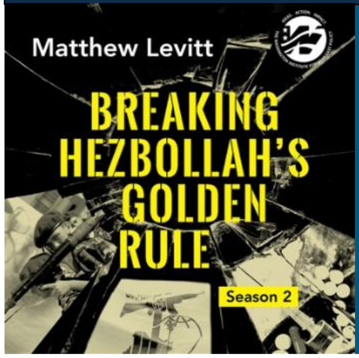
THE
WASHINGTON INSTITUTE
for Near East Policy



Episode 5: Hezbollah’s Digital Footprint

Script

Matthew Levitt
Fromer-Wexler Fellow, Washington Institute for Near East Policy

October 25, 2023

Matthew Levitt:
Fun fact, Hezbollah has produced its own video game. Several, in fact. It might come as a surprise that the group has expanded into that world. But over time, it has developed and deployed a wide range of online activities. So let's delve into the group’s digital footprint.

INTRO:
I’m Matthew Levitt, and this is ‘Breaking Hezbollah’s Golden Rule,’ a podcast that shines a bright spotlight on the criminal, militant, and terrorist activities of Lebanese Hezbollah. Hezbollah is an organization that engages in everything from overt social and political activities in Lebanon to covert militant, criminal, and terrorist activities around the world.

One Hezbollah operative was taught by his commander that the golden rule of the group’s terrorist unit is this, quote: “The less you know, the better.”

In this podcast, we set out to break this rule.

During the 2006 Lebanon War, Hezbollah launched sophisticated cyberattacks against communications systems in multiple countries that supported Israel, including the United States. Hackers trolled the Internet for vulnerable sites to communicate with one another and to broadcast messages from Al-Manar television, Hezbollah’s television station.

But, it was in 2010 that Hezbollah got a glimpse of the kind of impact cyber attacks could have. That year, a computer worm called “Stuxnet” infected more than 20,000 devices in fourteen Iranian nuclear facilities. It led to the destruction of about 900 centrifuges. Although unconfirmed, the United States and Israel are suspected to be behind the attack.

After witnessing the Stuxnet attack, Iran got inspired. It started expanding its own cyber operations and digital surveillance capabilities. Tehran also provided cyber training and technology to Hezbollah operatives and helped the group build its own cyber unit.

Alma Keshavarz:
Hezbollah is interesting in a case study itself within cyber because it was among the first non-state actors to have a cyber presence. Cyber isn’t just ransomware, malware, or espionage. It’s also about information operations. It’s about propaganda.

Levitt:
That was Alma Keshavarz from U.S. Cyber Command, the U.S. Department of Defense military command that focuses on cyberspace capabilities. *Just a quick disclaimer: The views expressed by Alma in this episode are hers alone and do not reflect the official position of the Department of Defense or the United States Government.*

Douglas London:
You have to start with acknowledging that Hezbollah has a sophisticated intelligence service, and one has to look at it as being on par with any first-world power in terms of intelligence capabilities and approach.

Levitt:
Douglas London is a thirty-four-year veteran of CIA's Clandestine Service and author of *The Recruiter: Spying and the Lost Art of American Intelligence.*

London:
But at the same time, one has to look at it as how autocratic countries tend to use their intelligence services. Whereas the CIA, my alma mater, is a strategic service. We're focused primarily on informing decision making, but we also conduct covert action. We support the military, so there's an actionable component. Hezbollah is primarily tactical in its intelligence efforts. It's primarily looking to defend and support its own regime. And it's also very tied in with its patron, which is Iran, the IRGC and MOIS.

So cyber is the same, whereas Hezbollah, just like CIA, is going to use cyber as a means to securely recruit assets, the assets Hezbollah are recruiting tend to be for actual purposes. They tend to be to conduct terrorist operations, to influence public opinion, or for counterintelligence purposes. It is like other sophisticated intel services, weaponizing intelligence, which means weaponizing cyber to accomplish its goals, be it recruiting agents, be it transferring funds, fundraising, radicalization, disinformation and, in fact, disruptive operations against its adversaries.

