Critical Infrastructure Protection:
Evolution of Israeli Policy

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

ABSTRACT

Cyber Warfare holds a grave hazard of striking national infrastructure while circumventing traditional defense systems. This article examines the evolution of Critical Infrastructure Protection (CIP) policy in Israel and analyses its performance. Israel has developed a unique legal and regulatory model for critical infrastructure protection, which was implemented in late 2002. Recently, a comprehensive review of cyber security posture has been conducted, and significant policy changes are in progress. The Israeli approach to CIP and beyond, fostering cooperation between public, security, academic and private sectors, appears to be successful. This study of the evolution of Israeli Critical Infrastructure Protection policy may assist policy-making in other countries.

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

INTRODUCTION

An international comparative study on 'cyber defense' of 23 developed countries recently awarded Israel with a top grade, alongside Sweden and Finland (Grauman, 2012). This is commonly viewed as a natural outcome of a nation's human capital, academic and industrial capacities and economic well-being. The article claims that the policy aspect is critical in national cyber security, yet it is neglected in both scholarly and public debates.

To fill this void, this article presents and examines the evolution of Critical Infrastructure Protection (CIP) policy in Israel and analyses its performance. 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 relations.

CRITICAL INFRASTRUCTURE PROTECTION IN ISRAEL, 2002 – 2011: REGULATION AND COOPERATION

Following the accumulated understanding of civilian infrastructures vulnerabilities for cyber-attack, the Ministry of Defense (MoD) Defense R&D directorate (Hebrew: *Maf'at*) has initiated

DOI: 10.4018/ijcwt.2013070106

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

staff work at the National Security Council. Its outcome resulted in Special Resolution B/84 on "The responsibility for protecting computerized systems in the State of Israel", of the ministerial committee on national security of December 11, 2002. After years of occasional activities, the governmental decision opened an era of national civilian cyber security policy. In fact, it might have been one of the first centralized national Critical Infrastructure Protection policies in the developed world.

The definitions stated in the B/84 Resolution are worth examining. First, 'cyberspace' was not an independent area of operation, but one interconnected with all physical spaces. Second, 'information' system is differentiated from 'control' system. An information system "performs mechanized activities of input reception, processing, storage, processing, and conveyance of information." On the other hand, a control and supervision system is a "computer-integrated system that controls and supervises the frequency and regulation of measureable activities, which are carried out by mechanized means within the information system itself."

The responsibility for protecting computerized systems rests with the users and state regulators. A 'user' is a supervised organization, which is in charge over financing all operation, protection, maintenance, upgrading, backup and recovery of its critical IT systems, as it shares information and activities 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 is in charge over the 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."

The steering committee was established within the National Security Council, and comprised of senior government officials, representatives from the Bank of Israel, and the security forces. While the steering committee has a policy perspective, the 'national unit' - National Information Security Authority (NISA, Hebrew: *Re'em*) - has the professional authority[1].

The government's decision delegates eight responsibilities for NISA:

1. To assess the threat landscape – subject to the steering committee approval;
2. To suggest classifying systems as critical and suggest oversight to the steering committee;
3. To develop protective doctrine and methods;
4. To integrate intelligence;
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.

The Israeli law only permits the General Security Service (GSS, Hebrew: *Shabaq*) and the police to intervene with civilian matters for security purposes. Designating the responsibility for protecting vital computerized systems in public and privately owned civilian bodies to the army would create an ethical problem and a legal hurdle. At the time, on top of its common duties, the Israeli police was inundated with criminal and terrorist activity sourced in the Palestinian Authority. In the GSS, NISA was in place within the GSS Protective Security Division long before 2002; it attended to information-security concerns at the governmental departments, Israeli embassies abroad, and state-owned companies. Broadening the authorities was the self-evident track of development, although one resulting in a substantial expansion of the workforce and the unit's budget (Assaf, 2008).

