020.
88 Robin Simcox, "Radical Islamists Are Still A Threat Behind Bars," *Foreign Policy*, January 15, 2020.
89 Joe Cochrane, "Deadly Uprising by ISIS Followers Shakes Indonesia's Prison System," *New York Times*, May 10, 2018.
90 Ibid.
91 Ibid.
92 Thomas Joscelyn, "ISIS Claims Its 'Soldiers' Are Responsible for Prison Riot in Indonesia," FDD's Long War Journal, May 9, 2018.
93 Ibid.
94 Joe Cochrane, "ISIS-Linked Indonesian Jail Riot Ends as Police Raid Cellblock," *New York Times*, May 9, 2018.
95 Ibid.
96 "Deadly Prison Riot Reported In Northern Tajikistan," Radio Free Europe/Radio Liberty, November 8, 2018.
97 Ibid.
98 "Tajikistan Makes First Comments About Prison Riot," Radio Free Europe/Radio Liberty, November 21, 2018.
99 "[The number of victims in the riot in Khujand is approximately 50]," Radioi Ozodi, November 12, 2018.
100 "Islamic State Says It Was Behind Deadly Prison Riot," Radio Free Europe/Radio Liberty, November 9, 2018.
101 "Tajikistan blames Islamic State for prison riot, 32 killed," Reuters, May 20, 2019.
102 Ibid.
103 Farangis Najibullah, "Tajik Prison Riot Puts Spotlight On Alleged Role Of Turncoat Police Colonel's Son," Radio Free Europe/Radio Liberty, May 21, 2019.
104 Ibid.
105 Ibid.
106 "[List: Convicted persons who were neutralized or died as a result of the riot at High Security Prison 3/2 on May 19th and 20th, 2019]."
107 Ibid.; "Tajikistan Makes First Comments About Prison Riot."
108 Richard Spencer, "Isis leader Baghdadi calls for prison camp raids in Syria and Iraq," *Times*, September 17, 2019; Joscelyn, "Islamic State confirms Baghdadi's death, names new 'Emir of the Faithful.'"
109 "Handbook on the Management of Violent Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons."
110 "UNODC promotes deradicalization and reintegration for high risk detainees and suspected terrorists," United Nations Office on Drugs and Crime, April 2015.
111 "Sahel Programme Progress Report."
112 Ibid.
113 "Information on State Parties to be Examined- Tajikistan," submission to the United Nations Human Rights Committee, Freedom Now, July 2019; Kamila Ibragimova, "Tajikistan's prison system claims victims and makes monsters," Eurasianet, October 16, 2019; Cameron Sumpter, "Reintegration in Indonesia: Extremists, Start-ups and Occasional Engagements," International Centre for Counter-Terrorism-The Hague, February 19, 2019; Aisyah Llewellyn, "Indonesia's prison system is broken," Diplomat, May 23, 2018.
114 "Information on State Parties to be Examined- Tajikistan;" Sumpter; Cochrane, "Deadly Uprising by ISIS Followers Shakes Indonesia's Prison System;" Catherine Putz, "What Really Happened at Khujand Prison in Tajikistan," Diplomat, November 27, 2018; Farangis Najibullah and Ainura Asankojoeva, "Activist Gives Rare Glimpse Of Tajik Prison Where Deadly Violence Occurred," Radio Free Europe/Radio Liberty, May 26, 2019.
115 Ibid.
116 "Handbook on the Management of Violent Extremist Prisoners and the Prevention of Radicalization to Violence in Prisons."
117 Ibid.
118 Ibid.