CSIS BRIEFS

Understanding Hamas's and Hezbollah's Uses of Information Technology

By Daniel Byman and Emma McCaleb

JULY 2023

THE ISSUE

Hamas's and Hezbollah's information technology (IT) strategies heavily reflect their roles in governance. Terrorist organizations like al Qaeda and the Islamic State eschew nationalism in favor of a broad pan-Islamist vision and focus media operations primarily on recruitment and at times operations. In contrast, Hamas and Hezbollah are nationalist as well as Islamist in orientation and favor traditional forms of communication over social media in order to legitimize their political power—a preference reinforced by the policies of technology companies and, in general, the limited capacity of these terrorist groups to use social media without considerable risk. Because Hamas and Hezbollah govern and provide goods, services, and information to their constituents, it is harder to target their IT infrastructure without risking humanitarian consequences.

Hamas and Hezbollah are among the world's most important and multifaceted terrorist groups. In addition to conducting terrorist attacks, they run hospitals and schools and otherwise engage in social and political activities that make them important in the daily lives of many Palestinians and Lebanese, including those who do not support their ideologies. Perhaps their greatest influence, however, is through governing. Hamas is the de facto government of Gaza, and for many years Hezbollah has been part of the Lebanese government, effectively governing southern Lebanon, occupying cabinet positions directly and via its allies and often acting as a kingmaker, or at least veto player, for the country's prime minister. These roles stand in contrast to the aims of groups like the core of al Qaeda, which has focused primarily on terrorism, or in the case of the Islamic State, war. Today core Al Qaeda and the Islamic State play little or no role in governing.

Governing shapes how Hamas and Hezbollah use communications technologies. Although both groups use social media and other technologies to recruit and, at times, support operations, their primary focus is using more traditional media to gain support from Arab and Muslim populations and bolster morale within their organizations, with their constituents in the Palestinian territories and Lebanon comprising their most important audiences. Counterterrorism also shapes this focus: social media-run operations are highly vulnerable, and Israeli counterterrorism can exploit this to disrupt attacks.

This paper describes how Hamas and Hezbollah use information technology (IT), highlighting their similarities and differences and comparing them with groups like the Islamic State. The paper concludes by identifying the implications for counterterrorism.

HAMAS'S IT STRATEGY

Hamas has fought Israel and sought dominance in the Palestinian national community for over 30 years. Although the militant Palestinian movement has faced

aggressive Israeli counterterrorism, repression at the hands of rival Palestinian organizations, and international isolation, today it enjoys de facto political control over the Gaza Strip and is influential among Palestinians in the West Bank and the rest of the world. Indeed, as Palestinians prepare for the departure of Palestinian Authority and Palestine Liberation Organization leader Mahmoud Abbas, who is 87, some worry Hamas's influence will grow further and that it might emerge as the dominant organization in the West Bank. Some of Hamas's success comes from its use of violence and terrorism, but the organization has proved skilled at running hospitals and schools. Its occasional success in out-governing the West Bank-based Palestinian Authority, its main rival, has made Hamas attractive to Palestinians who do not necessarily share the organization's religious zeal or support for violence. Although Gaza faces many problems under Hamas rule, the organization is able to deflect some blame on Israel and argue that the Palestinian Authority is complicit with Israel, while Hamas is resisting.

Propaganda plays a critical role for Hamas as it seeks to shore up its popularity. The most common Hamas propaganda themes concern justifying the group's place within the Palestinian community and legitimizing its rule in Gaza. Hamas propaganda also devotes considerable attention to its relationships vis-à-vis other Palestinian factions as well as important international actors such as the United States and Egypt.[1] The actions of the Palestinian Authority and its many governance problems, as well as its collaboration with Israel on security issues, are the subject of particular criticism.

Hamas's propaganda also tries to paint Israel as an oppressive occupier whose military operations and policies harm Palestinians, especially innocent civilians, including children. Much Hamas content concerns Israeli policies and operations in Gaza, but Hamas also highlights Israel's occupation of the West Bank and activities elsewhere in the region. Hamas's websites have long lists of "Zionist crimes," detailing Israeli killings of Palestinian worshippers and children.[2] The Israeli army is usually cast as the primary villain, but Hamas claims all Israelis are responsible given the country's near-universal conscription policy—a spin that justifies its violence against Israeli civilians.[3] Some of the tropes

People with Hezbollah flags at the Hezbollah political party rally on May 13, 2022, in Baalbek in Bekaa Valley, Lebanon.

