Cyberdefense Policy of Israel: Evolving Threats and Responses

Lior Tabansky
Yuval Ne'eman Workshop for Science, Technology and Security
Tel Aviv University, Israel

January 2013 – Article n° III.12

Lior Tabansky is a Ph.D. candidate at the Department of Political Science at Tel Aviv University, his thesis examining Cyberspace in comparative national security perspectives, and a Senior Researcher at the Yuval Ne'eman Workshop for Science, Technology and Security. His expertise builds on combining a solid academic record and research skills in politics and security with professional experience in corporate IT management.

Keywords: *Israel, Cyber Security, Critical Infrastructure Protection, CIP, Policy*

This article presents and examines the cyberdefense policy of Israel. We describe the main threat scenario, and the evolution of national response to it. The CIP policy has been built upon the insights of defense establishment and evolved from a limited involvement with IT branches of government, toward an early adoption of national CIP, and has recently moved towards a comprehensive effort aimed at attaining global leadership, contributing to national security, the economy, and foreign affairs.
An international comparative study of 23 developed countries recently awarded Israel with a top grade on 'cyberdefense', alongside Sweden and Finland[1] *. This result is usually perceived as the outcome of a nation's human capital and technologic power. We claim that a policy aspect is critical in national cybersecurity, yet it is neglected in both scholarly and public debates.*

[1] Grauman, B. "Cyber-Security : The Vexed Question of Global Rules : An Independent Report on Cyber-Preparedness around the World." edited by Security & Defence Agenda (SDA) and McAfee Inc. Brussels: Security & Defence Agenda (SDA), 2012.

The threat perspective

Researching cyberdefense of Israel is hardly trivial. Optimally, formal public policy is clearly expressed; this review utilizes the existing official public sources. However, in reality organizations and individuals deal with challenges and react without a centralized transparent decision-making process. In addition, the whole topic is shrouded with secrecy and overclassification, especially since the defense and intelligence organs were traditionally major stakeholders in cyberdefense. This excessive secrecy is a burden on public cybersecurity debate in Israel and other developed states.
Israel has never published an open, formal cybersecurity strategy. In fact, this is an unfortunate yet common state of affairs in defense issues in Israel. Despite the dynamic environment shifting threats and opportunities, and the resulting security research in the Israeli defense establishment, the political preference to avoid formal binding declarations is evident. The following analysis of the threat derives from the author's research and interviews.

Cyberspace has enabled an information sphere, where individuals have unprecedented communication potential. Countless accounts of the expected benefits of IT in fields as diverse as agriculture, education and political change, and in of the Internet particular, have been published. It appears that the authoritarian regimes have indeed feared the destabilizing social and political effects of Cyberspace, and have taken various precautions. Cyberthreats can be placed on a continuum between those residing solely in the information sphere, to those with purely physical manifestation.[2] The potential of the communication infrastructure to motivate people for undesired actions will be placed towards the information edge. Indeed, propaganda, subversion, radicalization, etc. in cyberspace are commonly discussed issues. However, it appears that these issues were not deemed as a serious concern in Israel. It was the opposite edge of the continuum where the attention focused. Cyberspace opened a Pandora's Box: it enables a direct strike on national infrastructure while circumventing traditional defense systems. For the first time in history, it is theoretically possible to attack strategic targets (such as critical infrastructures) without physically being in the place where they are located, without confronting the defending armies, and without exposure and clear attribution. This concept that was long recognized in some parts of the Israeli defense community became the driving force of Israeli cyberdefense. The circulation of a novel threat scenario takes time and energy. The most frequent response is a dismissal of a new nuisance and its promoters. However, in this case the threat was eventually recognized, and a response was called for. The next chapters describe the evolving cyberdefense policy.

2002 – 2011: Regulation and Cooperation

Who should be in charge of providing cyberdefense, and who should be protected by the state? This substantial topic, that consumes leadership resources worldwide to this day, had reached a culminating point in Israel over a decade ago. After years of departmentalised activities in various branches, the Special Resolution B/84 on 'The responsibility for protecting computerized systems in the State of Israel' by the ministerial committee on national security of December 11, 2002, launched the *national civilian* cyberdefense policy. It formed the procedural basis of national Critical Infrastructure Protection (CIP) policy.

