ANNUAL SUMMARY 2023

In the Midst of the ”Iron Swords” War

INCD
Israel National
Cyber Directorate

Gaby Portnoy

Director General,
Israel National Cyber Directorate

In 2023, the Israel National Cyber Directorate (INCD) continued its efforts in building a robust national defense system through collaborative endeavors with various stakeholders: the government, public sector, security community, private sector, international organizations, and other countries. Our capacity to safeguard the Israeli economy has notably strengthened, reflecting a shift in INCD's approach towards proactive defense and enhancing resilience across all fronts. Guided by the INCD's leadership, organizations have made significant strides in elevating cyber protection standards, setting a benchmark for the entire economy.

As we move into 2024, our focus remains on bolstering our defenses and preparedness across multiple fronts, amidst evolving cyber capabilities and heightened threats targeting our civilian infrastructure. This dynamic landscape necessitates a continuous enhancement of resilience, proactive anticipation of threats, and swift response protocols across all sectors, particularly in light of the escalating frequency of cyberattacks witnessed in 2023. Our preparedness demands not only skilled personnel, innovative thinking, and technological capabilities but also legislative support and governmental readiness to ensure we remain resilient and decisive in the face of cyber threats.

Reflecting on our cyber journey thus far, particularly during times of conflict, we outline five key insights:

Unified Efforts: The spirit of collaboration demonstrated by all stakeholders since October 7th has propelled us to new heights of cooperation, both domestically and internationally.

Holistic Approach: Recognizing the borderless nature of cyber threats, we have adopted a holistic approach to cyber defense, exemplified by initiatives like the "Cyber Dome," which actively defends the State of Israel against cyber threats.

Adaptability: From day one of the conflict, the INCD swiftly activated emergency protocols, adapting to evolving threats and deploying innovative solutions to uncharted territories, such as safeguarding against foreign influence in the digital sphere.

Agility: As adversaries escalated their cyber capabilities, we responded with increased agility, preempting threats and swiftly mitigating potential incidents that could impact multiple organizations simultaneously.

Human Factor: Amidst our reliance on technology, the dedication, resilience, and creativity of individuals have remained paramount, ensuring the uninterrupted functioning of our home front.

Looking ahead, the INCD remains steadfast in its mission, navigating through turbulent waters while staying committed to our course. The wake-up call on October 7th reminded us of the strength found in unity. By remaining united, I am confident that we will rise to the challenges ahead, continuously working to safeguard the digital space for all.

Reliable and Secure Digital Space

In 2023, there was an intensification of influence campaigns designed to manipulate public perception and undermine trust. Since October 7th, Israel has seen a surge in cyberattacks. According to the INCD, the national view of cyberspace includes the threat landscape of the attacks, resilience activities, ecosystem operations, and a protected awareness space.

”Iron Swords” War in the Cyber Dimension

The ”Iron Swords” war that began on October 7th has also brought up an increase in cyber attacks that intensified gradually and moved from focusing on stealing information to causing disruption and damage. While at the beginning of the war the attacks were simple and unsophisticated and aimed mainly at creating a public echo, over time they became more focused at the actual disruption of organizations. The defilement attacks are aimed rather at essential organizations and try to create a broad effect by targeting companies that are considered a supply chain for many organizations. With the progress of the war, more attack groups were identified as working on behalf of Iran and Hezbollah to promote cyber attacks accompanying the fighting.

”Iron Swords” War in the Cyber Dimension

Main Trends

Intensity and purpose of the activity

An increase in the volume of the attacks and a shift from focusing on stealing information to promoting attacks aimed at disruption and shutdown, including increasingly intensified attempts against essential bodies.

Targeting hospitals

The health sector has become a target, which state attack groups consider as legitimate for cyber attacks with the aim of harming citizens.

Combat support

Attacks aimed at trying to undermine the war effort and gather information about the deployment of forces. In addition, a strong activity against supply chain companies has been detected.

Influence as an essential tool

A significant tool supporting the entire activity of the attackers aimed at destabilizing, damaging the sense of personal security and supporting the Palestinian narrative.