Photo Source: Francesca Volpi/Getty Image News/ Getty Images

Hamas presents are anti-Semitic as well as anti-Israel.[4] Hamas's attacks, in turn, are portrayed as self-defense or as retaliation for Israeli aggression.[5]

Hamas asks its audiences—fellow Palestinians, the broader Arab and Muslim communities, and the world in general—to witness Israeli aggression and the suffering of the Palestinian people and to condemn Israel and support Hamas accordingly.[6] Hamas's websites and postings are in Arabic, English, French, and Hebrew, though Arabic is the dominant language given Hamas's focus on communicating to its immediate constituents in Gaza and efforts to appeal to supporters in the West Bank.[7] Thus, while Hamas uses a broad array of technologies to convey similar messages across different audiences, its primary audience remains its constituents.

In its propaganda campaigns, Hamas uses various technologies to legitimate its governance in Gaza and demonize Israel. Hamas's television and radio stations—both based in Gaza and named Al Aqsa—offer a range of programs including news, dramas, and even children's entertainment. Even its children's content has animated characters who die at the hands of the Israeli military or because of Israeli policies.[8] Hamas's online presence focuses on the group's teachings, history, and mission. Hamas websites offer biographies of key figures like founder Sheikh Ahmed Yassin. Hamas also uses images to glorify suicide bombers and other supposed martyrs for the Palestinian cause and has posted their "living wills" online.[9]

Operationally, Hamas has used social media to a limited degree. In what Israeli officials dubbed Operation Broken Heart, Hamas operatives on Facebook, WhatsApp, Telegram, and Instagram posed as attractive young women, trying to convince Israeli troops to download spyware to their mobile devices via dating applications—a variant of the classic honey trap intelligence agencies have long used. The organization also created fake dating apps for the same purpose. When downloaded, the malware granted Hamas access to the devices' location data and cameras and allowed the operators to turn on the phones' recording devices.[10] Similarly, Hamas used a World Cup–related app that offered live-streamed games and updates for the 2018 competition as a way of clandestinely implanting malware to control users' phones.[11] Some of these apps were available for download via Google Play before being removed.[12] Such efforts on social media, however, appear to be a minor part of Hamas's overall operations.

HEZBOLLAH'S IT STRATEGY

Like Hamas, Hezbollah employs a wide array of technologies to support its communication strategy. Overall, Hezbollah exhibits a high level of skill, especially for a nonstate actor, in part because of its close ties to Iranian government, which has invested heavily in its cyber capabilities in recent years. Hezbollah's exploitation of technology is dynamic, reflecting the level of Iranian support, the emergence of new technologies, the actions of technology companies, and pressure from its enemies, especially Israel.

Image and narrative are important parts of conflicts and rivalries in the Middle East, and Hezbollah uses technology to shape perceptions of friends and foes alike.[13] Hezbollah devotes much of its technology use to its propaganda campaigns, which emphasize resistance, martyrdom, and military success. It also highlights the group's provision of public services and other good public relations stories.[14] In keeping with its primary targets and audiences, Hezbollah at times publishes in English and even Hebrew, but most of its content is in Arabic.[15] Its focus on Arabic language content further reflects Hezbollah's position in governance, as its primary audience largely consists of its constituents.

Much of Hezbollah's propaganda focuses on supporters—both fighters and the broader community.[16] Hezbollah's websites provide exhaustive details on the group's previous military operations and highlight the roles and sacrifices of its many martyrs.[17] Part of the purpose of this focus is recruitment, but maintaining the morale of existing supporters is also vital. Hezbollah propaganda often features speeches by leaders like Hassan Nasrallah attempting to justify Hezbollah's actions against Israel or intervention in Syria, among other topics.

Hezbollah also sends messages to Israel and other enemies through its propaganda. The group has posted videos of its soldiers practicing ambushes on Israeli soldiers and, more subtly, close-up footage of Israeli patrols, both of which were intended to convey threats.[18] In addition, it broadcasts battlefield footage of Israeli soldiers being killed and wounded, hoping to use this content to undermine Israeli morale.[19]

As Hezbollah's enemies have changed, so too has the focus of its propaganda. Still, the organization seeks a grand narrative that knits disparate threats together. As Hezbollah became embroiled in the Syrian civil war after 2011 and began to fight the Islamic State and other Sunni jihadist groups like Jabhat al-Nusra there, its propaganda highlighted the threat these groups posed to Shiites and ordinary Lebanese. However, it also portrayed these Sunni jihadist groups as serving Israeli and U.S. interests by distorting Islam.[20]

Al Manar satellite television is an important means of strategic communication for Hezbollah. Hezbollah began the station in 1991, initially broadcasting only in Lebanon. In 2000, Al Manar became a satellite station.[21] It offers a mix of news, music videos, family dramas, and other content. The station has millions of viewers, both inside and outside of Lebanon, and its viewership has soared during times of crisis, such as the 2006 Hezbollah war with Israel.[22] One of its best-known news shows is *The Spider's House*, which focuses on Israeli and Palestinian issues. The United States declared Al Manar a Specially Designated Global Terrorist entity in 2006, leading to an array of restrictions, including deterring donations and funding, and alerting other governments to U.S. concerns.[23]