[2] For conceptual reviews of cybersecurity, see:
Ben Israel, Isaac , and Lior Tabansky. "An Interdisciplinary Look at Security Challenges in the Information Age." *Military and Strategic Affairs* 3, no. 3 (November 2011).
Tabansky, Lior. "Basic Concepts in Cyber Warfare." *Military and Strategic Affairs* 3, no. 1 (May 2011).
Rid, Thomas. *Cyber War Will Not Take Place*. London: Hurst, 2013.

The responsibility for protecting computerized systems of organizations defined 'critical' was shared among both the users and the regulators. A 'user' referred to a supervised organization, which is in charge over financing all operation, protection, maintenance, upgrading, backup and recovery of its critical IT systems, while sharing relevant information with the regulator. The regulators are the existing chiefs of security at government ministries, who are professionally responsible for guided bodies: for example, the Ministry of Communication regulates the (then state-owned monopoly) telephone company Bezeq). Two additional regulators are established: 'The top steering committee for the protection of computerized systems in the State of Israel,' and 'the national unit for the protection of vital computerized systems.' While the steering committee has a policy perspective, the 'national unit' - National Information Security Authority (NISA, Hebrew: *Re'em*)[3] - has the professional authority and these eight duties:

1. To assess the threat landscape and present it to the steering committee for approval.
2. To suggest oversight to the steering committee what systems should be deemed critical and receive the oversight
3. To develop protective doctrine and methods.
4. To integrate intelligence from various sources.
5. To provide professional instruction to the supervised organization.
6. To set standards and operating procedures for the benefit of supervised organization.
7. To develop technological expertise and cooperation with partners in Israel and abroad.
8. To initiate and support research for developing defensive capabilities, in cooperation with the defense community.

Tasking the military with protecting vital computerized systems of domestic public and privately owned civilian organizations would create an unacceptable legal and, more importantly, ethical hurdle. The Israeli law permits the Israel Security Agency (ISA, Hebrew: *Shabaq*) or the police to intervene with civilian matters for security purposes. In the ISA, an Information Security unit was in place long before 2002; it attended to information security concerns at the Israeli embassies and state-owned corporations. Expanding its authorities and establishing on this foundation the National Information Security Agency (NISA), while building upon existing expertise - was the self-evident track of development.

To implement the new arrangement, the 'Regulation of Security in Public Bodies act of 1998' was amended, to provide the new bodies – the steering committee and NISA – with authority to supervise public bodies in the field of informations security.[4] It should be stressed that despite the word 'public', private ownership of 'critical infrastructure' does not diminish the authorities of the law. Over a dozen of public and private civilian organizations and firms have been initially deemed critical and thus requiring tighter protection.

In the following decade, NISA was actively involved in cyberdefense and often initiated proposals to the steering committee to adapt to the changing environment. The cyber-risks have indeed intensified rapidly with the accelerated growth of cyberspace. During these years, growing voices in Israel stressed the need for major changes. The next chapter is devoted to the review process, which heralded a new era in Israeli cybersecurity policy.

The National Cyber Initiative of 2010

The tempo of a democratic government, confined by political and legal constrains, is understandably slower than that of Information Technology. After several attempts to initiate a change, Prime Minister

[3] http://www.shabak.gov.il/about/units/reem/Pages/default.aspx (Hebrew).
[4] "Regulation of Security in Public Bodies Law". Jerusalem, 5758-1998 (Hebrew).

Benjamin Netanyahu approached the Israeli National Security Council requesting a review on cybersecurity and Israel's policy. It looks as though the National Security Council did not fulfil this task. The Prime Minister then approached retired brigadier-general professor Isaac Ben-Israel, the head of the National Council for Research and Development in the Ministry of Science, to take on this mission. He indeed accepted this request in August 2010, and in the following months the prime minister's National Cyber Initiative has performed a broad review in Israel's national cyber policy.