Levitt:
Hezbollah's cyber attacks have long been a source of concern for Middle Eastern and Western governments. In 2010, the Obama administration described Hezbollah as "the most technically-capable terrorist group in the world." In March 2021, U.S. intelligence found that "Hezbollah Secretary General Hassan Nasrallah supported efforts to undermine former President Trump in the 2020 U.S. election," and concluded that Nasrallah probably saw this as a low-cost means to mitigate the risk of a regional conflict while Lebanon faced political, financial, and public health crises. These kinds of activities are seen as Hezbollah doing its part in Iran's larger revolutionary agenda – a role that has expanded over time.

London:
So looking at Hezbollah, as I have over the years, I've been operating against them over the entirety of my career, from the early eighties to my retirement in 2019, I saw some interesting trends and development in looking at them as an adversary.

In the early days, Hezbollah might have been less organized and tied more around family allegiances. But it's a little less sophisticated in the sense that it opens them up to nepotism, which could be bad, you would think, in terms of professionalizing, but allowed them to be very agile and very independent. And as Hezbollah has suffered some significant losses, I saw Hezbollah become a bit more bureaucratic, a bit more under Iran's thumb, which made it ever less agile, still very capable – after all the Iranians were providing them training, providing them material support. But it also took away some of the things that made them a bit more unpredictable, a bit more creative, and a bit more dangerous. So you still have the nepotism in the organization, you still have a fair bit of corruption in the organization, especially as it affects advancement. And now you add a more bureaucratic nature where they're shifting away from being Lebanese, and they're sort of embracing this, well, we're part of the Shia revolution, the Iranian revolution.

Levitt:
Hezbollah continued its cyber operations under the direction of Iran's Quds Force. In January 2021, it was discovered that a Hezbollah-affiliated cyber unit called Lebanese Cedar APT launched attacks on telecommunications companies and internet providers. The unit's targets included the United States, United Kingdom, Israel, Egypt, Saudi Arabia, Lebanon, Jordan, Palestine, and the United Arab Emirates.

Alma Keshavarz again.

Keshavarz:
Lebanese Cedar or Volatile Cedar, as most commonly known, is an Advanced, Persistent Threat actor that's been around for just about a little over a decade. They're looking at Lebanese dissidents, any sort of opposition groups within Lebanon that they want to target.

Levitt:
Lebanese Cedar agents have hacked into the internal networks of at least 250 web servers of dissident or Western companies to collect sensitive data. Their trademark is to use a remote access tool, which allows the group to avoid exposure and remain inside compromised systems for long periods of time.

The initial report describing the breach does not directly implicate Hezbollah. But based on the targets, operational methods, and resources required, the attack has been attributed to the group. Regardless, Lebanese Cedar shows how strong the cyber capability of a non-state actor can be.

Keshavarz:
Lebanese Hezbollah, arguably, in my personal opinion, set a baseline for non-state actor cyber threats. So, cyber campaigns aren't secondary forms of warfare anymore. It's now more at the forefront. And it can be non-attributable. And being non-attributable, they can be lethal, and they can have devastating secondary and tertiary effects. But in Lebanese Hezbollah's case, in their cyber units, they do have their own objectives. Some of it is countering foreign espionage in areas where they operate for their own interests. So they may mean targeted opposition groups in Lebanon, that may mean Lebanese dissidents, that may mean collecting and monitoring information through telecommunications companies, through social network sites, gaining access to networks that have that kind of sensitive, personally identifiable information.

Hezbollah's technical cyber capabilities, I think their sophistication has grown over time. I don't think that Hezbollah is as sophisticated as a nation state, for example, nor do I think that they are as targeted as ISIL once was in their prime in the cyber arena. But that could just be by design.

Levitt:
One incredibly dangerous trait of Hezbollah's digital footprint is the group's patience.

