Tal Pavel

DOI: 10.2478/cmc-2024-0022

IZOGIBANJE »DIGITALNEMU 7. OKTOBRU«: ŠTUDIJA O KIBERNETSKEM VOJSKOVANJU PROTI IZRAELU MED VOJNO OKTOBRA 2023

AVOIDING A 'DIGITAL 7 OCTOBER': A STUDY ON CYBERWARFARE AGAINST ISRAEL DURING THE OCTOBER 2023 WAR

Povzetek Palestinska militantna skupina Hamas je 7. oktobra 2023 začela obsežno skupno ofenzivo proti Izraelu. Hkrati s kinetičnimi napadi so različni povzročitelji kibernetskih groženj, ki jih pripisujejo Hamasu, Hezbolahu, Iranu in Rusiji, sprožili kibernetske napade na izraelske informacijske sisteme v komercialnem, industrijskem in vladnem sektorju. Ta prispevek analizira te kibernetske napade in izraelske protiukrepe na področju kibernetske varnosti. Čeprav je Izrael sicer vzdržal napad kibernetskega napadalca »digitalni 7. oktober«, ključne ugotovitve kažejo na to, da lahko tovrstni napadi znatno vplivajo na različne institucije in jim povzročijo škodo ter da je treba tako v Izraelu kot po svetu temeljito spremeniti opredelitev kibernetske obrambe in odpornosti, zlasti kar zadeva civilno družbo in infrastrukturo.

Ključne besede ***Izrael, Hamas, kibernetsko vojskovanje, kibernetska varnost, hibridno vojskovanje.***

Abstract On 7 October, 2023, the Palestinian militant group Hamas launched a massive combined offensive against Israel. Concurrent with the kinetic attacks, various cyber threat actors attributed to Hamas, Hezbollah, Iran, and Russia initiated cyberattacks targeting Israeli information systems across commercial, industrial, and governmental sectors. This paper analyses these cyberattacks, as well as Israel's cybersecurity countermeasures. Key findings indicate that while Israel was able to withstand the »Digital 7 October« onslaught from cyber attacker, the attacks demonstrated the potential to significantly impact and damage different institutions; the need for a fundamental shift in defining cyber defence and resilience, especially regarding the civil society and infrastructure, in Israel and worldwide.

Key words ***Israel, Hamas, cyber warfare, cyber security, hybrid warfare.***

Introduction

„The potential for the next Pearl Harbor could very well be a cyber-attack".
(Leon Panetta, CIA Director, 11 February 2011) (ABC News, 2011)

On 7 October 2023, at 06:30 local time, Hamas launched a comprehensive attack, simultaneously firing thousands of rockets toward populated villages deep within Israel and launching waves of massive invasion and raids on the towns and villages near the Gaza border, resulting in a massacre in which 1,200 civilians and soldiers were killed and 250 living and dead hostages were abducted to Gaza. The massacre led to an ongoing Israel Defense Forces (IDF) war in Gaza, named „Operation Iron Swords".

Just minutes after the Hamas raid, a massive and ongoing cyberattack targeted the computer systems and websites of Israeli commercial and industrial companies, governmental agencies and institutions (Kahan, 2023c). These cyberattacks continued with diverse intensity, scope, duration, complexity and success rates, carried out by around a hundred different cyber actors, mainly Iranian-backed cyber actors („Agrius", „CyberAv3ngers", „Adl Ali") with Hamas („Gaza Cybergang") and Hezbollah („Lebanese Cedar") collaboration, and Russian-affiliated groups („Killnet" and „Anonymous Sudan"). In addition to these were „Team_Insane_Pakistan" and „The Mysterious" groups, „Black Cyber Army" and „Anon Ghost", among others, most of them anti-Israeli and pro-Palestinian groups (Check Point Research, 2023; CYFIRMA, 2023; Kahan, 2023f; Meyran, 2023; Milenkoski, 2023; Mimran, 2023; Recorded Future, 2023; Wullman, 2023; Andriani, 2024). The cyber-attacks had two goals: to steal sensitive information, including personally identifiable information and intellectual property, and to cause significant damage and destruction by deleting data and harming critical operational systems.

This research aims to analyse both the cyberattacks targeted at Israel from 7 October 2023 onwards and the countermeasures put in place, by examining various publications in Hebrew and English published by local and foreign media outlets and governmental agencies, including the Israel National Cyber Directorate (INCD). Even though the Directorate's website has versions in English, Arabic, Russian, French, Spanish, and Hebrew, only some publications are available in English. For example, the Israel Internet Association's survey of March 2023 revealed that just 1% of the INCD web pages were available in Arabic (14 pages translated into Arabic, of 1,572 in Hebrew), and only 5% in the survey of January 2024 (The Israel Internet Association (ISOC-IL), 2023b, 2024). For this reason, the Hebrew version of the relevant publications was used in those cases.

The research goals are as follows: (1) to analyse the cyberattacks imposed on Israel from 7 October 2023, their types and perpetrators, and the damage and implications; (2) to analyse the official Israeli countermeasures and recommendations, mainly from the INCD; and (3) to analyse the lessons that should be learned in Israel and worldwide.

The research employs a qualitative research method, based on public analyses and reports by various international and local cyber security research corporations and Israeli governmental institutions and NGOs, to analyse the cyber threats and attacks on Israel during the conflict from October 2023 onwards.

The limitations of this research are (1) reliance on public analyses and reports due to the lack of access to classified information – this means that the study's scope is limited to publicly known incidents and may not cover covert operations or unreported attacks; (2) challenges in attributing cyber-attacks and separating fact from potential disinformation campaigns; (3) the study's scope is limited to the time after October 2023, so the availability of data is limited to a specific short timeframe – future studies will have a broader time perspective; (4) geopolitical factors and state involvement can lead to biases or blind spots in reporting/analysis.

1 CYBER THREATS

1.1 Cyberwarfare

During the war, cyber-attacks and operations were aimed at two main targets: machines (computerized systems) and human beings (media consumers). The cyber-attacks may target either information technology to leak and destroy data and for website defacement, or operation technology to damage and destroy operating systems of infrastructure, companies and organizations, in addition to different online influences and psychological operations against Israeli citizens and internet users to generate and disseminate Fake News and even attempts to engage them in online spying against their own country.

