Chapter 21
Israel's Cyber Security Policy:
Local Response to the Global Cybersecurity Risk

Lior Tabansky
The Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University, Israel

ABSTRACT

Cyberspace opened a Pandora's Box: it enabled a direct strike on national infrastructure while circumventing traditional defence systems. Analysing the national responses to Cybersecurity challenges reveals the power of "Cyber War" metaphor and the resulting militarization of cyberspace. But these are unsuitable against cyber disruption of civilian national infrastructure. Further, the persistent trend towards militarization of cybersecurity has negative outcomes. How then should democratic societies provide Cybersecurity? One way of addressing the challenge is presented in the second part of the chapter. Israeli Cyber Defence stresses three lessons. 1. Despite the global risks, a national response is feasible. 2. Israel did not to task the IDF with cyber defence in civilian realm. 3. Technical prowess is not enough for national Cybersecurity, without political measures to settle conflicts and overcome barriers.

INTRODUCTION: THE RISE OF CYBERSECURITY POLICY

Cyberspace consists of all computerized devices regardless of their connectivity; The Internet and the World Wide Web are just parts of cyberspace. Cyberspace creates new opportunities and vulnerabilities. The latter can, and sometimes are exploited by what we call "threats". Cyber threats can be placed on a continuum between those that exist solely in the information sphere, to those who have purely physical manifestation. On the information edge of the continuum we can find the potential of the communication infrastructure to motivate people to undesired actions. Indeed, propaganda, subversion, radicalization, etc. in cyberspace are commonly discussed issues. But on the physical edge we find new ways to disrupt and destroy the functioning of a modern society. How should modern, developed, democratic societies provide cybersecurity for their citizens? Cybersecurity has become a central challenge for policy makers. They navigate largely uncharted waters to provide security to the societies and the individuals.

DOI: 10.4018/978-1-4666-8793-6.ch021

Societal problems such as of war and crime are rarely "solved" but only reduced to manageable levels. The same is true for cybersecurity. But improvement to cybersecurity posture has great societal value, comparable to reducing criminal activity or maintaining periods of peace. Similarly to these realms, while some experts are confident that better technology holds the key to better future, the fact remains that most cybersecurity-enhancing means have serious implications for privacy and other civil liberties. Trade-offs between numerous conflicting values are inevitable; the most promising way to settle conflicting interests is through the national democratic political and policy-making processes.

This is the major difference between IT security - which is a rather technical activity, and cybersecurity, which had to address cardinal issues from social, ideological, economic, psychological and other realms.

What Is Cybersecurity?

Security in cyberspace (i.e., cybersecurity) is about technologies, processes, and policies intended to reduce the negative impact of events that can happen as the result of deliberate actions against information technology by a malevolent actor. The complexities of modern Information Technology (IT) systems combined with the traditional human factor create cybersecurity problems. These issues rise to prominence because of three factors: societal reliance on IT for most functions, the presence of vulnerabilities in IT systems, and the rather unsurprising presence of malevolent actors in cyberspace. (Ben Israel & Tabansky, 2011; Betz & Stevens, 2011; Libicki, 2007; Rid, 2011; Tabansky, 2011)

The act of protecting ICT systems and their contents has come to be known as *cybersecurity*. This should be referred to as IT security. The field IT security is vast and complicated. A major focus is on attacks that exploit a weakness in software programs that run on computers. A successful attack requires the ability to perform arbitrary tasks on a target system. All complex software systems will have some unanticipated weaknesses as potential vectors of attack. Many of the weaknesses are old and known, yet have not been "patched" by the owners of the system for various reasons. Exploiting a new, undiscovered vulnerability is referred to as a 'Zero Day' attack. Better software engineering can reduce the likelihood of vulnerabilities, but will never eliminate the risk completely. As for hardware risks, supply chain control is the path to reduce it. However, experience shows that the most severe breaches, leaks and attacks has been the result of abuse by a trusted insider who exploit their privileged access for some inappropriate gain, whether it be personal, ideological, financial profit or for revenge.[1] Most common examples are of information leaks, but destructive cyber-attacks have been performed by knowledgeable insiders as well. A disgruntled ex-employee of Australian firm that installed SCADA (Supervisory Control and Data Acquisition) sewage equipment for the Maroochy Shire Council in Australia, decided to get his revenge by repeatedly tampering with the sewage regulation systems and causing 800,000 liters of raw sewage to spill into local parks and rivers over the course of two months in 2000.

Criminal groups increasingly attack systems for monetary gain. Often, criminal groups extort money from an organization by demonstrating the ability to breach the corporate network in a cyber-attack, then threatening to release sensitive information. Ransomware, malware that infiltrates the system and encrypts the data, increasingly targets corporations as well as citizens. The many cases of victims complying with demands and paying ransom to the criminals are usually unpublished.

Cybercrime has developed into a serious, organized, global commerce that operates according to advanced business methods. One central characteristic is the widespread adoption of specializa-