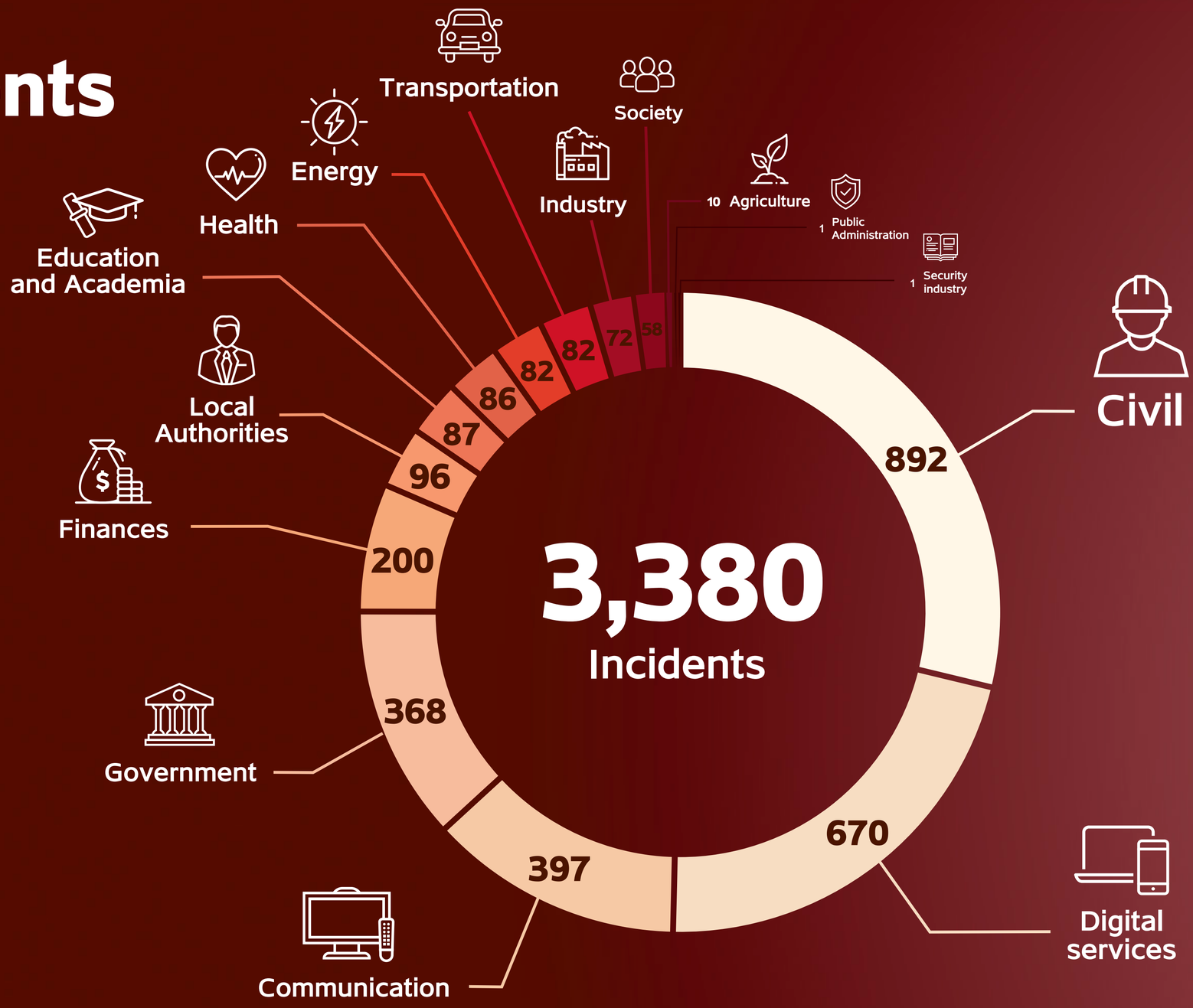
Strengthening collaboration

between Iran and Hezbollah while sharpening and focusing the activity against Israel.

Significant Incidents During the War

3,380 Incidents
(2.5 times more than usual)

800 with significant damage potential



”Iron Swords” War in the Cyber Dimension

Main Attack Tactics Used to Attack Israeli Cyber Space During the War

Wide Spraying Activity	Widespread use of Distributed Denial of Service (DDoS) attacks	Many attempts to penetrate various assets in order to obtain a hold and exploit knowledge and / or delete information
Linux systems attack including Wiper activation	Security cameras breach	Influence operations
Phishing attacks	Impersonate smartphone apps	Targeting organizations belonging to the MSP sector

”Iron Swords” War in the Cyber Dimension

The INCD Operations Toward Accelerated Strengthening of the Economy’s Resilience During the War

- Legislation of a temporary order on dealing with serious attacks in the digital services sector
- Accelerated activity for mapping and closing security gaps in hospitals
- Mapping hundreds of attack surfaces for the purpose of closing security gaps
- Cross-sector activities to reduce attack surfaces in controllers in the energy field
- Investigating terrorist financing wallets and transferring them to confiscation or freezing
- Emergency regulation for Biometric Information to Identify Casualties and Missing Persons
- Mapping and increasing resilience in the critical supply chain
- Increasing awareness regarding the protection of security cameras
- Publication of Guidelines for Enhancing Security
- Increasing resilience in about 150 local authorities
- Increasing response to the citizens in cyber hot line 119
- Raising preparednes in the economy
- Global collaboration

INCD
Israel National
Cyber Directorate

Reports Received at 119 Center

The INCD 119 Center receives thousands of reports a year about cyber attacks, attempts, vulnerabilities, security breaches, and more.

WHO YA GONNA CALL?

CERT119

Reports Received at 119 Center

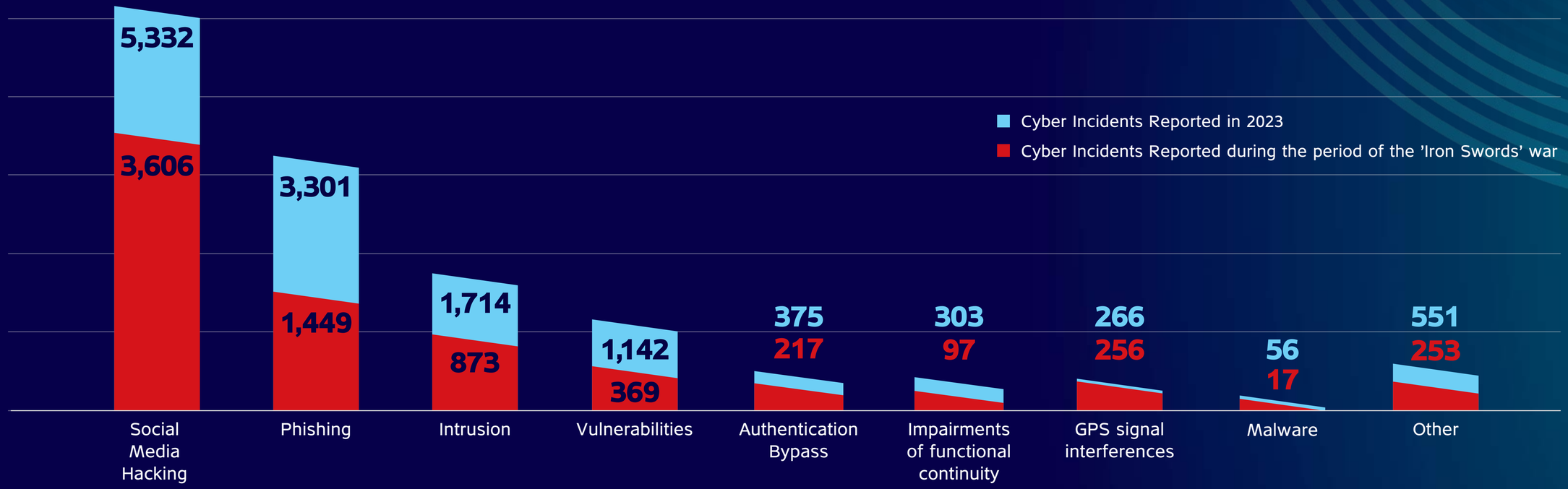
In 2023, the Center 119, which can be reached by direct dial or online 24/7, received 13,040 reports from citizens and organizations that were verified as cyber incidents.
It's worth mentioning that 68% of these reports arrived during the period of the 'Iron Swords' war (from October 7 to the end of 2023).