The INCD stated in a report, published at the end of December 2023, that the offensive cyber activity against Israel during the fighting in Gaza gradually intensified (Israel National Cyber Directorate, 2023j). The attacks evolved from simple ones, such as the defacement of websites and theft of information, to more sophisticated and targeted ones aimed at harming organizations which were primarily critical infrastructures. These attacks were intended to disrupt and damage activity and create a wide-ranging effect by attacking companies which act as a supply chain for numerous organizations. The cyber-attacks included DDoS attacks[1] (including against Israel's government website system at gov.il, a day after the Hamas raid). In most cases, the disturbances had only minor effects, if any, in addition to website defacement[2],

[1] *"A denial of service technique that uses numerous hosts to perform the attack." (National Institute of Standards and Technology (NIST), no date a)*

[2] *"Defacement (also website or web defacement) is an attack on a website that alters its visual appearance or informational content. Often, cybercriminals add messages of a social, religious or political nature, or swear words and other text that is unrelated to the subject of the site. Defacement can be described as graffiti in electronic form. People who deface websites are called defacers." (Kaspersky IT Encyclopedia, no date)*

phishing attacks[3], leaks and deletion of information, and even use of malware by Hamas (BiBi-Linux wiper) against Israel with „capabilities that resemble that of an advanced cyber weapon“ (Bestuzhev, 2023; Check Point Research, 2023; Kahan, 2023d, 2023a, 2023e; Yoachimik and Pacheco, 2023).

Gil Shwed, founder and CEO of Check Point, has asserted an 18% increase in cyber-attacks on Israel since the beginning of the war, with most of the attacks aimed at government agencies, marking a jump of 52% in attacks on government websites. Most of these were „not very sophisticated“. He reported that the number of ransomware attacks were double that of the previous year, which included „slightly more sophisticated“ attacks perpetrated by „close to a hundred Iranian, Russian and other groups which attack at the same time“ (Shulman, 2023).

On 16 November 2023, „Cyber Toufan Al-Aqsa“ claimed responsibility for one of the most prominent attacks during the war on Gaza, one which had sustained implications, targeting Signature-IT, an Israeli website hosting and online shopping solutions company. In their written statement, the attackers claimed to have been able to steal data files totalling approximately 16 GB, and to have wiped and destroyed over one thousand servers and critical databases belonging to over 150 victims, among them leading commercial and industrial companies and governmental institutions and ministries, while disrupting their online activity (Security Joes, 2023; Pines, 2024). Among a dozen others, the Israel State Archives was targeted with devastating and evident implications. Since the attack, the following message has been displayed on both versions, English and Hebrew, of the website: „The company that hosts the website of the Israel State Archives has undergone a cyber-attack. Unfortunately, the attack has disrupted the services enabling you to search the site and to view archival material“ (Israel State Archives, no date). Indeed, for at least three months, any search on the web for any document has led the user to the same error page.

On 1 December 2023, the US and Israel‘s security and cyber authorities announced that the Iranian Government Islamic Revolutionary Guard Corps (IRGC) affiliated cyber actors, CyberAv3ngers, had published „both legitimate and false claims“ of attacks against Israeli systems in the water, energy, shipping, and distribution sectors between 18 September and 30 October 2023. A claim of responsibility from 18 October argued that over 50 servers, security cameras, and smart city management systems in Israel had been compromised, but the „majority of these claims were proven false“. Another wave of attacks began on 22 November 2023, with compromising default credentials in the Israeli company Unitronics’ devices used in control and automation systems, indicating that these attacks had already affected several states across the US (Cybersecurity & Infrastructure Security Agency (CISA), 2023; Israel National Cyber Directorate, 2023b).

---

[3] *“A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.” (National Institute of Standards and Technology (NIST), no date b)*

On 18 December 2023, the INCD reported on a combined attempt by Iran and Hezbollah to disrupt Ziv hospital's operations. The directorate's statement declared that the orchestrated attack „ultimately failed", but at the end of the third (of five) paragraph, the statement admits: „However, the attackers managed to extract private data stored in the hospital's systems" (Israel National Cyber Directorate, 2023i). Indeed, local media outlets reported the hacker's claim of possessing „over 500 gigabytes of information, including 700,000 medical documents, among which 100,000 pertain to the IDF", and shared screenshots of medical documents dating back to 2022 (Ben Shushan, 2023).

The waves of cyber-attacks on Israel harmed a wide range of targets from various sectors. Local media outlets indicated that the computer systems of the municipality of Elad had been hacked: „the attackers succeeded in disrupting the communication systems but not extracting information" (Kolodetsky, 2024). The websites of two relief groups providing aid to Israel and Gaza were also under cyber-attack (Siddiqui, 2023). Ono Academic College was attacked by a hacker group named „Malek Team", where „approximately 250,000 records, including sensitive student information, were targeted in the attack, „putting the privacy and security of its students at risk (Israeli Financial Insider, 2023; Mann, 2023b). The Israeli daily The Jerusalem Post was targeted by multiple cyberattacks the day after the Hamas onslaught (Hindustan Times, 2023).

1.2 Cyber Espionage

During the Gaza war, several reports indicated various online attempts by Iran and its affiliates to gather information and intelligence on relevant local assets.

Between November 2023 and January 2024, the Israel Security Agency (ISA) and the Israeli Defense Forces (IDF) uncovered and thwarted Hamas and Iranian attempts to recruit Israelis and extract sensitive information from IDF soldiers over various social media platforms, including Telegram and Instagram, and to carry out spying missions in favour of Iran, including assassination, in exchange for money, while also exacerbating social divisions in Israel. The agency indicated that since the beginning of the war, it had identified that „the activity efforts of Iranian security forces have greatly intensified, while using digital space for the purposes of intimidation, conveying messages or advancing terror activity" (Ben Kimon, 2023; CTech, 2023; Fabian, 2024; Zitun, 2024).

In December 2023 the INCD reported on cyber-attacks against web and security cameras (CCTV), aimed at damaging the ability to use this equipment to maintain the required security of physical space, and as attempts to gather intelligence from the areas observed by these cameras (Israel National Cyber Directorate, 2023d).

1.3 Influence Operations

Alongside the offensive cyber-attacks, there has been evidence of numerous online attempts at information warfare, mainly by Hamas, using old and new media to generate fake news. Some has been disguised as coming from local, right-wing, politically-motivated Israeli actors, but also some of the fake news and conspiratory theories have really been circulated by local, right-wing, politically-motivated Israeli actors, with and without sophisticated technology (IDF, no date; Ring, 2023).

AI – The Israel Internet Association has indicated that most distributed fake news has included images and content already published and reused during the war, in some cases images allegedly of Palestinians, mainly children wounded or in poverty, and fake social network profiles and pages generated by Artificial Intelligence (AI) as part of pro-Palestinian information warfare. In this regard, Israeli research from February 2024 revealed pro-Palestinian usage of AI to produce fake Hebrew messages using Chat GPT, to be disseminated in Hebrew channels on social media (Mann, 2023a; The Israel Internet Association (ISOC-IL), 2023a; Abu Ali Express, 2024a; Shwartz Altshuler and Yasur, 2024).

Fake News – Israeli research has unveiled fake reports of conspiracy theories of „the Enemy Within", allegedly an internal betrayal of the Israeli political and military establishment which supposedly cooperated with Hamas to enable the unbearable catastrophe aimed at undermining and overthrowing the Israeli prime minister and its right-wing government. These conspiracies were produced by both external and internal actors, disseminated from marginal Telegram channels into the Israeli mainstream, and echoed by local right-wing politicians (BZ, 2023; Czerny, 2024b).

