Atlantic Council

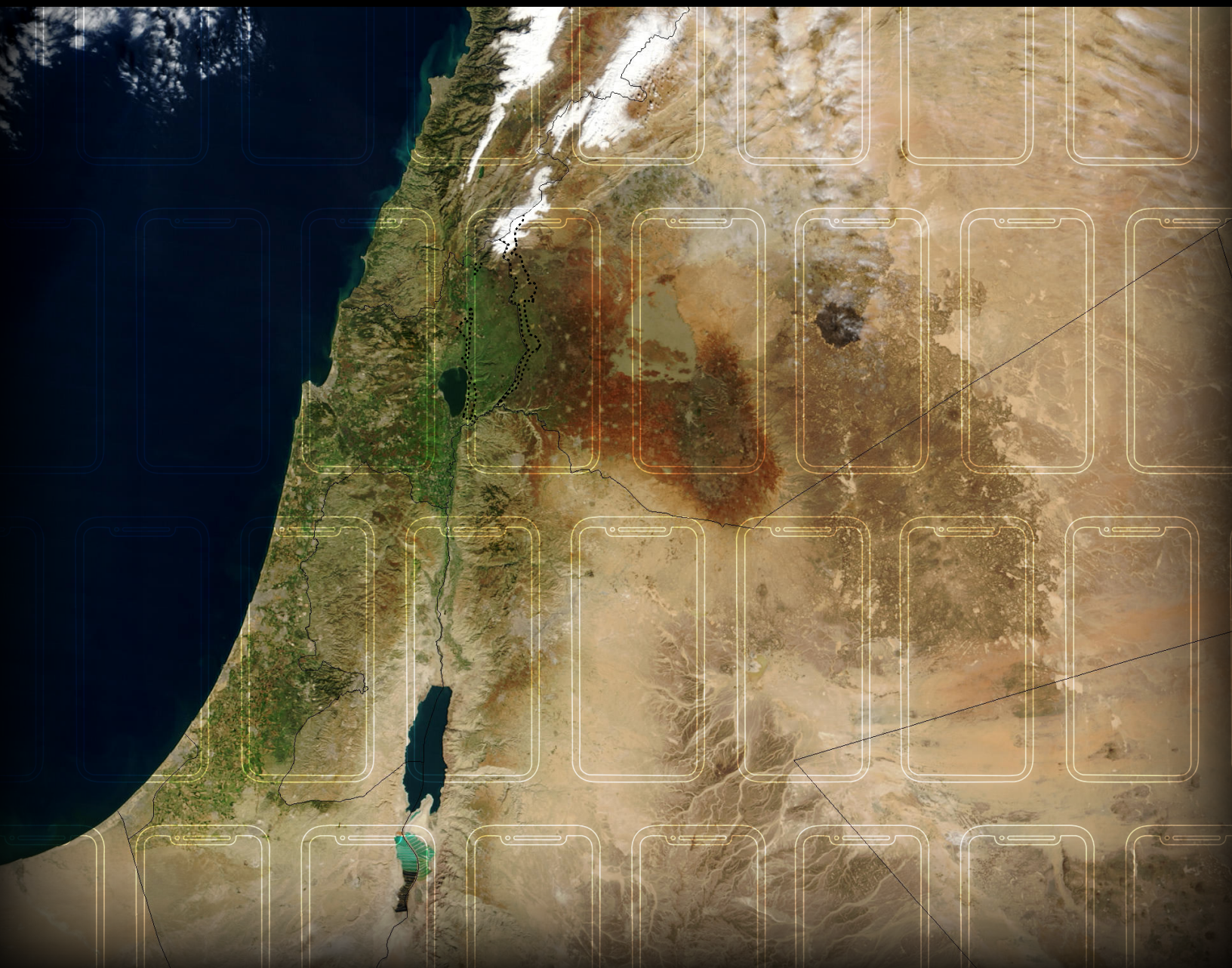
CYBER STATECRAFT INITIATIVE

DFRLab

THE CYBER STRATEGY AND OPERATIONS OF HAMAS:

Green Flags and Green Hats

By Simon P. Handler



CYBER STATECRAFT
INITIATIVE

DFRLab

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

© 2022 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

Cover image:

CYBER STATECRAFT
INITIATIVE

DFRLab

THE CYBER STRATEGY AND OPERATIONS OF HAMAS:

Green Flags and Green Hats

By Simon P. Handler

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyberspace as a domain of conflict often creates an asymmetric advantage for comparably less capable or under-resourced actors to compete against relatively stronger counterparts.[1] As such, a panoply of non-state actors is increasingly acquiring capabilities and integrating offensive cyber operations into their toolkits to further their strategic aims. From financially driven criminal ransomware groups to politically inspired patriot hacking collectives, non-state actors have a wide range of motivations for turning to offensive cyber capabilities. A number of these non-state actors have histories rooted almost entirely in armed kinetic violence, from private military companies to drug cartels, and the United States and its allies are still grappling with how to deal with them in the cyber context.[2] Militant and terrorist organizations have their own specific motivations for acquiring offensive cyber capabilities, and their operations therefore warrant close examination by the United States and its allies to develop effective countermeasures.

While most academic scholarship and government strategies on counterterrorism are beginning to recognize and address the integral role of some forms of online activity, such as digital media and propaganda on behalf of terrorist organizations, insufficient attention has been given to the offensive cyber capabilities of these actors. Moreover, US strategy,[3] public intelligence assessments, and academic literature on global cyber threats to the United States overwhelmingly focuses on the "big four" nation-state adversaries—China, Russia, Iran, and North Korea. Before more recent efforts to address the surge in financially driven criminal ransomware operations, the United States and its allies deployed policy countermeasures overwhelmingly designed for use against state actors.

To the extent that US counterterrorism strategy addresses the offensive cyber threat from terrorist organizations, it is focused on defending critical infrastructure against the physical consequences of a cyberattack. Hamas, despite being a well-studied militant and terrorist organization, is expanding its offensive cyber and information capabilities, a fact that is largely overlooked by counterterrorism and cyber analysts alike. Overshadowed by the specter of a catastrophic cyberattack from other entities, the real and ongoing cyber threats posed by Hamas prioritize espionage and information operations.

This report seeks to highlight Hamas as an emerging and capable cyber actor, first by explaining Hamas's overall strategy, a critical facet for understanding the group's use of cyber operations. Next, an analysis will show how Hamas's cyber activities do not indicate a sudden shift in strategy but, rather, a realignment that augments operations. In other words, offensive cyber operations are a new way for Hamas to do old things better. Finally, the policy community is urged to think differently about how it approaches similar non-state groups that may leverage the cyber domain in the future. This report can be used as a case study for understanding the development and implementation of cyber tools by non-state entities.

1 Michael Schmitt, "Normative Voids and Asymmetry in Cyberspace," *Just Security*, December 29, 2014, https://www.justsecurity.org/18685/normative-voids-asymmetry-cyberspace/.

2 Emma Schroeder et al., *Hackers, Hoodies, and Helmets: Technology and the Changing Face of Russian Private Military Contractors*, *Atlantic Council*, July 25, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/technology-change-and-the-changing-face-of-russian-private-military-contractors; Cecile Schilis-Gallego and Nina Lakhani, "It's a Free For All: How Hi-Tech Spyware Ends Up in the Hands of Mexico's Cartels," *Guardian* (UK), December 7, 2020, https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption.

3 The White House, *National Security Strategy*, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.; Emma Schroeder, Stewart Scott, and Trey Herr, *Victory Reimagined: Toward a More Cohesive US Cyber Strategy*, *Atlantic Council,* June 14, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/victory-reimagined/.

As the title of this report suggests, Hamas is like a *green hat hacker*—a term that is not specific to the group but recognized in the information security community as someone who is relatively new to the hacking world, lacking sophistication but fully committed to making an impact and keen to learn along the way.[4] Hamas has demonstrated steady improvement in its cyber capabilities and operations over time, especially in its espionage operations against internal and external targets. At the same time, the organization's improvisation, deployment of relatively unsophisticated tools, and efforts to influence audiences are all hallmarks of terrorist strategies. This behavior is in some ways similar to the Russian concept of "information confrontation," featuring a blend of technical, information, and psychological operations aimed at wielding influence over the information environment.[5]

Understanding these dynamics, as well as how cyber operations fit into the overall strategy, is key to the US development of effective countermeasures against terrorist organizations' offensive cyber operations.

