Divisions and Authorities

The National Cyber Bureau

Head of the Bureau

Background for the establishment of the Bureau

Bureau's Activities

Contact Us

Mission Of the Bureau

The Bureau functions as an advising body for the Prime Minister, the government and its committees, which recommends national policy in the cyber field and promotes its implementation, in accordance with the law and government resolutions.

The Bureau works to promote the national capability in cyberspace and to improve Israel's preparedness in dealing with the current and future challenges in cyberspace.

It is charged with improving the defense of national infrastructures critical to the continuation of normal life in the State of Israel and to protect them, as much as possible, from cyber attack, while advancing Israel's position as a center of information technology development, and at the same time encouraging cooperation between academia, industry and the private sector, government offices and the security community.

The Bureau is charged with promoting three central areas in the cyber field in Israel:

Additional Links

To the Hebrew Website

1. Advancing defense and building national strength in the cyber field
2. Building up Israel's lead in the cyber field
3. Advancing processes that support the first two tasks

The Bureau's tasks are outlined in Government Resolution No. 3611 dated August 7, 2011:
Regarding the consolidating of a national cyber policy
1. To advise the Prime Minister, the government and its committees regarding cyberspace. In matters of foreign affairs and security, the advice provided to the government, to its committees and to the ministers, will be provided on behalf of the bureau by means of the National Security Council.
2. To consolidate the government's administrative work and that of its committees in the cyber field; to prepare them for their discussions and follow-up on implementation of their decisions. In matters of foreign affairs and security, the consolidation of administrative work, preparation for discussions and follow-up on implementation of decisions will be carried out by the National Security Council.

3. To make recommendations to the Prime Minister and government regarding national cyber policy; to guide the relevant bodies regarding the policies decided upon by the government and/or the Prime Minister; to implement the policies and follow-up on their implementation.
4. To inform all the relevant bodies, as needed, about the complementary cyber-related policy guidelines resulting from Government Resolutions and committee decisions.
5. To advance coordination and cooperation between governmental bodies, defense community, academia, industrial bodies, businesses and other bodies relevant to the cyber field.
6. To advance legislation and regulation in the cyber field.
Regarding the enhancement of cyber security
7. To serve as a regulating body regulating body in fields related to cyber security, as detailed in Article I of Addendum B.
8. To determine and reaffirm, once a year, the national threat reference in defending cyberspace.
9. To formulate a national concept on dealing with emergency situations in cyberspace.
10. To conduct national and international exercises to improve the State of Israel's preparedness in the cyberspace.
11. To assemble intelligence picture from all parties in the intelligence community regarding cyber security.
12. To assemble the national situation status regarding cyber security from all relevant parties.
13. To advance and increase public awareness to threats in cyberspace and mechanisms to cope with them.
14. To formulate and publish warnings and information for the public regarding cyberspace threats, as well as practices for preventative behavior.
Regarding the strengthening of Israel's lead in the cyber field
15. To promote research and development in the cyber field and supercomputing in the professional bodies.
16. To advance the formulation of national education plans and wise use of cyberspace.
17. To work to encourage cyber industry in Israel.
18. To promote cooperation with relevant bodies abroad

To all units

Head of the Bureau

Eviatar Matania, Ph.D

Dr. Eviatar Matania is the Head of the National Cyber Bureau in the Prime Minister office of Israel.

Dr. Matania is a graduate of the elite Talpiot program. He holds a B.Sc. (cum-laude) in Physics and Mathematics (Hebrew University), a M.Sc.(cum-laude) in mathematics (Tel-Aviv University) with an expertise in game theory, and a Ph.D (Hebrew University) in Judgment and Decision Making.

Dr. Matania brings a vast experience in the national level of R&D projects and System Analysis, as well as in the academic field of Judgment and Decision Making.

