INCD
Israel National
Cyber Directorate

ISRAEL NATIONAL CYBER SECURITY STRATEGY

2025

Foreword

By Gabi Portnoy
Head of the National Cyber Directorate

The October 7th attack on Israel and the ensuing "Iron Swords" operation highlight the fact that Israel stands at **the frontline of cyber warfare**, with cyberspace now a fully-fledged battlefield. Alongside physical combat operations, we faced extensive cyber-attacks from our enemies, particularly Iran and its digital proxy- Hezbollah.

In this era, where the digital space is integral to the daily lives of nations, organizations, and citizens, Israel stands at the vanguard of confronting cyber threats that challenge its national, economic, and social security.

Numerous attacks sought to disrupt and compromise daily life in both the physical and digital domains, across multiple sectors, government digital assets and critical national infrastructure, exposing vulnerabilities in the process, along with intense attempts to undermine the public spirit and trust, and malignly influence public opinion in Israel and worldwide. That said, the cyber warfare also highlighted effective solutions at the organizational, the sectoral, and the national levels.

We need to continuously improve our defenses against threats, for example, by advancing **"Cyber Dome" concept**, which provides a multi-layered, dynamic, and proactive defense system based on extensive data processing and advanced artificial intelligence capabilities.

The war has accentuated the fact that **the public** constitutes an integral part of the national defense apparatus.

Phishing attacks and attempts to collect sensitive information stress the need to increase **public awareness**. National cyber education is required to successfully address this challenge.

We have learnt that **cyber-terror** is not merely a local threat but a global one, requiring **a united response** against attackers emerging from every corner of the globe.

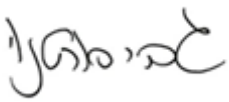
We are required to **function as one complete operational arm**, working jointly together- security agencies, government, the private sector, collaborating with regional and international community. The more we succeed in combining **innovation, public awareness, and regional and international cooperation**, the better we can protect Israel from future threats.

As one of the global leaders in startups and technological innovation, the State of Israel is fully cognizant of the fact that securing cyberspace is a **prerequisite for prosperity and national resilience**.

This updated strategy aims to **establish a clear vision and practical objectives for strengthening Israel's cyber resilience**. These include securing critical infrastructures and essential services, providing the market with access to defensive tools and services, implementing a national program for secure digital identification, establishing a more secure cognitive space from malign foreign influence, jointly managing defensive efforts, preparing the groundwork to prevent and address unexpected national digital crises, and lastly - investing in high-quality technological and human capabilities to contend with future challenges.

Realizing this vision will secure Israel's posture as a global technological and cyber power equipped to address present and future challenges posed by the cyber domain.

Sincerely,



Gabi Portnoy

Head of the National Cyber Directorate

AGENDA

Introduction.....6

National vision and founding principles.....16

Pillar One : Securing the National Cyber Space.....20

Chapter One: Safer Citizens and Stronger Businesses.....21

1.1 Objective One: Raising Awareness and Literacy Against Cyber Threats.....21

1.2 Objective Two: Accessible Services and Tools for the Economy.....22

1.3 Objective Three: Motivating Businesses to Strengthen Their Security.....23

1.4 Objective Four: National Plan for Secure Digital identity 24

Chapter Two: Safer Essential Services.....25

2.1 Objective One: Zero Significant Damage to Critical Infrastructure.....25

2.2 Objective Two: Ensuring Adequate Security in Essential Organizations.....26

2.3 Objective Three: Securing IT within Government and Security Agencies 27

Chapter Three: Spatial Security. 29

3.1 Objective One: Ensuring the Availability of the Online Space.....29

3.2 Objective Two: Strengthening the "Technological Supply Network".....29

3.3 Objective Three Securing Information Assets Holistically.....30

3.4 Objective Four: Resilient Public Mindspace to Malicious Foreign Influence.....31

Pillar Two : National Formation.....34

Chapter Four: Joint Security.....35

4.1 Objective One: Joint Management of National Defense Efforts.....35

4.2 Objective Two: Security via Advanced Technological Tools.....36

4.3 Objective Three: Implementation of the National SOC (NSOC).....37

4.4 Objective Four: National Response to Cybercrime.....37

Chapter Five: Cyber Surprise and Readiness for a Digital Crises 39

5.1 Objective One: Avoiding and preparing for Digital Surprises.....39

5.2 Objective Two: Effective National Digital Crises Management.....,.,.....40

Chapter Six: Threat Elimination.....41

6.1 Objective One: Response to Attackers.....41

Pillar Three : Developing Strategic Partnership and Future Capabilities.....43

Chapter Seven: Developing Cooperation and Partnerships.....44

7.1 Objective One: Developing Strategic Partnerships with Technology Companies.....44

7.2 Objective Two: Deepening Ties with Leading Cyber Partners.....45

7.3 Objective Three: Participation in Shaping International Etiquette.....46

7.4 Objective Four: Assistance to Friendly Countries 46

Chapter Eight: Capacity Building in the Face of Future Challenges.....47

8.1 Objective One: Developing Future Technologies and Capabilities.....47

8.2 Objective Two: Safe Adoption of Artificial Intelligence.....48

8.3 Objective Three: Development of a Skilled Human Capital.....49

Summary and next steps.....51

INTRODUCTION

The updated national cyber strategy was developed in the wake of the horrific October 7 attack and the subsequent "Iron Swords" war forced upon Israel. **These events mark a strategic and historic turning point that has mandated a complete reassessment of our national security concepts—including our national approach to cyberspace**. In this context, we ought to determine what might constitute a strategic surprise in the digital realm and how to prepare for it at the national level.

The insights and lessons learnt during this conflict, as well as insights from significant cyber incidents elsewhere in the world, have been incorporated into this document, which grapples with the unique characteristics and challenges of the cyber domain—challenges that differ significantly from those of conventional theaters.

The digital revolution of recent decades, culminating in the "Information Age," characterized by big data and advanced processing tools, has transformed the lives of individuals, how organizations conduct themselves, and how governments operate.

Cyberspace is constantly expanding and impinging on ever bigger chunks of every aspect of our lives; this is evident in fast-paced adoption of digital applications and products, substantial growth of remote work, and implementation of AI based on ever-greater computing power. Tighter integration of cyberspace with the physical domain, and the way people perceive reality, make it an inseparable part of the fabric of everyday modern life.

With the growing dependence of daily life on cyberspace, threats are also intensifying - in scope, pace, and sophistication. Hostile actors with diverse motivations, primarily ideological and economic, are launching attacks in cyberspace with broader scope and ever-more advanced techniques.