4 Clare Stouffer, "15 Types of Hackers + Hacking Protection Tips for 2022," Norton, May 2, 2022, https://us.norton.com/internetsecurity-emerging-threats-types-of-hackers.html#Greenhat.

5 Janne Hakala and Jazlyn Melnychuk, "Russia's Strategy in Cyberspace," NATO Strategic Communications Centre of Excellence, June 2021, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf.

"PWN" GOAL

In the summer of 2018, as teams competed in the International Federation of Association Football (FIFA) World Cup in Russia, Israeli soldiers followed the excitement on their smartphones from an Israel Defense Forces (IDF) base thousands of miles away. Like others in Israel, the soldiers were using a new Android application called Golden Cup, available for free from the Google Play store. The program was promoted in the lead up to the tournament as "the fastest app for live scores and fixtures for the World Cup."[6] The easy-to-use application delivered as advertised—and more.

Once installed, the application communicated with its command-and-control server to surreptitiously download malicious payloads onto user devices. The payloads infected the target devices with spyware, a variety of malware that discreetly monitors the target's device and steals its information, usually for harmful use against the target individual.[7] In this particular case, the spyware was intentionally deployed after the application was downloaded from the Google Play store in order to bypass Google's security screening process.[8] This allowed the spyware operator to remotely execute code on user smartphones to track locations, access cameras and microphones, download images, monitor calls, and exfiltrate files.

Golden Cup users, which included Israeli civilians and soldiers alike, did not realize that their devices were infected with spyware. As soldiers went about their daily routines on bases, the spyware operators reaped reams of data from the compromised smartphones. In just a few weeks of discreet collection, before discovery by IDF security, the adversary successfully collected non-public information about various IDF bases, offices, and military hardware, such as tanks and armored vehicles.[9]

The same adversary targeted Israeli soldiers with several other malicious Android applications throughout the summer of 2018. A fitness application that tracks user running routes collected the phone numbers of soldiers jogging in a particularly sensitive geographic location. After collecting these numbers, the adversary targeted the soldiers with requests to download a second application that then installed spyware. Additional targeting of Israeli soldiers that same summer included social engineering campaigns encouraging targets to download various spyware-laced dating applications with names like Wink Chat and Glance Love, prompting the IDF to launch the aptly named Operation Broken Heart in response.[10]

Surprisingly, this cyber espionage campaign was not the work of a nation-state actor. Although the clever tradecraft exhibited in each operation featured many of the hallmarks of a foreign intelligence service, neither Israel's geopolitical nemesis Iran nor China,[11] an increasingly active Middle East regional player, was involved.[12] Instead, the campaign was the work of Hamas.

6 Roy Iarchy and Eyal Rynkowski, "GoldenCup: New Cyber Threat Targeting World Cup Fans," Broadcom Software, July 5, 2018, https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/goldencup-new-cyber-threat-targeting-world-cup-fans.

7 "Spyware," MalwareBytes, https://www.malwarebytes.com/spyware.

8 Taylor Armerding, "Golden Cup App Was a World Cup of Trouble," Synopsys, July 12, 2022, https://www.synopsys.com/blogs/software-security/golden-cup-app-world-cup-trouble/.

9 Yaniv Kubovich, "Hamas Cyber Ops Spied on Hundreds of Israeli Soldiers Using Fake World Cup, Dating Apps," *Haaretz*, July 3, 2018, https://www.haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773.

10 Ruth Eglash, "Israel Says Hamas Tried to Infiltrate Its Military Using Dating and Sports Apps," *Boston Globe*, July 3, 2018, https://www.bostonglobe.com/news/world/2018/07/03/israel-says-hamas-tried-infiltrate-its-military-using-dating-and-sports-apps/yC2HfakeUXDlhZw5XhMSBN/story.html; https://www.idf.il/en/minisites/hamas/hamas-online-terrorism/.

11 J.D. Work, *Troubled Vision: Understanding Recent Israeli–Iranian Offensive Cyber Exchanges*, *Atlantic Council*, July 22, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/.

12 Amos Harel, "How Deep Has Chinese Intelligence Penetrated Israel?" *Haaretz*, February 25, 2022, https://www.haaretz.com/israel-news/.premium-how-deep-has-chinese-intelligence-penetrated-israel-1.10633942.

1. INTRODUCTION

The asymmetric advantage afforded by cyberspace is leading a panoply of non-state actors to acquire and use offensive cyber capabilities to compete against relatively stronger counterparts. The cyber threat from criminal ransomware organizations has been well documented, yet a range of other non-state actors traditionally involved in armed kinetic violence, from private military companies to drug cartels, is also trying their hand at offensive cyber operations, and the United States and its allies are still grappling with how to respond. Each actor has a discreet motivation for dabbling in cyber activities, and lumping them all into one bucket of non-state actors can complicate efforts to study and address their actions. The operations of militant and terrorist organizations in particular warrant close examination by the United States and its allies in order to develop effective countermeasures.

A robust online presence is essential for modern terrorist organizations. They rely on the internet to recruit members, fund operations, indoctrinate target audiences, and garner attention on a global scale—all key functions for maintaining organizational relevance and for surviving.[13] The 2022 Annual Threat Assessment from the US Intelligence Community suggests that terrorist groups will continue to leverage digital media and internet platforms to inspire attacks that threaten the United States and US interests abroad.[14] Recent academic scholarship on counterterrorism concurs, acknowledging the centrality of the internet to various organizations, ranging from domestic right-wing extremists to international jihadists, and their efforts to radicalize, organize, and communicate.

The US government has taken major steps in recent years to counter terrorist organizations in and through cyberspace. The declassification of documents on Joint Task Force Ares and Operation Glowing Symphony, which began in 2016, sheds light on complex US Cyber Command efforts to combat the Islamic State in cyberspace, specifically targeting the group's social media and propaganda efforts and leveraging cyber operations to support broader kinetic operations on the battlefield.[15] The latest US National Strategy for Counterterrorism, published in 2018, stresses the need to impede terrorist organizations from leveraging the internet to inspire and enable attacks.[16]

Indeed, continued efforts to counter the evolving social media and propaganda tools of terrorist organizations will be critical, but this will not comprehensively address the digital threat posed by these groups. Counterterrorism scholarship and government strategies have paid scant attention to the offensive cyber capabilities and operations of terrorist organizations, tools that are related but distinct from other forms of online influence. Activities of this variety do not necessarily cause catastrophic physical harm, but their capacity to influence public perception and, potentially, the course of political events should be cause for concern.

13 "Propaganda, Extremism and Online Recruitment Tactics," Anti-Defamation League, April 4, 2016, https://www.adl.org/education/resources/tools-and-strategies/table-talk/propaganda-extremism-online-recruitment.

14 Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community*, February 7, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

15 National Security Archive, "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY," January 21, 2020, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

16 The White House, *National Strategy for Counterterrorism of the United States of America*, October 2018, https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf.

Several well-discussed, politically significant non-state actors with histories rooted almost entirely in kinetic violence are developing, or otherwise acquiring, offensive cyber capabilities to further their interests. More scrutiny of these actors, their motivations, and how they strategically deploy offensive cyber capabilities in conjunction with evolving propaganda and kinetic efforts is warranted to better orient toward the threat.

Hamas, a Palestinian political party and militant terrorist organization that serves as the de facto governing body of the Gaza Strip, is one such actor. The group's burgeoning cyber capabilities, alongside its propaganda tactics, pose a threat to Israel, the Palestinian Authority, and US interests in the region—especially in tandem with the group's capacities to fund, organize, inspire, and execute kinetic attacks. This combination of capabilities has historically been the dominion of more powerful state actors. However, the integration of offensive cyber capabilities into the arsenals of traditionally kinetic non-state actors, including militant organizations, is on the rise due to partnerships with state guarantors and the general proliferation of these competencies worldwide.