A fake report published on 11 January 2024, in Hebrew, allegedly about three 8200 unit officers being killed in Iran's missile attack on Erbil in Iraq, was posted on a probably fabricated website under the name of the „Jerusalem Times" (Abu Ali Express, 2024b). In addition, during the war pro-Palestinian hackers released a leaked file on 6.5 million Israelis, which had already been stolen and published in 2021 (Kahan, 2023g).

Harassment – Online activities involving harassment and intimidation have served as a primary method of influence to instil fear, uncertainty and doubt (Irwin, 1998) among Israelis during the war. A week after Hamas' raid and the beginning of the war, pro-Palestinian hackers disseminated an impersonated rocket alert application (RedAlert) on the Google Play Store. The same was reported in August 2018 when Hamas tried to take control of cellular devices and enable tracking and outgoing calls (Melman, 2018). Others exploited a vulnerability in another application (Red Alert: Israel) and sent fake alerts to some app users, including a message that a „nuclear bomb is coming" (Cluley, 2023; Darché et al., 2023).

As part of the cyber-attack on the Israeli company Signature-IT, the attackers managed to gain access to mailing lists „stored on the company's servers, through which they

distributed SMS messages and emails with hateful messages to thousands of Israelis" by spoofing the email address so it looked as if it had been sent from signature-it.com (Kabir, 2023; see also Pines, 2024). Another online psychological influence operation was reported at the end of October 2023, while many Israelis reported „disturbing video and audio calls on WhatsApp" from unknown numbers, which immediately disconnected. Fake messages and links were sent to the smartphones, emails and digital platforms of Israeli users, officials and government ministers, with the justice minister claiming to have received over 40,000 such messages (Eichner, 2023b, 2023a; Ifargan, 2023; Kahan, 2023b). The INCD believed that the calls and messages originated from Hamas supporters, and did not cause any damage to phones nor gain unauthorized access (Walla!, 2023).

Another method of influence was to display harassing messages publicly. In one case, a hacked billboard displayed the Palestinian flag, and in another, pro-Palestinian Turkish hackers targeted Israeli cinema advertising screens, projecting threatening messages in Hebrew and offensive 7 October massacre images (Check Point Research, 2023; I24NEWS, 2023; Kutub, 2024).

Anti-Israel Content – Various social media and platforms, such as Telegram and TikTok, were flooded with anti-Israeli content by Hamas supporters, while TikTok denied pushing pro-Palestinian content and allegedly failed to remove thousands of videos supporting terrorism (Eichner, 2023c; Reuters, 2023; Zohar, 2023), Telegram partially blocked Hamas channels, some of which posed as pro-Israel channels scams for donations (Kahan, 2023h; Mann, 2023c).

Domestic Influence – Several local researchers unveiled a „poison machine", an online, local, right-wing, politically-motivated campaign aimed at influencing the regional general public in favour of the current government; creating constant incitement against political opponents and gatekeepers, such as the media and the judiciary law enforcement, the public service and the security establishment; inciting parts of Israeli society against each other, including by opposing and undermining the protests against the government, among them the families of those kidnapped and taken to Gaza; and demanding the Israeli government act for their immediate release, including by releasing Hamas prisoners (BZ, 2023; Shem Ur, 2023; Agari, 2024a, 2024b; Czerny, 2024b; Fake Reporter, 2024).

A unique phenomenon was revealed and reported in January 2024, in which Israelis tried persistently to modify the Hebrew version of Wikipedia's articles about events and local military officers, political figures and groups regarded as affiliated to the left wing of Israeli politics, in order to put the blame and responsibility for the Hamas attack on them, alongside modification attempts of Wikipedia's article about right-wing ministers and political figures to minimize their blame and responsibility for the catastrophe under the pretext of „removing marginal information", with an attempt to emphasize their alleged contribution to preventing and minimizing it (Czerny, 2024a).

Another domestic influence operation against Israelis was reported on 12 December 2023, claiming the IDF Operations Directorate's Influencing Department, which is responsible for psychological warfare operations against the enemy and foreign audiences, operated a Telegram channel called ‚72 Virgins – Uncensored' which targeted Israeli audiences with „exclusive content from the Gaza strip" including „the bodies of Hamas terrorists". A military official denied the reports, admitting on 4 February 2024 that „its staff was behind the graphic Gaza Telegram channel" (Kubovich, 2023, 2024).

1.4 Cryptocurrencies and Online Crowdfunding

Terrorist organizations, Hamas among them, use the internet and social media as a platform to raise funds for their terrorist operations, including through cryptocurrencies (Monroe, 2023). The US Deputy Treasury Secretary, Wally Adeyemo, stated that „cryptocurrencies are still used by terrorist groups like Hamas, but their use is limited compared to more traditional alternatives" (Binance News, 2023).

Over the years, the National Bureau for Counter-Terror Financing of Israel (NBCTF) has seized millions of ILS (the new Israeli shekel) worth hundreds of cryptocurrency digital wallets linked to Hamas (National Bureau for Counter Terror Financing of Israel, 2021, 2022b, 2022a, 2023a), the Quds force, a branch of Iran's Islamic Revolutionary Guard Corps, and Hezbollah (National Bureau for Counter Terror Financing of Israel, 2023b). During the war in Gaza, reports have indicated that Hamas allegedly used cryptocurrencies to receive financial support from Iran while evading detection (Berwick and Talley, 2023). The NBCTF published a list of „ongoing crowd-funding campaigns run by Hamas and other terrorist designated entities", indicating that „since the outbreak of the „Swords of Iron" war, there has been a significant increase in the scope of online crowdfunding campaigns„ (National Bureau for Counter Terror Financing of Israel, no date).

Over 100 Hamas-linked cryptocurrency accounts on Binance, the world's largest cryptocurrency exchange, accounting for about half of all crypto activity, have been closed since 7 October 2023, which has led to the largest settlements in history, with a leadership change and fine of over 4.3 Billion USD on Binance for not guarding against money laundering. It „failed to implement safety programs aimed at preventing suspicious transactions" to Hamas, the Palestinian Islamic Jihad, Al Qaeda and the Islamic State of Iraq and Syria (ISIS) (Binance Blog, 2023; Bushard, 2023; Harty and Sutton, 2023; United States Department of Justice, 2023; US Department of the Treasury, 2023; Versprille, 2023).

However, there are claims that Israel failed to halt Hamas' cryptocurrency fundraising which meant that „in certain instances, action was taken only after 7 October, by which point the majority of the funds had already been withdrawn" (Czerny, 2023).