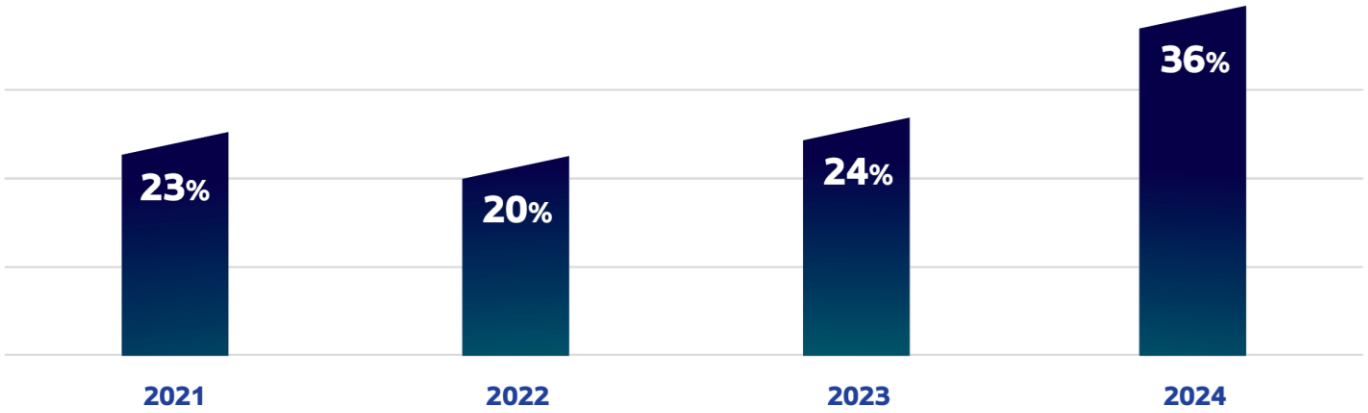
Cyber threats constitute a matter of national security to the Israeli economy. Israel is one of the most cyber-attacked countries in the world, reaching a peak during the "Iron Swords" war. Major attacks against the State of Israel tripled, including hybrid attacks combining multiple warfare dimensions (physical, kinetic, cognitive) in an attempt to gather intelligence and influence military efforts. **Malign foreign influence campaigns were particularly notable,** seeking to undermine trust in government institutions, erode the sense of personal security, and fracture social resilience.

Economic damage from cyber-attacks has increased dramatically in recent years. The global cost of cyber-attacks is estimated at $8 trillion - equivalent to the size of the world's third-largest economy. **In Israel, damage from cyber-attacks is estimated at approximately 12 billion NIS annually**. What's more, major cyber incidents are liable to undermine public trust in cyberspace and discourage citizens and organizations from fully utilizing the digital domain – potentially harming growth in the medium and long term.

While confronting these threats, **the Israeli cyber industry continues to flourish**, serving as an economic growth engine for the Israeli market. Investment in cybersecurity in 2024 reached a record 36% of total high-tech sector investments, a sharp rise compared to previous years (approximately 20-25% of total investments), despite security challenges. The innovation and

creativity characterizing the Israeli cyber industry is instrumental in securing the economy from escalating threats.

Percentage of investments in cyber out of total investments in Israeli Hi-tech sector



A National Cyber Directorate analysis based on data from the 2024 Annual Report on the Israeli high-tech ecosystem published by Startup Nation Central

The vital need to protect cyberspace, alongside technological developments, the growing threat landscape, and changes in attack objectives both domestically and globally, call for the national cyber security strategy to be updated to one that embraces the entire economy and all the security agencies, to create a broader, more sophisticated, and better integrated response.

This document presents Israel's national strategy for cyber security, building on the 2017 national strategy that defined the defense concept regarding attacks on the Israeli cyberspace.

The writing of this document and the strategic concept underpinning it were formulated by the National Cyber Directorate along with security agencies, in consultations with relevant government ministries, representatives of the various economic sectors, cyber experts from academia and industry, and by analyzing the strategies of leading cyber nations – driven by an acute awareness

that effective cyber security requires collaborative action at both national and international levels.

Accordingly, this strategy is aligned with other national digital data and AI strategies based on a holistic view of the digital domain.

The document presents the perception of cyberspace, the national vision for this domain, the principles for its implementation, the defined objectives and lines of action for governmental and national organization to better secure the economy, the main capability building efforts across various sectors, and the cooperation required to achieve these goals.

A national implementation plan will be derived from this National Strategy Document, targeted to be completed by the next three years, namely, until 2028. The implementation plan will define how the strategic objectives will be translated into an action plan, and will be executed through a national team combining government entities, security agencies, cyber industry representatives, and additional experts.

As cyberspace is dynamic by its nature, it will be only appropriate to update the strategy more frequently than others, and whenever new strategic shifts emerge.

Characteristics of cyberspace

Cyberspace is unique and fundamentally differs from other domains. As a global virtual space, it transcends physical boundaries and enables communication and movement of information without distance or time limitations. The speed at which information travels in this space enables immediate effect, both for beneficial uses and for propagating cyber-attacks and causing damage. Additionally, cyberspace characteristics allow attackers to

operate remotely with relative anonymity, which complicates identification, investigation, and law enforcement against attackers.

It should also be noted that users and owners of digital assets in cyberspace do not control production stages and operational aspects of digital applications and products they own or use, a fact that emphasizes the need for regulating responsibility at the national level.

The complex connectivity between computing systems and networks facilitate attacker accessibility by targeting supply chains composed of interconnected entities, organizations, and individuals, together creating a complex network of mutual dependency, where damage to a single point can spread and affect many other systems.

The tightening interfaces between cyberspace and the physical world, and between humans and machines are manifested in online control of the surrounding, from smart homes to autonomous vehicles, industrial systems and essential services. The risk of disruption to operational continuity in the economy, is growing, for example, through damage to critical and essential infrastructure such as power grids, water systems, banks, and hospitals. The emergence of emerging technologies, particularly Generative Artificial Intelligence based on Large Language Models (LLM), which are becoming accessible to the general public, makes it easier for attackers to master various attack capabilities.

An additional complexity of cyberspace lies in the fact that it is a shared "playground," where legitimate users operate alongside malicious actors using the same ICT infrastructure.

Furthermore, the boundaries between adversaries in this domain are blurring. For example, cyber-crime groups provide cyber-attack services to rogue states and terrorist organizations, while rouge states use cyber-attacks characteristic of criminal organizations for ideological or economic purposes. This blurring of boundaries requires a paradigm shift in response.

The rate of change in this domain is very high compared to other domains, and it continues to expand both in terms of the scope of systems and databases that need security, and in terms of deepening their integration with other domains.

As a relatively new domain, the domestic legal framework and norms of responsible state and organizations' behavior in the digital space are still under construction. The gap in detailed rules and the difficulty in reaching international binding norms, among other factors, challenge the ability to effectively deter attackers.

Israel's Unique Characteristics in Cyber

Israel is among the first countries to identify the need to elevate cybersecurity across its entire economy, and consequently, the need to establish a dedicated national response to cyber threats. The National Cyber Bureau established in 2012, which evolved into the National Cyber Directorate, operates according to several government resolutions, together with a complete national array of entities aimed to securing Israeli cyberspace, regulating the market, as well as developing and positioning Israel as a leading cyber nation.

Israel is known as a global leader in technological innovation. An impressive cybersecurity industry has grown within its developed high-tech industry, known for both its innovation and scope. This industry is based, among other things, on experienced cyber human capital and academic excellence, jointly

manifested in a fertile technological ecosystem that combines artificial intelligence and cybersecurity, with the second-largest investment volume in the world.

Additional characteristics that give Israel a comparative advantage in cyber security are the high level of connectivity between various entities in the Israeli ecosystem and the social commitment binding parts of the country together—particularly in the face of threats to national security. These enable the mobilization of experts and companies from the private sector to develop innovative defense solutions and provide mutual assistance to the economy. This high social commitment was expressed during the "Iron Swords" war, when many companies throughout the economy volunteered to assist in securing small businesses and mitigate cyber-attacks.

Conversely, as a relatively small market, Israel's influence on the international regulatory landscape alone is relatively limited, and consequently, there is an increasing need to develop international coalitions and take active part in professional global forums.