This report seeks to highlight the offensive cyber and information capabilities and behavior of Hamas. First, a broad overview of Hamas's overall strategy is provided, an understanding of which is key for evaluating its cyber activities. Second, this report analyzes the types of offensive cyber operations in which Hamas engages, showing that the adoption of cyber capabilities does not indicate a sudden shift in strategy but, rather, a realignment of strategy and an augmentation of operations. In other words, offensive cyber operations are a new way to do old things better. Third, this report aims to push the policy community to think differently about its approach to similar non-state groups that may leverage the cyber domain in the future.

2. OVERVIEW OF HAMAS'S STRATEGY

Principles and Philosophy

Founded in the late 1980s, *Harakat al-Muqawamah al-Islamiyyah*, translated as the Islamic Resistance Movement and better known as Hamas, is a Palestinian religious political party and militant organization. After Israel disengaged from the Gaza Strip in 2005, Hamas used its 2006 Palestinian legislative election victory to take over militarily from rival political party Fatah in 2007. The group has served as the de facto ruler of Gaza ever since, effectively dividing the Palestinian Territories into two entities, with the West Bank governed by the Hamas-rejected and Fatah-controlled Palestinian Authority.[17]

Hamas's overarching objectives are largely premised on its founding principles—terminating what it views as the illegitimate State of Israel and establishing Islamic, Palestinian rule.[18] The group's grand strategy comprises two general areas of focus: resisting Israel and gaining political clout with the Palestinian people. These objectives are interconnected and mutually reinforcing, as Hamas's public resistance to Israel feeds Palestinian perceptions of the group as the leader of the Palestinian cause.[19]

Despite Hamas's maximalist public position on Israel, the organization's leaders are rational actors who logically understand the longevity and power of the State of Israel. Where the group can make meaningful inroads is in Palestinian politics, trying to win public support from the more secular, ruling Fatah party and positioning itself to lead a future Palestinian state. Looming uncertainty about the future of an already weak Palestinian Authority, led by the aging President Mahmoud Abbas, coupled with popular demand for elections, presents a potential opportunity for Hamas to fill a leadership vacuum.[20]

To further these objectives, Hamas attracts attention by frequently generating and capitalizing on instability. The group inflames already tumultuous situations to foster an environment of extremism, working against those who are willing to cooperate in the earnest pursuit of a peaceful solution to the Israel–Palestine conflict. Hamas uses terror tactics to influence public perception and to steer political outcomes, but still must exercise strategic restraint to avoid retaliation that could be militarily and politically damaging. Given these self-imposed restraints, Hamas seeks alternative methods of influence that are less likely to result in blowback.

The map shows Israel and surrounding countries with international borders, the national capital Jerusalem, district capitals, major cities, main roads, railroads, and major airports.
SOURCE: Nations Online Project.

17 "Hamas: The Palestinian Militant Group That Rules Gaza," BBC, July 1, 2022, https://www.bbc.com/news/world-middle-east-13331522.

18 "The Covenant of the Islamic Resistance Movement," August 18, 1988, https://avalon.law.yale.edu/20th_century/hamas.asp.

19 Gur Laish, "The Amorites Iniquity – A Comparative Analysis of Israeli and Hamas Strategies in Gaza," *Infinity Journal* 2, no. 2 (Spring 2022), https://www.militarystrategymagazine.com/article/the-amorites-iniquity-a-comparative-analysis-of-israeli-and-hamas-strategies-in-gaza/.

20 Khaled Abu Toameh, "PA Popularity Among Palestinians at an All-Time Low," *Jerusalem Post*, November 18, 2021, https://www.jpost.com/middle-east/pa-popularity-among-palestinians-at-an-all-time-low-685438.

Terrorism Strategy

Hamas's terror tactics have included suicide bombings,[21] indiscriminate rocket fire,[22] sniper attacks,[23] incendiary balloon launches,[24] knifings,[25] and civilian kidnappings,[26] all in support of its larger information strategy to project a strong image and to steer political outcomes. Through these activities, Hamas aims to undermine Israel and the Palestinian Authority[27] and challenge the Palestine Liberation Organization's (PLO)[28] standing as the "sole representative of the Palestinian people."

Terrorism forms the foundation of Hamas's approach, and the organization's leadership openly promotes such activities.[29] While the group's terror tactics have evolved over time, they have consistently been employed against civilian targets to provoke fear, generate publicity, and achieve political objectives. Israeli communities targeted by terrorism, as well as Palestinians in Gaza living under Hamas rule, suffer from considerable physical and psychological stress,[30] driving Israeli policymakers to carry out military operations, often continuing a vicious cycle that feeds into Hamas's information campaign.

These terrorist tactics follow a coercive logic that aligns with Hamas's greater messaging objectives. Robert Pape's "The Strategic Logic of Suicide Terrorism" specifically names Hamas as an organization with a track record of perpetrating strategically timed suicide terrorist attacks for coercive political effect.[31] In 1995, for example, Hamas conducted a flurry of suicide attacks, killing dozens of civilians in an attempt to pressure the Israeli government to withdraw from certain locations in the West Bank. Once negotiations were underway between Israel and the PLO, Hamas temporarily suspended the attacks, only to resume them against Israeli targets when diplomatic progress appeared to stall. Israel would eventually partially withdraw from several West Bank cities later that year.[32]

21 "16 Killed in Suicide Bombings on Buses in Israel: Hamas Claims Responsibility," CNN, September 1, 2004, http://edition.cnn.com/2004/WORLD/meast/08/31/mideast/.

22 "Hamas Rocket Fire a War Crime, Human Rights Watch Says," BBC News, August 12, 2021, https://www.bbc.com/news/world-middle-east-58183968.

23 Isabel Kershner, "Hamas Militants Take Credit for Sniper Attack," *New York Times*, March 20, 2007, https://www.nytimes.com/2007/03/20/world/middleeast/19cnd-mideast.html.

24 "Hamas Operatives Launch Incendiary Balloons into Israel," AP News, September 4, 2021, https://apnews.com/article/technology-middle-east-africa-israel-hamas-6538690359c8de18ef78d34139d05535.

25 Mai Abu Hasaneen, "Israel Targets Hamas Leader after Call to Attack Israelis with 'Cleaver, Ax or Knife,'" *Al-Monitor*, May 15, 2022, https://www.al-monitor.com/originals/2022/05/israel-targets-hamas-leader-after-call-attack-israelis-cleaver-ax-or-knife.

26 Ralph Ellis and Michael Schwartz, "Mom Speaks Out on 3 Abducted Teens as Israeli PM Blames Hamas," CNN, June 15, 2014, https://www.cnn.com/2014/06/15/world/meast/west-bank-jewish-teens-missing.

27 The Palestinian National Authority (PA) is the official governmental body of the State of Palestine, exercising administrative and security control over Area A of the Palestinian Territories, and only administrative control over Area B of the Territories. The PA is controlled by Fatah, Hamas's most significant political rival, and is the legitimate ruler of the Gaza Strip, although Hamas exercises de facto control of the territory.

28 The Palestine Liberation Organization (PLO) is the political organization that is broadly recognized by the international community as the sole legitimate representative of the Palestinian people. The PLO recognizes Israel, setting it apart from Hamas, which is not a member of the organization.

29 Hamas is designated as a foreign terrorist organization by the US State Department and has earned similar designations from dozens of other countries and international bodies, including Australia, Canada, the European Union, the Organization of American States, Israel, Japan, New Zealand, and the United Kingdom. Jotam Confino, "Calls to Assassinate Hamas Leadership as Terror Death Toll Reaches 19," *Jewish Chronicle*, May 12, 2022, https://www.thejc.com/news/world/calls-to-assassinate-hamas-leadership-as-terror-death-tolls-reaches-19-19wCeFxlx3w40gFCKQ9xSx; Byron Kaye, "Australia Lists All of Hamas as a Terrorist Group," Reuters, March 4, 2022, https://www.reuters.com/world/middle-east/australia-lists-all-hamas-terrorist-group-2022-03-04; Public Safety Canada, "Currently Listed Entities," Government of Canada, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx; "COUNCIL IMPLEMENTING REGULATION (EU) 2020/19 of 13 January 2020 implementing Article 2(3) of Regulation (EC) No 2580/2001 on Specific Restrictive Measures Directed Against Certain Persons and Entities with a View to Combating Terrorism, and Repealing Implementing Regulation (EU) 2019/1337," *Official Journal of the European Union*, January 13, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2020:008I:FULL&from=EN; Organization of American States, "Qualification of Hamas as a Terrorist Organization by the OAS General Secretariat," May 17, 2021, https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-051/21; Ministry of Foreign Affairs, "Japan's Foreign Policy in Major Diplomatic Fields," Japan, 2005, https://www.mofa.go.jp/policy/other/bluebook/2005/ch3-a.pdf; "UK Parliament Approves Designation of Hamas as a Terrorist Group," *Haaretz*, November 26, 2021, https://www.haaretz.com/israel-news/.premium-u-k-parliament-approves-designation-of-hamas-as-a-terrorist-group-1.10419344.