2 ISRAEL'S COUNTERMEASURES

To confront these cyberattacks, the INCD issued several general recommendations for the public (Israel National Cyber Directorate, 2023o) and small and medium businesses on how to mitigate malicious online activities (Israel National Cyber Directorate, 2023p), alongside specific recommendations, mainly in Hebrew. The directorate launched a campaign to „empower citizens in discerning fake news and enhancing online security amid the rising prevalence of digital disinformation" (Israel National Cyber Directorate, 2023e), alongside a similar campaign by the Israel Internet Association (The Israel Internet Association (ISOC-IL), no date); guidelines about warning signs for hacked social media accounts (Israel National Cyber Directorate, 2023f); how to recognize and avoid phishing (Israel National Cyber Directorate, 2023g, 2023h); a recommendation to replace webcam passwords immediately (Israel National Cyber Directorate, 2023m);, and how to protect children from improper online material (Israel National Cyber Directorate, 2023r), including during online distance learning (Israel National Cyber Directorate, 2023k). In addition, the INCD issued several cyber warnings about Iranian cyber-attacks (Israel National Cyber Directorate, 2023t, 2023c), a planned phishing attack (Israel National Cyber Directorate, 2023q) and reports summarizing the cyber-attacks during the war (Israel National Cyber Directorate, 2023d).

The INCD has launched several initiatives to improve local and national cyber resilience, such as the TITAN project (Team for Information Threat Analysis and Neutralization) „to generate the sharing of technical information in a rapid and reciprocal manner between all parties involved in order to maximise the realisation of the collective ability of the community to identify and prevent cyber-attacks as early as possible" (Israel National Cyber Directorate, 2024); a marketplace of cyber defence solutions by local vendors, free of charge for a limited time (Israel National Cyber Directorate, 2023l, 2023n); a working group to confront fake news (Israel National Cyber Directorate, 2023s), and a forum for the cyber events Incidents Response service local providers (Israel National Cyber Directorate, 2023a).

On 26 December 2023, the Knesset (Israeli Parliament) approved a temporary provision for a seven-month „Bill authorising Cyber Directorate, Israeli Security Agency and Director of Security of the Defense Establishment to instruct digital or storage service supplier to take measures to detect, prevent, or contain cyber-attack", aiming to „provide an effective response for coping with the challenges the State of Israel faces in the cyber field". It authorized the INCD, when faced with a cyber-attack, „to instruct the attacked [digital or storage service supplier] to take measures to detect, prevent, or contain the attack" (The Knesset, 2023).

Conclusion

The ground invasions of Israeli villages by Hamas terrorists on 7 October 2023 were accompanied by days and weeks of cyber-attacks on Israeli digital assets, which caused some damage, mainly to information technology, at least in terms of stolen information, alongside various information operations.

The first days and weeks of the war marked an intensification of the quantity and quality of cyber offensive activities across Israel and demonstrated the blending of kinetic and non-kinetic means of warfare into a ‚hybrid warfare', with various and contradictory motivations, and actors aiming to leverage cyberspace as an added battlefield to harm Israel's critical information and operation systems and create chaos, and to tear Israeli society apart by spreading fake news and conspiracy theories by external and even internal political actors, including nation state-based cyber-actors and more than a hundred pro-Palestinian cyber groups, hacktivists, cybercriminals and cyber-terrorists, and even Israeli politically-motivated fake news and conspiracy theory originators and distributors.

Similar to the physical military dimension, Israel is seen as a regional and even a global cyber power, mainly in the light of its capabilities in technology development, intelligence and offensive uses of cyber tools. However, Israel must conduct a reassessment and a strategic conceptual change relating to the cyber protection of its digital and physical assets. Although this round of cyber-attacks and operations did not have as much critical damage and impact as the physical attacks, the cyber-attacks and online influence operations demonstrated the need to redefine concepts such as „cyber power" and „cyber resilience" of states and organizations.

A future ‚Digital 7 October' could include cyber onslaughts by various cyber actors, with diverse motivations and levels of sophistication, carrying out ‚hybrid warfare', which could affect information systems by leaking sensitive information or destroying the system itself and other vital infrastructure, alongside influence operations to manipulate the general population according to the attackers' agenda, and even cyber espionage operations. An alarming conclusion is the involvement of local politically motivated actors in generating and disseminating fake news and conspiracy theories which can find their way from the margins to mainstream media outlets, alongside attempts to rewrite history by the manipulation of Wikipedia articles.

We must avoid a ‚Digital 7 October' in Israel and worldwide, as it could have consequences many times more severe, since cyber-attacks on vital infrastructure and information systems can yield tangible, kinetic outcomes that disrupt local operations and can lead to extensive chaos and collateral damage in a modern state. Preparedness should include not only technological means and capabilities, but also a comprehensive perspective of cyber capabilities and the resilience of the private and government sectors. Bruce Schneier stated in April 2000 that „security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognise the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches" (Schneier, 2000).

References

1. *ABC News, 2011. CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor. Available at: https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905 (Accessed: 4 February 2024).*
2. *Abu Ali Express, 2024a. The Palestinians harness artificial intelligence to produce fabricated images in order to evoke pity. Available at: https://abualiexpress.com/en/the-palestinians-harness-artificial-intelligence-to-produce-fabricated-images-in-order-to-evoke-pity/ (Accessed: 27 January 2024).*
3. *Abu Ali Express, 2024b. The pro-Iranian militias set up a fake website in Hebrew that claims that three people from the 8200 unit were killed in an attack in Erbil in Iraq at the beginning of the new year. Available at: https://abualiexpress.com/en/the-pro-iranian-militias-set-up-a-fake-website-in-hebrew-that-claims-that-three-people-from-the-8200-unit-were-killed-in-an-attack-in-erbil-in-iraq-at-the-beginning-of-the-new-year/ (Accessed: 27 January 2024).*
4. *Agari, C., 2024a. The new target of Netanyahu's propaganda system: the families of the abductees, The Seventh Eye. Available at: https://www.the7eye.org.il/508670 (Accessed: 16 February 2024).*
5. *Agari, C., 2024b. Towards the shuffling stage: Netanyahu's poison machine updates messages, The Seventh Eye. Available at: https://www.the7eye.org.il/507342 (Accessed: 16 February 2024).*
6. *Andriani, M., 2024. Under siege: how DDoS security transformed during Hamas war, Ynet. Available at: https://www.ynetnews.com/business/article/bkednzpup (Accessed: 28 January 2024).*
7. *Berwick, A., and Talley, I., 2023. Hamas Needed a New Way to Get Money From Iran. It Turned to Crypto, The Wall Street Journal. Available at: https://www.wsj.com/world/middle-east/hamas-needed-a-new-way-to-get-money-from-iran-it-turned-to-crypto-739619aa?st=155dhbzks7578zf (Accessed: 28 January 2024).*
8. *Bestuzhev, D., 2023. BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows, BlackBerry Blog. Available at: https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows (Accessed: 4 February 2024).*
9. *Binance Blog, 2023. Binance Announcement: Reaching Resolution With U.S. Regulators. Available at: https://www.binance.com/en/blog/leadership/binance-announcement-reaching-resolution-with-us-regulators-2904832835382364558 (Accessed: 28 January 2024).*
10. *Binance News, 2023. Cryptocurrencies Still Used by Terrorist Groups, but Limited Compared to Traditional Alternatives. Available at: https://www.binance.com/en/feed/post/2023-10-27-cryptocurrencies-still-used-by-terrorist-groups-but-limited-compared-to-traditional-alternatives-1522926 (Accessed: 28 January 2024).*
11. *Bushard, B., 2023. Justice Department Cites Hamas' Use Of Binance In $4.3 Billion Settlement, Forbes. Available at: https://www.forbes.com/sites/brianbushard/2023/11/21/justice-department-cites-hamas-use-of-binance-in-43-billion-settlement/?sh=49b1725b30f0 (Accessed: 28 January 2024).*
12. *BZ, I., 2023. Enemies from within, The Seventh Eye. Available at: https://www.the7eye.org.il/498847 (Accessed: 16 February 2024).*
13. *Check Point Research, 2023. The Iron Swords War – Cyber Perspectives from the First 10 Days od the War in Israel. Aailable at: https://blog.checkpoint.com/security/the-iron-swords -war-cyber-perspectives-from-the-first-10-days-of-the-war-in-israel/ (Accessed: 2 November 2023).*
14. *Cluley, G., 2023. Hacktivists send fake nuclear attack warning via Israeli Red Alert app, Bitdefender. Available at: https://www.bitdefender.co.uk/blog/hotforsecurity/hacktivists-send-fake-nuclear-attack-warning-via-israeli-red-alert-app/ (Accessed: 31 January 2024).*

