SEPTEMBER 2017

ISRAEL NATIONAL CYBER SECURITY STRATEGY
IN BRIEF

STATE OF ISRAEL
PRIME MINISTER'S OFFICE
NATIONAL CYBER DIRECTORATE

Vision and Objective

The government of Israel has set a vision for Israel to be a leading nation in harnessing cyberspace as an engine of economic growth, social welfare and national security.

Israel national cyber security strategy is, first and foremost, a means of realizing the Israeli cyber vision by keeping cyberspace safe and by confronting the various cyber threats, in accordance with the country's national interests. In addition, the strategy aims to ensure Israel's continuing role in the international arena, as a leader in technological innovation and as an active partner in the global processes of shaping cyberspace.

The national cyber security strategy is the conceptual and practical foundation for achieving these goals. Designed to efficiently structure the national efforts and to ensure a stable, long-term solution, it establishes new concepts and approaches, adapted to the unique features and challenges arising from the use of cyberspace.

Development of Israel's national cyber security efforts

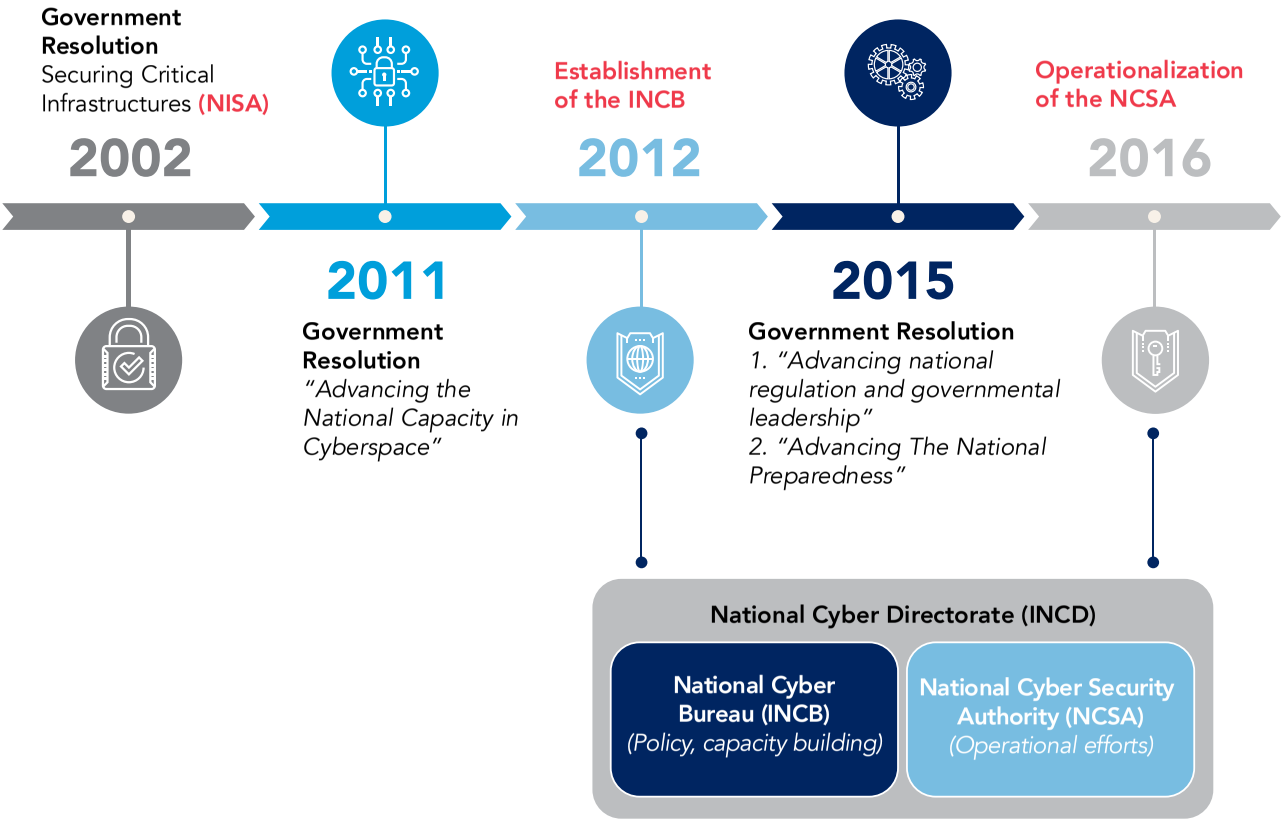
The first milestone in the development of Israel's national cyber security efforts was laid in 2002, when the Israeli government authorized the **National Information Security Authority** (NISA) to instruct and protect vital computerized systems of selected public and private civil organizations.