30 Nathan R. Stein et al., "The Differential Impact of Terrorism on Two Israeli Communities," *American Journal of Orthopsychiatry*, American Psychological Association, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3814032/.

31 Robert A. Pape, "The Strategic Logic of Suicide Terrorism," *The American Political Science Review*, August 2003, https://www.jstor.org/stable/3117613?seq=6#metadata_info_tab_contents.

32 "Arabs Celebrate Israeli Withdrawal," *South Florida Sun-Sentinel*, October 26, 1995, https://www.sun-sentinel.com/news/fl-xpm-1995-10-26-9510260008-story.html.

Similarly, just several months before Israel's 1996 general election, incumbent Labor Party Prime Minister Shimon Peres led the polls by roughly 20 percent in his reelection bid against Benjamin Netanyahu and the Likud Party. However, a spate of Hamas suicide bombings cut Peres's lead and Netanyahu emerged victorious.[33] The attacks were designed to weaken the reelection bid of Peres, widely viewed as the candidate most likely to advance the peace process, and strengthen the candidacy of Netanyahu. Deliberate terror campaigns such as these demonstrate the power Hamas wields over Israeli politics.[34]

The Israeli security establishment has learned lessons from the phenomenon of suicide terrorism, implementing countermeasures to foil attacks. Since the mid-2000s, Hamas has shifted its focus to firing rockets of various ranges and precision from the Gaza Strip at civilian population centers in Israel.[35] The rocket attacks became frequent after Israel's disengagement from Gaza in 2005, ebbing and flowing in alignment with significant political events.[36] For instance, the organization targeted towns in southern Israel with sustained rocket fire in the lead up to the country's general election in 2009 to discourage Israelis from voting for pro-peace candidates.[37]

Strategic Restraint

Each of these terror tactics has the powerful potential to generate publicity with Israelis, Palestinians, and audiences elsewhere. However, unrestrained terrorism comes at a cost, something Hamas understands. Hamas must weigh its desire to carry out attacks with the concomitant risks, including an unfavorable international perception, military retaliation, infrastructure damage, and internal economic and political pressures.

Hamas addresses this in a number of ways. First, it limits its operations, almost exclusively, to Israel and the Palestinian Territories. Hamas has learned from the failures of other Palestinian terrorist organizations, whose operations beyond Israel's borders were often counterproductive, attracting legitimate international criticism of these groups.[38] Such operations also run the risk of alienating critical Hamas benefactors like Qatar and Turkey.[39] These states, which maintain important relationships with the United States—not to mention burgeoning ties with Israel—could pressure Hamas to course correct, if not outright withdraw their support for the organization.[40] The continued flow of billions of dollars in funding from benefactors like Qatar is critical, not just to Hamas's capacity to conduct terror attacks and wage war,[41] but also to its efforts to reconstruct infrastructure and provide social

33 Brent Sadler, "Suicide Bombings Scar Peres' Political Ambitions," CNN, May 28, 1996, http://www.cnn.com/WORLD/9605/28/israel.impact/index.html.

34 Akiva Eldar, "The Power Hamas Holds Over Israel's Elections," *Al-Monitor*, February 11, 2020, https://www.al-monitor.com/originals/2020/02/israel-us-palestinians-hamas-donald-trump-peace-plan.html.

35 Yoram Schweitzer, "The Rise and Fall of Suicide Bombings in the Second Intifada," *The Institute for National Security Studies*, October 2010, https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1289896644.pdf; Beverley Milton-Edwards and Stephen Farrell, *Hamas: The Islamic Resistance Movement* (Polity Press, 2013), https://www.google.com/books/edition/Hamas/ozLNNbwqIAEC?hl=en&gbpv=1.

36 Ministry of Foreign Affairs, "Rocket Fire from Gaza and Ceasefire Violations after Operation Cast Lead (Jan 2009)," State of Israel, March 16, 2016, https://embassies.gov.il/MFA/FOREIGNPOLICY/Terrorism/Pages/Palestinian_ceasefire_violations_since_end_Operation_Cast_Lead.aspx.

37 "PA: Hamas Rockets Are Bid to Sway Israeli Election," Associated Press, September 2, 2009, https://web.archive.org/web/20090308033654/http://haaretz.com/hasen/spages/1062761.html.

38 National Consortium for the Study of Terrorism and Responses to Terrorism, "Global Terrorism Database," University of Maryland, https://www.start.umd.edu/gtd/search/Results.aspx?page=2&casualties_type=&casualties_max=&perpetrator=838&count=100&expanded=yes&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table

39 US Congress, House of Representatives, Subcommittee on the Middle East and North Africa and Subcommittee on Terrorism, Nonproliferation, and Trade, *Hamas Benefactors: A Network of Terror, Joint Hearing before the Subcommittee on the Middle East and North Africa and the Subcommittee on Terrorism, Nonproliferation, and Trade of the Committee on Foreign Affairs*, 113th Congress, September 9, 2014, https://www.govinfo.gov/content/pkg/CHRG-113hhrg89738/html/CHRG-113hhrg89738.htm.

40 "Hamas Faces Risk, Opportunity from Warming Israel–Turkey Ties," France 24, March 16, 2022, https://www.france24.com/en/live-news/20220316-hamas-faces-risk-opportunity-from-warming-israel-turkey-ties; Sean Mathews, "Israeli Military Officials Sent to Qatar as US Works to Bolster Security Cooperation," *Middle East Eye*, July 8, 2022, https://www.middleeasteye.net/news/qatar-israel-military-officials-dispatched-amid-us-efforts-bolster-security.

41 Nitsana Darshan-Leitner, "Qatar is Financing Palestinian Terror and Trying to Hide It," *Jerusalem Post*, February 18, 2022, https://www.jpost.com/opinion/article-696824.

A rocket fired from the Gaza Strip into Israel, 2008.
SOURCE: Flickr/paffairs_sanfrancisco

services in the Gaza Strip, both key factors for building its political legitimacy among Palestinians.[42]

Second, with each terrorist attack, Hamas must weigh the potential for a forceful Israeli military response. The cycle of terrorism and retaliation periodically escalates into full-scale wars that feature Israeli air strikes and ground invasions of Gaza. These periodic operations are known in the Israeli security establishment as "mowing the grass," a component of Israel's strategy to keep Hamas's arsenal of rockets, small arms, and infrastructure, including its elaborate underground tunnel network, from growing out of control like weeds in an unkempt lawn.[43] Hamas's restraint has been apparent since May 2021, when Israel conducted Operation Guardian of the Walls, a roughly two-week campaign of mostly airstrikes and artillery fire aimed at slashing the group's rocket arsenal and production capabilities, crippling its tunnels, and eliminating many of its top commanders. Hamas is thought to be recovering and restocking since the ceasefire, carefully avoiding engaging in provocations that could ignite another confrontation before the group is ready.

Third, and critically, since mid-2021, the last year-plus of the Israel–Hamas conflict has been one of the quietest in decades due to the Israeli Bennett–Lapid government's

42 Shahar Klaiman, "Qatar Pledges $500M to Rebuild Gaza, Hamas Vows Transparency," *Israel Hayom*, May 27, 2021, https://www.israelhayom.com/2021/05/27/qatar-pledges-500m-to-gaza-rebuild-hamas-vows-transparency; Jodi Rudoren, "Qatar Emir Visits Gaza, Pledging $400 Million to Hamas," *New York Times*, October 23, 2012, https://www.nytimes.com/2012/10/24/world/middleeast/pledging-400-million-qatari-emir-makes-historic-visit-to-gaza-strip.html.