15. *CTech, 2023. IDF uncovers covert 'Avatar' network targeting Israeli soldiers for information. Available at: https://www.calcalistech.com/ctechnews/article/s1mv11zbxa (Accessed: 4 February 2024).*
16. *Cybersecurity & Infrastructure Security Agency (CISA), 2023. IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa-23-335a (Accessed: 27 January 2024).*
17. *CYFIRMA, 2023. ISRAEL GAZA CONFLICT: THE CYBER PERSPECTIVE. Available at: https://www.cyfirma.com/outofband/israel-gaza-conflict-the-cyber-perspective/ (Accessed: 25 January 2024).*
18. *Czerny, M., 2023. How Israel Failed to Halt Hamas' Cryptocurrency Fundraising, Shomrim. Available at: https://www.shomrim.news/eng/how-israel-failed-to-halt-hamas-cryptocurrency-fundraising (Accessed: 31 January 2024).*
19. *Czerny, M., 2024a. Subliminal Maneuvering: The War on the October 7th Narrative is going strong in Wikipedia's archives, שומרים. Available at: https://www.shomrim.news/hebrew/war-wikipedia (Accessed: 4 February 2024).*
20. *Czerny, M., 2024b. The Crazier, The Better: How Fake News Spreads from Tiny Telegram Groups to the Israeli Mainstream, שומרים. Available at: https://www.shomrim.news/eng/how-fake-news-spreads-to-the-israeli-mainstream (Accessed: 16 February 2024).*
21. *Darché, B., Boursalian, A., and Castro, J., 2023. Malicious "RedAlert - Rocket Alerts" application targets Israeli phone calls, SMS, and user information, Cloudflare. Available at: https://blog.cloudflare.com/malicious-redalert-rocket-alerts-application-targets-israeli-phone-calls-sms-and-user-information/ (Accessed: 31 January 2024).*
22. *Eichner, I., 2023a. Indonesian cyber attack on government ministers' phones: 'We will kill you', Ynet. Available at: https://www.ynetnews.com/business/article/h1i1h001up (Accessed: 31 January 2024).*
23. *Eichner, I., 2023b. Israeli officials swamped by online threats in cyber onslaught, Ynet. Available at: https://www.ynetnews.com/business/article/h1y2izlva (Accessed: 31 January 2024).*
24. *Eichner, I., 2023c. TikTok says video supporting Hamas 'not against community guidelines', Ynet. Available at: https://www.ynetnews.com/business/article/r111y1vet (Accessed: 30 January 2024).*
25. *Fabian, E., 2024. Shin Bet says it thwarted Iranian attempt to recruit Israeli spies via social media, The Times of Israel. Available at: https://www.timesofisrael.com/shin-bet-says-it-thwarted-iranian-attempt-to-recruit-israeli-spies-via-social-media/ (Accessed: 20 January 2024).*
26. *Fake Reporter, 2024. The campaign against the families of the abductees. Available at: https://www.fakereporter.net/pdf/campaign%20against%20hostages%20families-0224.pdf (Accessed: 16 February 2024).*
27. *Harty, D., and Sutton, S., 2023. Historic fine on Binance over alleged Hamas financing signals new era in crypto crackdown, POLITICO. Available at: https://www.politico.com/news/2023/11/21/feds-hit-crypto-giant-with-4-4b-in-fines-alleging-hamas-financing-sanctions-violations-00128278 (Accessed: 28 January 2024).*
28. *Hindustan Times, 2023. Israeli daily Jerusalem Post hit by multiple cyberattacks. Available at: https://www.hindustantimes.com/world-news/israel-hamas-war-palestine-conflict-jerusalem-post-cyberattack-101696750348298.html (Accessed: 27 January 2024).*
29. *I24NEWS, 2023. Pro-Palestinian Turkish Hackers Target Israeli Cinema Screens. Available at: https://www.i24news.tv/en/news/israel-at-war/1706020332-pro-palestinian-turkish-hackers-target-israeli-cinema-screens (Accessed: 30 January 2024).*
30. *IDF, n. d. Understanding HAMAS' Information Warfare. Available at: https://docsend.com/view/5aceqwjx6b533gfy (Accessed: 27 January 2024).*

