Israel Is a Cyber Superpower But Chooses Bombs to Fight Hackers in Gaza

Emanuel Maiberg, Lorenzo Franceschi-Bicchierai ⋮ 5-7 minutes ⋮ 5/20/2021

One way Israel describes itself as an exceptional Middle Eastern nation is with its technological prowess. It produces mountains of scientific research, Nobel laureates, and, as Motherboard has reported over the years, is a major cybersecurity player globally, both because of its government operations and booming private sector, which exports everything from network security products to hacking tools from firms like NSO Group and Cellebrite.

Earlier this year, Israel's intelligence capabilities were on full display when Iran's nuclear program was once again sabotaged. No one has confirmed exactly what happened, but an explosion killed the power to Iran's Natanz uranium enrichment site, sabotaging centrifuges. Israel's Prime Minister Benjamin Netanyahu didn't confirm Israel was behind the attack, but raised a glass with the Mossad in a thinly veiled celebration of a successful operation. The operation also of course conjured up memories of the Stuxnet virus, which was infamously used in 2010 to sabotage Iran's nuclear program and is largely believed to be made in collaboration between Israel and the United States.

Videos by VICE

However, when it comes to Hamas militants in Gaza, Israel's most intimate enemy and most persistent security threat to daily lives of its citizens, the Middle East's cybersecurity superpower suddenly only knows how to respond with conventional bombs, many of which are supplied by the U.S., and that killed more than more than 200 people, according to the health ministry in Gaza. Some of these bombs, according to the Israeli Defense Force, are being used to retaliate against Palestinian cyber operations.

Last week, Israel's air force tweeted that it had attacked a site where Hamas stored "cyber equipment" in the northern Gaza strip. On Wednesday, it tweeted that it attacked three Hamas members in an apartment that was used for cyber operations. "This attack is part of tens of operations against [Hamas's] cyber capabilities," it said.

Even the globally condemned bombing and collapsing of a building that housed Associated Press and other international media offices was targeting the "electronic department of the military wing of Hamas," according to Israel. According to CNN, a senior Israel Defense Forces official said the building was used for researching and developing high end capabilities for sensitive attacks against Israel. Israel said bombing the building was "the only way" to take out that particular threat, according to CNN.

Even if we choose to believe that every single building that Israel has bombed in Gaza is a legitimate threat to Israel's security (and not, for example, a beloved book store or a shop that 3D prints desperately needed tourniquets), where is the world's most moral army, the Middle East's inventive and resourceful nation, the same one that stealthily infiltrates Iran's

closely guarded nuclear operation, when it comes to Gaza? Is dropping bombs on one of the most densely populated places on Earth, which is under Israel's blockade and only an hour drive away from Tel Aviv, the only way for Israel to slow down Hamas's "cyber capabilities?"

"Unless the 'cyber' shit is currently directly leading to kinetic damage then it should be off limits. Israel has some of the best cyber folks in the world. They just wanted to bomb shit and engineered an excuse after." A cyber threat analyst who works in the defense industry, and who asked to remain anonymous because he's not authorized to speak to the press, told Motherboard. "I just find it hard to believe Israel deemed that Hamas cyber operation such a threat that all their folks working in cyber couldn't deal with and they had to drop a bomb instead."

"I wouldn't take this story too seriously," Daniel Moore, a cyber warfare researcher and a former teaching fellow at the War Studies Department King's College in London, told Motherboard. "I assume Israel's dwindling target bank had some entries flagged as used by Hamas for cyber activities, but bombings are not likely to reduce operational effectiveness for cyber. Hamas has some capabilities, more so for Intel collection than any offensive efforts, but I doubt these play any meaningful role in their overall offensive posture."

Hamas does hack Israel, and Israel boasts about its cyber operations against Hamas. One reason Israel has to carry out sophisticated and covert operations against Iran's nuclear program is because simply dropping bombs on the Natanz uranium enrichment site will have potentially dire consequences, from Iran and the international community. This is demonstrably not the case when Israel bombs Gaza. Israel has withstood Hamas's retaliations for decades, and is protected and funded by the U.S.

As Motherboard has written before, bombing "cyber operatives" and "cyber capabilities" isn't "cyber war." It's just war, and it's one that Israel is willing to fight with bombs as opposed to sophisticated supply chain attacks, even if it means demolishing media offices and killing children.

***Correction**: a previous version of this story identified Daniel Moore as a former PhD candidate at King's College. He was actually a teaching fellow there. We regret the error.*

Subscribe to our cybersecurity podcast CYBER, here.