43 Adam Taylor, "With Strikes Targeting Rockets and Tunnels, the Israeli Tactic of 'Mowing the Grass' Returns to Gaza," May 14, 2021, https://www.washingtonpost.com/world/2021/05/14/israel-gaza-history/.

implementation of a sizable civil and economic program for Gaza.[44] The program expands the number of permits for Palestinians from Gaza to work in Israel, where the daily wages of one worker are enough to support an additional ten Palestinians.[45] Israel's Defense Ministry signed off on a plan to gradually increase work permit quotas for Palestinians from Gaza to an unprecedented 20,000, with reports suggesting plans to eventually increase that number to 30,000.[46] For an impoverished territory with an unemployment rate of around 50 percent, permits to work in Israel improve the lives of Palestinians and stabilize the economy. The program also introduced economic incentives for Hamas to keep the peace—conducting attacks could result in snap restrictions on permits and border crossing closures, leading to a public backlash, as well as internal political blowback within the group. The power of this economic tool was evident throughout Israel's Operation Breaking Dawn in August 2022, during which Israel conducted a three-day operation to eliminate key military assets and personnel of the Palestinian Islamic Jihad (PIJ), another Gaza-based terrorist organization. Israel was careful to communicate its intention to target PIJ, not Hamas. Ordinarily a ready-and-willing belligerent in such flare-ups, Hamas did nothing to restrain the PIJ but remained conspicuously on the sidelines, refraining from fighting out of its interest in resuming border crossings as quickly as possible.[47]

Searching for Alternatives

Given these limitations, blowbacks, and self-imposed restraints, Hamas is finding alternative methods of influence. Under the leadership of its Gaza chief Yahya Sinwar, Hamas is endeavoring to inspire Arab Israelis and West Bank Palestinians to continue the struggle by taking up arms and sparking an intifada while the group nurses itself back to strength.[48] To further this effort, Hamas is turning to more insidious means of operating in the information space to garner support and ignite conflagrations without further jeopardizing its public reputation, weapons stockpiles, infrastructure, or the economic well-being of the Palestinians living under its control. Like many state actors working to advance strategic ambitions, Hamas has turned to offensive cyber operations as a means of competing below the threshold of armed conflict.

Deploying offensive cyber capabilities involves exceptionally low risks and costs for operators. For groups like Hamas that are worried about potential retaliation, these operations present an effective alternative to kinetic operations that would otherwise provoke an immediate response. Most national cyber operation countermeasures are geared toward state adversaries and, in general, finding an appropriate response to non-state actors in this area has been challenging. Many state attempts to retaliate and deter have been toothless, resulting in little alteration of the adversary's calculations.[49]

44 "What Just Happened in Gaza?" Israel Policy Forum, YouTube, https://www.youtube.com/watch?v=XqHjQo0ybvM&t=59s.

45 Michael Koplow, "Proof of Concept for a Better Gaza Policy," Israel Policy Forum, August 11, 2022, https://israelpolicyforum.org/2022/08/11/proof-of-concept-for-a-better-gaza-policy; Tani Goldstein, "The Number of Workers from Gaza Increased, and the Peace Was Maintained," *Zman Yisrael*, April 4, 2022, https://www.zman.co.il/302028/popup/.

46 Aaron Boxerman, "Israel to Allow 2,000 More Palestinian Workers to Enter from Gaza," *Times of Israel*, June 16, 2022, https://www.timesofisrael.com/israel-to-allow-2000-more-palestinian-workers-to-enter-from-gaza/.

47 "Operation Breaking Dawn Overview," Israel Policy Forum, August 8, 2022, https://israelpolicyforum.org/2022/08/08/operation-breaking-dawn-overview/.

48 Aaron Boxerman, "Hamas's Sinwar Threatens a 'Regional, Religious War' if Al-Aqsa is Again 'Violated,'" *Times of Israel*, April 30, 2022, https://www.timesofisrael.com/sinwar-warns-israel-hamas-wont-hesitate-to-take-any-steps-if-al-aqsa-is-violated/.

49 Safa Shahwan Edwards and Simon Handler, "The 5×5—How Retaliation Shapes Cyber Conflict," *Atlantic Council*, https://www.atlanticcouncil.org/commentary/the-5x5-how-retaliation-shapes-cyber-conflict/.

3. HAMAS'S CYBER STRATEGY

The nature of the cyber domain allows weak actors, like Hamas, to engage and inflict far more damage on powerful actors, like Israel, than would otherwise be possible in conventional conflict.[50] This asymmetry means that cyberspace offers intrinsically covert opportunities to store, transfer, and deploy consequential capabilities with far less need for organizational resources and financial or human capacity than in industrial warfare. Well-suited to support information campaigns, cyber capabilities are useful for influencing an audience without drawing the attention and repercussions of more conspicuous operations, like terrorism. In these ways, cyber operations fit into Hamas's overall strategy and emphasis on building public perception and influence. Making sense of this strategy allows a greater understanding of past Hamas cyber operations, and how the group will likely operate in the cyber domain going forward.

MORE THAN MEETS THE EYE

Hamas's cyber capabilities, while relatively nascent and lacking the sophisticated tools of other hacking groups, should not be underestimated. It comes as a surprise to many security experts that Hamas—chronically plagued by electricity shortages in the Gaza Strip, with an average of just ten to twelve hours of electricity per day—even possesses cyber capabilities.[1] Israel's control over the telecommunications frequencies and infrastructure of the Gaza Strip raises further doubts about how Hamas could operate a cyber program.[2] However, in 2019, Israel deemed the offensive cyber threat to be critical enough that after thwarting an operation, the IDF carried out a strike to destroy Hamas's cyber headquarters,[3] one of the first acknowledged kinetic operations by a military in response to a cyber operation. However, despite an IDF spokesperson's claim that "Hamas no longer has cyber capabilities after our strike," public reporting has highlighted various Hamas cyber operations in the ensuing months and years.[4]

This dismissive attitude toward Hamas's cyber threat also overlooks the group's operations from outside the confines of the Gaza Strip. Turkish President Recep Tayyip Erdoğan and his AKP Party share ideological sympathies with Hamas and have extended citizenship to Hamas leadership.[5] The group's leaders have allegedly used Turkey as a base for planning attacks and even as a safe haven for an overseas cyber facility.[6] Hamas maintains even more robust relationships with other state supporters, namely Iran and Qatar, which provide financing, safe havens, and weapons technology.[7] With the assistance of state benefactors, Hamas will continue to develop offensive cyber and information capabilities that, if overlooked, could result in geopolitical consequences.

1 "Gaza: ICRC Survey Shows Heavy Toll of Chronic Power Shortages on Exhausted Families," International Committee of the Red Cross, July 29, 2021, https://www.icrcnewsroom.org/story/en/1961/gaza-icrc-survey-shows-heavy-toll-of-chronic-power-shortages-on-exhausted-families.

2 Daniel Avis and Fadwa Hodali, "World Bank to Israel: Let Palestinians Upgrade Mobile Network," Bloomberg, February 8, 2022, https://www.bloomberg.com/news/articles/2022-02-08/world-bank-to-israel-let-palestinians-upgrade-mobile-network.

3 Israel Defense Forces (@IDF), "CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed," Twitter, May 5, 2019, https://twitter.com/IDF/status/1125066395010699264.

4 Zak Doffman, "Israel Responds to Cyber Attack with Air Strike on Cyber Attackers in World First," *Forbes*, May 6, 2019, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/?sh=654fbba9afb5.

5 "Turkey Said to Grant Citizenship to Hamas Brass Planning Attacks from Istanbul," *Times of Israel*, August 16, 2020, https://www.timesofisrael.com/turkey-said-to-grant-citizenship-to-hamas-brass-planning-attacks-from-istanbul/.

6 Anshel Pfeffer, "Hamas Uses Secret Cyberwar Base in Turkey to Target Enemies," *Times* (UK), October 22, 2020, https://www.thetimes.co.uk/article/hamas-running-secret-cyberwar-hq-in-turkey-29mz50sxs.