13,040
reports in **2023**

A **43%**
increase in reports compared to **2022**

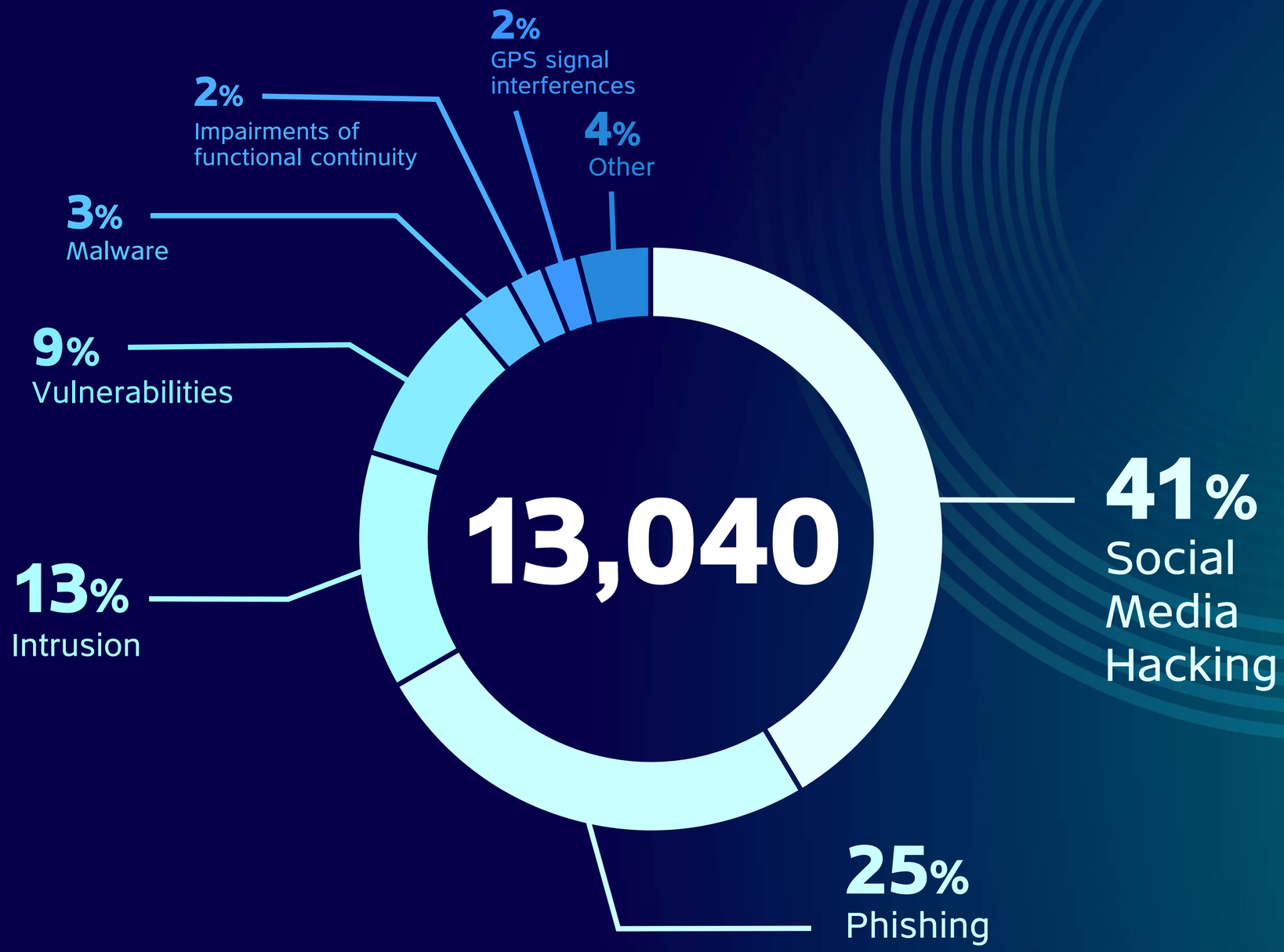
68%
of the reports during the "Iron Swords" war.

500
inquiries per day on average during the war
(**10** times more than usual)



Cyber Incidents Reported to 119 Center

in 2023



INCD
Israel National
Cyber Directorate

CyberSecurity Alerts

in 2023

CyberSecurity Alerts

in 2023

During 2023, the INCD issued **367 alerts & warnings** to the economy, about **43%** of them during the war **(158 alerts)**

142

TLP Clear Alerts

Disclosure is not limited

40

TLP Amber & TLP Amber + Strict

Limited disclosure, restricted to participant's organization.

183

Alerts intended for a specific organization

* TLP according to Traffic Light Protocol (TLP) Definitions

Common Vulnerabilities and Exposures Exploited by Attack Groups

The investigation of numerous cyber incidents conducted by the INCD in 2023 has uncovered four primary vulnerabilities exploited by attack groups throughout the year. These groups specifically targeted organizations that neglected to apply essential security updates or adjust configurations as recommended.

