SUBMITTED STATEMENT FOR THE RECORD OF

KATHRYN WALDRON

FELLOW, NATIONAL SECURITY AND CYBERSECURITY POLICY

R STREET INSTITUTE

KRISTEN NYMAN

SPECIALIST, GOVERNMENT AFFAIRS

R STREET INSTITUTE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY

UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON

GLOBAL TERRORISM: THREATS TO THE HOMELAND, PART I

SEPTEMBER 10, 2019

GLOBAL TERRORISM: THREATS TO THE HOMELAND, PART I

CHAIRMAN THOMPSON, RANKING MEMBER ROGERS AND MEMBERS OF THE COMMITTEE:

Thank you for holding this hearing on global terrorism and threats to the American homeland. For more than a decade, combatting terrorism has been one of the primary national security priorities of the United States. On the eve of the anniversary of the September 11th attacks, it is particularly fitting to hold his hearing on the current threat posed by international terrorism. As new technologies emerge and become more easily accessible, so do new methods with which to spread terror and violence. Not surprisingly, over the past decade we have seen those hostile to America embrace cyberspace as a battleground, in part because it may provide them with the type of asymmetric advantage they usually seek when confronting a more powerful and advanced adversary. A terrorist no longer has to go through airport security to wreak havoc and destruction in another country—all they need is access to a computer.

Our names are Kathryn Waldron and Kristen Nyman, and we are members of the National Security and Cybersecurity team at the R Street Institute. The R Street Institute is a nonprofit, nonpartisan public policy research organization whose mission is to engage in policy research and outreach to promote free markets and limited, effective government. Our scholars write extensively on the national security threats posed by innovation and technological development.

Introduction

Consideration of cyber threats to American national security often focuses on the risks posed by nation-states such as Russia, China and North Korea. Russian interference in the 2016 presidential election has raised valid concerns about our adversaries' capacities and willingness to undermine American democratic institutions with information warfare, while China's relentless use of hackers in pursuit of economic espionage and exploitation of American companies shows the breadth of domains in which malicious actors can abuse technology.

But nation-states aren't the only actors we should be concerned about. Just as technology now touches upon every aspect of our lives, it opens up a host of new tools for terrorist groups to recruit followers, spread propaganda, launder money and engage in acts of cyberterrorism.

According to a 2014 report by the U.S. Army War College's Strategic Studies Institute, "...Islamic fundamentalist organizations such as Hamas, al-Qaeda, Algeria's Armed Islamic Group, Hezbollah, and the Egyptian Islamic Group are known to be versed in information technology."[1] Many of these groups are supported by governments hostile to the United States—such as Iran, which has historically supported both Hezbollah and Hamas—and these governments may provide these terrorist groups with offensive cyber tools.[2]

The first known act of cyberterrorism occurred in 1998, when a Tamil group known as the Internet Black Tigers spammed Sri Lankan embassies with 800 emails a day for two weeks.[3] Since then, cyberspace has become attractive to terrorists for a variety of reasons. With limited resources available, terrorist groups may view cyberspace as an opportunity to inflict widespread damage inexpensively in areas where they lack a strong physical presence. As scholars Murat Dogrul, Adil Aslan and Eyyup Celik have put it, "With traditional terrorist activities, such as bombings, the impacts are isolated within specific physical locations and communities. Large part of the population acts [sic] only as observers and they are not directly affected by terrorist acts. […] The ability of cyberterrorism activities to effect wider part [sic] of the population may give the groups involved greater leverage in terms of achieving their political and social objectives."[4]

As with other forms of politically motivated conflict, determining whether a particular destructive act fits the definition of terrorism can be difficult. Bringing these acts into the cyber domain only complicates this issue further, since it requires the detection, interpretation and accurate attribution of any particular malicious cyber activity. The Federal Bureau of Investigation (FBI) defines cyberterrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant

---

[1] Thomas M. Chen, "Cyber Terrorism after STUXNET," U.S. Army War College Strategic Studies Institute, June 2014, p. 15. https://ssi.armywarcollege.edu/pdffiles/pub1211.pdf.
[2] Ben Hubbard, "Iran's Allies Feel the Pain of American Sanctions," *The New York Times*, March 28, 2019. https://www.nytimes.com/2019/03/28/world/middleeast/iran-sanctions-arab-allies.html.
[3] Tribune News Services, "U.S. TELLS OF E-MAIL 'ATTACK' BY REBELS," *Chicago Tribune*, May 5, 1998. https://www.chicagotribune.com/news/ct-xpm-1998-05-05-9805050148-story.html.
[4] Murat Dogrul et al., "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," NATO Cooperative Cyber Defence Centre of Excellence: 2011 3rd International Conference on Cyber Conflict, p 32. https://ccdcoe.org/uploads/2018/10/DevelopingAnInternationalCooperation-Dogrul-Aslan-Celik.pdf.

targets by sub-national groups or clandestine agents."[5] James Lewis at the Center for Strategic and International Studies (CSIS) has a similar definition, determining cyberterrorism is "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population."[6]

Not all malicious activity perpetrated by terrorist groups falls under these definitions of cyberterrorism. For example, terrorist groups may also turn to cybercrime for financial gain. In 2005, the FBI reported Al Qaeda terrorist cells in Spain were supporting themselves through stolen credit cards. The dark web allows terrorist organizations to transport and sell drugs throughout the world to fund terrorist activities. In 2016, Drug Enforcement Administration (DEA) officials discovered a money laundering ring connecting Colombian drug lords to Lebanese members of Hezbollah.[7] Other Islamist terrorist groups using the Internet to raise funds include Hamas and Lashkar e-Taiba.[8] International terrorist groups have also raised funds by establishing online charities. For example, in 2008 Texas-based charity the Holy Land Foundation was discovered to be supporting Hamas.[9]

Hezbollah

Hezbollah provides a good example of the variety of ways in which terrorists can abuse cyberspace. Hezbollah (or Hizballah), whose name translates to "Party of God" in Arabic, is a radical Shiite Islamist organization based out of Lebanon. Originally created in 1982, it was designated a terrorist organization by the U.S. State Department in 1997.[10] Although Hezbollah claims to have been created primarily to rid Lebanon of foreign invaders, the group is heavily

---

[5] Margaret Rouse et al., "Cyberterrorism," TechTarget, May 2019. https://searchsecurity.techtarget.com/definition/cyberterrorism.
[6] James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies. https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats.
[7] James Bargent, "DEA Operation Reveals Hezbollah-Colombia Connection," *InSight Crime*, Oct. 12, 2016. https://www.insightcrime.org/news/brief/dea-operation-reveals-hezbollah-colombia-connection/.
[8] Michael Jacobson, "Terrorist Financing and the Internet," *Studies in Conflict and Terrorism* 33:4, June 15, 2009, p. 53. https://www.tandfonline.com/doi/full/10.1080/10576101003587184.
[9] Ibid.
[10] John W. Rollins, "The Foreign Terrorist Organization List," Congressional Research Service, Jan. 15, 2019. https://fas.org/sgp/crs/terror/IF10613.pdf.

supported by the regimes in both Iran and Syria. Most of Hezbollah's terrorist activities have been directed against Israel and the West's support of Israel. They are extremely hostile to the United States. Before 9/11, Hezbollah had killed more Americans than any other terrorist organization.[11] One of their leaders, Sayyid Muhammad Husayn Fadlallah, once stated in an interview that "We believe there is no difference between the United States and Israel; the latter is a mere extension of the former."[12]

Hezbollah has been engaged in information warfare since the launch of al-Manar—the organization's television station, based in Beirut—in 1991. Their media operations have since expanded to include television, radio, print publications and online enterprises. In 2004 al-Manar was added to the Terrorist Exclusion list under section 212(a)(3)(B)(vi)(II) of the Immigration and Nationality Act and subsequently banned from the United States.[13] With an annual budget of approximately $15 million, al-Manar is considered a "station of resistance" by Hezbollah and is quite popular in the Arabic speaking world, especially in southern Lebanon and the Palestinian territories. Since its creation, al-Manar has been a voice for anti-American and anti-Israeli propaganda, aiming to encourage resistance by calling for suicide attacks.[14]

In addition to using traditional media, Hezbollah has embraced the cyber realm as a way to spread propaganda and recruit new followers. Hezbollah has a significant online presence, maintaining over 50 websites. In 2010, as a recruitment tool, Hezbollah released an online game in which players kill prominent Israeli politicians and other designated enemies.[15]

In 2012, in a statement before the U.S. House of Representatives Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure Protection