To implement the new arrangement, the "Regulation of Security in Public Bodies act of 1998" was amended, to provide the new

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

bodies – the steering committee and NISA – with authority to supervise public bodies. It should be noted that despite the word 'public', private ownership of 'critical infrastructure' does not diminish the authorities of the law. The law defines "activities for protecting vital computerized systems" as "activities required to preserve those vital computerized systems, information stored in them, confidential information related to them, as well as preventing damages to those systems or the information in question". The supervised public body will appoint dedicated personnel on its behalf, which will be responsible for implementing the instructions of the authority.

NISA was actively involved in cyber-security policy development and often initiated proposals to the steering committee. Some may consider this as a breach in "separation of authorities": is it legally appropriate for the professional operational body to intervene with the policy work of the steering committee? However, this state of affairs has not raised any legal criticism in Israel. The cyber-risks have indeed intensified rapidly with the accelerated growth of cyberspace. There were growing voices in Israel, stressing the need for defensive updates and revisions. The next chapter is devoted to the review process, which heralded a new era in Israeli cyber-security policy.

Circa 2006, the steering committee and NISA reached the conclusion that the Tel-Aviv Stock Exchange (TASE) – with operations wholly dependent on computerized systems – should be designated as 'critical infrastructure'. The legislative process enables an organization to state its position on the matter. The CEO of the TASE, Mrs. Ester Levanon, presented two arguments against the decision, both through the official channels and via mass media:

1. The head of the TASE personally[2] and the organization as a whole have a sound expertise in information security. Therefore, the organization does not need state oversight;
2. TASE is required to administer itself in the global financial market. Any supervision of the stock exchange's computerized infrastructure by a clandestine intelligence service will severely tarnish the Israeli financial market reputation and divest foreign capital. Therefore, the proposed supervision will damage national economy.

After much deliberation, the injunction that designates the Tel Aviv stock exchange as a 'critical infrastructure', thus subject to supervision by NISA - was approved in 2008. In late 2011 the oversight was extended to eight more companies - cellular and internet service providers, totalling over two dozen entities. In the decade that the current arrangement was enacted, there was a single objection. Despite the costs mandated by the regulatory guidance, the study clearly demonstrates a high level of cooperation between the state authorities and the critical infrastructure owners and operators.

THE NATIONAL CYBER INITIATIVE OF 2010

Prime Minister Benjamin Netanyahu approached the Israeli National Security Council in 2010 requesting a review on cyber security and Israel's policy. It looks as though the National Security Council did not implement this task. The Prime Minister then approached retired brigadier-general professor Isaac Ben-Israel, who at that time was 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, and during 2010, the prime minister's initiative was launched. The National Cyber Initiative has formed the basis for a substantial change in Israel's national cyber policy. The Initiative's activity, organization and structure are presented to understand the mechanism of the policy-design process.

The Initiative performed a systematic overview of the challenges and opportunities that the State of Israel would face as the cyber threat develops. The vision that guided the initiative is "To preserve Israel's standing in the world as a center for information-technology development, to provide it with superpower capabilities

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

in cyberspace, to ensure its financial and national resilience as a democratic, information-based, and open society" (NCR&D 2011).

The initiative dealt with three key questions:

1. How can cyber-technology be incentivized and developed in Israel, to ensure Israel's standing as one of the top five leaders in the world by 2015?
2. Which infrastructures are needed to develop high-performance computing in Israel?
3. What arrangements (organization, responsibility, policy and regulation) are required in order to best deal with the challenges and threats in cyberspace?

The team composition reflected the Initiative's vision. For six months, eighty experts worked on the project: military representatives, academic experts, research and development institutional directors, 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. Below is a brief review of the key subcommittees findings and recommendations[3].

THE KEY PRODUCTS OF THE NATIONAL CYBER INITIATIVE

The *subcommittee on monitoring and supervision* acted to produce updated recommendations related to cyber protection in Israel, focusing on the components that should be encouraged to develop the field in Israel, to upgrade the State of Israel posture and ensure its resilience.