At an operational level, Hezbollah also uses IT to spy on its enemies. Between 2012 and 2015, it launched a campaign called Volatile Cedar using customized malware to gather information and track targets in the United States, Canada, Israel, and other countries. Targets included media companies and educational institutions.[24] Experts did not consider the campaign highly sophisticated, but it was nevertheless effective in infecting many devices.[25] Starting in 2019, a Hezbollah proxy called Lebanese Cedar infiltrated around 250 servers in the United States, Great Britain, Egypt, Jordan, Lebanon, Israel, and Palestine using techniques probably derived from Iranian methods.[26] Over the course of months and possibly years, the group stole data from targets as varied as Vodafone Egypt, Egypt-based TE Data, Hadara (used by the Palestinian Authority), internet providers in the United Arab Emirates and Saudi Arabia, the Oklahoma Office of Management and Enterprise Services, and a Connecticut-based company called Frontier Communications. In its hacking efforts, Hezbollah "used an updated variant of its Explosive remote access tool (RAT) against the unpatched servers."[27] Hezbollah operatives also posed as women on Facebook, trying to persuade targets to install a correspondence app laden with malware on their mobile devices so that Hezbollah could track the targets.[28]

Finally, although open data are limited, Hezbollah has used social media and other platforms for operations, recruiting prospective operatives, surveilling targets, organizing cells, and transferring money for operations. Facebook, YouTube, Twitter, and other major companies are most aggressive in taking down Hezbollah posts related to violence, but Hezbollah has grown more subtle in response. Hezbollah media organs often show parades, speeches, and religious celebrations—important parts of its propaganda but ones that do not feature violence. Social media companies focus on taking down violence, an understandable priority but one that often allows non-violent propaganda to slip through. In addition, Hezbollah uses proxies, such as charities and Al Manar, its ostensibly independent broadcaster, to post content that is widely available on social media channels.[29]

Social media companies focus on taking down violence, an understandable priority but one that often allows non-violent propaganda to slip through.

COMPARING HAMAS'S AND HEZBOLLAH'S IT STRATEGIES WITH THOSE OF OTHER TERRORIST ORGANIZATIONS

Terrorist organizations have long recognized social media's utility in reaching a global audience at a lower cost than traditional technologies. As a result, social media have become a communication tool of choice for several terrorist organizations as well as fragmented networks, such as those involved in right-wing terrorism.[30] Hezbollah's and Hamas's communication strategies, however, demonstrate a preference for one-to-many and one-to-one methods of communication, including TV broadcasts, radio stations, web pages, and

Thousands of supporters of the ruling Hamas party attend a rally in Gaza City on December 15, 2006, to listen to an address by Palestinian prime minister and the leader of Hamas Ismail Haniyeh.

Photo Source: Mahmud Hams/AFP/Getty Images

encrypted messaging channels, as opposed to many-to-many forms of communication, including social media. Such a choice reflects both their strategic priorities as governing actors and the fierce counterterrorism environments in which they operate.

Social media have proven revolutionary to communications because they facilitate many-to-many interactions, enabling groups of people, most of whom would have had little ability to reach large audiences in the past, to more intimately interact, shape narratives, and disseminate ideas among each other in real time.[31] Terrorist organizations have leveraged many-to-many media for both their strategic and operational benefit. Strategically, social media allow organizations to tailor messages and propaganda to the specific perspectives of different groups, expanding interest in the organization and improving recruitment. Operationally, social media has facilitated real-time planning of travel and attacks. As a result, many modern terrorist organizations have taken advantage of social media to globalize their strategic and operational reach.

The Islamic State most famously relied on social media to develop a global organization and demonstrated social media's full potential as a many-to-many form of communication. Seeking recruits from around the world for its caliphate, the Islamic State leveraged social media's many-to-many nature to cultivate different messages for different groups of recruits, therefore building "layered support."[32] Moreover, instead of using a central organization to disseminate propaganda narratives, the Islamic State core relied on unofficial spokespeople and fanboys to disseminate propaganda because they better understood the interests and cognitive openings of the specific audience.[33]

Nonetheless, while the Islamic State's media wing sought some control over the organization's public messaging, the growth of the movement on many-to-many platforms naturally limited its control of the narrative. Various fanboys and influencers would chop up official Islamic State video, adding local events to make it relevant to different contexts, creating soundtracks, inserting video game–style effects, and otherwise modifying it. The benefit for the Islamic State was that these modifications greatly expanded

the propaganda's reach, appealing to new audiences and enabling it to reach different niches of its overall supporter market more effectively. The downside was the many different Islamic State narratives that emerged.