Despite the high level of digitization in the economy, there appears to still be a gap in awareness of cyber threats, particularly among the general public and small and medium-sized businesses, which are targets for attackers, both as direct victims and as vectors for attacking other organizations.

On the normative level, security guidelines have evolved organically, across various tiers, causing variations in obligations and authorities between sectors in the economy. For example, critical national infrastructures (hereinafter: "CI") are guided, in cybersecurity contexts, under the Security Regulation in Public Entities Law of 1998. The Privacy Security Law of 1981, particularly in light of the enforcement powers amendment enacted this year, regulates obligations throughout the economy that apply to holders of personal information

databases for privacy security purposes. Additionally, the Computer Law of 1995 establishes criminal offenses and civil torts.

Several government decisions in the cyber domain have been made in the past decade, including decisions to establish the National Cyber Directorate and define its roles, and the decision regarding the Government Cyber Security Unit in the Digital Israel Initiative.

Entities subject to sectoral regulation are required to operate according to guidelines from various regulators anchored in procedures, supervisory directives, CEO circulars, and additional normative sources.

Yet, there is a regulatory gap in cyber security for organizations essential to the proper functioning of the market and the society. This document aims to address this gap, similar to practices in other developed countries.

Cyber Threat Assessment

Israel is one of the most cyber-attacked countries in the world. The sources of threats to the State of Israel in this domain include **superpowers and rouge states**, with emphasis on Iran and its terrorist proxies, aiming at harming Israel's security, collecting sensitive information, spreading fear among its citizens, deepening societal divides, and undermining Israel's legitimacy, by influencing public opinion domestically and globally. As a democratic country and as a member of the Western Bloc, Israel is a target for hostile actors who abuse cyberspace as an arena for confrontation, competition, and influence.

The threat of **cybercrime**, as a rapidly growing global phenomenon, constitutes one of the significant challenges for Israel as well, particularly the growing number and variety of Ransomware and extortion attacks. Additionally, there is a threat from "hacktivists" operating of ideological motives to disrupt routine and proper functioning of the Israeli economy.

Another significant challenge lies in **internal risks**, where individuals with legitimate access to information and systems in organizations, such as employees, service providers, etc. might cause damage. This risk can materialize accidentally, through deception or negligence, for example due to breaches of security protocols, or alternatively, through data theft, sabotage, or espionage.

During the "Iron Swords" war, the number of attack groups targeting Israel doubled, and intense attempts were observed, primarily from Iran and its terrorist proxies, to damage critical infrastructure. During the war, a significant increase in attacks against citizens and small businesses was also observed, as well as attacks through supply chains as penetration vectors.

Foreign malicious influence operations on public opinion intensified to an unprecedented extent, becoming a significant threat to national security and social resilience. The purpose of these attacks is to undermine trust in government institutions, erode the sense of personal security through cyber-terrorism, deepen social divides, and damage community cohesion.

The proliferation of advanced attack tools, resulting from **strengthening ties between rivals, enemies, and criminals**, means an increased risk from advanced attacks and a greater potential for significant surprises. The ability to exploit security vulnerabilities easily and with unprecedented speed makes the threat landscape even more complex. This necessitates updating threat assessment and deepening knowledge of evolving offensive capabilities across a wider spectrum of cyber adversaries and rivals, in order to prepare for coming threats.

Israel's attack surface is growing, partly due to the implementation of modern communication systems with greater bandwidth, integration of IoT devices and applications interfacing with the physical domain, migration to the cloud, and

adoption of artificial intelligence technology. All these significantly increase the risk of cyber- attacks and potential damage.

Due to the fundamental difference between cyberspace and other domains, and the changes it has undergone, innovative paradigms are required as we formulate an appropriate response to this dynamic challenge.

NATIONAL VISION

A TRUSTWORTHY, AVAILABLE AND SAFE
DIGITAL SPACE THAT ENABLES THE BENEFITS
OF A THRIVING & ADVANCED WORLD

Founding principles

Active defense

Joint security

Resilience and
readiness for crisis

Leveraging innovation and
technological excellence

INCD
Israel National
Cyber Directorate

The foundational premise is that the security of cyberspace is a central and essential component for Israel's national security and prosperity. Given how this domain and the threats to it have evolved, and the proliferating interfaces with other domains, a vision broader in scope is needed, that encompasses the entire digital space. With this in mind, Israel has updated the national vision to:

A trustworthy, reliable and safe digital space that enables the benefits of a thriving and advanced world

The vision is built around three core complementary components: **trustworthiness** – the ability to rely upon the authenticity of information, content, and identities operating in the space; **availability** – ensuring continuous accessibility to digital services for all users; **safety** – comprehensive protection against cyber threats to ensure the functioning of the economy, including activities conducted in the digital space, digital assets, as well as user privacy, safety and security, from the level of the individual up to the national level.

Integration of all three components will enable everyone to securely enjoy the many advantages of the digital era, economic growth, technological innovation, and better quality of life for our citizens.

As stated, the national vision sheds light on the **digital** space expressing a broader scope that extends beyond cyberspace, one that encompasses all aspects of virtual life and the growing impact that technology has on society and culture.

Realization of the vision will be based on several core principles arising from how the domain is conceptualized and from Israel's unique characteristics. These principles will underpin our national cybersecurity defense actions and be expressed in each pillar of the strategy:

Joint Defense -The unique characteristics and complexity of the defense mission means that no one entity can bear the burden of this task alone, nor can it be easily divided. Accordingly, the guiding principle woven throughout the strategy is - defending together. The government has a central role in leading and regulating cyber security in the economy. Since the Government plays a key leadership and regulatory role in cybersecurity, collaborative defense calls for closer cooperation between government agencies engaged in cybersecurity to leverage their relative advantages and exercise their powers to the full by holistically working jointly together. Moreover, **cybersecurity is a whole-of-society effort**, meaning a shared mission for the government, security agencies, private sector, and citizens, alongside friendly countries and multinational corporations, in accordance with democratic values and accepted international norms.

Leveraging Innovation and Technological Excellence for Better Security - this principle reflects the comparative edge of Israel's technological ecosystem. Securing the economy can be achieved in part by adopting automated and artificial intelligence-based defense concepts (such as "Cyber Dome") and by making innovative security solutions for operational efficiency accessible.

Active Defense - this principle calls for a proactive approach to cyber security, early detection of intentions to attack, preemptive immunizing of the economy, and preemptive disruption of threats.

Resilience and Crisis Management This principle stems from the premise that digital crises are inevitable, and therefore, the national security must also be based on building a more resilient economy and rapid recovery capability. The October 7th attack underscored the threat of significant surprises – requiring preparedness for surprise in cyber as well.

The realization of this vision will be achieved via a broad defense apparatus, that adapts to the changing realities, and is deployed across several operational domains, detailed in the three pillars of the strategy:

First Pillar: Securing the National Cyber Space – describes what is required to protect the different types of assets, and in particular, creating tailored responses that factor in the unique characteristics of assets and their reciprocal influence on one another. This layer is divided into three parts: Safer Citizens and stronger Businesses (Chapter 1); More Resilient Critical and Essential Services (Chapter 2); and Spatial Security (Chapter 3), which focuses on securing the shared digital space from a cross-sectoral perspective.

Second Pillar: National Formation - describes the concrete organizational and operational concept on which the cyber security systems of government entities are based. This pillar is divided into three: Joint Security (Chapter 4), including the system of governmental defense system and operational collaborations required with the economy; Readiness for Cyber Surprises and Digital Emergency (Chapter 5); and Threat Elimination (Chapter 6).