Keshavarz:
What we have seen in open-source is this capacity to remain dormant, which is ideal for espionage and data collection.

Levitt:
This means the group will penetrate a computer system and then just quietly hang out there for years, collecting information.

Keshavarz:
Going undetected is the most successful tactic in any cyber campaign, and I think Hezbollah has really, kind of, set a standard for that.

Levitt:
At some point, Hezbollah realized that alongside pursuing "classic" cyber-espionage and cyber-sabotage activities, they can also leverage social media. The growth of companies such as Facebook, YouTube, Telegram, WhatsApp, Signal, and Twitter provided Hezbollah with the ability to gather and display information to an audience of unprecedented scale. That helped them develop and pursue cyber-influence operations.

Douglas London explains:

London:
They use cyber to radicalize communities, generally extending outward towards other Shia communities around the world in Gulf countries, throughout the Levant, even in North Africa, where it could find Shia communities that it could

hope to radicalize against regimes that are either majority Sunni or otherwise hostile to Hezbollah's and Iran's interests. And it's disseminating information and disinformation. It's important for Hezbollah to try to achieve its own narrative, and that narrative serves its own domestic intent with the Lebanese community, on which they depend on at home, as well as communities abroad, that they depend on either for fundraising, for agents of whatever mission they may be looking for, or whatever logistical purposes on which they need to depend on outsiders.

Levitt:
In an increasing digital age, terrorist groups like Hezbollah have turned to virtual means to recruit members, facilitate contact between individuals to form operational cells, and provide instructions on how to carry out attacks. Operations that rely on in-person recruitment and training are time consuming, costly, and risk exposing Hezbollah members and networks. Online recruitment, on the other hand, reduces these costs and offers a layer of plausible deniability. This allows Hezbollah to expand its reach into places that have high levels of physical security, like the West Bank.

Hezbollah has a long history of recruiting operatives in and around the West Bank. By mid-2001, Hezbollah and Iran's Islamic Revolutionary Guard Corps began a far-reaching campaign to directly recruit Palestinians to plan and carry out terror attacks on their behalf. Palestinians wounded in the second intifada were the primary source of these early Hezbollah recruits. Not only had they already demonstrated their commitment to fighting Israel, but their injuries provided a perfect pretext for them to leave the country. A seemingly humanitarian organization called the Iranian Committee for Aiding Wounded Victims of the Intifada flew hundreds of wounded Palestinians to Tehran and provided them with free medical care at military hospitals. During their recuperation, some were recruited by Hezbollah.

However, Hezbollah did not begin to heavily employ cyber tactics to recruit and instruct targets in the West Bank until the mid 2010s. When Israeli security and intelligence forces began to uncover these plots in early 2016, they found an organized virtual recruitment program. In 2016 and 2017, Hezbollah engaged in an online campaign to recruit Israeli Arabs and Palestinians living in the West Bank to attack Israeli targets. These Hezbollah "virtual planners" used Facebook to establish contact with a prospective recruit and form a personal relationship.

Douglas London, former CIA operative.

London:
They really depend on human relationships. So like many intel services, including our own, they will try to engage a potential target as a friend. They have variously made use of alias Facebook accounts, personas they try to develop, and try to lure in a potential target who they've been able to engage online, identify, look for, you know, background to try to get familiarity to see if they could get them to hit on a banner, hit on a link, or otherwise accept some sort of phishing tool that's not necessarily that sophisticated in of itself, but it's based on sort of that human dynamic and tradecraft, and Hezbollah has been good at that, and they've been able to touch on emotional issues, religious issues, cultural issues by doing their homework, by looking at these communities, by looking for people who are already online, who already have a footprint. I mean, today with, you know, open information and the net, it's a great tool with great vulnerabilities for all of us, but also provides for great opportunities.

Levitt:
After the Hezbollah "virtual planners" established a personal relationship, they typically handed the recruit over to a Hezbollah operative who continued the recruitment process through email this time. The Hezbollah operative would pivot from recruiter to handler and would send instructions on how to use encrypted communication platforms to minimize detection. The handlers used fake names during this process to remain anonymous.

