A look inside the cyberwar between Israel and Hamas reveals the civilian toll

May 6 2024, by Ryan Shandler, Daphna Canetti and Tal Mimran

Credit: Pixabay/CC0 Public Domain

The news about the Israel-Hamas war is filled with reports of Israeli families huddling in fear from relentless rocket attacks, Israeli tanks and artillery flattening buildings in the Gaza Strip, hundreds of kidnapped

hostages imprisoned in subterranean tunnels, and millions of people driven from their homes by fighting.

But beyond the visceral violence lies a hidden layer of the war—an online conflict. We are scholars of cyberwarfare who have cataloged and analyzed the various cyber operations conducted during the war by Hamas, Israel and other nations and hacking groups supporting one side or the other. The data paints a picture of an unseen facet of the conflict, and it offers insights about the nature of cyber conflict more broadly.

The main conclusion we've drawn is that the consequences of cyber conflict are primarily felt by civilians, not the soldiers or militants actively engaged in the fighting. We find that the damage cyberattacks inflict on digital systems is far less significant than the resulting harm to humans, and the resulting upward spiral of violence.

Hamas' cyberwarfare activities

The cyberattacks hitting Israeli government and civilian systems have had mixed effects. Some technically simple attacks succeeded in obtaining crucial intelligence that assisted Hamas fighters' incursion into Israel. Other attacks employed a scattershot approach, targeting anything within digital reach—hospitals, universities, banks and newspapers. These attacks didn't serve any military purpose, but simply aimed to disrupt Israeli life and terrorize the public.

The quantity and sophistication of the attacks have made clear that hackers working for the government of Iran, a key Hamas funder and supplier, are supporting Hamas' online warfare. Other "hacktivists" and private hacking groups based in countries as varied as Sudan, Pakistan and Russia have also joined the fray.

Before the deadly Oct. 7, 2023, terror attack on Israel that sparked the current war, Hamas cyber operatives were working to support the attack planning. A Hamas hacking unit called Gaza Cybergang spied on Israel in search of sensitive information about Israeli military installations. The information they gleaned was instrumental during the attack.

Hamas hackers also conducted phishing attacks, relatively simple attacks in which fake email or text messages resemble legitimate ones and encourage a user to either reply with sensitive information or click on a link that downloads malicious software to their computer or mobile phone.

As the Oct. 7 attack unfolded, the pro-Palestinian hacktivist group AnonGhost released a mobile app with the same name as a prominent reputable app that gives Israeli citizens warnings about impending attacks from Hamas into Israel. AnonGhost issued false alerts —including, reportedly, one about a nuclear attack—and collected users' data, including their contacts, call logs and text messages.

However, since full-fledged hostilities erupted, Hamas has been largely unable to carry out effective cyberattacks that aid its war efforts. As a result, the group turned to information warfare, seeking to evoke panic and shift public opinion.

The most common type of attack that Hamas' cyberwarriors and their allies use now is a distributed denial-of-service, when a barrage of nonsense internet traffic is aimed at one or more websites, email servers or other internet-connected systems. They get overwhelmed by the nonsense traffic and either shut down or cease to function properly.

Denial-of-service attacks have hit websites for news media outlets, banks, financial institutions and government agencies. One attack took the Jerusalem Post website offline for two days. The group that claimed

responsibility for that attack was a religious hacktivist group called Anonymous Sudan, with known connections to Russian hacking groups.

Hamas and its online allies are also using wiper malware, which infects a computer and destroys its data. This kind of attack does not serve a purpose such as extortion or surveillance—it just aims to destroy everything in its wake.

We also recorded several attacks that infiltrated databases and released their contents, such as one where the private data of students at Ono Academic College was published online.

Another series of attacks took control of digital billboards to display the Palestinian flag in sites around Israel, along with false news about military defeats. These attacks are part of a broader misinformation effort designed to shape domestic debate and terrorize Israeli civilians.

Israel's activities

By contrast with Hamas, Israel is a global cyber power whose military possesses some of the strongest cyber warfare capabilities in the world.

Yet the effectiveness of Israel's cyber arsenal is limited because Hamas doesn't depend on the internet very much. Without any targets to strike on a digital battlefield, Israel's primary strategy has been to turn on or off internet connectivity in Gaza. It can do this because Israel controls the electricity and internet cables that serve Gaza.

On Oct. 27, 2023, Israel imposed a near-total telecommunications blackout that lasted for approximately 34 hours. The telecommunications blackout was condemned by international organizations, including the World Health Organization, whose director general posted that the blackout made it "impossible for ambulances to

reach the injured." Without internet or telephone connections, injured Palestinians in Gaza can't call an ambulance, nor can medical staff stay connected with their dispatch centers.

Similar internet shutdowns have occurred frequently since then. Due to damage, displacement and power and internet disruptions, internet connectivity in Gaza has been reduced to 15% of the typical rate.

During periods when there was internet service in Gaza, pro-Israeli hacktivists got involved. For example, the group WeRedEvils crashed the Gaza Now news site. As hostilities intensified, up to 60% of all traffic to Palestinian websites was made up of denial-of-service attack traffic, according to Cloudflare, a U.S.-based data-transfer and tracking company. The bulk of the attacks were aimed at banks and technology companies.

The U.S. is involved, too. The federal Cybersecurity and Infrastructure Security Agency is working with the Israelis to help thwart some cyberattacks.

A few observations about online conflict

In contrast to Hollywood depictions of cyber warfare, where unstoppable hackers can cripple entire armies and countries with the push of a button, the reality of cyber power is more constrained. Digital battles cannot win wars. Most of the online operations in the Israel-Hamas war have little effect on the actual battlefield. They involve spying or propaganda, not wholesale destruction.

Our data shows that cyber warfare doesn't necessarily give terror groups the ability to face major powers on more equal terms. Hamas' online operations have not been able to offset Israel's military superiority. But Israel's online capabilities are not a significant advantage against a

largely offline opponent.

Perhaps most importantly, though, is our recurring finding that civilians are the foremost victims of cyberattacks during war. In our experiments, conducted among more than 10,000 people over 10 years, we have seen that cyberattacks arouse severe psychological distress—akin even to the harm generated by physical terrorism. When confronted with cyberattacks, people feel trapped and anxious, and their sense of safety plummets. As a result, victims lash out and demand strong retaliation in a way that fuels cycles of violence.

As Israel and Hamas volley cyberattacks back and forth, innocent people are caught in the crossfire. This human dimension of cyber warfare is the threat that worries us.

Provided by The Conversation

Citation: A look inside the cyberwar between Israel and Hamas reveals the civilian toll (2024, May 6) retrieved 20 May 2024 from https://techxplore.com/news/2024-05-cyberwar-israel-hamas-reveals-civilian.html