The next and major milestone level was the establishment, in January 2012, of the **Israel National Cyber Bureau** (INCB) reporting directly to the Prime Minister, following a governmental resolution from August 2011. INCB was tasked with: devising the State's national cyber policy and strategy, promoting national processes, developing national cyber capabilities and strengthening Israel's leadership in the field.

On February 15, 2015, the government of Israel adopted two pioneering resolutions, which reflected the major recommendations of the national cyber security strategy, developed by the Bureau. These resolutions included the establishment of the **National Cyber Security Authority** (NCSA), a dedicated government entity leading the operational cyber security efforts of the State of Israel.

Together the INCB and the NCSA constitute the INCD – Israel National Cyber Directorate.

ISRAEL'S JOURNEY IN CYBER SECURITY

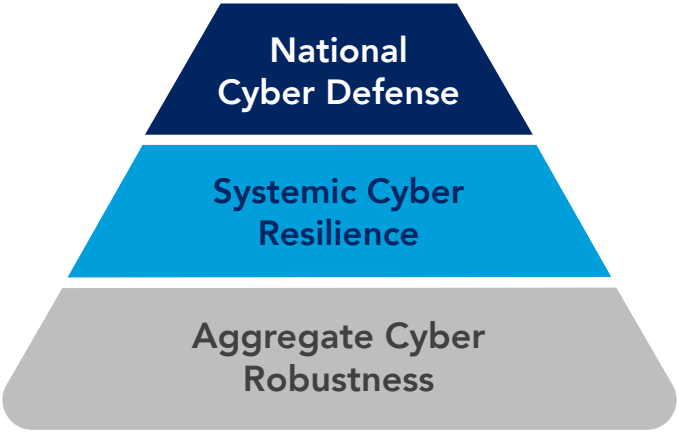


CONCEPT OF OPERATIONS

General

Israel's cyber security strategy is based on a generic concept of operations for national cyber security – a conceptual framework for all of the state's efforts and functions in the context of national cyber security. This framework includes both direct State actions to confront cyber threats and indirect efforts aimed at encouraging and supporting security activities in the private sector and collaborating with it.

The concept of operations defines three operational layers: **Aggregate Cyber Robustness, Systemic Cyber Resilience and National Cyber Defense**. The three-layer approach derives from the unique nature of the cyber threat and the central role of private organizations in achieving national cyber security. The three layers differ from one another in their goals, in the role of the State and in the relations between the State and private organizations.



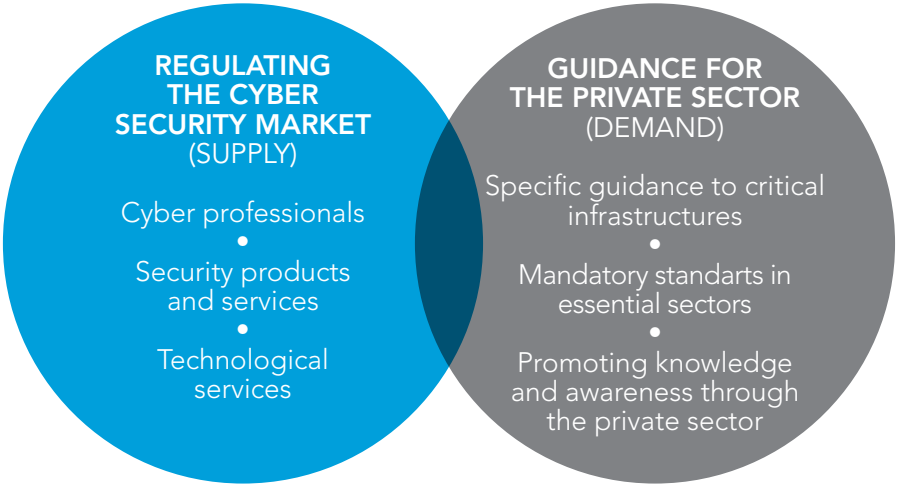
First Layer | Aggregate Cyber Robustness

Cyber robustness is the ability of organizations and processes to continue operating despite a routine of cyber threats by repelling and preventing most of the attacks.