Indeed, this lack of control became obvious after high-profile operations, when the group would have had its best chance of reaching a range of audiences. For example, the Islamic State core struggled to create a cohesive public message in the aftermath of the shooting in San Bernardino, California, perpetrated by Tashfeen Malik, who used social media to voice support for the Islamic State. After the attack, the Islamic State attempted to both praise and claim responsibility for the attack while cautioning women against participating in violence, stating that the conditions for women to participate in jihad had not been met.[34] Thus, groups leveraging social media for communications must concede some control of their messaging in exchange for the ability to communicate to broader audiences.

In contrast to the Islamic State, Hamas and Hezbollah are nationalist as well as Islamist. Hamas emphasizes Palestinian nationalism, and Hezbollah has emphasized its role in resisting foreign intervention in Lebanon. Although Hezbollah, usually working with Iran, has sent operatives to numerous countries, it does not aspire to lead a caliphate or otherwise have the vast ambitions of the Islamic State. Given their more localized strategic objectives, Hamas and Hezbollah therefore feel less compelled to rely on social media as a tool to enable their global reach.

Another contrast with the Islamic State and al Qaeda is that Hamas and Hezbollah face pressure to tightly control their narratives in order to improve their political positions and secure their power. Hamas and Hezbollah control territory and have populations they aim to lead. They want to carefully signal their strategic and operational stance to Israel and other adversaries, as well as have more controlled messages to potential constituents. For example, Hezbollah wants to convey defiance to Israel but also seeks to avoid a ruinous all-out war: its propaganda highlights Israel's weaknesses and Hezbollah's preparation, but usually stops short of calling its supporters to go to war. As a result, both groups have prioritized technologies that reaffirm the legitimacy of their roles in politics. One-to-many forms of communication like TV stations, radio, and newspapers allow Hamas and Hezbollah to articulate objectives from a single, united voice. Hamas, for example, heavily relies on its TV station, Al Aqsa, to present Hamas and its governance in a positive light. Propaganda on Al Manar highlights Hezbollah-run schools and hospitals, camps for kids, and the services Hezbollah provides to the Lebanese Shiite community.

One-to-many forms of communication also allow both groups to clearly articulate their demands and threats to their enemies. Both groups have proven very innovative in developing one-to-many communication technologies that push a sustained target focus on Israel and legitimize their role in government. Hezbollah, for example, developed a video game in 2010 in which players could shoot Israeli politicians for target practice and then wage war against Israeli soldiers.[35]

Even the Islamic State's internal communication strategy followed a similar pattern upon the organization stepping into a governing role. As a government, the Islamic State recognized the need to craft a tighter narrative to legitimize its position of political power. Thus, the Islamic State's communications in the caliphate relied more on radio, news bulletins, and operational reports than its external communications and pushed a message "more focused on maintaining brand consistency than action instigation."[36] Its internal communication strategy highlights the utility of one-to-many technologies in governance.

In contrast, social media play a vital role in white supremacist and right-wing violence—often because group structures are weak to nonexistent.[37] As a result, there is often no coherent group or set of leaders to control would-be followers. They freely express themselves on social media. This results in considerable propaganda being generated and widespread attention to white supremacist and other hateful ideas. On the other hand, there is no control over the narrative: it embraces a staggering variety of causes, with numerous factions and subfactions constantly forming and splitting. Operations may be encouraged via social media, but the lack of training or operational security of recruits often leads to their discovery. This decentralization and amateurism stand in sharp contrast to Hamas and Hezbollah.

Hamas's and Hezbollah's fierce counterterrorism

environments may also explain their preference for one-to-many technologies and more limited use of social media. On an operational level, the omnipresent threat from Israel reinforces both Hamas's and Hezbollah's need for secure channels, making it less inclined to prefer many-to-many networks that expose vulnerabilities in operational security. While Hezbollah attempted to use social media and other platforms for operational support—including recruiting prospective operatives, surveilling targets, organizing cells, and transferring money—Israel has often monitored this activity successfully. Using the accounts of more prominent members with social media followings on platforms like Facebook—such as Jawad Nasrallah, a son of the Hezbollah leader who is also a poet and writer—Hezbollah has reached out to potential recruits in Palestinian areas, trying to exploit unrest there. The group has also created pro-Palestinian Facebook profiles and has engaged with Palestinians who visited these. Hezbollah would then use email and encrypted platforms to make further connections.[38] Nonetheless, it is important to recognize that these efforts were largely a failure for Hezbollah.

