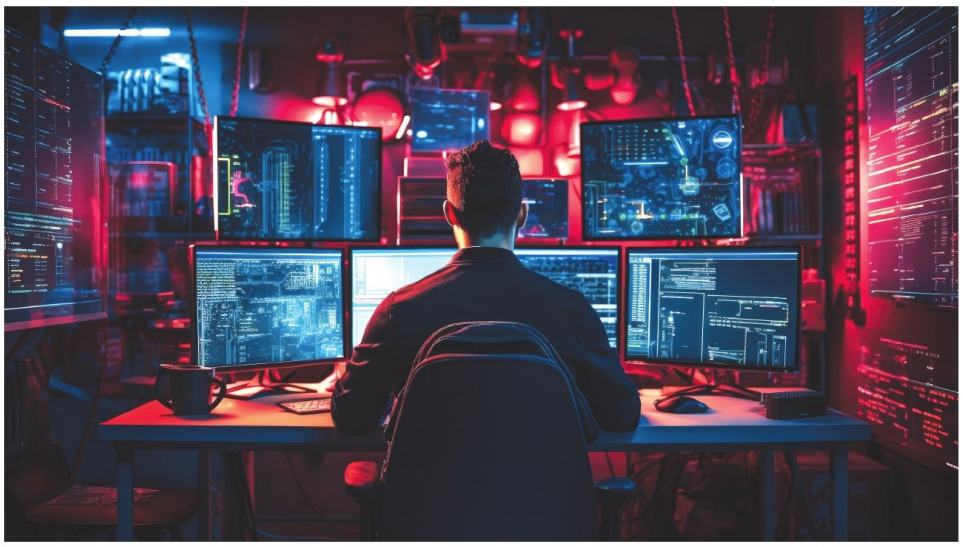
Unmasking Putin's Schadenfreude and His Suspected Cyberwarfare

Amy Neustein



Bewilderment, angst and fear would grip an entire world on Oct. 7 as savagery and barbarism were unleashed by the Hamas terrorist group on the kibbutzim and towns in Israel along the Gazan border in the early morning hours of Simchas Torah and Shabbat.

Astonishingly, Israel, known for its superior reconnaissance and military savvy, was caught off guard; the consequences were verily catastrophic. Cybersecurity gaps may have contributed to this debacle.

Deputy Editor James Coker of Infosecurity Magazine reported last week that Radware, a publicly-traded cybersecurity company headquartered in Tel Aviv-Yafo with offices in Europe, Africa and Asia Pacific, found that Israel topped the list worldwide in its receipt of DDoS (Distributed Denial of Service) attacks just five days before the Hamas raid and in the days that followed. Such cyberattacks involve multiple connected online devices, collectively known as "botnet," in which a targeted website is overwhelmed with fake traffic.

Coker stated Israel received 143 such DDoS attacks "making it the most targeted nation" in the world during that period. Radware found that more than a third of the claimed DDoS attacks were aimed at Israeli governmental agencies. Killnet, a pro-Russian (and purportedly Kremlin-associated) cybersecurity threat group that engaged in DDoS attacks targeting websites in countries that supported Ukraine following the Russian invasion, claimed several attacks on Israel's cybersystem along with pro-Palestinian hacktivist groups.

Radware pointed to Killnet's claim on Telegram Messenger, a cloud-based, cross platform instant messaging service, to targeting Israel's banks and government sites that included Shabak.gov.il, Israel's internal security service. The Jerusalem Post wrote on X (formerly Twitter) that it suffered downtime due to cyberattacks two days subsequent to the massacre.

Rob Joyce, director of cybersecurity at the National Security Agency, a national level intelligence agency of the United States Department of Defense, weighed in on the significance of cyberattacks. As reported in Fortune, Joyce, speaking at a security conference on Sea Island in Georgia, cautioned that "there may be more significant events coming, more hacktivists, and more people taking up cyber arms in defense of their cause." Explaining why vigilance is of utmost importance, Joyce pointed out that though cyberattacks "might not be sophisticated ... sometimes you don't need sophisticated to have an impact."

Rabbi Shmuel Bergman, the chief rabbi at the Young Israel of Fort Lee, New Jersey, alerted the congregation on Oct. 8 to the threat of cyberwarfare. In a missive sent out to the community right after yom tov, the rabbi implored everyone to "be mindful of attempts by hackers." He stated, "I have been informed of misleading messages [about security concerns and related matters] that have been circulated" on phones and computers of those in Israel.

Cheering in the gallery of warped spectators was Vladimir Putin, who within days of the catastrophic ambush of unsuspecting Israeli civilians mockingly pointed to the United States security intelligence breach, no doubt aggravated by the malicious disruption of the connectivity of online devices that are crucial to Israel's ability to protect the security of its population.

At a meeting with Iraqi Prime Minister Mohammed al-Sudani, Putin said: "This is a vivid example of failure of United States policy in the Middle East." He later expanded, claiming the United States involvement in the Russia-Ukraine war had distracted their attention that should have been paid to Israel, indisputably America's strongest ally in that region of the world.

Putin's glee, I'm afraid, bespeaks a more sinister reality we can no longer deny. The adroitness with which Hamas carried out this "9/11" type raid suggests a much larger force than encountered in prior terrorist attacks on Israel. Similarly, the magnitude of the *pari-passu* U.S. response — 2,000 U.S. troops ready to be deployed to the Mideast, the sending of two of our largest aircraft carriers along with an array of F16, F15 and F35 fighter jets, proposing to Congress a munificent aid package to be sent to Israel, and an unprecedented wartime visit to Israel by the president himself — points to a redoubtable enemy at Israel's door.

Can we deny that what appears to be Hamas' active jamming of Israel's communication system just days before the early-morning ambush of Israeli towns and kibbutzim and the cyberattacks that occurred in the wake of the massacre may very well adumbrate the workings of Russian-style cyberwarfare? Iran, a known Hamas backer, supporter and financier is also the purveyor of military equipment to sustain Putin's war against Ukraine.

If it is Russia that is behind the heinous Hamas assault on Israel, then perhaps Prime Minister Benjamin Netanyahu hit the nail on the head when he predicted just hours after the attack that this would unfortunately be "a long war." ■

Amy Neustein 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.

Kaleb/ AdobeStock