Four Main Vulnerabilities Exploited in Cyber Attacks in Israel this year:

Exchange servers' vulnerabilities
Attackers utilized various methods, notably the ProxyShell technique, to gain control over servers and install webshells for continued access or lateral movement.

Vulnerabilities in outdated versions of editors such as FCKeditor and TinyMCE
Wrong security configurations in these older versions provided openings for malicious exploitation.

Vulnerabilities in VPN components, particularly Forti and Pulse
Throughout the year, numerous vulnerabilities in these products facilitated attackers' relatively straightforward access to the core of organizational systems

Vulnerabilities in file upload interfaces on websites
These interfaces frequently served as a primary point of attack.

Common Attack Vectors This Year:

Use of Stolen Login Data
Attackers utilized usernames and passwords obtained from a supply chain entity to infiltrate other organizations.

Classic Phishing
Attackers employed email campaigns leading to fake websites, prompting users to enter sensitive details like usernames and passwords. This tactic successfully compromised numerous employees, resulting in unauthorized access to the organization's systems.

Active Defense

Activity towards Reducing Vulnerabilities in the Israeli Cyber Space

Active Defense

Activity towards Reducing Vulnerabilities in the Israeli Cyber Space

Pro-active defense that aims at being one step ahead of the attackers, and identifying vulnerabilities and trends in the Israeli cyberspace. The INCD operates ”Program for Responsible Disclosure of Vulnerabilities” inviting security researchers to discreetly report on vulnerabilities they have found in various product and websites. INCD manages the interface with the vulnerable vendor organization and grants the reporter public recognition in the Hall of Fame.

This year there was a **25% increase in the number of VDP reports** and a **10% increase in the number of signed CVE reports** compared to last year. **95% of all Vulnerabilities** reported to INCD were closed.

Days for Average Closed Reports

Numbers of CVE reports signed

Number of reporters credited in the Hall of Fame

VDP reports received

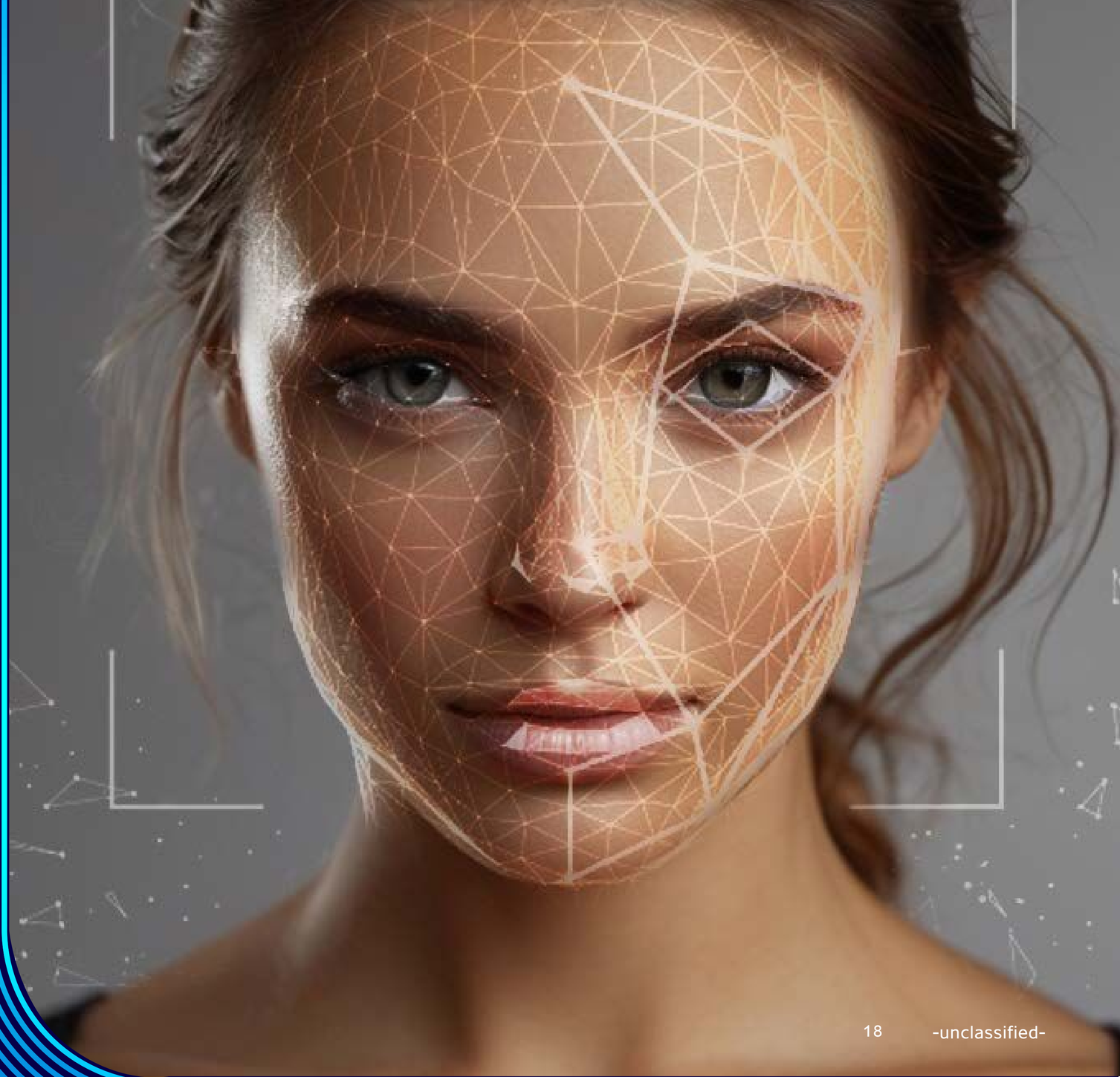
Handling phishing infrastructures - addresses that have been closed