31. *Ifargan, S., 2023. 'I have no idea how they got my details. They didn't hack into my phone or computer', Mako. Available at: https://www.mako.co.il/nexter-news/Article-a118bcc0a-e51c81026.htm?partner=tagit (Accessed: 31 January 2024).*
32. *Irwin, R., 1998. What is FUD? Available at: https://web.archive.org/web/20190114060827/http://www.cavcomp.demon.co.uk/halloween/fuddef.html (Accessed: 31 January 2024).*
33. *Israel National Cyber Directorate, 2023a. A call to join the IR companies forum of the National Cyber Directorate. Available at: https://www.gov.il/he/departments/news/kol_kore_ir (Accessed: 27 January 2024).*
34. *Israel National Cyber Directorate, 2023b. A joint report by the Israel National Cyber Directorate and American cyber defence bodies warns of Iranian attacks on industrial controllers. Available at: https://www.gov.il/he/departments/news/report021223 (Accessed: 27 January 2024).*
35. *Israel National Cyber Directorate, 2023c. A new phishing attack from Iran is trying to delete information from organisations. Available at: https://www.gov.il/he/departments/news/iranf5_2612 (Accessed: 27 January 2024).*
36. *Israel National Cyber Directorate, 2023d. A new report by the Israel National Cyber Directorate, intended for cybermen and women, summarises the first months of the iron sword war in the cyber dimension and states: an increase in the intensity of cyber attacks against Israel. Available at: https://www.gov.il/he/departments/news/published24122 (Accessed: 27 January 2024).*
37. *Israel National Cyber Directorate, 2023e. Empowering Vigilance: Combating Digital Disinformation Together. Available at: https://www.gov.il/en/departments/news/shatefet_1012 (Accessed: 27 January 2024).*
38. *Israel National Cyber Directorate, 2023f. Has your social network been hacked? This way, you can check that your accounts will not be compromised. Available at: https://www.gov.il/en/departments/news/social_network_2711 (Accessed: 27 January 2024).*
39. *Israel National Cyber Directorate, 2023g. How to Avoid Phishing Scams? Available at: https://www.gov.il/en/departments/news/avoid_phishing_2711 (Accessed: 27 January 2024).*
40. *Israel National Cyber Directorate, 2023h. How to Recognise Phishing Scams? Available at: https://www.gov.il/en/departments/news/recognize_phishing_2711 (Accessed: 27 January 2024).*
41. *Israel National Cyber Directorate, 2023i. Iran and Hezbollah behind an attempted cyber attack on an Israeli Hospital. Available at: https://www.gov.il/en/departments/news/ziv181223 (Accessed: 27 January 2024).*
42. *Israel National Cyber Directorate, 2023j. 'Iron swords' war in the cyber dimension: insights and ways of coping. Available at: https://go.gov.il/cyber_report (Accessed: 20 January 2024).*
43. *Israel National Cyber Directorate, 2023k. Learning remotely? This is how you make sure that the video meeting is safe. Available at: https://www.gov.il/he/departments/news/learning_remotely_this_is_how_you_make_sure_your_video_meeting_is_safe (Accessed: 27 January 2024).*
44. *Israel National Cyber Directorate, 2023l. Marketplace for Cyber Defense in War. Available at: https://www.gov.il/he/departments/news/market_place (Accessed: 27 January 2024).*
45. *Israel National Cyber Directorate, 2023m. Owners of home cameras – change your password urgently! Available at: https://www.gov.il/he/departments/news/home_camera_owners_change_your_password (Accessed: 27 January 2024).*
46. *Israel National Cyber Directorate, 2023n. Public organisations and companies in the economy – need assistance in cyber defence during the war? We have an offer for you! Available at: https://www.gov.il/he/departments/news/call_kore_help_and_protection (Accessed: 27 January 2024).*

47. *Israel National Cyber Directorate, 2023o. Recommendations from the Israel National Cyber Directorate to stay safe online during war. Available at: https://www.gov.il/he/departments/news/recommendations_from_the_israel_national_cyber_directorate_to_stay_safe_online_these_days (Accessed: 27 January 2024).*
48. *Israel National Cyber Directorate, 2023p. Seven iron rules for cyber protection for small and medium businesses: Available at: https://www.gov.il/he/departments/news/iron_rules_for_cyber_protection_for_small_and_businesse (Accessed: 27 January 2024).*
49. *Israel National Cyber Directorate, 2023q. The Israel National Cyber Directorate warns of a planned phishing attack. Available at: https://www.gov.il/he/departments/news/fishing_alert (Accessed: 27 January 2024).*
50. *Israel National Cyber Directorate, 2023r. This is how you protect your child from exposure to inappropriate online content. Available at: https://www.gov.il/he/departments/news/protect_your_child_from_exposure_to_inappropriate_online_content (Accessed: 27 January 2024).*
51. *Israel National Cyber Directorate, 2023s. Together, we will defeat fake news. Available at: https://www.gov.il/he/departments/news/kol_kore_fake_news (Accessed: 27 January 2024).*
52. *Israel National Cyber Directorate, 2023t. Urgent warning: an Iranian attack group has implemented a targeted phishing campaign impersonating the F5 company. Available at: https://www.gov.il/he/departments/publications/reports/alert_1691 (Accessed: 27 January 2024).*
53. *Israel National Cyber Directorate, 2024. A call for participation in a professional information-sharing group – the TITAN project. Available at: https://www.gov.il/he/departments/publications/reports/kol_kore0201c (Accessed: 27 January 2024).*
54. *Israel State Archives, n. d. Available at: https://catalog.archives.gov.il/en/ (Accessed: 26 January 2024).*
55. *Israeli Financial Insider, 2023. Cyber Attack Targets Ono Academic College; Student Records Compromised. Available at: https://www.ifi.today/news/2665-Cyber-Attack-Targets-Ono-Academic-College-Student-/ (Accessed: 26 January 2024).*
56. *Kabir, O., 2023. Dozens of Israeli retailers hit by cyberattack, Ctech. Available at: https://www.calcalistech.com/ctechnews/article/1fgigj3l8 (Accessed: 26 January 2024).*
57. *Kahan, R., 2023a. Government websites under attack by hackers – were unavailable for a short time, YNET. Available at: https://www.ynet.co.il/digital/technews/article/h1p00y8lwa (Accessed: 31 January 2024).*
58. *Kahan, R., 2023b. Hamas hackers are trying to scare Israelis with fake SMS messages and news sites, Ynet. Available at: https://www.ynetnews.com/business/article/hjoy4f8mp (Accessed: 28 January 2024).*
59. *Kahan, R., 2023c. Hamas invasion accompanied by powerful cyberattack, report claims, Ynet. Available at: https://www.ynetnews.com/business/article/bjeg7nug6 (Accessed: 28 January 2024).*
60. *Kahan, R., 2023d. Hamas using 'BiBi' malware against Israel. Available at: https://www.ynetnews.com/business/article/h1eaerema (Accessed: 31 January 2024).*
61. *Kahan, R., 2023e. Increasingly sophisticated hackers threaten Israeli online shoppers, Ynet. Available at: https://www.ynetnews.com/business/article/b1sydni7a (Accessed: 31 January 2024).*
62. *Kahan, R., 2023f. Most dangerous Iranian hacker group bolsterers attack capabilities, Ynet. Available at: https://www.ynetnews.com/business/article/hyim5si7t (Accessed: 28 January 2024).*
63. *Kahan, R., 2023g. Pro-Palestinian hackers leak file with information on 6.5 million Israelis, Ynet. Available at: https://www.ynetnews.com/business/article/bjdmvsv11a (Accessed: 28 January 2024).*