Israel's savvy online presence has pushed Hezbollah to emphasize security for operational planning. For example, it has employed Telegram because of its built-in encryption and because of the platform's more hands-off policy toward policing its users.[39] It has also constructed a fiber-optic network in areas it controls to improve data security, giving it better connectivity and allowing it to avoid transmitting wireless data, which Israel has often intercepted.[40] Hezbollah has used closed telephone circuits, Voice over Internet Protocols, and private cell networks to communicate efficiently and—its leaders probably hope—securely.[41]

Although both Hamas and Hezbollah have used social media to spy on enemies and for operations, in general this is a less important part of their use of these technologies. Much of this is due to Israeli counterterrorism: operations on social media are often more easily compromised by effective intelligence services that can exploit platforms' anonymity and, often, weak security procedures to uncover plotters and unravel networks.[42] It is likely that both groups will continue to direct the occasional operation via social media, especially to inspire potential terrorists to act on their own, but they will be careful to limit the exposure of key operatives on their side.

Finally, social media crackdowns have also motivated both groups' preferences for one-to-many technologies. Due to the actions of various companies, often spurred by pressure from Israel and its supporters, the official social media sites of Hamas and Hezbollah and their leaders are regularly removed, and much of their content taken down. Israel has a dedicated government unit that works with social media companies to flag content from anti-Israel groups like Hamas and Hezbollah, making thousands of requests each year.[43] Recognizing the limited strategic reach they can achieve amid constant consent takedowns, Hamas and Hezbollah have instead prioritized traditional technologies over social media.

This is not to say Hamas and Hezbollah are absent from social media. Both still have a social media presence, but supporters unaffiliated with the central organization largely manage it and push out global messaging. Most postings are from Hamas sympathizers rather than official representatives of the organization itself. Supporters share Hamas propaganda videos and images, often drawing on what is broadcast on Al Aqsa or other official Hamas outlets.[44] They have used Twitter to organize international protests, have posted videos via Instagram and YouTube to criticize Israeli air strikes and the eviction of Palestinians from their homes, and have made solidarity videos on TikTok, among many other examples. Such efforts, however, are often spontaneous and decentralized.[45] In addition, some Hamas-linked media, such as its children's magazine, claim they are independent of the organization and are run by individuals or groups that are Hamas sympathizers but not formal members. This development benefits both organizations in some regard as it allows them to focus on operational security and localized messaging while benefiting from the global reach its supporters provide.

IMPLICATIONS FOR COUNTERTERRORISM

Counterterrorism actors face varied challenges when confronting Hamas's and Hezbollah's IT strategies. Given their roles in governance, their communications technologies have dual civilian and military uses. Thus, counterterrorist actors should consider how

their roles in governance constrain policy options and inform their approaches.

It is important to recognize that the governance situation differs for Hamas and Hezbollah. Hezbollah, on the one hand, is formally part of the Lebanese government. Despite recent electoral setbacks, Hezbollah dominates many government ministries, including the Port of Beirut.[46] As a result, any major action involving the government of Lebanon requires Hezbollah's blessing. Foreign governments and companies cannot work with the Lebanese government to curtail Hezbollah even though the government is nominally responsible for activities on its soil**.** The overlap between Lebanese infrastructure and Hezbollah's relationship with the Lebanese government, which in the past worked with the United States and other Western powers, makes it difficult to take action against the group. Disruptions of Hezbollah communications, if not carefully targeted, could spread to Lebanon's broader communications infrastructure. In addition, technology provided to the Lebanese government is likely to end up in Hezbollah's hands.

Hamas, on the other hand, is the de facto government of Gaza, and in this capacity, it often has important messages to communicate to the Palestinian public, such as the availability of vaccines or other vital information. Nonetheless, Hamas is skilled at fusing the activities of its military and political branches, increasing the probability that counterterrorism responses will harm civilians. Hamas-linked hospitals, for example, increase the group's popularity among Gazans, enable it to order supplies it can siphon off for military purposes, and provide access to a pool of personnel it can vet based on performance and dedication in a legitimate activity. Israeli officials also claim that Hamas uses legitimate humanitarian activities to hide military personnel, store rockets, and make targeting of Hamas rockets more complex.[47] However, removing healthcare and other humanitarian entities' social media presences and websites reduces information about legitimate and important services Hamas provides. For example, the primary purpose of Hamas hospitals is to provide medical services desperately needed in Gaza, so by taking down a website, Israel might remove the location and hours of a Gaza hospital from the internet. Efforts to reduce support for Hamas can also hinder charitable giving and other humanitarian support.[48] Therefore, blocking all Hamas communication channels could hinder the well-being of ordinary Palestinians.