One prominent Hezbollah operative tasked with online recruitment in the West Bank was Jawad Nasrallah, the son of Hezbollah leader Hassan Nasrallah. In Lebanon, Jawad was known for writing poetry criticizing Israel and for condemning media networks and journalists critical of Hezbollah. According to Israel's Shin Bet security service, Jawad was tasked with finding potential recruits in Israel and the West Bank via the Internet, and was "intimately involved" in recruiting a young Palestinian living in the West Bank.

> *Clip: According to the Shin Bet, the Tulkarm-based cell was planning shootings and a suicide bombing. Thirty-two--year-old Jawad Nasrallah recruited the cell via social media and set up an email account to give instructions to the cell's leader on the ground.*

Levitt:
Jawad Nasrallah, along with another Hezbollah handler who went by the name Fadi, instructed the young Palestinian to recruit other individuals, gather intelligence and carry out terrorist attacks. Over the next few weeks, the Palestinian received sixteen encrypted emails that contained instructions for carrying out suicide bombings and requests for information about IDF training bases – that's Israel Defense Forces.

The Palestinian recruited four other men into his cell, and they planned to carry out a shooting attack targeting an IDF officer. He sent his handler, Fadi, personal information and photos of the IDF officer, and asked Hezbollah for $30,000 to buy weapons for the attack. Hezbollah attempted to send the cell $25,000 from abroad, but the Shin Bet prevented the full amount of funds from being transferred, and they only received $5,000. The operatives then bought a machine gun and ammunition in preparation for the attack. But before they could carry it out, the Shin Bet busted the cell in January 2016.

> *Clip: And we move to Israel where security forces say they have thwarted a Hezbollah-led shooting attack, which oversaw a terror cell in the Tulkarm area of the northern West Bank, this according to Israel's security agency, the Shin Bet. Mahmoud Za'alul, the leader of the cell and resident of Tulkarm, was recruited online by Jawad Nasrallah, the son of the Hezbollah leader.*

Levitt:
Over the next year, Israeli intelligence thwarted five additional social media recruitment plots. All five plots consisted of Hezbollah operatives initially reaching out to Palestinian recruits via Facebook.

But the Israelis were not the only ones investigating such cases. In 2018, the Czech Republic's security service shut down servers operated by Hezbollah. Beginning in 2017, Hezbollah operatives used Facebook profiles of attractive women to trick targets, mainly men in the Middle East and Central and Eastern Europe, into installing spyware-infected apps. Those apps allowed operatives to retrieve content from the victims' phones. As a result of the investigation, Facebook and Twitter removed a large number of Hezbollah-operated accounts from their platforms.

Hezbollah's long-established reputation for conducting psychological operations has also moved into cyberspace. Hezbollah runs disinformation boot camps in Lebanon for the purpose of building up the "electronic armies" of Iran's proxy groups around the region.

In August 2020, *The Telegraph* reported that since at least 2012, Hezbollah has been flying individuals into Lebanon for courses teaching participants how to digitally manipulate photographs, manage large numbers of fake social media accounts, make videos, avoid Facebook's censorship, and effectively spread disinformation online.

Students from Bahrain, Iraq, Saudi Arabia, and Syria were among the thousands of Iran-backed social media activists who attended the ten-day courses, taught, of course, by Hezbollah specialists. One former trainee told *The Telegraph* that this is quote: "the illusion industry. Hezbollah is making millions of dollars running these courses, but for the clients it's worth spending the money."

With these trained technological operatives, Hezbollah has run large-scale, ruthless social media campaigns. It uses its networks to distribute videos that aggressively target public figures opposed to Hezbollah. A common technique is creating large networks of fake accounts that amplify certain messages by liking, commenting, and sharing each other's posts. The result is a highly-effective disinformation campaign targeting Hezbollah's detractors.