Third Pillar: Developing Strategic Partnerships and Future Capabilities - this pillar is divided into two: Development of Infrastructure for Cooperation and Partnerships (Chapter 7); and Investment in Quality Capacity Building in Light of Future Challenges (Chapter 8).

Pillar 1:

Securing the National Cyber Space

Concerted efforts to protect the national cyberspace are designed to prevent harming of Israel's economy and national security and include closing digital, normative, and behavioral gaps, and prioritizing essential services, businesses and citizens.

INCD
Israel National
Cyber Directorate

In this pillar, securing the national cyberspace is broken down into three components, with dedicated and tailored solutions for each. The first component is **citizens and small and medium-sized businesses** which constitute the largest and most vulnerable layer in the Israeli economy, both as direct targets and as entry vectors to other organizations (as part of the supply chain). The second component is **essential services**, including critical infrastructure and organizations providing necessary services, damage to which could cause severely compromise the functioning and security of the State of Israel and its residents. The third component is **spatial security**, referring to the shared public cyberspace. Defense here will focus on threats arising from the interface between virtual space and physical and cognitive domains, strengthening the security of online infrastructure, protecting State information assets, and countering foreign influence operations targeting public perception.

1. Safer Citizens and Stronger Businesses

Supporting citizens and businesses for a safer cyber space

1.1 Objective One: Raising Awareness and Literacy Against Cyber Threats

Maintaining strong awareness of threats and how they manifest themselves, and adopting safe and cautious online behavior are prerequisites for preventing cyber-attacks and minimizing the damage they cause. Israel will invest in strengthening awareness about cyber threats, knowledge of existing defensive measures, and response options, designed to drive cultural and social change

that encourages prudent behavior in cyberspace by citizens and organizations in Israel.

Public awareness will be raised through extensive public education, both ongoing and in response to specific incidents; publishing alerts and recommendations about vulnerabilities and cyber threats menacing the economy; expanding the variety of courses and educational content made accessible to the public; and providing relevant information on security tools and cyber services. Enhanced awareness will be tailored to the relevant target populations, with emphasis on business communities, early childhood, , and digitally challenged population. These initiatives will be based, where possible, on existing educational frameworks, social initiatives, NGOs, local authorities, relevant business and professional chambers and associations, all with Government encouragement.

1.2 Objective Two: Accessible Tools and Services for the Economy

Assisting with effective response to cyber-attacks, the National Cyber Directorate operates the National Computer Emergency Response Team (CERT) designed to help organizations deal with cyber incidents in the civilian domain in Israel. CERT operates a helpline – 119 hotline and an online option – the address and first responder for the public to report suspected cyber-attacks to immediately. The helpline is staffed 24/7 and provides an initial response to citizens and organizations based on the severity of the attack, the damage potential, and the characteristics of the incident. Accordingly, the center

provides preliminary guidance on how to handle incidents and instructions for strengthening defenses.

Number of reports received annually by the 119 hot-line

In order to provide the public with a better service, a national system will be established for reporting of all types of cyber-attacks, with user-friendly online access that ensures privacy protection. This system will help increase report rates of cyber-attacks, providing a better and more detailed picture of the situation countrywide.

Israel will also leverage its technological strengths to improve security in the private sector by providing better access to basic cybersecurity tools and services for scanning and identifying vulnerabilities and by providing early warnings to the economy, including through a national portal.

1.3 Objective Three: Motivating Businesses to Strengthen Their Security

Israel will motivate the private sector and civil sector to voluntarily strengthen their cyber security and promote the following measures:

a. Developing the cyber insurance market - Cyber risk insurance, besides compensating for residual damage, may also promote better resilience across the board due to the prerequisite requirements of the insurance companies,

similar to vehicle or real estate insurance. Israel will promote awareness among small and medium size businesses of the benefits of cyber insurance, and among the insurance market as a tool for increasing resilience.

b. Encouraging organizations to consume cyber services and products similar to practices in other developed countries, while considering incentivizing of businesses and providing with relevant knowledge, including through: updated databases of responsible service providers in cyber security; reassessment and promotion of the certification of professionals in the cyber field; and promoting the awarding of government resilience badge to companies that meet appropriate cyber security requirements.

1.4 Objective Four: Developing a National Plan for Secure Digital Identity

Digital identity is a method that uniquely identifying a person by a combination of digital characteristics and attributes that distinguish that person from others. To verify users' identities, various biometric characteristics and identifiers could be used.

A secure digital identity is a significant component in digital domain security, as it enables citizens and organizations to access and consume digital services reliably and securely, both as recipients of services from the government and as identified users interacting with suppliers and companies in the economy.

Digital identity theft currently constitutes the most common breach pathway in cyberspace. According to publications, about a fifth of cyber-attacks reported globally are related to identity theft or the use of fictitious virtual identities. The increasing use of advanced forgery capabilities (deep fake) amplifies the risk. Consequently, reliable digital identification could prevent undesirable phenomena, such as the use of fictitious or stolen identities, dissemination of

fake news, efforts to influence Israeli citizens, fraud, and even terrorism and organized crime.

Israel will promote the formulation of a comprehensive national policy that defines a normative framework for assuring the digital identity of users and organizations, using user-centric principles. This policy will clarify the government's role regarding standards and establishing national mechanisms for digital identification in the private market, in order to encourage and maximize online services. The policy will address privacy protection, accessibility by all segments of the population, and economy-wide interoperability of the means of identification. The policy will address the need to update the means in accordance with technological developments in identification methods and changes in attack TTPs.

2. Safer Essential Services

Advanced defense of the critical and essential services to ensure economy continuity, national security and residents' wellbeing

2.1 Objective One: Zero Significant Damage to Critical Infrastructure

Israel has taken a unique approach. Under the Security Regulations Law, a list was defined of entities that constitute critical national infrastructures requiring enhanced cyber security, given their importance for the continued proper functioning of the Israeli economy. The ISA and the National Cyber Directorate monitor and guide these critical infrastructures using a unique methodology that has thus far yielded the desired results. The State of Israel will continue to place national emphasis on protecting these entities. As threats evolve, the methodology for securing such organizations including defense industrial base

organizations, will be updated with an expansive outlook that anticipates emerging threats, while instilling principles of preparedness for surprises, diversification of security measures, advanced scanning and tracking of attackers, and the creation of a real-time situational awareness of these entities. Rigorous security of the supply chains of the critical infrastructure entities will also be addressed in order to reduce their attack surface.

2.2 Objective Two: Ensuring Adequate Cyber Security in Essential Organizations

Many organizations in the national economy provide essential services to the general public and to a large number of businesses. A breach in these organizations is liable to impair the proper functioning of the State, society, and the Israeli economy. Unlike the critical infrastructures, that are regulated under the Security Regulations Law, this layer of essential services organizations is not currently adequately regulated in terms of cyber security.

While some regulators have imposed security obligations on these organizations under their sectoral regulatory authority, gaps remain in both powers and enforcement of cyber security across the various sectors. Similar to practices in developed countries, the government intends to enact a dedicated law that regulates national cyber security efforts. The law will define which organization qualifies as an "essential organization" in terms of cyber and stipulate the obligations applicable to them – the foremost being the obligation to manage cyber risks effectively and the obligation to report certain cyber-attacks. In addition, the proposed national legislation will define the powers of the sectoral regulators to equip them with the appropriate tools to supervise and enforce the implementation of the provisions of such law by these essential organizations.