---

[11] "Hezbollah," Counter Extremism Project, 2019. https://www.counterextremism.com/threat/hezbollah.
[12] Robert Anthony Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (Random House, 2005), p. 136.
[13] Adam Ereli, "Addition of Al-Manar to the Terrorist Exclusion List," U.S. Department of State, Dec. 28, 2004. https://2001-2009.state.gov/r/pa/prs/ps/2004/40081.htm
[14] Avi Jorisch, "Beacon of Hatred: Inside Hizballah's al-Manar Television," The Washington Institute, Oct. 2004. https://www.washingtoninstitute.org/policy-analysis/view/beacon-of-hatred-inside-hizballahs-al-manar-television.
[15] Colin P. Clarke, "How Hezbollah Came to Dominate Information Warfare," *The RAND Blog*, Aug. 13, 2017. https://www.rand.org/blog/2017/09/how-hezbollah-came-to-dominate-information-warfare.html.

and Security Technologies, Director of George Washington University's Homeland Security Policy Institute Frank Cilluffo stated that Hezbollah had created a companion cyber organization in 2011. Mr. Cilluffo stated, "Law enforcement officials note that the organization's goals and objectives include training and mobilizing pro-regime (that is, Government of Iran) activists in cyberspace. In turn and in part, this involves raising awareness of, and schooling others in, the tactics of cyberwarfare. Hezbollah is deftly exploiting social media tools such as Facebook to gain intelligence and information."[16] Cilluffo also stated in a later testimony that Hezbollah is suspected to be connected to the 2012 cyberattacks known as SHAMOON, in which approximately 30,000 computers belonging to Saudi Aramco and Qatari company RasGas were compromised.[17]

In 2008, CNN reported that British and American intelligence officers were concerned about the possibility of Hezbollah sleeper cells launching a cyberattack at the request of Iran.[18] Hezbollah's cyber capabilities have been on display since its 2006 war with Israel, which saw thousands of cyberattacks from both Hezbollah and Israel. Many of these were denial of service (DDOS) attacks, although Hezbollah's hackers also penetrated computers belonging to Israel's military.[19] Hezbollah has continued to engage in malicious cyber activity aimed at Israel since then. In a 2015 interview with the *Times of Israel*, an Israeli Defense Forces (IDF) officer stated that they had seen an increase in cyberattacks. "Attacks were conducted by all the players—Hezbollah, Hamas, Palestinian hacker groups, and Iran, and they displayed strong capabilities that have gotten considerably better over the years."[20] This echoed the statement of Israeli Prime Minister Benjamin Netanyahu in June 2013, "that Israel had seen a 'significant increase in the

---

[16] Testimony of Frank J. Cilluffo, House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence; and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, "The Iranian Cyber Threat to the United States," 112th Congress, April 26, 2012. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-071c.pdf.

[17] Testimony of Frank J. Cilluffo, House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, "Emerging Cyber Threats to the United States," 114th Congress, Feb. 2, 2016. https://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf.

[18] Paula Newton, "Hezbollah and Cyber War," CNN, March 14, 2008. http://edition.cnn.com/WORLD/blogs/security.files/2008/03/hezbollah-and-cyber-war.html.

[19] Sabrine Saad et al., "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield," 2011. http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf.

[20] David Shamah, "Official: Iran, Hamas conduct cyber-attacks against Israel," *The Times of Israel*, Aug. 13, 2015. https://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

scope' of cyber attacks on its 'vital national systems' by hackers backed by Iran and its terrorist proxies Hezbollah and Hamas."[21]

Iranian Revolutionary Guard Corps (IRGC)

Iran is weaker militarily than its primary regional rival, Israel. As a result, Iran's regime has shown itself willing to fund a variety of terrorist groups to achieve its political goals through asymmetric means.[22] In April 2019, the Trump administration designated the Iranian Revolutionary Guard Corps (IRGC)—the division of Iran's armed services tasked with carrying out cyber activities—as a foreign terrorist organization.[23] In the president's statement, he said that Iran utilizes terrorism as "statecraft." The IRGC acts at the direction of Iranian Supreme Leader Ayatollah Ruhollah Khomeini and has enormous capabilities, as the third-wealthiest organization in Iran and intelligence arm of the Iranian military forces.