An examination of the threat 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).

The subcommittee reached the conclusion that the current measures are insufficient. No national agency for comprehensive cyber policy existed in Israel. The civilian space is exposed more than ever to cyber-attacks, yet 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.

The main objective proposed was to develop and deploy ground-breaking capacity that will provide Israel with an advantage in cyberspace. Israel's main assets are: A first-rate academic establishment, which contributes to research and innovation, a range of state and security organizations possessing information security expertise, and an extensive high-tech sector, including world leading information security companies. However, various obstacles for productive collaboration were recognized. The major challenge is to incentivize the industry to invest in innovative cyber research and development, and to motivate higher education to research this field and develop a workforce. Another challenge is the establishment of a coordinating body, which will deal with organizational obstacles, conflicts of interests, and other problems, in order fashion optimal policy.

The subcommittee formulated six major recommendations to improve national cybersecurity:

1. To raise awareness and education through, beginning with basic best practice and leading to advanced interdisciplinary R&D;
2. To develop knowledge and R&D infrastructure, especially for secure code development; to encourage the academia to launch multidisciplinary programs on cyber security, and to establish a national cyber-simulator;

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

3. To create a statewide protective shield based on domestic R&D, while addressing privacy concerns;
4. To develop national operational capabilities in cyberspace for routine and emergency, while confronting moral, legal, and financial challenges;
5. To upgrade the defense by combining technical and legislative measures;
6. To deploy unique Israeli technologies, developed cooperatively by scientific and industrial sectors, with the government encouraging local procurement.

The *subcommittee on cipher and simulation* asserted that cryptography is essential to guard state secrets and intellectual property. The assumption that Israel has leading capacities in the scientific and theoretical areas was reaffirmed. Yet, in terms of industrial implementation, the conclusion was that Israel's scientific potential is not fulfilled. State-imposed export restrictions exemplify hurdles that make cipher development unprofitable.

It was recommended to encourage collaboration between the IDF and the academia. Another recommendation was to encourage the public to use available commercial encryption. The need for simulation for research and training is clearly raised in academia and the defense establishment; it is recommended to develop a large-scale simulation facility that will cater to all consumers.

The *subcommittee on super-computing and broadband* claimed that High Performance Computer (HPC) is a necessary tool, yet Israel cannot purchase a super computer because of political constraints. The subcommittee's work concluded that Israel has "islands" of super-computing competence in the defense establishment, academia, and industries. The major recommendation was to establish a national center for super-computing, which will be available to all consumers. The report presents alternatives and their costs.

The *subcommittee on the economic benefits* stated that security is a public good, and the market cannot fully supply it. Still, the private sector is fundamental in developing Israeli capacities in cyberspace. Therefore, if the state has to improve cyber security, it must engage the market. Encouraging cyber security industry would result in security and economic benefits.

The main recommendations were:

- To increase relevant defense R&D, while improving the export capacity of the products;
- To increase transparency and cooperation in government and the Ministry of Defense, defense industrial base, and the civilian industry, while resolving secrecy restrictions;
- To encourage early-stage market in order to promote innovations;
- To develop cyber-protection criteria for organizations, to help selecting optimal solutions and also to contribute to risks insurance and financial grading.

The *subcommittee for examining the academic benefits* key recommendation was to establish a research excellence center on cyber-related issues, as part of I-Core: Israeli Centers of Research Excellence plan, adopted in a March 2010 government resolution[4].

The *subcommittee on policy and legislation* reviewed and showcased the various relevant Israeli legislation and regulations, assessed the disparities, and recommended solutions to some of the legal issues. It reviewed national and international activity in ENISA, EU, EU-FP7, EUREKA, OECD, NATO, UN-ITU. The recommendation for Israel was to publish a formal policy document, and to participate in international initiatives, with an emphasis on the Council of Europe Convention on Cybercrime – 2001 (The Budapest Convention) to promote cyber-defense.