64. *Kahan, R., 2023h. Telegram channel posing as pro-Israel hacker group scams Israelis for donations, Ynet. Available at: https://www.ynetnews.com/business/article/s1vglmchp (Accessed: 28 January 2024).*
65. *Kaspersky IT Encyclopedia, n. d. What is website or web defacement? Available at: https://encyclopedia.kaspersky.com/glossary/deface/ (Accessed: 17 May 2024).*
66. *Ben Kimon, E., 2023. Iran plot to enlist Israelis for terrorism uncovered, Shin Bet, Ynet. Available at: https://www.ynetnews.com/article/hjbffazva (Accessed: 28 January 2024).*
67. *Kolodetsky, M., 2024. A cyber attack disabled the computers of the Municipality of Modi'in Illit, HaMehadesh. Available at: https://hm-news.co.il/440086/ (Accessed: 25 January 2024).*
68. *Kubovich, Y., 2023. Graphic Videos and Incitement: How the IDF Is Misleading Israelis on Telegram, Haaretz. Available at: https://www.haaretz.com/israel-news/security-aviation/2023-12-12/ty-article/.premium/graphic-videos-and-incitement-how-the-idf-is--misleading-israelis-on-telegram/0000018c-5ab5-df2f-adac-febd01c30000 (Accessed: 4 February 2024).*
69. *Kubovich, Y., 2024. Israeli Army Admits Its Staff Was Behind Graphic Gaza Telegram Channel, Haaretz. Available at: https://www.haaretz.com/israel-news/2024-02-04/ty-article/.premium/israeli-army-its-admits-staff-was-behind-graphic-gaza-telegram--channel/0000018d-70b4-dd6e-a98d-f4b6a9c00000 (Accessed: 4 February 2024).*
70. *Kutub, A., 2024. Hackers broke into Tel Aviv movie theater system and screened October 7 images, Ynet. Available at: https://www.ynetnews.com/article/bygmwdtft (Accessed: 26 January 2024).*
71. *Mann, Y., 2023a. Draw me a war: How AI fakes Israel's war against Hamas, Ynet. Available at: https://www.ynetnews.com/business/article/s1aj0b5qa (Accessed: 28 January 2024).*
72. *Mann, Y., 2023b. In the shadow of the war: Hackers broke into the Ono Academy, Ynet. Available at: https://www.ynet.co.il/digital/technews/article/ryhhfjzwt (Accessed: 26 January 2024).*
73. *Mann, Y., 2023c. Telegram partially blocks Hamas channels, Ynet. Available at: https://www.ynetnews.com/business/article/b16q8shm6 (Accessed: 28 January 2024).*
74. *Melman, Y., 2018. Hamas attempted to plant spyware in 'Red Alert' rocket siren app, The Jerusalem Post. Available at: https://www.jpost.com/arab-israeli-conflict/hamas-attempted-to-plant-spyware-in-red-alert-rocket-siren-app-564789 (Accessed: 31 January 2024).*
75. *Meyran, R., 2023. Cyber Aggression Rises Following the October 2023 Israel-Hamas Conflict, Radware. Available at: https://www.radware.com/blog/ddos-protection/2023/10/cyber-aggression-rises-following-the-october-2023-israel-hamas-conflict/ (Accessed: 28 January 2024).*
76. *Milenkoski, A., 2023. Gaza Cybergang | Unified Front Targeting Hamas Opposition, SentinelOne. Available at: https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/ (Accessed: 30 January 2024).*
77. *Mimran, T., 2023. Israel – Hamas 2023 Symposium – Cyberspace – the Hidden Aspect of the Conflict, Lieber Institute, West Point. Available at: https://lieber.westpoint.edu/cyberspace-hidden-aspect-conflict/ (Accessed: 28 January 2024).*
78. *Monroe, B., 2023. Unraveling a complex web: A primer on Hamas funding sources, Iranian support, global connections and compliance concerns, considerations, Association of Certified Financial Crime Specialists. Available at: https://www.acfcs.org/unraveling-a--complex-web-a-primer-on-hamas-funding-sources-iranian-support-global-connections--and-compliance-concerns-considerations (Accessed: 28 January 2024).*
79. *National Bureau for Counter Terror Financing of Israel, 2021. Minister of Defense Benny Gantz Signs an Administrative Order to Seize Electronic Wallets Used by Hamas to Trade Different Types of Cryptocurrency. Available at: https://nbctf.mod.gov.il/en/pages/CryptoSeizureEN072021.aspx (Accessed: 27 January 2024).*

80. *National Bureau for Counter Terror Financing of Israel, 2022a. Minister of Defense Gantz signed a Seizure Order of cryptocurrencies for 2.6 million ILS belonging to a terror organisation related to Hamas in the Gaza Strip. Available at: https://nbctf.mod.gov.il/en/pages/31.12.21E.aspx (Accessed: 27 January 2024).*
81. *National Bureau for Counter Terror Financing of Israel, 2022b. The third time within a year: The Defense Minister Gantz signed a seizure order of cryptocurrency intended to assist Hamas. Available at: https://nbctf.mod.gov.il/en/pages/280222E.aspx (Accessed: 27 January 2024).*
82. *National Bureau for Counter Terror Financing of Israel, 2023a. Defense Minister, Yoav Gallant, signed a seizure order for 81 digital accounts and hundreds of digital wallets linked to Hamas. Available at: https://nbctf.mod.gov.il/en/pages/Defense-Minister,-Yoav--Gallant,-signed-a-seizure-order-for-81-digital-accounts-and-hundreds-of-digital-wallets--linked-to-Ha.aspx (Accessed: 27 January 2024).*
83. *National Bureau for Counter Terror Financing of Israel, 2023b. The defense establishment thwarted terrorist infrastructure belonging to Hezbollah and the Iranian Quds Force, which operated to transfer funds through digital currencies for Quds Force and Hezbollah. Available at: https://nbctf.mod.gov.il/en/pages/28062023EN.aspx (Accessed: 27 January 2024).*
84. *National Bureau for Counter Terror Financing of Israel, n. d. List of ongoing Hamas crowdfunding campaigns. Available at: https://nbctf.mod.gov.il/he/pages/22102023HE.aspx (Accessed: 27 January 2024).*
85. *National Institute of Standards and Technology (NIST), n. d. a. DDoS. Available at: https://csrc.nist.gov/glossary/term/ddos (Accessed: 17 May 2024).*
86. *National Institute of Standards and Technology (NIST), n. d. b. Phishing. Available at: https://csrc.nist.gov/glossary/term/phishing (Accessed: 17 May 2024).*
87. *Pines, M., 2024. Cyber Toufan Al-Aqsa Signature-IT Attack, Cyberint. Available at: https://cyberint.com/blog/dark-web/cyber-toufan-al-aqsa-signature-it-attack/ (Accessed: 26 January 2024).*
88. *Recorded Future, 2023. Hamas Application Infrastructure Reveals Possible Overlap with TAG-63 and Iranian Threat Activity. Available at: https://go.recordedfuture.com/hubfs/reports/cta-2023-1019.pdf (Accessed: 30 January 2024).*
89. *Reuters, 2023. TikTok denies pushing pro-Palestine content, Ynet. Available at: https://www.ynetnews.com/business/article/bywdl7mma (Accessed: 28 January 2024).*
90. *Ring, E., 2023. How Telegram, Twitter and TikTok Have Become Lethal Tools of Hamas Psychological Warfare, Haaretz. Available at: https://www.haaretz.com/opinion/2023-12-25/ty-article-opinion/.premium/how-telegram-twitter-and-tiktok-have-become-lethal-tools-of-hamas-psychological-warfare/0000018c-a0ae-d502-af9f--b2ff5f050000?gift=fe302fa4bae94a5aa02beb98de1495ed (Accessed: 27 January 2024).*
91. *Schneier, B., 2000. Essays: The Process of Security, Schneier on Security. Available at: https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.htm (Accessed: 17 February 2024).*
92. *Security Joes, 2023. Mission 'Data Destruction': A Large-scale Data-Wiping Campaign Targeting Israel, BlackBerry Blog. Available at: https://www.securityjoes.com/post/mission-data-destruction-a-large-scale-data-wiping-campaign-targeting-israel (Accessed: 4 February 2024).*
93. *Shem Ur, B., 2023. Bar Shem-Ur Bar Shem-Ur on X: 'In the last few days, fliers with very high traffic, who are also followed by Likud politicians, are spreading conspiracies here about the alleged involvement of Ehud Barak in the terrible massacre, making allegations about participants in blue shirts and sowing disinformation. We reached one of those responsible for the distribution. The full article https://t.co/ff7l1srLPF', @Bar_ShemUr. Available at: https://twitter.com/Bar_ShemUr/status/1714617437662941269 (Accessed: 16 February 2024).*