Common vulnerabilities and exposures	An international effort to identify and report vulnerabilities in product. The program is managed by MITRE, a non-profit American organization.
CVE	The INCD is a partner in MITRES organization’s global program for reporting and vulnerabilities is authorized to register
VDP	Program for ”Responsible Vulnerability Disclosure for coordinating reports from the general public and information security researchers in particular, on vulnerabilities in websites in Israel

Secure Identification and Biometrics

The activity addressing identification processes and biometric applications within the Cyber Directorate is performed on three main levels:

1. Oversight, guidance and recommendation on policy in the biometric field
2. Guidance and building capacity in the field of secure digital identification
3. Management of a national biometric laboratory



Secure Identification and Biometrics

Among the projects promoted this year:

Publishing the Biometric Applications
Commissioner's report No. 13
addressing the oversight activity over the e-passports & e-IDs project and the national biometric database.

A project to develop
a digital documentation wallet
on mobiles allowing to prove identity in a convenient and safe way (in collaboration with the Population Authority).

Publishing a summary report regarding working with **55 government ministries**, examining the compatibility of the digital services' accessibility with the policy for secure identification.

26 government ministries reported on making digital services accessible to citizens, and **4 government ministries** are being accompanied and guided to complete compliance with the policy.

Publishing a summary report addressing the guidance activity with **12 public bodies and government ministries** that utilize biometric databases.

3 laboratory tests to examine challenges and biometric technologies for government bodies.

Promotion of Legislation and National Strategy in the Field of Cyber Defense

While cyber attacks are becoming more and more sophisticated over the years, the legislative framework in Israel that regulates cyber defenses for various sectors has been quite static. This creates a situation when each regulator deals with the issue with different tools and actual level of economy protection is insufficient. On the other hand, the world shows the tendency towards strengthening and expanding the regulation of cyber protection and anchoring it in primary legislation. The National Cyber Directorate promotes national legislation in accordance with internationally accepted standards aimed at increasing the level of resilience of organizations essential to functional continuity.

Principles of the Cyber Protection Law

- Strengthening the powers of government ministries regulating various sectors, in the cyber field.
- Determining an appropriate level of protection (obligation to manage risk) for essential entities.
- Determining the obligation to report a serious cyber attack at the essential entities.
- A mechanism for determining an essential organization and adding sectors.
- Determining the designation, roles and powers of the INCD.

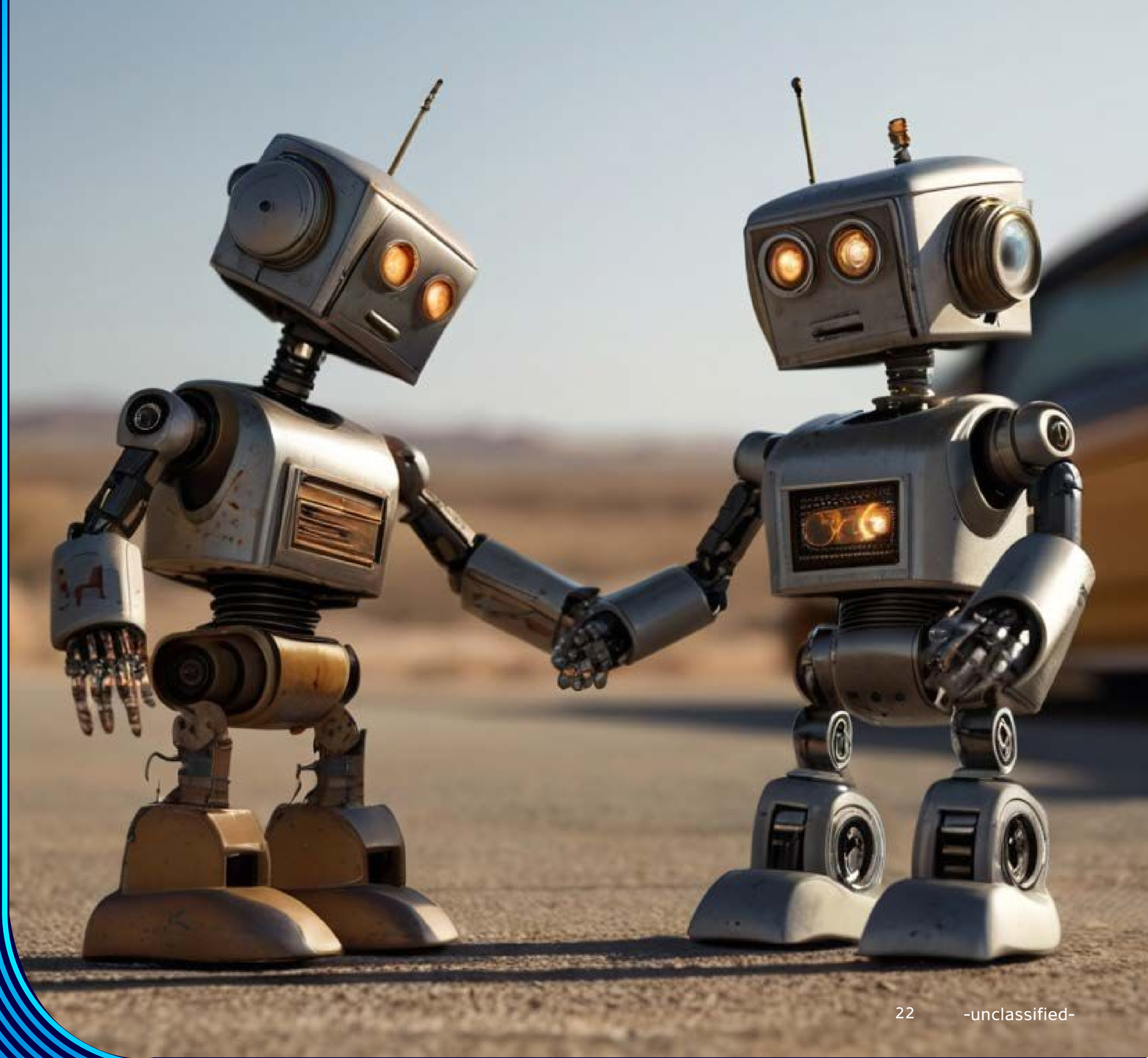
Temporary Legislation to deal with Cyber Attacks on Digital Services