Background for the establishment of the Bureau

The State of Israel was among the first countries in the world to recognize the importance of defending its critical computerized systems. In 1997, "Tehila" (Government Infrastructure for the Internet Age – Israel's e-GOV project) was launched with the goal of protecting the connection of government offices to the internet and providing secure hosting for the governmental sites. In 2002, the Government of Israel resolved (in Resolution 84/b) to determine the areas of responsibility for protecting computerized systems in Israel, defining critical computerized infrastructure and establishing NISA (the National Information Security Authority), which regulates and advises critical infrastructures in the field of information security.

Given the development of cyberspace and the expansion of threats in that domain, in November 2010, the Prime Minister of Israel instructed that a taskforce be established which would work to formulate national plans that would place Israel among the top five countries leading the cyber field. This work, named "The National Cyber Initiative", was led by the High Committee for Science and Technology, headed by Chairman of the National Council for Research and Development, Prof. Gen. (Res.) Isaac Ben-Israel. The taskforce that was established included representatives of the main bodies in the cyber field in Israel (research, development, defense, etc.), and comprised a number of sub-committees, which examined the components essential for Israel's preparedness in cyberspace, as well as analyzing the national benefit with regard to the economic, academic and national security aspects.

The central recommendation made in the framework of the cyber initiative was to establish a national cyber bureau that would serve as an advising body serving the Government and its head. The main activities of the Bureau relate to the overall government policy and actions in the cyber sphere with a broad point of view, civilian and military alike. On August 7, 2011, the Government of Israel approved the establishment of the National Cyber Bureau and determined that the Bureau would lead the promotion of the cyber related matters in Israel, coordinate between the various bodies, enhance the protection of national infrastructure from cyber attack and encourage the advancement of the subject in the industrial sphere. All of this, with the vision of placing Israel among the top five countries leading in the field within a relatively short number of years.

Bureau's Activities

Alongside forming the Bureau and establishing it, which is a considerable task on its own, last year the Bureau promoted many significant activities in various fields in cooperation with industry, academia and the governmental sector. Several of them are listed below:

In the field of cyber defense:

• Working to formulate a national defense strategy and is beginning to build the way in which it will be implemented in cooperation with the relevant bodies.
• Establishing a national cyber situation room, in the Bureau, which is tasked with forming the national cyber situation picture, as well as sharing information between the defense community, the public sector and the private sector.
• Working to establish cross-industry and industry-specific regulation, adapted to each area in cooperation with government offices.
•The INCB also established a committee for the definition of the cyber professions.
• Promoting cyber security within the civilian and private sectors, in cooperation with other government offices.
• Working towards the establishment of a national cyber situation assessment and the definition of the national cyber threat reference.

Promoting Israeli cyber defense industry:

• Establishing the "Kidma" (Advancement of Cyber Defense R&D) program to prioritize the cyber defense industry, in cooperation with the Chief Scientist of the Ministry of Industry, Trade and Labor, in the amount of 80 million NIS over two years beginning in 2013.
• Establishing the "Masad" (Dual Cyber R&D) program to promote national and defensive cyber technologies together, in cooperation with Mafat (Directorate of Defense R&D in the Ministry of Defense), in the amount of 10 million NIS for 2012-2013.
• Encouraging investments by international companies in the State of Israel.

Developing academia and human capital:

• Establishing an academic research fund for cyber security in cooperation with the Ministry of Science and Technology, in the amount of 32 million NIS for 2012-2014.
• Granting scholarships to students studying for advanced academic degrees in the cyber field, in cooperation with the Ministry of Science and Technology, in the amount of 16 million NIS for 2012-2014.
• Initiating the establishment of advanced degree programs in the cyber field.

• In addition, the Bureau supported the establishment of the "Magshimim Leumit" program, which is a three-year excellence program focusing on training and developing expertise in the cyber and computer fields among outstanding students aged 16-18 residing in peripheral areas.
• Working with the Council for Higher Education and relevant academic institutes to establish a strategic plan for the advancement of the academia in the cyber field.
• Working to establish an online school and a research institute for cyber studies.

In the international cooperation field:

• The Bureau acts to develop foreign relations in the cyber field with friendly countries for various purposes such as information sharing, mutual R&D and more.