The findings of the subcommittees were then integrated in a final report, which was submitted to the government. The fate of the "National Cyber Initiative" report was different than that of many other reviews and reports: the government soon adopted most of the recommendations. The Government resolu-

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

tion 3611 "Advancing the national capacity in cyberspace" of August 2011, which adopts the recommendations of the "National Cyber Initiative," was intended 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."

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.

THE NATIONAL CYBER BUREAU (INCB): THE INAUGURAL YEAR

Similar to the nature of the earlier "steering committee" the INCB is not an operational branch. The 2002 critical infrastructure protection arrangement remains in place until further notice. This new body will coordinate policies, acting to implement the professional recommendations. The resolution designates INCB with the following duties:

- To advise to the prime minister, the government and its committees on cyber-related issues and too 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 cyber security 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, mainly sourced from "impounding" existing funding from various sources.

A glimpse into the bureau's activities was provided by the INCB head Dr. Evyatar Matania, who gave a keynote address to the Yuval Ne'eman Workshop for Science, Technology and Security Second International Cyber Conference.[5]

The INCB main task is drafting a new comprehensive national cyber-strategy. Dr. Matania specifically mentioned the transition from "defense" to "security", in line with the shifting national security perspective which broadens to consider the individual wellbeing. The vision includes a national cyber-protection center, in which a national situation room will be established. The issue of information sharing, which is achieved by prying at computer networks of various organizations, is extremely hard, in view of privacy, secrecy, anti-trust regulations, and others. The oversight will continue to integrate regulations, with information and support offered to company managements.

The INCB acts to improve the academic infrastructure in Israel in cooperation with the Ministry of Science, planning to invest ILS 50 million to promote competitive academic research, and assist high-school education. The INCB will promote the establishment of a national lab, mainly by combining existing resources of various agencies.

A program to encouraging innovative industry is being designed, resembling the 1993 government "Yozma" initiative which developed the venture capital industry in Israel and assisted the impressive growth of the high-tech

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

sector. In 2012, over 150 start-up companies were operating in Israel in the field of cyber security. In October 2012, the INCB, along with the MODDR&D (*Maf'at*), launched a dual-use, civilian and defense cyber R&D plan (MASAD) with a budget of one million ILS for 2013.[6] The Office of the Chief Scientist (OCS) at the Ministry of Industry, Trade, and Labor supports competitive R&D; in 2011, the OCS allocated ILS 62 million for 21 early-stage cyber security initiatives. In 2012, ILS 90 million was allocated for 45 early-stage cyber security initiatives. In addition, the OCS will operate a new plan (KIDMA) to support initiatives at the earliest (pre seed) stage.

The bureau recognizes the significance of international cooperation in cyberspace, and acts to advance the processes of having Israel join existing treaties and arrangements.

The INCB inaugural year can be summed up as launching several paths of action, the outcomes of which remain to be seen in a few years' time.

CONCLUSION AND RECOMMENDATIONS

Design and implementation of a comprehensive national cyber-security arrangement is an ambitious venture. Israel's continued position as a world-class cyber power is often acknowledged and seen as the 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 cyber security, The missing ingredient is the ability of the political and governmental systems to coordinate and foster collaboration for a comprehensive national policy. This article is an attempt to fill this gap in understanding Cyber Warfare.

Studying Critical Infrastructure Protection Policy in Israel is not trivial. Optimally, formal public policy is clearly expressed. However, in reality organizations and individuals deal with challenges and react without a centralized transparent decision-making process. These actions accumulate and manifest eventually a complex set, which can be seen de facto as policies. The informal aspects are elusive, but vital for comprehensive understanding of policy-making processes.

The actual policy, which was examined in this article, provides several insights.

