Fighting Cyberwarfare: One of the Hidden Benefits of a Standalone US Aid Bill for Israel

Amy Neustein, Ph.D.

Newly elected House Speaker Mike Johnson called on President Biden to split his 105-billion-dollar supplementary budget request between aid for Ukraine and Israel amid concerns over the waning Republican support for continued funding of Ukraine. This makes practical sense given the immediacy of Israel's need for subvention for their air and missile defenses, whereas a bilateral aid bill risks ominous bottlenecks as legislators hammer out their differences across the aisle. But there are other benefits to separating out Israel from Ukraine, Taiwan and other entities in a foreign aid bill.

One such benefit is the increased granularity afforded to a standalone bill. That is, when designating one specific entity for receipt of government largess – rather than combining different recipients whose military needs may vary significantly – a more discrete, detailed and descriptive plan can be architected and thought out. In this regard, one must consider the importance of appropriating funds to combat cyberwarfare when assigning aid to Israel. The reason for this is that major cyberattacks became manifest before the Oct. 7 Hamas massacre of Israel's southern towns and kibbutzim near the Gazan border and following the massacre as well.

Ynetnews.com reported just a few weeks before the massacre that "Iranian hackers managed to penetrate the networks of about 32 Israeli companies." The targeted companies spanned a diverse corporate terrain: medicine and healthcare, IT, technology, law, financial services, retail, architecture and civil engineering. Alas, about half the companies targeted were affected by secondary attackers who gained access to victims' networks.

However, as explained by Ynetnews.com, the danger of cyberattacks went beyond the private sector, and included "intrusion into networks of defense companies, municipalities, or even national infrastructures and governmental companies." ESET, a Slovak-based cybersecurity company speaking to Ynetnews.com, found that "Iranian hacking groups regularly operate against targets in Israel. At any time there are a large number of attempts to identify weak points in corporate, government, and military networks and exploit them."

Iranian-backed cyberattacks against Israel's private and government sectors were prevalent even before Prime Minister Benjamin Netanyahu declared war against Hamas following the savage murder of 1,400 civilians, soldiers and foreign nationals and the taking of 229 hostages. However, now that Israel is at war with the Iranian-backed Hamas terrorist group, they must be even more prepared for cyberattacks.

Here are several examples of malicious cyberattacks associated with the Hamas raid on Israel:

After the surprise attack on Israel, Android cell phone users who downloaded an application from a web link, rather than from the Google Play Store, found themselves vulnerable to a malicious cyberattack. Cloudfare's Cloudforce One Threat Operations Team reported on their blog that days after the slaughter they "became aware of a website hosting a Google Android Application ... impersonating the RedAlert - Rockets Alert application."

While the purpose of this popular RedAlert - Rockets Alert application is to warn Israelis of incoming missile attacks so they can take proper life-saving precautions, the infected application sent bogus alerts to cell phone users, prompting panic among young and old who launched an escape plan even though there was no risk to their safety. At the same time, sensitive user data, namely access to contacts, call logs, SMS, account information and an overview of all installed apps, was extracted by this malicious application, further compounding the effects of cyberwarfare on its victims.

In fact, the malicious attack on RedAlert - Rockets Alert was not an anomaly. Around the same time, another mobile app called "RedAlert: Israel," which serves the same purpose of alerting its users to a missile attack, was targeted by hacktivists causing the app to send out fake alerts about incoming rockets.

In addition to mobile apps, cyberwarfare groups were also found to infect websites. Cloudfare reported that shortly after the Hamas raid on Israeli kibbutzim and towns, government websites "that provide critical information and alerts to civilians on rocket attacks" were targeted by hacktivists. Specifically, such websites were jammed by hackers at a rate of 100,000 RPS (requests per second) – later followed by a "second much larger attack" that peaked at 1 million RPS, – causing a blitz of specious requests of the site.

Such attacks are called DDoS (Distributed Denial of Service) because they are launched from a multitude of origination points that are cloned – so as to amplify the volume of requests – and distributed across many computers and, potentially, cellular and IoT (Internet of Things) devices as well. This creates a maelstrom as a website is blitzed with a simultaneity of requests that it cannot possibly handle. During the massacre, the onslaught of spurious requests from the malware paralyzed the Israeli government websites, making it impossible for users to access any information at that time. In concrete terms, inhabitants of the kibbutzim and towns under attack who successfully escaped to "safe rooms" were, nonetheless, unable to access information and alerts on government websites due to DDoS attacks that jammed Israel's communication and alert system.

With the expansion of ground offensives, it is plausible that DDoS attacks might escalate to more sophisticated and larger scale forms of cyberattacks, such as API vulnerability exploits, stealing admin privileges, and infiltrating secure networks. This is why appropriating funds to fight cyberattacks deserves special attention. A separate aid package for Israel would afford the granularity in the enumeration of military expenditures, which is vital in the war against Islamic terrorists. ■

Amy Neustein, Ph.D., of Fort Lee, New Jersey, is the author/editor of 16 academic volumes. She serves as an editor of the Springer Series in Signals and Communication Technology.

adobe stock / putilov_denis