And then, there are the video games. Remember? Hezbollah really likes this medium because it can engage young people in radical ideologies in fun and subtle ways.

Galen Lamphere-Englund is the co-founder of the Extremism and Gaming Research Network.

Galen Lamphere-Englund:
Games are not fundamentally an issue, right? Video games do not cause offline violence inherently. For the most part, games are inevitably pro-social, beneficial activities for people to engage in.

Levitt:
But, he warns that there are ways in which extremist groups do misuse games.

Lamphere-Englund:
One is by developing their own game, and that's generally as an exercise of propaganda, an attempt to radicalize, an attempt to recruit, an attempt to disseminate their own ideas. And that's usually reaching people who already have some interest in the organization, right? Because if you're building your own game, you have to go out and find that, it's not like these tend to show up right in front of you when you go to the game store and you go to Steam, or when you go online to download something.

We also see games being used to socialize individuals in online settings. And of course, if you're talking about recruitment, you're looking at a core target demographic. Gamers are now much more diverse than they used to be. It's about a 50/50 gender split, but they skew younger, and especially for first person shooter games, they tend to be more male. So if you're looking for a prime target recruitment demographic for armed groups globally, you're looking at young men primarily, right.

There's the potential for terrorist-related financing through game and gaming-related platforms. In this case, one of the most recent versions of Hezbollah's games you can purchase online and you can also order in a CD copy. But in kind of the broader sphere, there's the ability to sell in-game items. There's the ability to money launder through game key sales relatively easily with kind of lower overhead through traditional laundering methods.

Levitt:
Hezbollah has developed three of its own first-person, single-player shooter games to recruit, radicalize, and disseminate propaganda.

Lamphere-Englund:
So a single player game, you're in a built environment, you're not engaging other players. The entire experience is designed and created, and so, the narrative can be very tightly controlled. So inside of these three games, you have propagandistic storylines that are imbued with a specific ideological goals of Hezbollah, and you're trying to bring a player through a curated, narrated experience. So you're going through different levels and each game, you're going through different scenarios, and through those you're really engaging more deeply with the content of the group itself.

Levitt:
Hezbollah released its first game, titled *Special Forces*, in 2003 following Israel's retreat from southern Lebanon a few years prior. Players take on the role of a Hezbollah fighter killing IDF soldiers.

Lamphere-Englund:
So *Special Forces 1* is not a particularly remarkable title. It's a depiction of Hezbollah capacity and the desire to kind of show the ability to fight successfully against the country of Israel. So, you know, you see things like exploding tank scenes, there is burning Israeli flags. You know, kind of one thing that got a lot of media coverage was one of the actual training sessions where you're going to be going and shooting at the [Israeli] Prime Minister Ariel Sharon. So there's kind of these initial scene setting pieces.

Levitt:
The various missions are based on actual attacks on Israeli positions. In one game situation, the player fires simulated pistols and Kalashnikov rifles, seeking to, quote: "destroy the machines of the Zionist enemy and remind them that entering Lebanese villages is not a stroll." The session ends with a medal awarded by Hassan Nasrallah.

Lamphere-Englund:
It’s not graphically particularly phenomenal as the title, the design quality is, you know, middling, they improved in their subsequent titles.

Levitt:
In 2007, Hezbollah released its second game, *Special Forces 2*.

Lamphere-Englund:
So it’s based on the ‘06 War, it’s set in southern Lebanon once again, and the game is set and pitted against IDF soldiers once again. So they are riffing on *Special Forces 1*. There’s target practice, again against Israeli politicians to set up the game, and it follows a level-based first person shooter through southern Lebanon, across the game. It’s not particularly striking visually. It looks very similar to other first person shooters from the similar period.

Levitt:
Special Forces 2 recreates key phases of the 2006 conflict. The missions include freeing Lebanese people from an Israeli prison camp and fighting in the Battle of Bint Jabayal– a town in southern Lebanon where some of fiercest fighting took place. Weapons and points are accumulated by killing Israeli soldiers.