The vision that directed the work of the National Cyber Initiative was *"To preserve Israel's standing in the world as a center for information-technology development, to provide it with superpower capabilities in cyberspace, to ensure its financial and national resilience as a democratic, information-based, and open society"*.[5]

The team composition reflected the Initiative's vision. For six months, eighty experts worked on the project: defense representatives, academic experts, research and development leaders, and representatives from the ministries of finance and science and technology. The work was divided into seven subcommittees, and a business consultancy contributed an organizational-budgetary analysis.
The team dealt with three key questions:

1. How to ensure Israel's standing as one of the top five global cyberleaders by 2015?
2. Which infrastructures are needed to develop high-performance computing in Israel?
3. What arrangements are required in order to deal with challenges in cyberspace?

A concise review of the key findings and recommendations is outlined in the following pages.

The Key Products of the National Cyber Initiative

The team performed a systemic overview of the challenges and opportunities that the Israel would face as cyberspace evolves. It was reemphasized that some specific cyber-attacks may cause widespread national harm.

In view of the threat, the committee re-examined the current measures: Israel has implemented policies for the protection of the defense sector and the critical national infrastructures (as described in the previous chapter here). However, the civilian segment became exposed more than in 2002 to cyberattacks, and the existing protection arrangement does not cover it.

Some neglected types of threats are:

* Damage to civil services and services to private homes
* Threats to ‘concealed’ computers, such as navigational devices or controllers in cars
* Degradation of morale by cyber means

As in earlier threat estimates, the focus is on the physical aspects. Interstingly, there is a first of a kind reference to the other edge, the informational and cognitive aspects.

The recommendations to improve national cybersecurity were eventually proposed, and can be represented in clusters:

1. Improve education, from basic best-practice and to advanced interdisciplinary R&D.
   * Encourage the public to use available commercial security tools
   * Establish a research excellence center on cyber issues

[5] NCR&D. ""The National Cyber Initiative" – a Special Report for the Prime Minister ", edited by The State of Israel, Ministry of Science and Technology, the National Council on Research and Development and the Supreme Council on Science and Technology. Jerusalem, 2011 (Hebrew).

2. Develop knowledge and R&D infrastructure
    * Promote secure code development
    * Incentivise the academia to launch multidisciplinary programs on cybersecurity,
    * Develop and establish a national large-scale simulation facility that will cater to all consumers.
    * Develop and establish a national center for supercomputing

3. Create a statewide "protective shield" based upon the products of domestic R&D, while addressing privacy concerns.
    * Encouraging cybersecurity industry
    * Develop and implement cyber-protection criteria for organizations, to help selecting optimal solutions
    * Contribute information for risks insurance industry

4. Develop national operational capabilities in cyberspace for routine and emergency, while confronting moral, legal, and financial challenges
    * Encourage early-stage market in order to promote innovations

5. Upgrade the defense by combining technical and non-technical legislative measures
    * Participate in international initiatives, especially with the Council of Europe Convention on Cybercrime – 2001 (The Budapest Convention) to promote cyberdefense

6. Deploy unique technologies, developed cooperatively by domestic scientific and industrial sectors, with the government encouraging local procurement.
    * Increase R&D collaboration between the IDF and the academia, while minimizing the inhibiting effect of classification
    * Increase transparency and cooperation within the government agencies, and between the Ministry of Defense, the defense industrial base, and the civilian industry, while resolving secrecy restrictions.
    * Increase relevant defense R&D, while improving the export capacity of the products.

7. No national agency for comprehensive cyber policy existed in Israel. To achieve the recommendation, the need for such an agency was stressed.

The findings of all the subcommittees were then integrated in a final report, which was submitted to the government.

The current stage: striving for comprehensive cyberdefense and global advantage

The fate of the "National Cyber Initiative" report was different than that of many other reviews and reports: The Government resolution 3611 "Advancing the national capacity in cyberspace" of August 2011 adopted the recommendations of the "National Cyber Initiative," to *"improve the protection of national infrastructures essential for daily life in Israel, and to strengthen them, as much as possible, against cyber attacks, while promoting Israel's status as a center for ICT development, all through the cooperation of academia, industry, ministries, and the security organizations."* [6]

[6] "Government Decision 3611: Promoting National Capacity in Cyber Space." Jerusalem, Israel: PMO Secretariat, 2011 (Hebrew).