2.3 Objective Three: Securing the Digital Infrastructure within Government and Security Agencies

Governmental ICT infrastructures receive cyber security services from the National Digital Directorate, through the Cyber security Unit (hereinafter: "Yahav"), which is guided by the National Cyber Directorate. All of these entities deploy security standards, provide guidance to employees, and ensure oversight as a function of their role.

Governmental infrastructures protection efforts will aim to maintain high levels of security for governmental ICT systems, by employing skilled and up-to-date technological personnel, and by efficient processes and rapid procurement of cyber security tools and services when the operational need arises.

The Government will incorporate appropriate cybersecurity requirements in government tenders and contracts for the products and services it procures, starting from the planning and initiation phase. This will embed cybersecurity broadly across products and services throughout the government's supply chain while inspiring the market to consume secure products and services.

Government ministries have begun phased migration from governmental IT infrastructures to a public cloud located inside Israel (the "Nimbus" project), designed to preserve data sovereignty, streamline work processes and services for the economy, and improve cybersecurity.

Israel will work to integrate advanced cyber security solutions in the public cloud, develop skilled human capital, and securely implement artificial intelligence tools within government ministries, in order to better secure the governmental IT infrastructures and leverage optimally the benefits of the cloud.

In addition to government ministries, security agencies that work to defend the country and its citizens operate classified ICT and OT systems essential for their operational and routine activities. Naturally, such infrastructures require the highest level of security, to safeguard national security, prevent disruption and information leakage, and ensure smooth operations and availability. The office responsible for security within the defense systems provides the Ministry of Defense and the defense industry with guidance in this field. Security agencies will continue to work to strengthen their own high level of security as well as that of their supply chains to confront the evolving threat.

3. Spatial Security

Securing the common digital infrastructures for a safer online environment that facilitate prosperity

3.1 Objective One: Ensuring the Availability of Digital Space

The digital space is an integral part of the foundational framework that enables modern life, a sturdy economy, and well-being. Protecting this space begins with ensuring its very existence and availability amidst threats such as cyber-attacks, physical damage, technical malfunctions, human error, and other risks.

Israel will assess and map the risk factors to the internet and will ensure continuity of service by both establishing robust security measures and developing redundancies across a variety of services. Given the global and decentralized nature of the internet, these measures require close cooperation between the public and private sectors, as well as between Israel and its international partners.

3.2 Objective Two: Enhancing Broad Resilience through Strengthening the "Technological Supply Network"

The term "Technological Supply Network" conveys a broad, cross-sectoral economic perspective that emphasizes the unique impact of the key nodes in the provision of ICT services on securing cyberspace. This network includes the infrastructures, services, and digital products upon which so many in the economy depend on to manage their daily business routine.

Entities within the technological supply network are of particular importance—due to the reliance on their services and products, their widespread pervasiveness in the economy, and the fact that they might serve as entry vectors to the companies they support. At the same time, this wide accessibility carries the potential to strengthen resilience across the board, through targeted and efficient investment.

Israel will work to ensure up-to-date mapping of the entities that form part of this technological supply network and enhance their cyber security. In line with global trends, Israel will work to bolster the security of digital services and products by shifting part of the burden of mitigating cyber risks from end-users to those with a comparative advantage i.e., system operators and providers of digital services and products. To this end, a range of policy measures will be explored, that enable safer digital products and services without needlessly hindering technological innovation.

In this context, Israel will develop a framework for mandating security, technical, and methodological requirements in the provision of IoT products, similar to international standards and the regulatory steps taken in the European Union (Cyber Resilience Act) throughout the product lifecycle. To mitigate security vulnerabilities, Israel will promote the implementation of a "Secure by Design"

and "Secure by Default" policy within its development industry—in collaboration with both industry and academia and via international cooperation.

To ensure safe software throughout the product lifecycle, INCD will continue to operate and develop the national Vulnerability Disclosure Program that encourages responsible detection of vulnerabilities in software and systems, reporting and classifying them according to globally recognized standards (CVE) across all types of technology and sectors.

In addition, the state will examine various incentive mechanisms to facilitate the implementation of appropriate protective solutions for end users by internet service providers.

3.3 Objective Three: Securing Information Assets Holistically

In the information age, beyond securing technology itself, it is also vital to safeguard our information from the growing scale and sophistication of the threats. The digital space encompasses various types of information and databases (such as personal, business, secret information, and more). The growing use of cyberspace and the implementation of artificial intelligence significantly increase both the volume and dispersion of information—that is, the overall attack surface.

Malicious attackers are increasing able to curate and exploit unclassified information in order to cause physical and economic damage—for example, by stealing intellectual property, trade secrets, and exploit financial assets from various data bases; by engaging in espionage activity; by collecting sensitive data about citizens; and by influencing public perception through the aggregated collection of information from multiple databases and fusing them.

During the "Iron Swords" operation, both classified and unclassified data collected by the enemy from diverse sources—were used in attacks of a security–physical–psychological nature.

The security of information repositories and data is currently regulated primarily by privacy protection laws and by legislation aimed at safeguarding commerce and national security. The Privacy Security Authority has a key enforcement role in cases of privacy violations, following enhancement of its enforcement powers legislated only this year. Nevertheless, a complementary perspective is required—one that examines the security risk posed by the aggregated collection of information.

To ensure a comprehensive protective response to the growing scale and pace of threats, the State of Israel will work to identify vulnerabilities and eliminate them; to raise public awareness of the risks associated with careless possession and sharing of information; and to conduct a governmental review of the methodology used to classify information in organizations that hold sensitive security, technological, economic, or political data, with appropriate consideration given to hybrid threats.

3.4 Objective Four: Creating More Resilient Public Mindspace to Malicious Foreign Influence

With the evolution of media—and especially the expansion of social platforms that allow many-to many communication and rapid sharing of information to the masses—Foreign Malicious Information Manipulation and Interference Campaigns have proliferated. The increasing use of generative artificial intelligence technology by adversaries further magnifies the scale, speed, sophistication, and impact of this phenomenon exponentially.