7 David Shamah, "Qatari Tech Helps Hamas in Tunnels, Rockets: Expert," *Times of Israel*, July 31, 2014, https://www.timesofisrael.com/qatari-tech-helps-hamas-in-tunnels-rockets-expert; Dion Nissenbaum, Sune Engel Rasmussen, and Benoit Faucon, "With Iranian Help, Hamas Builds 'Made in Gaza' Rockets and Drones to Target Israel," *Wall Street Journal*, May 20, 2021, https://www.wsj.com/articles/with-iranian-help-hamas-builds-made-in-gaza-rockets-and-drones-to-target-israel-11621535346.

50 Andrew Phillips, "The Asymmetric Nature of Cyber Warfare," USNI News, October 14, 2012, https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare.

Aerial imagery of a Hamas cyber operations facility destroyed by the Israel Defense Forces in the Gaza Strip in May 2019.
SOURCE: Israel Defense Forces

For at least a decade, Hamas has engaged in cyber operations against Israeli and Palestinian targets. These operations can be divided in two broad operational categories that align with Hamas's overall strategy: espionage and information. The first category, cyber espionage operations, accounts for the majority of Hamas's publicly reported cyber activity and underpins the group's information operations.

Espionage Operations

Like any state or non-state actor, Hamas relies on quality intelligence to provide its leadership and commanders with decision-making advantages in the political and military arenas. The theft of valuable secrets from Israel, rival Palestinian factions, and individuals within its own ranks provides Hamas with strategic and operational leverage, and is thus prioritized in its cyber operations.

The Internal Security Force (ISF) is Hamas's primary intelligence organization, comprised of members of the al-Majd security force from within the larger Izz al-Din al-Qassam Brigades, a military wing of Hamas. The ISF's responsibilities range from espionage to quashing political opposition and dissent from within the party and its security apparatus.[51] The range of the ISF's missions manifests through Hamas's cyber operations.

Tactical Evolution

Naturally, Israel is a primary target of Hamas's cyber espionage. These operations have become commonplace over the last several years, gradually evolving from broad, blunt tactics into more tailored, sophisticated approaches. The group's initial tactics focused on a "spray and pray" approach, distributing impersonal emails with malicious attachments to a large number of targets, hoping that a subset would bite. For example, an operation that began in mid-2013 and was discovered in February 2015 entailed Hamas operators luring targets with the promise of pornographic videos that were really malware apps. The operators relied on their victims—which included targets across the government, military, academic, transportation, and infrastructure sectors—withholding information about the incidents from their workplace information technology departments, out of shame for clicking on pornography at work, thereby maximizing access and time on the target.[52]

Later, Hamas operations implemented various tactical updates to increase their chances of success. In September 2015, the group began including links rather than attachments, non-pornographic lures such as automobile accident videos, and additional encryption of the exfiltrated data.[53] Another campaign, publicized in February 2017, involved a more personalized approach using social engineering techniques to target IDF personnel with malware from fake Facebook accounts.[54]

51 "Internal Security Force (ISF) – Hamas," Mapping Palestinian Politics, European Council on Foreign Relations, https://ecfr.eu/special/mapping_palestinian_politics/internal_security_force/.

52 "Operation Arid Viper: Bypassing the Iron Dome," Trend Micro, February 16, 2015, https://www.trendmicro.com/vinfo/es/security/news/cyber-attacks/operation-arid-viper-bypassing-the-iron-dome; "Sexually Explicit Material Used as Lures in Recent Cyber Attacks," Trend Micro, February 18, 2015, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/sexually-explicit-material-used-as-lures-in-cyber-attacks?linkId=12425812.

53 "Operation Arid Viper Slithers Back into View," Proofpoint, September 18, 2015, https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View.

54 "Hamas Uses Fake Facebook Profiles to Target Israeli Soldiers," Israel Defense Forces, February 2, 2017, https://www.idf.il/en/minisites/hamas/hamas-uses-fake-facebook-profiles-to-target-israeli-soldiers/.

In subsequent years, the group began rolling out a variety of smartphone applications and marketing websites to surreptitiously install mobile remote access trojans on target devices. In 2018, the group implanted spyware on smartphones by masquerading as Red Alert, a rocket siren application for Israelis.[55] Similarly in 2020, Hamas targeted Israelis through dating apps with names like Catch&See and GrixyApp.[56] As previously mentioned, Hamas also cloaked its spyware in a seemingly benign World Cup application that allowed the group to collect information on a variety of IDF military installations and hardware, including armored vehicles. These are all areas Hamas commanders have demonstrated interest in learning more about in order to gain a potential advantage in a future kinetic conflict.[57]

According to the Israeli threat intelligence firm Cybereason, more recent discoveries indicate a "new level of sophistication" in Hamas's operations.[58] In April 2022, a cyber espionage campaign targeting individuals from the Israeli military, law enforcement, and emergency services used previously undocumented malware featuring enhanced stealth mechanisms. This indicates that Hamas is taking more steps to protect operational security than ever.[59] The infection vector for this particular campaign was through social engineering on platforms like Facebook, a hallmark of many Hamas espionage operations, to dupe targets into downloading trojanized applications. Once the malware is downloaded, Hamas operators can access a wide range of information from the device's documents, camera, and microphone, acquiring immense data on the target's whereabouts, interactions, and more. Information collected off of military, law enforcement, and emergency services personnel can be useful on its own or for its potential extortion value.

As part of its power struggle with the Palestinian Authority and rival Fatah party, Hamas targets Palestinian political and security officials with similar operations. In another creative cyber espionage operation targeting the Palestinian Authority, Hamas operators used hidden malware to exfiltrate information from the widely used cloud platform Dropbox.[60] The same operation targeted political and government officials in Egypt,[61] an actor Hamas is keen to surveil given its shared border with the Gaza Strip and role brokering ceasefires and other negotiations between Israel and Hamas.

Other common targets of Hamas's cyber espionage campaigns are members of its own organization. One of the ISF's roles is counterintelligence, a supremely important field to an organization that is rife with internecine political rivalries,[62] as well as paranoia about the watchful eyes of Israeli and other intelligence services. According to Western intelligence sources, one of the main missions of Hamas's cyber facility in Turkey is deploying counterintelligence against Hamas dissenters and spies.[63] Hamas is sensitive to the possibility of Palestinians within its ranks and others acting as "collaborators" with Israel, and the group occasionally summarily executes individuals on the suspicion of serving as Israeli intelligence informants.[64]

55 Yossi Melman, "Hamas Attempted to Plant Spyware in 'Red Alert' Rocket Siren App," *Jerusalem Post*, August 14, 2018, https://www.jpost.com/arab-israeli-conflict/hamas-attempted-to-plant-spyware-in-red-alert-rocket-siren-app-564789.

56 "Hamas Android Malware on IDF Soldiers—This is How it Happened," Checkpoint, February 16, 2020, https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/.

57 Yaniv Kubovich, "Hamas Cyber Ops Spied on Hundreds of Israeli Soldiers Using Fake World Cup, Dating Apps," *Haaretz*, July 3, 2018, https://www.haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773; Ben Caspit, "Gilad Shalit's Capture, in His Own Words," *Jerusalem Post*, March 30, 2013, https://www.jpost.com/features/in-thespotlight/gilad-schalits-capture-in-his-own-words-part-ii-308198.

58 Omer Benjakob, "Exposed Hamas Espionage Campaign Against Israelis Shows 'New Levels of Sophistication,'" *Haaretz*, April 7, 2022, https://www.haaretz.com/israel-news/tech-news/2022-04-07/ty-article/.premium/exposed-hamas-espionage-campaign-shows-new-levels-of-sophistication/00000180-5b9c-dc66-a392-7fdf14ff0000.

59 Cybereason Nocturnus, "Operation Bearded Barbie: APT-C-23 Campaign Targeting Israeli Officials," Cybereason, April 6, 2022, https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials?hs_amp=true.

60 Cybereason Nocturnus, "New Malware Arsenal Abusing Cloud Platforms in Middle East Espionage Campaign," Cybereason, December 9, 2020, https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign.

61 Sean Lyngaas, "Hackers Leverage Facebook, Dropbox to Spy on Egypt, Palestinians," December 9, 2020, CyberScoop, https://www.cyberscoop.com/molerats-cybereason-gaza-espionage-palestine/.