During the ”Iron Swords” war, the INCD promoted a temporary legislation that allows slowing down and handling serious cyber attacks on companies that provide digital services and that are connected to many entities in the economy. The temporary legislation was approved over the background of the increase in the volume and intensity of cyber attacks on companies of this type during the war. The detected cases show that these attacks have high potential to damage the public interest due to their connection to essential entities in the economy, including the systems critical to the security of the state and the functioning of the economy.

Israeli National Cyber Defense Strategy

The current National Cyber Defense Strategy has been devised in 2017, and needed to be updated. Thus, starting from this year, the INCD, in cooperation with various stakeholders, began devising an updated strategy setting a vision of a secure and trust worthy digital space, and the strengthening the national cyber resiliencies the different sectors according to risk assessment methodologies, in a systematic approach, deploying state of the art technologies, acting together with our government and private sector partners. Among the strategic objectives is delivering a concrete national implementation plan, which shall be a road map for the realization of the strategy.

Systems for Defense Cooperation – International



Systems for Defense Cooperation – International

Collaborations with Tech Companies

CyberShield

Monitoring infrastructure in government sectors and building a national monitoring center. The infrastructure combines automation and artificial intelligence (AI) capabilities to identify cyber incidents at the level of the sectors and the economy, as part of the ”Cyber Dome” project to increase the resilience of the Israeli economy.

6 Sectors

32 Monitored Entities

124 Monitoring sources

Crystal Ball

A system for international cooperation in the fight against ransomware attacks. The system was developed in cooperation with the INCD, the United Arab Emirates and Microsoft Israel.

55 Member countries

ACD Portal

Development of a portal for small and medium enterprises to provide self-service protection services to the Israeli economy.
The collaboration includes the establishment of a secure cloud infrastructure and joint work to upload the portal application to the cloud.

AI Defense infrastructure

Strategic cooperation to integrate artificial intelligence (AI) capabilities in the national Cyber Dome.

Publication of Guidance Documents with International Partners

Guidelines Document on the Secure Development of Artificial Intelligence Products

Secure Remote Access BY CISA, NSA, FBI, MS-ISAC

Security by Design and by Default

A Joint Report by the National Cyber Directorate and American Cyber Defense Bodies Warns of Iranian Attacks on Industrial Controllers

Human Capital

In 2023, the number of educational programs addressing the training of underrepresented populations for cyber and artificial intelligence professions was expanded. The programs refer to various training sequence and life stages, starting from middle school to more mature populations with the intention of significant army service and continuing to employment and academia.

Human Capital

Programs for teenage boys and girls from the geographic and social periphery

Magshimim (Fullfilling) & mamriot (takes off)

2,940
students

196
classrooms

38
Mamriot classrooms

158
Magshimim classrooms - cyber and AI

"Startech" program

2,000
students

125
classrooms

34
classes in the Druze sector

"Gasharim" (Bridges) program

18,000
students

71
schools

34
authorities

Programs for an adult population

"Tachlit" & "Hadasim"

Programs for the Haredi (ultra-religious) population

200
Haredi men started this year The "Mechina" preparation course

88
- Haredi men enlisted this year for technological positions

230
Haredi women who work in a variety of technological units in the IDF

"Cyberspace"

The National Enterprise for Digital Learning offers a variety of quality digital courses in all fields

270,000
Enrolled

15,000
Successfully completed the courses

Fighters to Cyber

194
soldiers, which have completed service in combat units, participated in the program

136
Successfully completed the courses

Partners

משרד המודיעין | משרד החינוך | קרן רשי RASHI FOUNDATION | המרכז לחינוך סייבר מצויינות טכנולוגית בשליחות חברתית | מערך הדיגיטל הלאומי نظام الديجيتال الوطني Israel National Digital Agency

INCD
Israel National
Cyber Directorate

The Cyber Industry in Israel

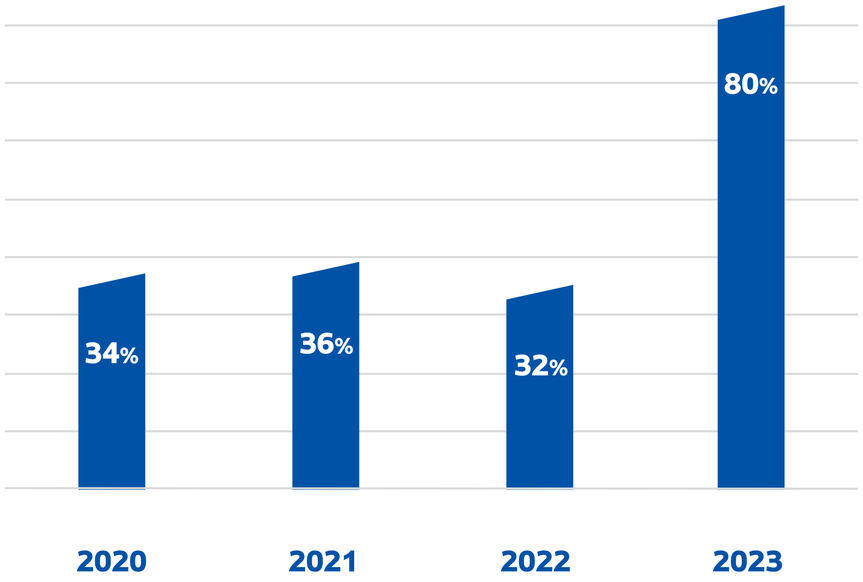
The State of Israel is widely regarded as one of the world's leading countries in cybersecurity, attributed in part to the development of innovative defense solutions that mature within the Israeli ecosystem - integrating the military, government, academia, and industry. Despite a significant decrease in investments across many sectors in the high-tech industry over the past two years, both in Israel and globally, data indicates that the decline in investments in cybersecurity companies in Israel was relatively low. In this regard, the cybersecurity industry continues to serve as a driving force for the entire high-tech sector and the Israeli economy.