Counterterrorism actors are unlikely to significantly degrade the capabilities of both groups. While Israel, the United States, and other enemies of these groups focus on Hamas's and Hezbollah's violent and hostile propaganda, there is less focus on much of the content that justifies the groups' actions to supporters, highlights their successes in governance, and otherwise speaks to their communities and potential sympathizers. On social media, where Hamas and Hezbollah supporters are predominantly responsible for peddling these narratives, this content would be permissible under most companies' terms of service as long as the organizations were not designated terrorist organizations. Social media companies blocking this content, especially when resources are limited, would mean removing resources directed toward other posts that pose a greater risk of violence. As Facebook's Brian Fishman told a *New York Times* reporter in 2019: "'If we have to make a hard prioritization decision, we're going to focus on stuff that directly calls for violence. . . . The blunt truth is that it is very difficult' to weed out."[49] Thus, the United States, Israel, and others, in their efforts to pressure social media companies to take down content supporting both groups, need to consider and accept the trade-offs in a world of finite resources. Keeping this usage limited is vital given the potential propaganda and recruiting power of social media.

In addition to having limited effects, pressing social media companies to expand the scope of their takedowns risks over-enforcing legitimate social media users. Such actions could raise serious questions around civil liberties, have a chilling effect on charitable organizations that work in Lebanon and the Palestinian territories, and even limit platforms' interest in investigating emergent threats and reporting them to law enforcement.[50] Thus, governments should seriously scrutinize the risks of blanket pressure on social media companies.

Given the risks associated with targeting Hamas's and Hezbollah's strategic communications related to governance and considering both groups' caution with social media as a tool of operational planning, counterterrorism actors should also focus their efforts on the traditional technologies both groups rely on

for operational coordination and target technologies such as encrypted messaging platforms. This targeted approach enables actors to degrade Hamas's and Hezbollah's ability to plan and execute attacks while minimizing the negative civilian impacts. This approach may involve high-end signals intelligence efforts as well as old-fashioned human spying. Despite considerable talk of encryption as a game changer for terrorist groups, governments have a strong record of penetrating supposedly encrypted communications, often due to a range of common user errors. Hezbollah, and to some degree Hamas, have better-trained operatives and more advanced systems than groups like the Islamic State or right-wing terrorists, making them a harder target.

. . . counterterrorism actors should also focus their efforts on the traditional technologies both groups rely on for operational coordination and target technologies such as encrypted messaging platforms.

CONCLUSION

IT is constantly evolving, and Hamas, Hezbollah, and other terrorist groups will use these technologies in both established and creative ways. Governments, social media companies, and others dedicated to disrupting these groups need to recognize the varied ways in which they use IT and that even the most aggressive efforts are likely to face many limits.

In addition, governments should distinguish the technologies Hamas and Hezbollah rely on for strategic communications versus operational planning: both groups favor traditional technologies for the former and prefer more niche and encrypted networks for the latter. Moderating content in the groups' encrypted channels also proves technologically challenging but presents the clearest link between the organizations and their use of violence. Therefore, targeting these channels via intelligence operations may represent the clearest way to thwart Hamas's and Hezbollah's attacks, but it comes with significant risks and costs. The groups' supporters, meanwhile, drive social media content.

This diversified IT strategy poses a challenge for all counterterrorist actors. Even if social media companies prioritize takedowns, they will limit resources for content that is generally more violent and threatening. Moreover, these actions will not affect Hamas's and Hezbollah's communication wings, as they generally rely on more traditional technologies that doubly support their roles in governance. ■

Daniel Byman *is a senior fellow with the Transnational Threats Project at the Center for Strategic and International Studies and a professor in the School of Foreign Service at Georgetown University.* ***Emma McCaleb*** *holds a BS of Foreign Service and an MA in Security Studies from Georgetown University, where she concentrated in terrorism and substate violence. She currently works on terrorism and counterterrorism issues in Washington, DC.*

The authors would like to thank Jon Alterman for his comments on a previous version of this paper.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

ENDNOTES

1 Devorah Margolin, "#Hamas: A Thematic Exploration of Hamas's English-Language Twitter," *Terrorism and Political Violence* 34, no. 6 (2022): 9.

2 Moran Yarchi and Ami Ayalon, "Fighting over the Image: The Israeli-Palestinian Conflict in the Gaza Strip 2018-19," *Studies in Conflict & Terrorism*, June 23, 2019, https://www.tandfonline.com/doi/full/10.1080/1057610X.2020.1751461; and Maura Conway, *Terrorist Web Sites: Their Contents, Functioning, and Effectiveness* (St Andrews, Scotland: University of St. Andrews, n.d.), 21, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.9794&rep=rep1&type=pdf.

3 Although Israel has universal conscription, the Israeli Arab and parts of the ultra-Orthodox community have exemptions.