The key aspect in the resolution is to establish the Israel National Cyber Bureau (INCB) in the Prime Minister's office, reporting directly to the PM.[7] Similar to the previous 'steering committee' the INCB is not an operational branch, but a counselling and coordinating organization with these duties:[8]

* To advise to the prime minister, the government and its committees on cyber-related issues and to coordinate the topic (excluding security and foreign relations).
* To council the government on a national cyber policy, to initiate legislation, to advertise the government policy, to follow-up on and inspect its implementation.
* To provide national cyber-threat estimate, combining relevant intelligence from all sources.
* To promote research and development on cyber and HPC topics by the professional bodies, and to fashion national plans for education and sensible use of cyberspace.
* To promote cyber-related industry in Israel.
* To promote public awareness on cybersecurity and publish information, warnings, and directives.
* To promote domestic and international collaboration on cyber-related issues.

The INCB was appropriated with an ILS 2.5 billion budget for the next five years – about ILS 500 ($130) million a year.

Conclusion and Outlook

Design and implementation of a comprehensive national cybersecurity arrangement is an ambitious venture. Israel's continued position as a world-class cyberpower is often acknowledged, but seen as some natural outcome of its qualified and innovative workforce. This article claims that scientific infrastructure, human capital, technological capacity and entrepreneurial spirit – are insufficient for national cybersecurity. This article is an attempt to fill this gap in understanding cyberdefense. The missing ingredient is the ability of the political and governmental systems to coordinate and foster collaboration for a comprehensive national policy.

The Israeli policy, as examined in this article, provides several insights.
While the origins of the Israeli national CIP policy date back to mid-90s,[9] it has evolved greatly. The continuous threat the society faces presumably smoothened the cooperation between the defence and the civilian sectors. These factors have also enabled the government and particularly the defense sector, which are commonly seen as rigid structures, to act in a flexible manner, allowing for innovative thinking. The examined case provides a rare example of proactive initiative in the governmental structures. Israel started developing a civilian CIP policy and implemented it *before a cyber-crisis occurred*. The government was able to initiate proactive policy measures, to show agility and responsiveness to changing demands – in stark contrast to the stigma of state organs.
Two major official milestones were discussed in this article: the creation of the legislative and organizational framework for CIP in 2002 and the adoption of the ambitious National Cyber Initiative of 2010, aiming for Israel to become a top five global cyber superpower by 2015. Beyond defense, the current vision is to bring macro-economic benefits and promote Israel as a highly capable actor on the international arena.[10]

---

[7] "Cabinet Approves the Creation of the National Cyber Directorate ". Press Release, http://www.pmo.gov.il/english/mediacenter/spokesman/pages/spokecyber070811.aspx .
[8] "Prime Minister's Office Divisions and Authorities the National Cyber Bureau Mission of the Bureau ". http://www.pmo.gov.il/english/primeministersoffice/divisionsandauthorities/cyber/pages/default.aspx .
[9] For example, the Ministry of Finance has officially hosted the inter-governmental IT infrastructure department which dealt with information security since 1997. See: http://www.tehila.gov.il/AboutUs/Pages/AboutUs.aspx (Hebrew)
[10] http://mfa.gov.il/MFA/PressRoom/2012/Pages/National_Cyber_Directorate_work_plan_7-Jun-2012.aspx

This brief overview of Israeli experience with cyberdefense policy may be of value to likeminded nations dealing with the impacts of rapidly changing technology. Public attitudes, ideology, social structure, economic development, market model, business competition, structure of the political system – are factors that are bound to shape cyberdefense, whether IT security experts and defense officials like it or not. Any technical expertise is insufficient for achieving a comprehensive national protection without a policy-making process. Future evolution of cyberdefense will inevitably bring more fundamental issues that will require much broader participation of the citizens. The democratic political system is the appropriate arena to accommodate the multitude of actors and to mediate conflicting values of freedom, morals, privacy, entrepreneurship, security, control and others.