The Cyber Industry in Israel

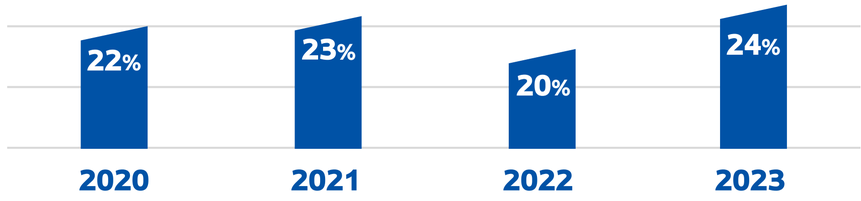
Cybersecurity Startup companies in 2023

- **8 out of the 10 top M&A exits**
  (over 100 million dollars) of Israeli companies are in the cybersecurity field.

- The cybersecurity sector saw M&A exits surge **to $2.8 Billion**
  (representing 80% of all M&A exits in Israeli high-tech for this year)



- The amount of private funding in Israeli cybersecurity companies is approximately **$1.9 Billion**
  (representing 24% of the total private funding in high-tech for this year)



Source: INCD processing of the 2023 ”Startup nation central” annual report on the Israeli high-tech ecosystem data

Cyber Innovation Labs

In recent years, the innovation activity of the cyber ecosystem in Beer Sheva has been strengthened, based on cooperation with Ben-Gurion University, the municipality, the IDF, international and Israeli industry, the INCD and other government bodies.
This year, new innovation labs that have already started their activities or are under establishment, have joined this ecosystem in Beer Sheva.

Cyber Innovation Labs

ICNL
ICS Cybersecurity National Lab

A national control and cyber innovation lab that simulates production processes such as electricity production and distribution, water desalination, smart homes and more, in a controlled experimental environment. The lab is capable of testing weaknesses in operational processes, malicious activities and various protection mechanisms. The lab started operating this year, promotes experiments and training.

* INCD operation with the INCD, the Directorate and the Ministry of Energy

FinSec
Innovation Lab

An innovation lab and facilitator for a testing and research environment in the field of digital payment processes, fintech and their connection to cyber defense that enables startup companies to test their product, receive support, guidance and consulting.

The laboratory has been supported many startups in the last year.

* In cooperation with the Ministry of Finance, the National Cyber Directorate, the Innovation Authority as well as MasterCard and EnelX.

CyITS Lab
Cyber Lab for Smart Transportation

The cyber lab performs experiments and research addressing vulnerabilities, malicious activities and defense mechanisms, and includes a training department.

* In cooperation with the Ministry of Transportation, Ayalon Routes Company, the National Cyber Directorate, Elta company, and with the participation of companies for cyber defense and Ben-Gurion University.

The National Laboratory for Testing and Verification of Artificial Intelligence - Based Models

To implement an artificial intelligence-based system in a production environment, it is required to examine aspects related to the robustness of the system, attempts of malicious users to damage and mislead it, and to implement appropriate protective measures to protect the databases and the artificial intelligence applications themselves. In order to handle the risk, the INCD is has established a national laboratory for testing and verification of artificial intelligence-based models. The laboratory shall produce methods and appropriate tools for testing the artificial intelligence-based models in terms of resilience.

* In cooperation with Ben Gurion University, Ministry of Finance, National Cyber Directorate, Innovation Authority, Mastercard, EnelX

INCD
Israel National
Cyber Directorate

Economic Analysis of the Damages of Cyber Attacks in Israel

Economic Analysis of the Damages of Cyber Attacks in Israel

Decision-making in the realm of cyber defense encompasses a spectrum of economic considerations at both macro and micro levels. An economic analysis conducted by the INCD reveals that the cumulative cost of cyber attacks in Israel amounts to approximately

12 billion NIS annually,

encompassing short, medium, and long-term expenses. These costs are projected to continue growing as technology becomes increasingly integrated into all facets of life, underscoring the imperative for comprehensive measures to enhance organizational and citizen-level protection.

Empirical analysis of studies and surveys conducted in Israel and globally on the impact of investment in cyber defense suggests that large, high-income enterprises reliant on e-commerce and cloud services can potentially reduce the likelihood of cyber attacks by **up to 50%** through the implementation of at least six fundamental security measures, such as robust password policies, regular software updates, and multi-factor authentication.

According to INCD analysis, the cost of implementing these security measures at the organizational or citizen level is significantly lower, potentially even negligible, compared to the potential damages incurred. This underscores the importance of proactive investment in cybersecurity to mitigate economic losses and safeguard critical assets.

[1] Based on research conducted by Neil Gandel and Noa Bernir from Tel Aviv University in collaboration with prominent researchers worldwide.

INCD
Israel National
Cyber Directorate

Raising Awareness of the General Public Regarding Cyber Threats

In 2023, the INCD initiated seven campaigns to bolster cyber security awareness among the general public. Following the outbreak of the war, the INCD swiftly launched an extensive social media campaign aimed at mitigating anticipated cyber threats, alongside a concerted effort to combat the spread of misinformation.