As one Hezbollah member of parliament says….

> *Clip: It is not only a game, it is an education and culture and it is part of the confrontation because the American and the Western companies created games featuring us as terrorists and it is widespread on the market. This achievement is an addition to the tools of resistance and confrontation.*

Levitt:
Over a decade later, in 2018, Hezbollah released its third video game – *Holy Defense.* This time, the enemy is ISIS and the battleground is Syria.

> *Clip: Special forces, special forces, get ready and stay calm! Allahu Akbar.*

Levitt:
In this mission, the player is fighting anti-Assad militants in the Syrian town of Qusayr, depicting the real-life seventeen-day assault in May 2013. Holding an assault rifle, you’re walking along buildings for cover and shooting any nearby militants.

> *Clip: To everyone, do not shoot at the mosque.*

Levitt:
In the background, you can hear heavy artillery airstrikes that occurred in the early hours of the bombardment.

> *Clip: Special operations, we congratulate you on your efforts. Congratulations guys. We have liberated the whole area.*

Lamphere-Englund:
It takes kind of this popular line of fighting against ISIS and mainstreams it as like Hezbollah’s actually one fighting ISIS here. It’s also level-based. So one point, you’re defending a Shiite shrine in Damascus. At another point, you’re trying to free kidnaped civilians. At another point, you’re defending a Hezbollah stronghold in Lebanon. So you’re kind of going through different key pivotal points that have ideological or religious significance. And then you’re trying to defend those against, you know, this terrible incursion.

Levitt:
In its introduction, *Holy Defense* states quote: “The game is not merely a game but, rather, a story that seeks to document one of the sacred stages of defense against the expansion of takfiri elements and against the American-Zionist plan. It is intended to document the many victims who fell in battle.” Takfiri, by the way, refers to Islamic State supporters.

Lamphere-Englund:
From a tech point of view, the game is a lot better designed. The graphics quality is better, the audio quality is better. You know, they’ve kind of stepped up their act here. It’s also paid, so you have to buy it. And it is you know, as best as I can tell, download numbers have been pretty low for them overall. You know, it’s tricky to get web data, but it looks like they get very, very few, fewer than 5,000 visits a month to at least the main download page for the site. But that being said, there is over 1,000 pages across the web that link back to it. So you have about 1,100 different pages that are linking back to this main website.

Levitt:
With this game, Hezbollah hoped to convince young Shiites that its forces form the sharp end of the spear in defense of the Shiite community in Lebanon and holy sites in Syria. The game also served as a tool to justify Hezbollah’s activity in Syria after receiving a wave of criticism for its involvement there.

So over a decade ago, Hezbollah began investing in cyber operations and online propaganda, which have been alarmingly successful. It should therefore be no surprise that the group continues to weaponize its online digital footprint today.

In our next episode, we’ll shift back into Hezbollah’s offline, or real world, operations, this time in the United States, and we’ll discuss the stories of Hezbollah Islamic Jihad operatives who lived in the U.S. as Hezbollah sleeper agents.

OUTRO:
Thanks for listening to ‘Breaking Hezbollah’s Golden Rule,’ brought to you by the Washington Institute for Near East Policy and hosted by me, Matthew Levitt.

This podcast is produced by Anouk Millet for Earshot Strategies, and written by myself, Lauren von Thaden, and Camille Jablonski, research assistants at the Washington Institute. Dubbing for this episode was provided by Eric Feely and Ahmad Sharawi.

The clips used in this episode are from Associated Press, I24 News, and ILTV Israel News.

To learn more about Hezbollah’s criminal, militant and terrorist activities, check out my book, *The Global Footprint of Lebanon’s Party of God*.

You can also visit the Washington Institute’s website at washingtoninstitute.org and explore our map and timeline of Hezbollah Worldwide activities.

If you liked what you’ve heard, leave us a review wherever you get your podcasts and subscribe so you don’t miss any future episodes.