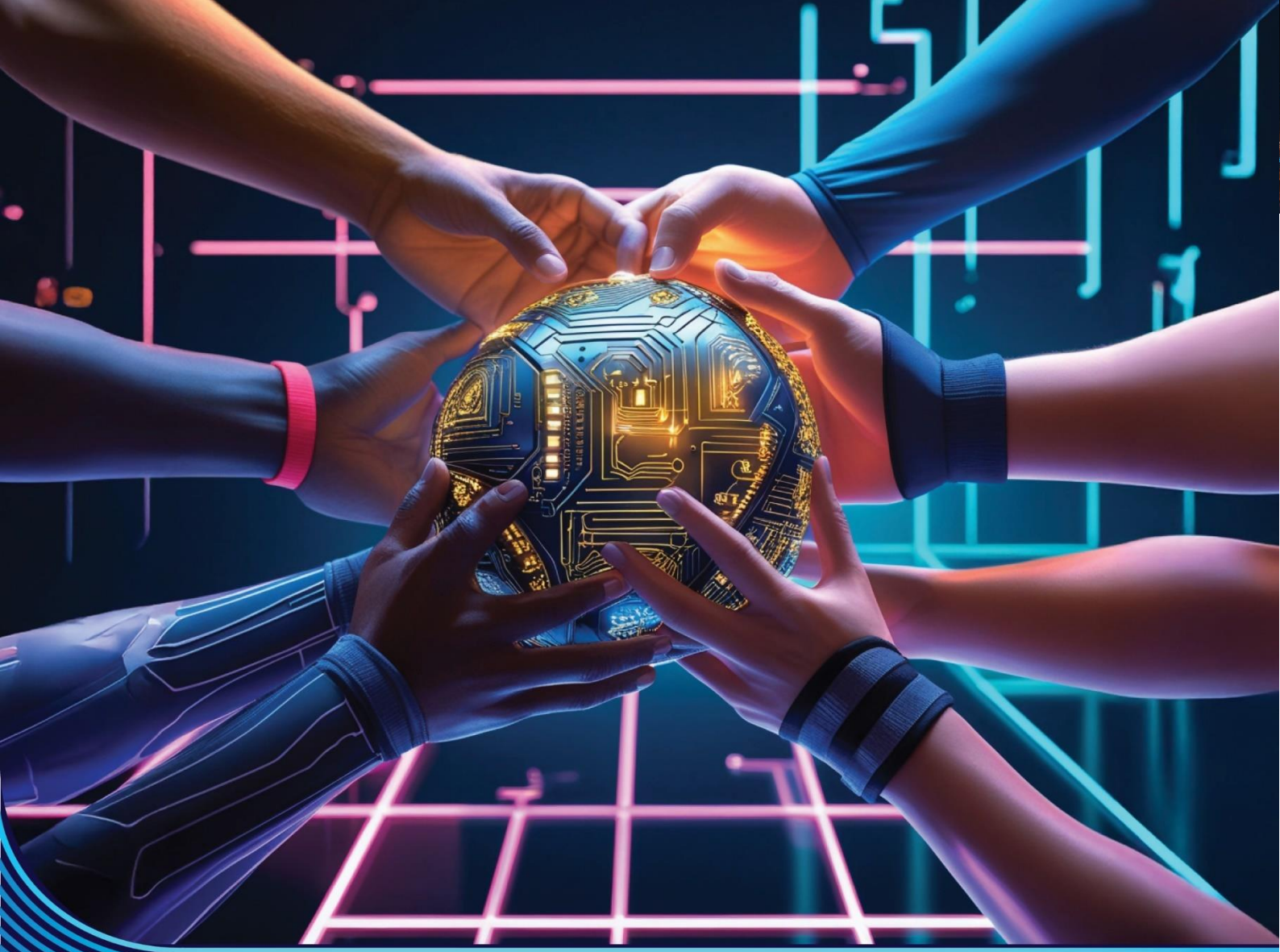
The October 7 attack and the ensuing war, as well as other incidents in the world, demonstrated that foreign malicious influence, combined with social media and artificial intelligence technologies, has the potential to compromise national security, social resilience, democracy, and individual sense of security. Some of these operations are designed specifically to undermine public trust in the digital space itself. These efforts were directed at influencing global public opinion and decision makers regarding the conflict.

Israel, like other leading countries and international organizations, recognizes the threat of foreign malicious influence on public mindset as a severe and growing threat. Protecting the public and countering such malicious influence attempts is set against the values of freedom of expression and freedom of choice for Israeli citizens. Therefore, in a democratic country like Israel, any state involvement must be carried out with caution, transparency, and under appropriate oversight.

During the "Iron Swords" conflict, security agencies, government ministries, and civilian organizations acted to detect malicious foreign involvement that violated the laws and terms of use of online platforms, and took steps to remove such malicious foreign content that endangered social resilience. In addition to such efforts, ways must be explored of **addressing the threat at an earlier stage while relying more on technological indicators rather than on content.**

Alongside continued efforts to monitor and detect malicious content involving foreign adversaries, Israel will deepen its dialogue with other countries and with social platforms to encourage efficient, independent, and rapid filtering of malicious content that violates terms of use or the law.

Israel will also promote the establishment of a national joint task force to foster reliable situational awareness of foreign malign influence efforts in the digital space, and develop an integrated mechanism for a holistic, balanced, and controlled response to the threat of foreign malicious influence and interference. Furthermore, Israel will work to bolster public education and awareness—from early childhood onward—to help citizen recognize the phenomenon and ways of countering it.



Pillar 2:

National Formation

The blurring boundaries between rouge states, criminal organizations and terror organizations that collaborate and share knowledge poses a challenge to law enforcement and security agencies roles and responsibilities. This requires a change in the *modus operandi* of governments and between governments, and calls for tightening collaboration and working jointly to thwart attacks and disrupt adversaries.

INCD
Israel National
Cyber Directorate

4. Joint Security

Shifting from Cooperation to Collaboration, working Jointly to thwart and disrupt adversaries

4.1 Objective One: Joint Management of National Defense Efforts

It is of paramount importance that government agencies responsible for various aspects of cyber security work hand-in-glove in an integrated manner, both routinely and in crisis. Consequently, a holistic and collaborative view of cyber assets and national interests is required to guide national security efforts.

Furthermore, given the evolving nature of the cyberspace and the geopolitical trends that bring adversaries and enemies (rouge states, criminals and terrorist organizations) closer together, intelligence collection efforts and research capabilities needs to be expanded. Gaining a broader scope will allow a deeper understanding of the evolving threat landscape, thereby enabling better preparedness for advanced threats and more effective security for the Israeli economy.

In Israel, an operational cyber security coordination mechanism is in place, established to strengthen cooperation between security agencies. This mechanism has proven effective in coordinating issues spanning organizations and in delivering a concerted response to complex cyber

incidents during normal operations—and even more so, during the "Iron Swords" fighting.

Israel will further enhance this mechanism by shifting from a model of inter-agency cooperation to one of joint action: in operational efforts, in capacity building, and in research efforts.

In addition, a cross-sectoral government coordination mechanism will be established for sharing information on cyber threats. Composed of the sectoral regulators — including representatives from the sectoral cyber units, the Cyber Directorate, and the relevant law enforcement agencies — it will create a common situational awareness, coordinate responses to ongoing incidents, and facilitate joint efforts to further systemic solutions.

National defense efforts will be directed on the basis of a cyber resilience index. Such index will enable the Government to identify security gaps within various sectors, improve defense capabilities, and effectively counter future attacks. Israel will develop a comprehensive measurement and evaluation mechanism that reflects a coordinated and pertinent situational report at the sectoral and national levels, both in terms of resilience and in terms of recovery potential.

4.2 Objective Two: Security via Advanced Technological Tools

Israel will adopt an approach that leverages technological excellence. To this end, Israel is implementing an advanced national techno-operational concept named the "**Cyber Dome**." Already in the preliminary operation stage, it will embrace a whole host of advanced capabilities and offer an across-the-board solution for a swifter response to the threats.

The “Cyber Dome's” systems will fuse and correlate various types of data, incorporating AI to create a holistic snapshot of all imminent attacks and threats to the economy. “Cyber Dome” will leverage intelligence to research and classify threats, and will utilize a variety of active defense tools to disrupt attacks, investigate hunt threats, and provide organizations with early warnings regarding potential attacks and actionable information.

4.3 Objective Three: Implementation of the National SOC (NSOC)

National holistic situational awareness is a prerequisite for effective national cyber defense. National holistic situational awareness is a prerequisite for effective national cyber defense The State of Israel will press ahead with a National Security Operation Center (NSOC) that consolidates information from the sectoral centers, which in turn will facilitate dedicated input for each sector. The NSOC will be fed with relevant data from existing collection sources in the economy and from the “Cyber Dome” systems, analyze the totality of the information, and recommend preventive measures as appropriate. Israel will continue to establish sectoral SOCs as necessary, and formulate SOPs and common terminology among the various SOCs.