7
Campaigns

Over **120M**
Impressions Generated by Awareness Campaigns

Fighting Disinformation

Since the onset of the ’Iron Swords’ war, the Directorate has identified enemy efforts to disseminate disinformation and fake news. In response, the Directorate launched a comprehensive public awareness campaign titled ’Overcoming Sharing’ in December. The program’s messages were positively received, contributing to a notable shift in public discourse regarding the harmful effects of spreading fake news.

Public Exposure and Attitudes toward the ”Overcome Sharing” Campaign

More than
68M Impressions
To the digital campaign

80%
of the public were exposed to the campaign by at least one of the media channels

94%
of the public perceived the campaign as innovative

70%
of the public know or have heard about threats in the digital space

Cyber Threats Familiar to the Public

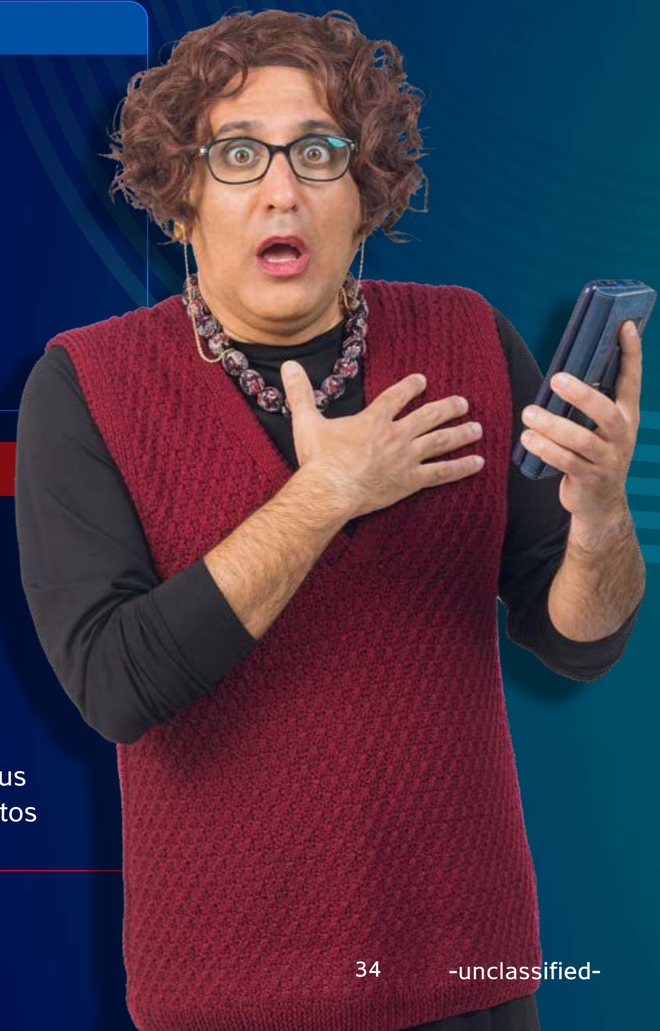
* more than one answer can be chosen

51%
Messages forwarded many times

42%
Requests for payment from an unknown party

56%
SMS messages with a suspicious link

39%
Receiving suspicious videos and / or photos



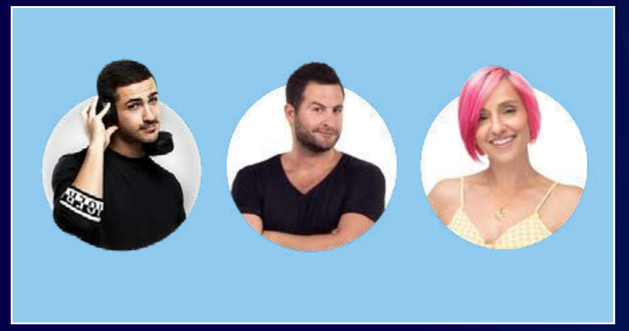
* Data from a survey by the Government Advertising Bureau conducted in December 2023 among a representative sample to examine the understanding of the messages from the ”Overcome Sharing” campaign.

Awareness Campaigns

Campaigns during the “Iron Swords” War

Securing Private Security Cameras: Best Practices

Cyber Defense Guidelines for the General Public

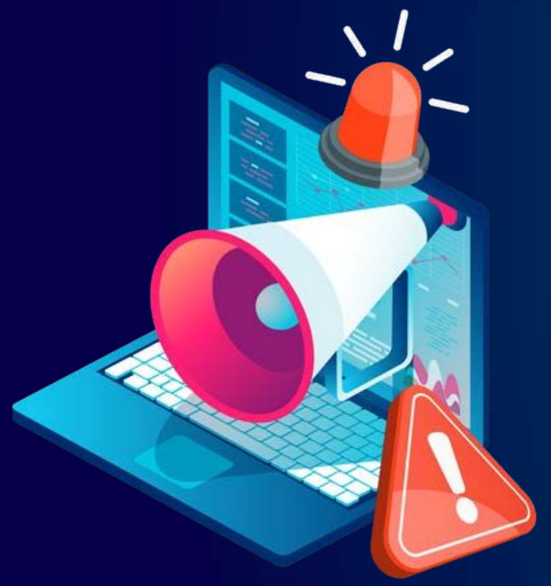


Raising Awareness about Cyber Protection for Youngsters through Online Influencers

Promotion of the **”Black Suitcases”** Podcast to Promote Public Understanding of the Cyber Field

Combatting Disinformation: The ’Overcome Sharing’ Initiative

Securing Social Media Guidelines



119
119@cyber.gov.il
www.cyber.gov.il

Writing and Editing:
Media and Information Department
Photos: shutterstock

INCD
Israel National
Cyber Directorate