While the origins of the Israeli national CIP policy date back to mid-90s, it has evolved greatly during the past decade. Two major milestones were discussed in this article: the creation of the legislative and organizational framework for CIP in 2002, and the National Cyber Initiative of 2010, aiming at an ambitious goal: to become one of the top five global cyber superpowers by 2015.

The National Cyber Initiative report suggested to apply a broader perspective and to view CIP as one of the cornerstones for a national cyber-security policy that would also bring macro-economic benefits and promote Israel's status as highly capable actor on the international arena. The majority of the National Cyber Initiative's recommendations were put in practice in 2012. The INCB, a central non-operational body was established to coordinate activities, mediate between the involved actors, and to advise the government. The Bureau reports directly to the Prime Minister, once again demonstrating the breadth of cyber-related issues. Confirming the assumption that national security plays a central role in any technological revolution and the information revolution in particular (Boot, 2006; Gat, 2006), the defense sector was a central actor in the beginning of the policy-making process. The very nature of national security had compelled the defense forces earlier to acquire expertize in the cyber area.

Naturally, the civilian sector was reluctant to accept further regulations and expenditure, but a number of cultural factors likely played a significant role in reaching compliance: The size of the nation and the informal Israeli attitudes provided for organizational flexibility. The continuous threat the society faces presumably

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

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 before a cyber-crisis occurred, and early on in a global comparison. The government was able to initiate proactive policy measures, to show agility and responsiveness to changing demands. This proactivity must have eased the decision-making process, as the stakeholders could assess new threats more objectively because the process was not overshadowed by a preceding crisis. Consequently, the somewhat trivial recommendation is to be proactive in respect to rapidly developing technologies.

Public attitudes, ideology, social structure, economic development, market model, business competition, structure of the political system – are factors that are bound to shape a CIP policy, whether IT security experts like it or not. Without a political policy-making process any level of technical expertise of a country is insufficient for achieving a comprehensive national protection. The main recommendations for national CIP policy are to reduce strictness, allow for innovative initiatives, and nurture the delicate combination of formal frameworks with informal ties. The state system has a multitude of actors and roles to play for fostering these recommendations: regulation, incentives, coordination, legislation, public-private partnership, academia and R&D infrastructure, civil-military cooperation and more. When designing and implementing a national policy to address a novel rapidly evolving issue of technological origin, a state must act quickly and flexibly, learn in process, accommodate new experience, and adjust the policies accordingly. There is no one-fits-all blueprint for a CIP policy, and its success will largely depend on whether a state is capable to mediate and manage the numerous stakeholders for a mutual benefit.

ACKNOWLEDGMENT

I would like to thank the Yuval Ne'eman Workshop for Science, Technology and Security at the Tel Aviv University and the Neubauer Research Fellowships Program at the Institute for National Security Studies (INSS).

REFERENCES

Assaf, D. (2008). Critical information infrastructure protection policy in Israel. *The CIP Report, 6*(12).

Boot, M. (2006). *War made new: Technology, warfare, and the course of history, 1500 to today*. New York, NY: Gotham Books.

Gat, A. (2006). *War in human civilization*. Oxford University Press.

Grauman, B. (2012). Cyber-security: The vexed question of global rules: An independent report on cyber-preparedness around the world. Brussels: Security & Defence Agenda (SDA).

NCR&D. (2011). The national cyber initiative – a special report for the Prime Minister. Tel Aviv.

ENDNOTES

1. Israel General Security Service's www.shabak.gov.il/about/units/reem/Pages/default.aspx
2. Prior to managing TASE, Mrs. Ester Levanon served as the GSS CIO.
3. One subcommittee dealt with security issues, and its findings are classified.
4. The Higher Education Reform Plan I-CORE. http://www.i-core.org.il/The-Higher-Education-Reform-Plan
5. June 2012, Tel Aviv University
6. The government spokesperson, MASAD www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokemasad311012.aspx

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.