4.4 Objective Four: National Response to Cybercrime

Cybercrime exhibits unique characteristics, including identity theft, sophisticated frauds, ransomware incidents, etc.

Israel will work to establish an effective framework that integrates the capabilities and powers of the security and enforcement agencies, while

ensuring information sharing among them—mainly the Israel Police and the national cyber directorate.

The framework will operate on three levels: building resilience (preventing attacks and providing security); managing attacks (containment, reporting, and recovery); and conducting enforcement and disruptive actions against the attacker in cooperation with foreign law enforcement agencies wherever possible. To this end, the powers of the investigation and enforcement agencies will be reviewed in order to adapt them to the rapidly evolving cyber threat landscape.

In combating cybercrime, the State of Israel will focus efforts on thwarting ransomware incidents, globally seen as a key contributor to economic damage from cyber- attacks, with estimated annual domestic costs at around one billion NIS.

The Government of Israel advocates not paying a ransom in order to thwart the attacker's intent, as payments do not guarantee recovery nor immunity from future attacks.

In the international arena, Israel will continue to serve as an active partner to the international Counter Ransomware Initiative (CRI) led by the United States, with dozens of other member states, which takes a multidimensional approach to combatting ransomware attacks.

Under this initiative, Israel, in collaboration with the United Arab Emirates are developing a platform for sharing information on ransomware attacks ("**Crystal Ball**"). The platform enables the transfer and joint analysis of

information on ransomware incidents among participating countries, so that all could mutually benefit from the shared knowledge, capabilities, and tools to contain ransomware attacks.

5. Cyber Surprise and Readiness for a Digital Crises

Minimizing surprises, recovering quickly and managing national digital crises effectively

5.1 Objective One: Avoiding and preparing for Digital Surprises

History demonstrates that major unpleasant surprises happen despite efforts to prevent them. The attack on Pearl Harbor, the "Yom Kippur" War, the September 11 and the October 7 terror attacks serve as reminders.

Therefore, it must be assumed—as a strategic axiom—that a significant surprise originating in the digital domain is a plausible scenario and must be anticipated. The human factor plays a critical role both in the advent of an unpleasant surprise and in management of the subsequent crisis. Cognitive and psychological biases, tend to underestimate the plausibility of a strategic surprise. These biases are due in part to difficulties in accurately assessing the magnitude of an event in advance, uncertainty about the timing, or attributing of causes steeped in misconceptions.

Preparations for such surprises include developing methodology and implementing processes that anticipate unexpected events. Such readiness should be achieved in two levels: First, the State of Israel will seek to reduce the likelihood of a cyber surprise by establishing a national team to periodically formulate surprise scenarios, assess changes in the domain, and identify vulnerabilities.

second, realizing that surprises can have cascading effects, Israel will work to embed principles for building an economy that is more resilient to digital crisis—through diversifying security measures, employing deception, developing next generation solutions, and by establishing rapid recovery capabilities to minimize damage and restore operation.

5.2 Objective Two: Effective National Digital Crisis Management

Israel unfortunately is accustomed to managing emergency situations in the context of war and terror. However, a national crisis can also result from a widespread cyber-attack or a significant failure in the digital domain that is not necessarily related to a military emergency.

In wartime, well-established mechanisms exist for declaring and managing emergencies, including measures to tackle associated cyber incidents. However, an emergency triggered by a cyber event might exhibit different characteristics—most notably, a rapid escalation that affects the civilian domain extensively and in a very short time.

Israel will establish a dedicated team, including members from the National Emergency Authority (Rachel) and other security agencies, that will define and propose a national response to a digital emergency. The team will map the needs relating to the national digital emergency management and work to establish the mechanisms, resources, and authorities required for this purpose.

6. Threat Elimination

Israel will take creative joint action to disrupt cyber adversaries, using various tools and capabilities

6.1 Objective One: Response to Attackers

Advanced cyber-attackers—whether state-sponsored, terrorists or criminals, challenge Israel's national interests and require an added response layer at the national level and require an added response layer at the national level: while previous efforts sought to enhance resilience in the cyber domain (i.e., preventing attacks and mitigating their impact after the fact), the need now is also to confront attackers in order to disrupt their malicious activity and deter them.

This additional layer of the national response should be implemented by means of a campaign that leverages the full range of national tools and capabilities—both retrospective enforcement mechanisms and

preventive measures—to actively confront significant cyber attackers. This campaign is complementary to and meshes with the efforts described in previous chapters, constituting yet another component to be developed within the comprehensive national cyber security strategy.

Israel will pursue a proactive approach creatively integrating its technological, intelligence, security, diplomatic, and legal tools to deter attackers by imposing costs, disrupting, and by neutralizing their operations. This approach includes formulating a policy of deterrence and attribution, developing an operational concept, and establishing mechanisms for knowledge sharing and coordinated action.

Given the inherently international nature of the cyber domain, effective disruption requires information sharing and joint action with friendly nations, in accordance with accepted norms and the rules of international law, with the aim of reducing the threat posed by cyber attackers.

Pillar 3:

Developing Strategic Partnerships and Future Capabilities

The evolving complexity, the accelerated change, and the global nature of the cyber domain necessitate the continuous development of national and international collaborations, investment in innovation, and the cultivation of skilled human capital as leverage to face off future challenges.

INCD
Israel National
Cyber Directorate

7. Developing Infrastructures for Cooperation and Partnerships

Israel will work to establish strategic partnerships to promote national and global security

7.1 Objective One: Developing Strategic Partnerships with Technology Companies

Global technology giants possess valuable expertise and have a major impact on the cybersecurity of nations, helping to prevent, respond to and recover from cyberattacks. The importance of Israel's ties with these companies in enhancing economic resilience and advance national interests becomes increasingly apparent in light of the ever-growing scope of cyber threats. As a nation with an innovative cyber industry, skilled human capital, and academic excellence, Israel may be a valuable asset to these technology companies and as a source of cyber expertise that will contribute to national security. Israel will therefore develop strategic partnerships with domestic and global technology companies in order to promote the design and development of next-generation security solutions at the national and international levels, implementation of innovative Israeli defense solutions, exchange of knowledge to build resilience, encouragement of authentic discourse on social networks preventing malicious foreign influence, incitement, and terrorism, and the promotion of a "Security by Design" approach for digital products as well as for systems widely used in Israel and around the world.

7.2 Objective Two: Deepening Ties with Leading Cyber Partners

Due to the inherently global nature of cyberspace, an operational need exist to develop and nurture reciprocal relationships with counterpart government agencies and foreign security and law enforcement organizations. Such relationships may encompass information exchanges, streamlining policy, joint investigations and operations, and even joint R&D. Israel receives and shares indicators of compromise and relevant information with dozens of countries worldwide, and participates in various regional and international forums dedicated to sharing best practices, establishing standards, and norm-setting.

Israel will continue to promote and strengthen its bilateral and multilateral cooperation in several focal areas, including intelligence sharing for real-time alerts, dissemination of information about common vulnerabilities and coordination with manufacturers to address them, combatting foreign influence operations targeting public perception, sharing best practices, effective enforcement against cybercrime, pursuing various cyber diplomacy initiatives in the national interests, promoting standardization, and developing advanced regulatory frameworks.