94. *Shulman, S., 2023. Gil Shwed: Cyber attacks on Israeli companies demanding ransom doubled during war, Ctech. Available at: https://www.calcalistech.com/ctechnews/article/epnilevsq (Accessed: 27 January 2024).*
95. *Ben Shushan, Y., 2023. Hackers steal IDF patient records from cyberattack on Israeli hospital, The Jerusalem Post. Available at: https://www.jpost.com/israel-news/defense-news/article-775843 (Accessed: 27 January 2024).*
96. *Shwartz Altshuler, T., and Yasur, I., 2024. When the 'Keyboard Mujahideen' discovered the AI, YNET. Available at: https://www.ynet.co.il/digital/technology/article/sjab7l1sa (Accessed: 16 February 2024).*
97. *Siddiqui, Z., 2023. Hackers hit aid groups responding to Israel and Gaza crisis, SWI swissinfo.ch. Available at: https://www.swissinfo.ch/eng/reuters/hackers-hit-aid-groups-responding-to-israel-and-gaza-crisis/48889666 (Accessed: 26 January 2024).*
98. *The Israel Internet Association (ISOC-IL, 2023a. Disinformation and artificial intelligence in the war of iron swords: the review of the Internet Association for the Science and Technology Committee of the Knesset. Available at: https://www.isoc.org.il/research/isoc-positions/use-of-ai-for-disinformation-committee (Accessed: 27 January 2024).*
99. *The Israel Internet Association (ISOC-IL), 2023b. The index for the accessibility of information and government services to the Arab society. Available at: https://www.isoc.org.il/index-websites-and-government-services-in-arabic-2023 (Accessed: 29 January 2024).*
100. *The Israel Internet Association (ISOC-IL), 2024. Making information and government services about war and emergency accessible to the Arabic language. Available at: https://www.isoc.org.il/government-services-about-war-emergency-accessible-to-the-arabic (Accessed: 4 February 2024).*
101. *The Israel Internet Association (ISOC-IL), n. d. Together we will defeat the fake news on the networks. Available at: https://www.isoc.org.il/public-action/fakenews (Accessed: 27 January 2024).*
102. *The Knesset, 2023. Approved in final readings: Bill authorising Cyber Directorate, Israeli Security Agency and Director of Security of the Defense Establishment to instruct digital or storage service supplier to take measures to detect, prevent, or contain cyber-attack. Available at: https://main.knesset.gov.il/en/news/pressreleases/pages/press261223q.aspx (Accessed: 27 January 2024).*
103. *United States Department of Justice, 2023. Binance and CEO Plead Guilty to Federal Charges in $4B Resolution. Available at: https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution (Accessed: 28 January 2024).*
104. *U.S. Department of the Treasury, 2023. U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws. Available at: https://home.treasury.gov/news/press-releases/jy1925 (Accessed: 28 January 2024).*
105. *Versprille, A., 2023. Binance Was Used to Funnel Money to Hamas, Other Terrorist Groups, Bloomberg. Available at: https://www.bloomberg.com/news/articles/2023-11-21/hamas-use-of-binance-cited-in-4-3-billion-settlement-with-us?embedded-checkout=true (Accessed: 28 January 2024).*
106. *Walla!, 2023. Israelis receive strange calls from Hamas supporters – Cyber Directorate, The Jerusalem Post. Available at: https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-770695 (Accessed: 27 January 2024).*
107. *Wullman, I., 2023, Iran, Hamas and Hezbollah collaborate in attacks against Israel, Cyber Directorate says, Ynet. Available at: https://www.ynetnews.com/business/article/rjsy00xiw6 (Accessed: 30 January 2024).*
108. *Yoachimik, O., and Pacheco, J., 2023. Cyber attacks in the Israel-Hamas war, Cloudfare. Available at: https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/ (Accessed: 2 November 2023).*
109. *Zitun, Y., 2024. Shin Bet discloses Iran's social media strategy to recruit Israelis, Ynet. Available at: https://www.ynetnews.com/article/hjwqhnmka (Accessed: 28 January 2024).*

110. Zohar, N., 2023. Hamas supporters flood TikTok with anti-Israel content and Americans are buying it, Ynet. Available at: https://www.ynetnews.com/business/article/rkwgf0twp (Accessed: 28 January 2024).

email: tal@cybureau.org

ORCID: 0000-0002-4046-0867

Dr. Tal Pavel je doktoriral iz bližnjevzhodnih študij na Univerzi Bar-Ilan v Izraelu (disertacija: »Spremembe vladnih omejitev uporabe interneta v Siriji, Egiptu, Savdski Arabiji in Združenih arabskih emiratih med letoma 2002 in 2005«). Je docent, raziskovalec in govornik v Izraelu in po svetu, specializiran za geopolitične vidike kibernetske varnosti - stične točke med mednarodnimi odnosi, politologijo in kibernetskim prostorom. Ti vključujejo kibernetske konflikte, kibernetsko vojno, kibernetske grožnje, kibernetske akterje nacionalnih držav, kibernetsko diplomacijo, kibernetski terorizem in hektivizem.

Tal Pavel, PhD, holds a PhD in Middle Eastern Studies from Bar-Ilan University, Israel (Dissertation: »Changes in Governmental Restrictions over the Use of the Internet in Syria, Egypt, Saudi Arabia and the United Arab Emirates between 2002 and 2005«). He is an assistant professor, researcher, and speaker in Israel and worldwide, specializing in the geopolitical aspects of cybersecurity – the tangent lines between international relations, political science, and cyberspace. These include cybered-conflicts, cyber warfare, cyber threats, nation-state cyber actors, cyber diplomacy, cyber terrorism, and hacktivism.

e-mail: Tal@cybureau.org

ORCID: 0000-0002-4046-0867