4 Margolin, "#Hamas."

5 Moran Yarchi, "Terror Organizations' Uses of Public Diplomacy: Limited versus Total Conflicts," *Studies in Conflict & Terrorism* 39, no. 12 (2016): 1071-83, https://www.tandfonline.com/doi/full/10.1080/1057610X.2016.1184064.

6 Ibid.

7 Margolin, "#Hamas."

8 Associated Press, "Cartoon Mouse Dies for a Cause," *Seattle Times*, June 30, 2007, https://www.seattletimes.com/nation-world/cartoon-mouse-dies-for-a-cause/.

9 Conway, "Terrorist Web Sites," 18-19.

10 Zak Doffman, "Honey Trap Malware—Here Are The Hamas Dating Apps That Hacked Israeli Soldiers," *Forbes*, February 16, 2020, https://www.forbes.com/sites/zakdoffman/2020/02/16/terrorist-android-malware-exposed-here-are-the-hamas-apps-that-targeted-israeli-soldiers/?sh=3408d8c023ae; Judah Ari Gross and Toi Staff, "After Facebook, Hamas Turns to Instagram to Lure IDF Soldiers, Army Says," *Times of Israel*, August 15, 2018, https://www.timesofisrael.com/after-facebook-hamas-turns-to-instagram-to-lure-idf-soldiers-army-says/; and Ruth Eglash, "Israel Says Hamas Hacked Facebook Accounts, Cellphones of Army Recruits," *Washington Post*, January 11, 2017, https://www.washingtonpost.com/world/middle_east/israel-says-hamas-hacked-facebook-accounts-cellphones-of-army-recruits/2017/01/11/f71543a4-d827-11e6-a0e6-d502d6751bc8_story.html.

11 "Hamas Tried to Hack Israeli Soldiers with World Cup App, Israel Says," DW News, July 3, 2018, https://www.dw.com/en/hamas-tried-to-hack-israeli-soldiers-with-world-cup-app-israel-says/a-44511193; and Christopher Burgess, "Hamas Is Using Apps for Social Engineering," BlackBerry, August 21, 2018, https://blogs.blackberry.com/en/2018/08/hamas-is-using-apps-for-social-engineering.

12 Rosie Perper, "Hamas Reportedly Created a Fake Dating App to Lure Israeli Soldiers and Steal Security Information," *Business Insider*, July 3, 2018, https://www.businessinsider.com/hamas-fake-dating-app-scam-israeli-soldiers-honeypot-glancelove-2018-7.

13 For a detailed discussion, see Lina Khatib, *Image Politics in the Middle East: The Role of the Visual in Political Struggle* (London: I.B. Tauris, 2012).

14 Colin P. Clarke, "How Hezbollah Came to Dominate Information Warfare," RAND Corporation, September 19, 2017, https://www.rand.org/blog/2017/09/how-hezbollah-came-to-dominate-information-warfare.html.

15 Avraham Levine, "What Is Hezbollah Trying to Tell Us? Information Warfare on the Social Media," Alma Research and Education Center, September 1, 2021, https://israel-alma.org/2021/09/01/what-is-hezbollah-trying-to-tell-us-information-warfare-on-the-social-media/.

16 Charlie Winter, "Redefining Propaganda: The Media Strategy of the Islamic State," *RUSI Journal* 165, no. 1 (March 17, 2020): 38-42, https://www.tandfonline.com/doi/abs/10.1080/03071847.2020.1734321?journalCode=rusi20.

17 Conway, "Terrorist Web Sites," 17.

18 Sheera Frenkel and Ben Hubbard, "After Social Media Bans, Militant Groups Found Ways to Remain," *New York Times*, April 19, 2019, https://www.nytimes.com/2019/04/19/technology/terrorist-groups-social-media.html.

19 Clarke, "How Hezbollah."

20 Yarchi, "Terror Organizations."

21 For background, see Avi Jorisch, "Beacon of Hatred: Inside Hezbollah's al-Manar Television," Washington Institution for Near East Policy, October 25, 2004, https://www.washingtoninstitute.org/policy-analysis/beacon-hatred-inside-hizballahs-al-manar-television.

22 Amir Mizroch, "Al Manar TV Soars into Ratings 'Top 10," *Jerusalem Post*, August 25, 2006, https://www.jpost.com/middle-east/al-manar-tv-soars-into-ratings-top-10.

23 U.S. Department of the Treasury, "U.S. Designates Al-Manar as a Specially Designated Global Terrorist Entity Television Station is Arm of Hizballah Terrorist Network," Press release, March 23, 2006, https://home.treasury.gov/news/press-releases/js4134.