Moreover, the State of Israel will strive to strengthen its presence and influence in international organizations such as the OECD, INTERPOL, and others, and will continue to initiate and develop cyber security cooperation in regional frameworks, such as the Abraham Accords nations and friendly countries in the Mediterranean basin, in order to improve security and promote advanced cybersecurity technologies.

7.3 Objective Three: Participation in Shaping International Etiquette

As a partner to international dialogue seeking to shape responsible behavior in cyberspace, Israel aims to influence global cyber security policies**,** including through its activities at the United Nations. This involvement becomes particularly urgent in light of emerging challenges such as foreign malicious influence on public opinion, the fight against cyberterrorism, efforts to abuse artificial intelligence and offensive cyber tools, and the growing prevalence of cybercrime executed as "crime as a service".

Israel recognizes the importance of promoting confidence-building measures among states as a foundation for international cooperation. Further efforts will be directed toward advancing and coordinating internationally agreed standards on various issues such as securing the cyber supply chain, enhancing the security of digital products, and safeguarding AI-based technologies, considering that norms in these areas will ultimately be shaped in the international arena.

7.4 Objective Four: Assistance to Friendly Countries

Israel is committed to sharing relevant knowledge and information with its allies and will continue to assist friendly nations in the event of a national cyber crisis. Israel will promote efforts to build cyber capacity by sharing Israeli cyber practices and solutions, and by leveraging regional and international development banks and institutions. Israel's efforts advance its foreign policy objectives while simultaneously enrich both the global knowledge and the Israeli experience in building resilience and effective response.

8. Capacity Building in the Face of Future Challenges

Maintaining a leading posture at the forefront of cyber security by nurturing scientific technological excellence

8.1 Objective One: Development of Future Technologies and Capabilities

Assuring Israel's future capabilities depends on the country maintaining its leadership at the forefront of global innovation, including in regard to emerging technologies and the security measures against the threats that might arise from abusing them.

Presently, Israel is home to several integrated centers of excellence in cyber security across various domains such as transportation, industry, biometrics, and artificial intelligence. These centers foster the development of innovative cyber security solutions.

Rapid technological progress and evolving threats raise the need for innovative development of the "next-generation" cyber security solutions. Israel will promote joint R&D efforts focused on delivering cyber security solutions for emerging technologies and on anticipating future trends.

With the technological landscape and corresponding threats evolving at an ever- faster pace, Israel will put processes in place to monitor and prepare for the development of technologies that dramatically alter the cyber security environment. The State of Israel will lead these efforts in close cooperation with academia, security agencies, and industry, with a particular focus on applied research and development that directly supports national defense.

Furthermore, Israel intends to expand the activities of its centers of excellence and laboratories in collaboration with the broader ecosystem, making them more accessible to the private sector, sharing knowledge gained and solutions developed in these labs for the benefit of companies domestically and internationally.

8.2 Objective Two: Safe Adoption of Artificial Intelligence

Generative Artificial Intelligence technology bears great potential to enhance cybersecurity by enabling faster vulnerability detection, shortened forensic investigations, processing of various types of data, cross-referencing and contextualizing information, etc.

At the same time, artificial intelligence might be exploited by adversaries to conduct more sophisticated and targeted attacks, reduce the time required to exploit vulnerabilities, launch extensive influence operations, "poison" models with inaccurate data, and bias decision-making outcomes.

Israel will pursue the safe adoption of artificial intelligence technology within the economy based on four main components:

- Securing AI systems from cyber threats throughout their entire lifecycle by conducting research and by developing methodologies for securing algorithms, high potency computing power systems, as well as by enhancing the National AI Laboratory for Applied Research in this field; the outcomes of this research will facilitate the development of methodologies that can be applied throughout the economy.
- Developing AI based cyber security mechanisms to improve the capacity to monitor, detect, and identify attackers and cyberattacks, analyze attack patterns, and develop predictive capabilities that support cyber security efforts.

- Research and develop measures to protect from adversarial AI.
- Secure implementation of AI tools in government, in order to streamline processes and improve services for citizens, while adhering to safety protocols that guarantee the reliability and availability of these services.

The insights gained from these initiatives, combined with increased awareness, development of dedicated solutions, and establishment of principles of defense, will enable the secured integration of AI in government systems and throughout the broader economy.

8.3 Objective Three: Development of a Skilled Human Capital

High-caliber technological human capital is critical to the success of Israel's high-tech sector, and the cyber industry specifically. The demand for skilled professionals in cybersecurity is growing in Israel and worldwide. In order to meet the level of cyber security required to counter increasing and emerging threats, Israel needs to vigorously expand its pool of competent cybersecurity and AI professionals, integrating populations currently underrepresented in the field.

To this end, Israel will undertake several initiatives:

It will expand entry opportunities into the world of cybersecurity by creating avenues for underrepresented populations in these professions, while removing obstacles specific to the various groups and mobilizing all relevant stakeholders- parents, teachers, school principals, local authorities, the Ministry of Education, and the Military, among others. Emerging technologies, including AI, will be incorporated in special programs. This initiative brings added value to national interests, particularly social inclusion and mobility, and will be implemented in a coordinated manner with a broad national vision.

Additionally, Israel will establish a holistic and synchronized continuum of training by expanding educational programs starting in elementary and middle schools, by broadening specialized programs in advanced studies in cybersecurity and artificial intelligence, and by encouraging individuals with cyber skills to pursue academic research in these fields.

Finally, Israel will work to break the "juniors' barrier"—the lack of initial experience in the cyber industry that often deters employers—by encouraging employment of wounded veterans from the "Iron Swords" conflict who have graduated from cybersecurity programs, in entry-level roles in government and industry, enabling them to gain experience and develop professionally.

The Israeli Cyber security Strategy is a national strategy, formulated according to the powers of Government resolution and in consultation with security agencies, government ministries and experts from various disciplines. Its implementation depends on the concerted action of various government entities, the broader economy, and international partners.

Given the dynamic nature of cyberspace, the national cyber security strategy may require timely updates, in response to significant developments and changes in the cyber domain, including changes in computing power, shifts in the human-machine interface (bio-convergence, robotics, etc.), and major geopolitical or regulatory changes.

To bring the strategy to fruition, a concrete implementation plan will be developed jointly to serve as a roadmap for its execution. Various government agencies will be entrusted with the overall implementation, coordinated by the National Cyber security Directorate.

Optimal implementation will enable the establishment of an advanced, reliable, available, and secure national digital space that will facilitate and accelerate economic prosperity for the State of Israel and enhance the well-being of its citizens.

***

The National Cybersecurity Strategy was written at the National Cyber Directorate by the Strategy and Policy Division team: Head of the Strategy Center, Yosi Aviram; Senior Director of Policy and Governance, Miri Zilberstein; Head of Regulatory Policy, Ayelet-Chen Cohen; under the guidance of the Senior Director of Strategy and Policy, Roy Friedman.

The advisory team within the National Cyber Directorate included the Senior Director of Technological Innovation, Dedi Gertler; the Head of the Active Defense Department, Yuval Sinai; Mr. Avner Ben-Efraim; the Head of the Intelligence Division; and the Head of the Communication Infrastructure Defense Center, Gil Engel.

Acknowledgement and heartfelt thanks to numerous senior Professors, cyber researchers, private sector experts, senior executives from the Cyber Directorate, government ministries and security agencies, whose contribution was significant and greatly appreciated.

INCD
Israel National
Cyber Directorate