62 Adnan Abu Amer, "Hamas Holds Internal Elections Ahead of Palestinian General Elections," *Al-Monitor*, February 26, 2021, https://www.al-monitor.com/originals/2021/02/hamas-internal-elections-gaza-west-bank-palestinian.html.

63 "Hamas Using Secret Cyber Warfare Base in Turkey, Report Says," *Haaretz*, October 23, 2020, https://www.haaretz.com/middle-east-news/palestinians/2020-10-23/ty-article/.highlight/hamas-using-secret-cyber-warfare-base-in-turkey-report-says/0000017f-e5f6-df5f-a17f-fffe23920000.

64 "Hamas Kills 22 Suspected 'Collaborators,'" *Times of Israel*, August 22, 2014, https://www.timesofisrael.com/hamas-said-to-kill-11-suspected-collaborators; "Hamas Executes Three 'Israel Collaborators' in Gaza," BBC, April 6, 2017, https://www.bbc.com/news/world-middle-east-39513190.

Information Operations

While the bulk of Hamas's cyber operations place a premium on information gathering, a subset involves using this information to further its efforts to influence the public. This broadly defined category of information operations comprises everything from hack-and-leaks to defacements to social media campaigns that advance beneficial narratives.

Hack-and-leak operations, when hackers acquire secret or otherwise sensitive information and subsequently make it public, are clear attempts to shift public opinion and "simulate scandal."[65] The strategic dissemination of stolen documents, images, and videos—potentially manipulated—at critical junctures can be a windfall for a group like Hamas. In December 2014, Hamas claimed credit for hacking the IDF's classified network and posting multiple videos taken earlier in the year of Israel's Operation Protective Edge in the Gaza Strip.[66] The clips, which were superimposed with Arabic captions by Hamas,[67] depicted sensitive details about the IDF's operation, including two separate instances of Israeli forces engaging terrorists infiltrating Israel—one group infiltrating by sea en route to Kibbutz Zikim and one group via a tunnel under the border into Kibbutz Ein HaShlosha—to engage in kidnappings. One of the raids resulted in a fight that lasted for roughly six hours and the death of two Israelis.[68] By leaking the footage, including images of the dead Israelis, Hamas sought to project itself as a strong leader to Palestinians and to instill fear among Israelis, boasting about its ability to infiltrate Israel, kill Israelis, and return to Gaza. These operations are intended to demonstrate Hamas's strength on two levels: first, their ability to hack and steal valuable material from Israel and second, their boldness in carrying out attacks to further the Palestinian national cause.

Defacement is another tool in Hamas's cyber arsenal. This sort of operation, a form of online vandalism that usually involves breaching a website to post propaganda, is not so much devastating as it is a nuisance.[69] The operations are intended to embarrass the targets, albeit temporarily, and generate a psychological effect on an audience. In 2012, during Israel's Operation Cast Lead in the Gaza Strip, Hamas claimed responsibility for attacks on Israeli websites, including the IDF's Homefront Command, asserting that the cyber operations were "an integral part of the war against Israel."[70] Since then, Hamas has demonstrated its ability to reach potentially wider audiences through defacement operations. Notably, in July 2014 during Operation Protective Edge, Hamas gained access to the satellite broadcast of Israel's Channel 10 television station for a few minutes, broadcasting images purportedly depicting Palestinians injured by Israeli airstrikes in the Gaza Strip. The Hamas hackers also displayed a threat in Hebrew text: "If your government does not agree to our terms, then prepare yourself for an extended stay in shelters."[71]

Hamas has conducted defacement operations itself and has relied on an army of "patriotic hackers." Patriotic hacking, cyberattacks against a perceived adversary performed by individuals on behalf of a nation, is not

65 James Shires, "Hack-and-Leak Operations and US Cyber Policy," War on the Rocks, August 14, 2020, https://warontherocks.com/2020/08/the-simulation-of-scandal/.

66 Ben Tufft, "Hamas Claims it Hacked IDF Computers to Leak Sensitive Details of Previous Operations," *Independent*, December 14, 2014, https://www.independent.co.uk/news/world/middle-east/hamas-claims-it-hacked-idf-computers-to-leak-sensitive-details-of-previous-operations-9923742.html.

67 Tova Dvorin, "Hamas: 'We Hacked into IDF Computers,'" *Israel National News*, December 14, 2014, https://www.israelnationalnews.com/news/188618#.VI2CKiusV8E

68 Ari Yashar, "IDF Kills Hamas Terrorists Who Breached Border," *Israel National News*, July 8, 2014, https://www.israelnationalnews.com/news/182666; Gil Ronen and Tova Dvorin, "Terrorists Tunnel into Israel: Two Soldiers Killed," *Israel National News*, July 19, 2014, https://www.israelnationalnews.com/news/183076.

69 "Website Defacement Attack," Imperva, https://www.imperva.com/learn/application-security/website-defacement-attack/.

70 Omer Dostri, "Hamas Cyber Activity Against Israel," The Jerusalem Institute for Strategy and Security, October 15, 2018, https://jiss.org.il/en/dostri-hamas-cyber-activity-against-israel/.

71 WAQAS, "Israel's Channel 10 TV Station Hacked by Hamas," Hackread, July 16, 2014, https://www.hackread.com/hamas-hacks-israels-channel-10-tv-station/.

unique to the Israeli–Palestinian conflict. States have turned to sympathetic citizens around the world for support, often directing individual hackers to deface adversaries' websites, as Ukraine did after Russia's 2022 invasion.[72] Similarly, Hamas seeks to inspire hackers from around the Middle East to "resist" Israel, resulting in the defacement of websites belonging to the Tel Aviv Stock Exchange and Israel's national airline El Al by Arab hackers.[73]

In tandem with its embrace of patriotic hackers, Hamas seeks to multiply its propaganda efforts by enlisting the help of Palestinians on the street for less technical operations. To some extent, Hamas uses social media in similar ways to other terrorist organizations to inspire violence, urging Palestinians to attack Jews in Israel and the West Bank, for instance.[74] However, the group goes a step further, encouraging Palestinians in Gaza to contribute to its efforts by providing guidelines for social media posting. The instructions, provided by Hamas's Interior Ministry, detail how Palestinians should post about the conflict and discuss it with outsiders, including preferred terminology and practices such as, "Anyone killed or martyred is to be called a civilian from Gaza or Palestine, before we talk about his status in jihad or his military rank. Don't forget to always add 'innocent civilian' or 'innocent citizen' in your description of those killed in Israeli attacks on Gaza." Other instructions include, "Avoid publishing pictures of rockets fired into Israel from [Gaza] city centers. This [would] provide a pretext for attacking residential areas in the Gaza Strip."[75] Information campaigns like these extend beyond follower indoctrination and leave a tangible mark on international public discourse, as well as structure the course of conflict with Israel.

Hamas's ability to leverage the cyber domain to shape the information landscape can have serious implications on geopolitics. Given the age and unpopularity of Palestinian President Mahmoud Abbas—polling shows that 80 percent of Palestinians want him to resign—as well as the fragile state of the Palestinian Authority,[76] the Palestinian public's desire for elections, and general uncertainty about the future, Hamas's information operations can have a particularly potent effect on a discourse that is already contentious. The same can be said, to some extent, for the information environment in Israel, where political instability has resulted in five elections in just three and a half years.[77] When executed strategically, information operations can play an influencing, if not deciding, role in electoral outcomes, as demonstrated by Russia's interference in the 2016 US presidential election.[78] A well-timed hack-and-leak operation, like Russia's breach of the Democratic National Committee's networks and dissemination of its emails, could majorly influence the momentum of political events in both Israel and Palestine.[79] Continued failure to reach a two-state solution in the Israeli–Palestinian conflict will jeopardize Israel's diplomatic relationships,[80] as well as stability in the wider Middle East.[81]

72 Joseph Marks, "Ukraine is Turning to Hacktivists for Help," *Washington Post*, March 1, 2022, https://www.washingtonpost.com/politics/2022/03/01/ukraine-is-turning-hacktivists-help/.

73 "Israeli Websites Offline of 'Maintenance' as Hamas Praises Hackers," The National, January 15, 2012, https://www.thenationalnews.com/world/mena/israeli-websites-offline-of-maintenance-as-hamas-praises-hackers-1.406178.