24 Mayan Sarnat, "Hezbollah's Communications Infrastructure," Alma Research and Education Center, March 9, 2021, https://israel-alma.org/2021/03/09/hezbollahs-communications-infrastructure-a-strategic-asset-for-its-operational-activity/.

25 Ibid.

26 Omer Benjakob, "Hezbollah Proxy Penetrates Telecom Systems Worldwide, Israeli Cybersecurity Firm Says," *Haaretz*, January 28, 2021, https://www.haaretz.com/israel-news/.premium-hezbollah-proxy-penetrates-telecom-systems-worldwide-israel-firm-says-1.9492257.

27 Emilio Iasiello, "Hezbollah's Information-Enabled Capabilities Are a Quiet Force," Strike Source, March 8, 2021, https://strikesource.com/2021/03/08/hezbollahs-information-enabled-capabilities-are-a-quiet-force/.

28 Sarnat, "Hezbollah's Communications Infrastructure."

29 Benjakob, "Hezbollah Proxy."

30 Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists* (Oxford: Oxford University Press, 2019).

31 Klaus Bruhn Jensen and Rasmus Helles, "The Internet as a Cultural Forum: Implications for Research," *New Media and Society* 13, no. 4 (2010): 517-33.

32 Charlie Winter et al., "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-strategies," *International Journal of Conflict and Violence* 14 (2020): 1-20, https://doi.org/10.4119/ijcv-3809; and Charlie Winter and Jordan Bach-Lombardo, "Why ISIS Propaganda Works," *The Atlantic*, February 13, 2016, https://www.theatlantic.com/international/archive/2016/02/isis-propaganda-war/462702/. More discussion in

33 Alexander Hitchens, Bennett Clifford, and Seamus Hughes, *Homegrown: ISIS in America* (London: I.B. Tauris, 2020).

34 Chelsea Daymon and Devorah Margolin, *Women in American Violent Extremism: An Examination of Far-Right and Salafi-Jihadist Movements* (Washington, DC: George Washington University Program on Extremism, June 2022), 59.

35 Clarke, "How Hezbollah."

36 Winter, "Redefining Propaganda."

37 Daniel Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism* (Oxford: Oxford University Press, 2022).

38 Michael Shkolnik and Alexander Corbeil, "Hezbollah's 'Virtual Entrepreneurs': How Hezbollah Is Using the Internet to Incite Violence in Israel," *CTC Sentinel* 12, no. 9 (October 2019): 28–35, https://ctc.usma.edu/hezbollahs-virtual-entrepreneurs-hezbollah-using-internet-incite-violence-israel/.

39 Counter Extremism Project, *Terrorists on Telegram* (New York, NY: Counter Extremism Project, May 2017), https://www.counterextremism.com/sites/default/files/Terrorists%20on%20Telegram_052417.pdf.

40 Chris Soghoian, "For Hezbollah, It's Fiber Warfare," CNET, May 13, 2008, https://www.cnet.com/tech/services-and-software/for-hezbollah-its-fiber-warfare/.

41 Sarnat, "Hezbollah's Communications Infrastructure."

42 Daniel Byman, "When Hate Goes Viral," *Foreign Policy*, March 23, 2022, https://foreignpolicy.com/2022/03/23/white-supremacist-terrorism-social-media-internet/.

43 Luke Goldstein, "How a Secretive Cyber Unit Censors Palestinians," American Prospect, July 12, 2021, https://prospect.org/world/how-secretive-cyber-unit-censors-palestinians/.

44 Frenkel and Hubbard, "After Social Media Bans."

45 Alex Ward, "The 'TikTok Intifada,'" Vox, May 20, 2021, https://www.vox.com/22436208/palestinians-gaza-israel-tiktok-social-media.

46 Lina Khatib and Jon Wallace, "Lebanon's Politics and Politicians," Chatham House, August 11, 2021, https://www.chathamhouse.org/2021/08/lebanons-politics.

47 Terrence McCoy, "Why Hamas Stores Its Weapons inside Hospitals, Mosques, and Schools," *Washington Post*, July 31, 2014, https://www.washingtonpost.com/news/morning-mix/wp/2014/07/31/why-hamas-stores-its-weapons-inside-hospitals-mosques-and-schools/.

48 Rob Kuznia, "Scrutiny over Terrorism Funding Hampers Charitable Work," *Washington Post*, April 19, 2017, https://www.washingtonpost.com/national/scrutiny-over-terrorism-funding-hampers-charitable-work-in-ravaged-countries/2017/04/18/146a585a-1305-11e7-9e4f-09aa75d3ec57_story.html.

49 Frenkel and Hubbard, "After Social Media Bans."

50 Brian Fishman, *Dual-Use Regulation: Managing Hate and Terrorism Online before and after Section 230 Reform* (Washington, DC: Brookings Institution, March 14, 2023).