Based on publicly available information, Iran and the United States have engaged in a seesaw-like exchange of malicious cyber activities for the better part of a decade, but thus far, these actions have been mostly focused on non-civilian or low-risk civilian targets.[24] While Iran has been accused of targeting U.S. hospitals and banks, the results of these malicious cyber activities have not been severely debilitating.[25] The majority of activity can be categorized as an inconvenience rather than an outright act of war. However, a recent U.S. cyber action on Iranian weapons systems and economic databases may have had a more severe impact on the tit-for-tat

---

[21] Annie Fixler and Frank Cilluffo, "Evolving Menace: Iran's Use of Cyber-Enabled Economic Warfare," Foundation for Defense of Democracies, November 2018. https://www.fdd.org/wp-content/uploads/2018/11/REPORT_IranCEEW.pdf.

[22] Ryan Browne, "State Department report finds Iran is top state sponsor of terror," CNN, June 2, 2016. https://www.cnn.com/2016/06/02/politics/state-department-report-terrorism/index.html.

[23] Donald J. Trump, "Statement from the President on the Designation of the Islamic Revolutionary Guard Corps as a Foreign Terrorist Organization," The White House, April 8, 2019. https://www.whitehouse.gov/briefings-statements/statement-president-designation-islamic-revolutionary-guard-corps-foreign-terrorist-organization/.

[24] Zak Doffman, "U.S. Attacks Iran With Cyber Not Missiles—A Game Changer, Not A Backtrack," *Forbes*, June 23, 2019. https://www.forbes.com/sites/zakdoffman/2019/06/23/u-s-attacks-iran-with-cyber-not-missiles-a-game-changer-not-a-backtrack/#515c9498753f.

[25] Nicole Perlroth and Katie Benner, "Iranians Accused in Cyberattacks, Including One That Hobbled Atlanta," *The New York Times*, Nov. 28, 2018. https://www.nytimes.com/2018/11/28/us/politics/atlanta-cyberattack-iran.html.

exchange between the two countries. Until recently, the activity has been proportional, and the concern is that as tensions increase, the offensive cyber activities of one or both parties will escalate considerably, possibly including actions that would result in loss of life and/or significant property damage. The IRGC possesses the cyber capabilities necessary to carry out large-scale attacks on U.S. critical infrastructure and its relatively weak government systems.[26]

In the past, Congress has attempted to sanction the IRGC, the Department of Treasury has initiated targeted sanctions against its leaders and the United States has also sanctioned the organization via executive order.[27] While sanctions can be effective, we caution against treating the organization as a legitimate government actor that might respond reasonably. We would argue that regardless of the IRGC's status as an arm of the Iranian government, Congress would do well to carefully craft policy in this case by treating the IRGC as a terrorist organization and acting accordingly rather than attempting to legislate on the organization solely as a representative of the state. The United States treats hostile foreign states and hostile foreign non-state actors entirely differently, but the U.S. government should use all the tools at its disposal when addressing this foreign hostile actor. Of course, with stakes as high as confrontation with the second largest oil-producing country in the region, and one that is potentially nuclear-capable, the United States will need allies to assist in pushing back against Iran.

Policy Recommendations

1. *Global U.S. Leadership, Information Sharing and Coordination*. Partnering with our allies will become increasingly important as terrorists further act in cyberspace. Because cyberspace allows individuals or organizations to organize attacks and conduct other malicious activities outside their geographic region, effectively combating these actions will require international cooperation. The United States must lead the global effort to detect, deter and defeat the full range of malicious cyber activities and cyber-enabled actions in which international

[26] "IRGC Cyber-Warfare Capabilities," International Institute of Counter-terrorism, April 29, 2019. https://www.ict.org.il/Article/2380/IRGC_Cyber-Warfare_Capabilities#gsc.tab=0.
[27] Donald J. Trump, "Executive Order 13876: Imposing Sanctions With Respect to Iran," The White House, June 24, 2019. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/13876.pdf.

terrorist groups and their state sponsors engage. The United States should work closely with its foreign partners to better ensure that all elements of national power—military, intelligence, law enforcement, and economic and diplomatic measures—are used to thwart international terrorist groups across all dimensions, including cyberspace. In particular, the United States and its allies should robustly share intelligence information on cyber-related threats from international terrorist groups, coordinate and deconflict operational activities, and work to develop meaningful and enforceable international legal norms in cyberspace to enhance the ability of state actors to deter and respond effectively to cyberterrorism.