This is the very basic level of cyber security. The State of Israel has set a goal to raise the overall level of cyber robustness as a means of preventing high-level damage and reducing the cumulative risk.

Government Resolution 2443 of February 15, 2015 introduced nation-wide efforts to enhance the national robustness through the promotion of security efforts undertaken by organizations (best practice, guidance, regulations, incentives, etc.) and by regulating the cyber security market.

Additional efforts were made to set the bar high for government cyber security so as to "lead by example" and to implement technological solutions and processes to raise overall robustness in the market.



Second Layer | Systemic Cyber Resilience:

The second layer in the concept of operations is the systematic ability to confront cyber-attacks before, during, and after incidents, prevent them from spreading and reduce their cumulative damage to the nation. While the first layer is focused on reducing attacks *a priori*, regardless of any specific event, this layer is event-driven by definition.

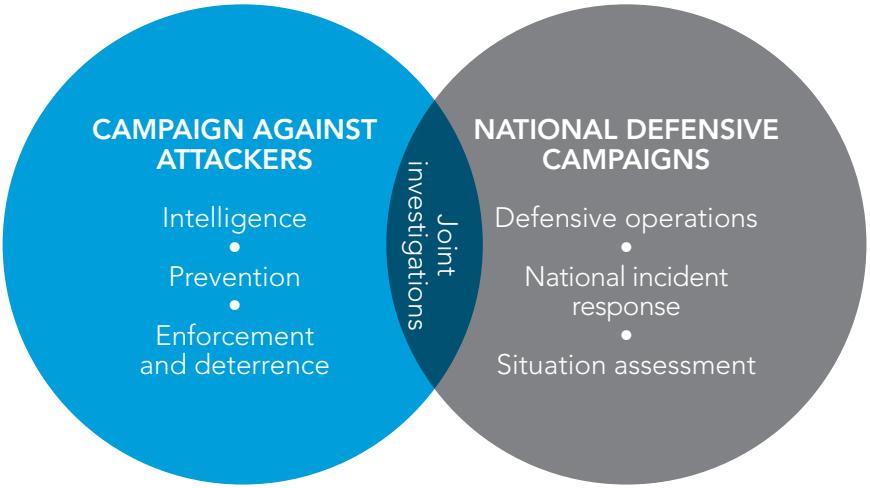
Systemic resilience can be achieved through state processes encouraging information sharing, generating and disseminating valuable information, and assisting organizations during cyber incidents.

This effort is led by the NCSA, with the national CERT at the forefront. The national CERT works closely with the private sector, both directly and through sector-based cyber centers which operate within the CERT.

The CERT strives to engage in global and local cooperation while supporting innovation and harnessing it for its goals.

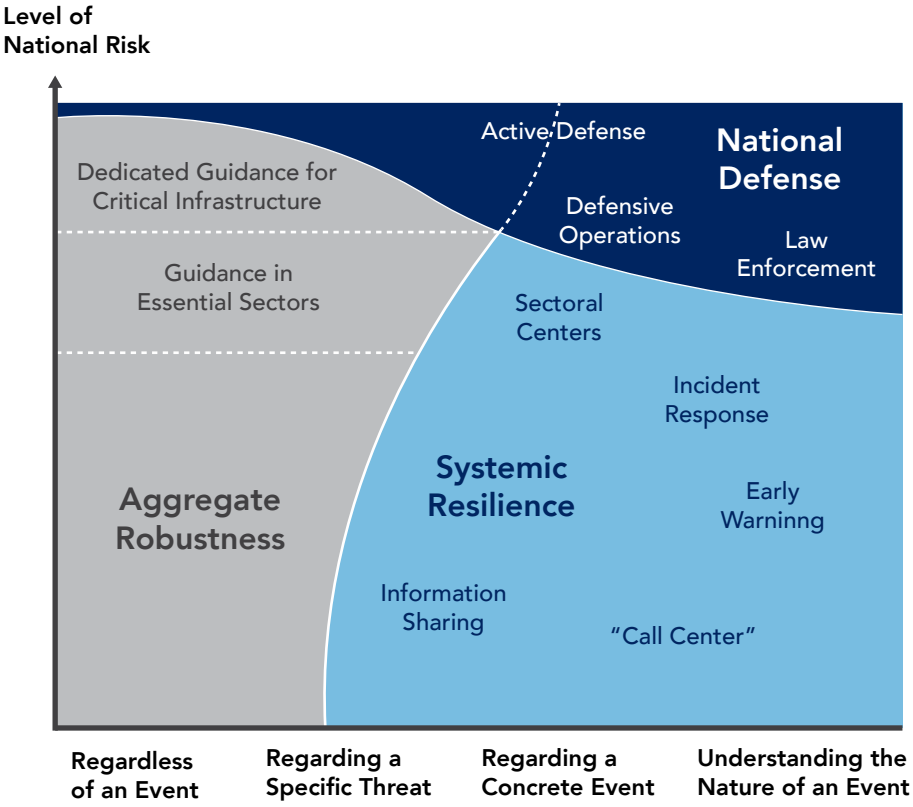
Third Layer | National Cyber Defense:

A national-level campaign is required against severe threats by determined, resource-rich attackers who pose serious danger to the nation. National defense campaigns incorporate defensive effort, to contain such attacks and their ramifications together with active efforts to confront the sources of the threats.



A Complete Solution

The three-layer approach offers a holistic solution, taking into account the differences in the level of risk, the nature of the threat and the degree of its clarity. The following graph illustrates the state's mode of action, according to the three-layer approach, given the context of the State's action (the horizontal axis) and the magnitude of the threat to the nation (the vertical axis). For example, the resilience layer enables a first response to incidents that do not present an immediate and severe threat, but may cause cumulative damage over time, or might and severe a national defense response as the understanding of the threat evolves.



THE NATIONAL CYBER SECURITY AUTHORITY

Establishing a Central Cyber Security Authority

To lead the operational cyber security efforts, the government of Israel decided, in Government Resolution 2444 of February 15, 2015, to establish a new government entity – the National Cyber Security Authority (NCSA). The NCSA is an operational agency, with cyber security as its sole concern, but also civilian in its nature, cooperating mainly and openly with the private-sector.

The NCSA serves as a hub of national knowledge, a primary cyber regulator and an operational center for managing cyber incidents. The NCSA also conducts integrated defensive campaigns with national security and law enforcement agencies.

Functions of the NCSA at the Three Layers:

Aggregate Robustness	Systemic Resilience	National Defense
Critical infrastructure regulation	Nation-wide information sharing	Managing defensive campaigns within the civilian sector
Security guidance (mainly through sectoral regulators)	Assistance to organizations under attack	Coordination between agencies
National knowledge hub	Identification and investigation of attacks	National situation assessment
Cyber security market regulation	Support for sectoral SOCs	

CAPACITY BUILDING

For several decades, Israel has been at the global forefront of innovation and scientific-technological knowledge in the field of cyber security. Cyber security is highly dependent on innovation to cope with the attacker's dynamic approach. Israel's culture of innovation, its unique human capital and its national security efforts create a perfect environment for cyber innovation, thus answering this need both locally and globally.

In its Government Resolution 3611 of August 7, 2011, "Advancing National Cyberspace Capabilities", the State of Israel made it a priority to strengthen Israel's scientific and technological cyber capabilities and innovation processes. This task was assigned to the National Cyber Bureau, as a crucial component of the national cyber security strategy, in order to ensure Israel's long term cyber security capability. This includes two main efforts:

1. **Research, development, and implementation of national level security capabilities and technologies**, including: secure and efficient information sharing platforms; solutions supporting the state's efforts to expose, investigate and contain cyber attacks; robust cyber processes; and centralized security services.

2. Strengthening the national science and technology (S&T) base in cyber: promoting **industrial innovation**, supporting **academic research** (including the establishment of six research centers in Israel's leading universities), enhancing the the nation's **human capital** in the cyber field and fostering an ecosystem for mutual enrichment. This includes the unique **CyberSpark** project – a concentrated and powerful cyber security ecosystem consisting of Israeli startups, global companies, academia and civilian and military cyber security centers – all within a walking distance of one another.

INTERNATIONAL COOPERATION

Cyberspace is a global sphere and cyber security is a global challenge. The State of Israel views international cooperation as a critical element in establishing cyberspace as a secure, free and global sphere of activity as well as a complementary component in its own national cyber security efforts. Israel is also engaged in efforts to assist partner nations in strengthening their national cyber security, while harnessing Israel's cyber capacities.

Israel invites partners around the world to work together, to share knowledge, to develop new solutions on the global level and to fulfill our shared vision of a secure and prosperous cyberspace.

לפמ

STATE OF ISRAEL
PRIME MINISTER'S OFFICE
NATIONAL CYBER DIRECTORATE