74 Dov Lieber and Adam Rasgon, "Hamas Media Campaign Urges Attacks on Jews by Palestinians in Israel and West Bank," *Wall Street Journal*, May 2, 2022, https://www.wsj.com/articles/hamas-media-campaign-urges-attacks-on-jews-by-palestinians-in-israel-and-west-bank-11651511641.

75 "Hamas Interior Ministry to Social Media Activists: Always Call the Dead 'Innocent Civilians'; Don't Post Photos of Rockets Being Fired from Civilian Population Centers," Middle East Media Research Institute, July 17, 2014, https://www.memri.org/reports/hamas-interior-ministry-social-media-activists-always-call-dead-innocent-civilians-dont-post#_edn1.

76 Joseph Krauss, "Poll Finds 80% of Palestinians Want Abbas to Resign," AP News, September 21, 2021, https://apnews.com/article/middle-east-jerusalem-israel-mahmoud-abbas-hamas-5a716da863a603ab5f117548ea85379d.

77 Patrick Kingsley and Isabel Kershner, "Israel's Government Collapses, Setting Up 5th Election in 3 Years," *New York Times*, June 20, 2022, https://www.nytimes.com/2022/06/20/world/middleeast/israel-election-government-collapse.html.

78 Patrick Howell O'Neill, "Why Security Experts Are Braced for the Next Election Hack-and-Leak," *MIT Technology Review*, September 29, 2020, https://www.technologyreview.com/2020/09/29/1009101/why-security-experts-are-braced-for-the-next-election-hack-and-leak/.

79 Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the US," *New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

80 Ben Samuels, "No Normalization with Israel Until Two-State Solution Reached, Saudi FM Says," *Haaretz*, July 16, 2022, https://www.haaretz.com/middle-east-news/2022-07-16/ty-article/.premium/no-normalization-with-israel-until-two-state-solution-reached-saudi-fm-says/00000182-0614-d213-adda-17bd7b2d0000.

81 Ibrahim Fraihat, "Palestine: Still Key to Stability in the Middle East," *Brookings Institution*, January 28, 2016, https://www.brookings.edu/opinions/palestine-still-key-to-stability-in-the-middle-east/.

4. WHERE DO HAMAS'S CYBER OPERATIONS GO FROM HERE?

As outlined in its founding charter, as long as Hamas exists, it will place a premium on influencing audiences—friendly, adversarial, and undecided—and mobilizing them to bend political outcomes toward its ultimate objectives.[82] Terrorism has been a central element of the group's influence agenda, but cyber and information operations offer alternative and complementary options for engagement. It stands to reason that as Hamas's cyber capabilities steadily evolve and improve, those of similar organizations will do the same.

Further Israeli efforts to curb terrorism through a cocktail of economic programs and advancements in defensive technologies, such as its integrated air defense system, raise questions about how Hamas and similar groups' incentive structures may change their calculi in light of evolving state countermeasures. There is no Iron Dome in cyberspace. Militant and terrorist organizations are not changing their strategies of integrating cyber and information operations into their repertoires. Instead, they are finding new means of achieving old goals. Important questions for future research include:

- If states like Iran transfer increasingly advanced kinetic weaponry to terrorist organizations like Hamas, PIJ, Hezbollah, Kata'ib Hezbollah, and the Houthis, to what extent does this assistance extend to offensive cyber capabilities? What will this support look like in the future, and will these groups depend on state support to sustain their cyber operations?

- What lessons is Hamas drawing from the past year of relative calm with Israel that may influence the cadence and variety of its cyber operations? How might these lessons influence similar organizations around the world?

- What sorts of operations, such as financially motivated ransomware and cybercrime, has Hamas not engaged in? Will Hamas and comparable organizations learn from and adopt operations that are similar to other variously motivated non-state actors?

- What restrictions and incentives can the United States and its allies implement to curb the transfer of cyber capabilities to terrorist organizations?

Cyber capabilities are advancing rapidly worldwide and more advanced technologies are increasingly accessible, enabling relatively weak actors to compete with strong actors like never before. Few controls exist to effectively counter this proliferation of offensive cyber capabilities, and the technical and financial barriers for organizations like Hamas to compete in this domain remain low.[83] Either by obtaining and deploying highly impactful tools, or by developing relationships with hacking groups in third-party countries to carry out operations, the threat from Hamas's cyber and information capabilities will grow.

Just like the group's rocket terror program, which began with crude, short-range, and inaccurate Qassam rockets that the group cobbled together from scratch, Hamas's cyber program began with rather unsophisticated tools. Over the years, as the group obtained increasingly sophisticated, accurate, and long-range rockets from external benefactors like Iran, so too have Hamas's cyber capabilities advanced in scale and sophistication.

82 Israel Foreign Ministry, "The Charter of Allah: The Platform of the Islamic Resistance Movement (Hamas)," Information Division, https://irp.fas.org/world/para/docs/880818.htm.

83 "The Proliferation of Offensive Cyber Capabilities," Cyber Statecraft Initiative, Digital Forensic Research Lab, *Atlantic Council*, https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/cyber-statecraft-initiative/the-proliferation-of-offensive-cyber-capabilities/.

CONCLUSION

Remarking on Hamas's creative cyber campaigns, a lieutenant colonel in the IDF's Cyber Directorate noted, "I'm not going to say they are not powerful or weak. They are interesting."[84] Observers should not view Hamas's foray into cyber operations as an indication of a sudden organizational strategic shift. For its entire existence, the group has used terrorism as a means of garnering public attention and affecting the information environment, seizing strategic opportunities to influence the course of political events. As outside pressures change the group's incentives to engage in provocative kinetic operations, cyber capabilities present alternative options for Hamas to advance its strategy. Hamas's cyber capabilities will continue to advance, and the group will likely continue to leverage these tools in ways that will wield maximum influence over the information environment. Understanding how Hamas's strategy and incentive structure guides its decision to leverage offensive cyber operations can provide insights, on a wider scale, about how non-state actors develop and implement cyber tools, and how the United States and its allies may be better able to counter these trends.

ACKNOWLEDGEMENTS

The author would like to thank several individuals, without whose support this report would not look the same. First and foremost, thank you to Trey Herr and Emma Schroeder, director and associate director of the Atlantic Council's Cyber Statecraft Initiative, respectively, for helping from the start of this effort by participating in collaborative brainstorming sessions and providing extensive editorial feedback throughout. The author also owes a debt of gratitude to several individuals for generously offering their time to review various iterations of this document. Thanks to Ambassador Daniel Shapiro, Shanie Reichman, Yulia Shalomov, Stewart Scott, Madison Cullinan, and additional individuals who shall remain anonymous for valuable insights and feedback throughout the development of this report. Additionally, thank you to Valerie Bilgri for editing and Donald Partyka for designing the final document.

ABOUT THE AUTHOR

Simon P. Handler is a fellow at the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). His research focuses on cyber conflict, counterterrorism, counterinsurgency, and the Middle East. He is also the editor-in-chief of the *5×5*, an Atlantic Council series on trends and themes in cyber policy. Previously, he was assistant director of the Initiative, a role in which he managed a wide range of projects at the nexus of geopolitics with cyberspace.

Prior to joining the Atlantic Council, Handler served as a special assistant in the United States Senate, where he worked on foreign policy issues. During his time on the Hill, he was a congressional fellow with the Wilson Center's Congressional Cybersecurity Lab and Congressional Artificial Intelligence Lab, and a part of the East-West Center's Congressional Staff Program on Asia.

Handler is earning his MA in Security Studies from Georgetown University's Walsh School of Foreign Service and is the associate editor for defense of the Georgetown Security Studies Review. He holds a BA in both International Relations & Global Studies and Middle Eastern Languages & Cultures from The University of Texas at Austin. He speaks Arabic and some Hebrew, and is also a Certified Bourbon Steward.

84 Neri Zilber, "Inside the Cyber Honey Traps of Hamas," *The Daily Beast*, March 1, 2020, https://www.thedailybeast.com/inside-the-cyber-honey-traps-of-hamas.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Todd Achilles
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Jarosław Grzesiak
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Umer Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Gil Tenzer
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of October 20, 2022

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org