2. *Improving Our Cyber Hygiene*. As for actions the United States should carry out to protect itself domestically, first and foremost the United States must improve the security of its public and private sector information systems. Critical government and private sector systems are severely underprotected. A necessary first step for the government would be to update and secure these systems at the federal, state and local levels. In order to better defend against malicious cyber actions, the government should establish a meaningful set of cyber metrics through the National Institute of Standards and Technology (NIST) to measure accurately how well individual governmental and commercial systems are protected and to conduct a full-scale audit to identify where it is vulnerable and rectify those vulnerabilities.

3. *Cyber Training and Education*. Basic cybersecurity training and education is another important issue. According to U.S. census data there are over 2 million full-time federal workers and 16.4 million state and local government workers who interact with these undersecured governmental systems.[28] The vast majority of these employees do not receive extensive enough cybersecurity training to prevent even the most common hacking attempts. As all malicious cyber actors become more sophisticated, so must the U.S. government. Government employees at all levels should have regular and useful cybersecurity training to identify and protect against common malicious cyber activities. Of course, the clerk in a local tax collector's office and an employee of the Department of Defense should receive different levels of training, but both officials have access

[28] "State and Local Governments Employ 16.4 Million Full-Time Equivalent Employees in 2011 Census Bureau Reports, " United States Census Bureau, Thursday, August 23, 2012. https://www.census.gov/newsroom/releases/archives/governments/cb12-156.html.

to sensitive data and systems that can cause significant harm to the public if targeted successfully by an adversary. Not adequately training seemingly lower-risk employees is akin to only sending a few employees to a fire drill. Every government employee—federal, state, local and tribal—should be well trained in cybersecurity.

4. *Hiring, Retaining and More Effectively Using a Talented Cyber Workforce*. Of course, not all attacks will be low-level spear phishing email attacks. Especially in the case of cyber-capable foreign terrorist organizations and their state sponsors, it's likely that many of these potential attacks will be sophisticated. For that reason, governmental entities must hire and retain the talent necessary to counter attacks on its high-risk and low-risk systems. Government agencies at all levels must hire and retain a wide variety of highly capable information technology and cybersecurity experts while competing with the private sector for such talent. Congress must find better ways to enable the government to compete more effectively in this space, including instituting and promoting programs that recruit the best talent from high schools, community colleges, universities and graduate programs by incentivizing students to spend some part of their career in government service. In addition, the federal government should be more aggressive in using "white hat" cybersecurity experts to help protect governmental systems by aggressively finding and fixing cyber vulnerabilities in those systems. The United States has used white hat hackers to conduct penetration tests to identify weaknesses in its own systems, which has helped make certain highly sensitive targets relatively well protected. However, the real work ahead is securing all governmental systems. All levels of government, not just the military and intelligence community, would benefit from consistent penetration testing, red/blue team training and consistent, on-call cybersecurity analysts and technologists who can properly assess and address potential attacks as they arise. When possible, these analysts should also be involved in securing the systems and addressing their vulnerabilities.

5. *Enhanced Interagency Communication*. Finally, perhaps the simplest recommendation is to increase interagency communication. Government agencies are woefully redundant in creating and carrying out cybersecurity programs and systems audits. Since funding is an obvious concern, agencies should consider sharing analysts, audit data and other information. Even a little

additional communication between departments at all levels of government could go a long way toward saving valuable resources and time.

Conclusion

FBI director Christopher Wray said in a 2018 address, "Virtually every national security and criminal threat the FBI faces is cyber-based or technologically facilitated. We face sophisticated cyber threats from foreign intelligence agencies, hackers for hire, organized crime syndicates, and terrorists."[29] As technology continues to become more prevalent, Congress must lead the charge in protecting domestic systems from attack by international terrorist organizations. As the committee considers implications of global terrorism, we urge them to consider policies surrounding cybersecurity.

We thank the committee for its recognition of the importance of combatting terrorism. If we can be of any assistance to members of the committee, please feel free to contact us or our colleagues at the R Street Institute.

Kathryn Waldron
Fellow, Cybersecurity and National Security
kwaldron@rstreet.org

Kristen Nyman
Specialist, Government Affairs
knyman@rstreet.org

[29] Christopher Wray, "Statement Before the Senate Homeland Security and Governmental Affairs Committee," United States Senate, Oct. 10, 2018. https://www.fbi.gov/news/testimony/threats-to-the-homeland-101018.