State of Israel
Prime Minister's Office
National Cyber Bureau

Background for the Government Resolutions Regarding Advancing the National Preparedness for Cyber Security and Advancing National Regulation and Governmental Leadership in Cyber Security

On February 15, 2015, Government Resolutions No. 2443 and 2444 on the matters under discussion were passed. Following is an excerpt from the explanatory remarks submitted by the National Cyber Bureau attached to the proposed resolutions as background.

General Background

The creation of cyberspace is the result of accelerated technological developments that occurred over the past several decades, and its contribution to the development of humanity is unquestioned. This space allows for a free flow of knowledge, capital and services with extremely low entry barriers, thereby improving social welfare and encouraging innovation. The reliance of many traditional activities on cyberspace is ever increasing (such as digital payments or command and control of manufacturing and operational processes), in parallel to the continuous development of new central activities therein (such as online commerce and social networks). As a result and given its extensive influence on the activities of individuals, organizations and countries, cyberspace is gaining strategic importance.

At the same time, cyberspace encompasses a multitude of threats unique in their scope, as a potential medium for hostile activities, both familiar and new, which may lead to damage therein (such as to information or functioning), as well as to damage outside it (such as physical or perceptual damage). Inter alia, these threats include: defacement of websites and denials of service, blackmail and harassment of individuals and organizations, privacy violation through stealing personal information, commercial espionage, obstruction or failure of processes and services essential for civilians and the economy, stealing state secrets, compromising infrastructure and systems essential for the economy and security bodies, harming human lives, etc. A range of hostile parties may realize these threats: individuals, groups of hackers, organized crime, terrorist organizations, or corporations and states; with many different motives: personal, ideological, economic, security-related, etc.

Over the past several years there has been a significant increase in the frequency of cyber incidents and their severity around the world and specifically in Israel. This trend is attributed to a large extent to the unique characteristics of cyberspace which enable hostile activities to be conducted therein: the short time periods typical of the changes in this space and what occurs therein, the irrelevance of physical distance to activities in cyberspace resulting in exposure to threats from around the world at a similar level of probability, the relative anonymity provided in cyberspace, the lack of a security force separating the attacker and its target, the low entry costs for developing active capability in cyberspace and an increase in surface area for attacks resulting from its rapid expansion. The danger from this deteriorating trend to personal security, economic activity and the state's security must be addressed at the national level.

Government Resolution No. 3611, regarding "Advancing the National Capacity in Cyberspace" of August 7, 2011, resolved to establish the National Cyber Bureau (hereinafter: the Bureau) and charged it, inter alia, with formulating a national defense policy for cyberspace. This policy was meant to replace the narrow policy that stood as the basis for the resolution of the Ministerial Committee on National Security Issues regarding "Responsibility for Defending Computerized Systems in Israel" from 2002, which only regularized addressing the security of essential computerized systems – systems which, if damaged, could possibly lead to significant physical or economic damage, the harming of human lives or which could adversely affect the supply of essential public services. Accordingly, since its establishment, the Bureau has worked in cooperation with the relevant professional parties to formulate the policy and a governmental outline for its deployment.

The fact that cyberspace is in essence a civilian space was at the center of the comprehensive staff work. The vast majority of cyberspace is based on civilian infrastructure, systems and technologies, operated by civilian individuals and organizations, and therefore the majority of threats in cyberspace are directed at the civilian sector, which also possesses most of the information about what is happening therein. In addition, it is unrealistic, as stated, that security bodies would stand as a barrier, let alone a hermetic barrier, between an organization and its attackers in cyberspace. In light of this fact and given that administering networks is inseparable from an organization's core processes (business-related, operational or others), only the organization can bear the responsibility for securing itself. On the other hand, a lone organization clearly cannot muster the expertise and resources needed to address the full range of threats described above, especially when it is only aware of what occurs in its bounds.

This complex state of affairs is at the heart of the fundamental understanding that cooperation, between the government and the organizations in the economy and between the organizations themselves, will be a central component in defending cyberspace, and this is also the prevailing approach among the majority of developed countries.

The State of Israel's current response to threats in cyberspace is incomplete and inadequate. To date, this response has almost exclusively focused on high quality defense of essential computerized systems and security bodies. Now a comprehensive national response is needed, with an emphasis on the civilian sector (including the governmental), which will establish the necessary cooperation, mobilize national capabilities and coordinate relevant efforts.

Following are the principles of the required national response, almost all of which are not currently implemented, let alone as part of an integrative whole: improving the level of preparedness of organizations in the economy through regulation, incentivization, licensing, qualification, standardization, awareness and training; fusing information and intelligence from commercial agreements, security bodies and the organizations themselves in order to expose and identify cyber threats before they are realized and formulating an ongoing national situational awareness; handling cyber incidents in real time, including assisting organizations in containing the incident, recovering from it and investigating it; implementing security capabilities; conducting continuous work with parallel bodies around the world; and developing and implementing horizontal processes and mechanisms for sharing information.

Given the above and with a view that looks beyond current problems and anticipates the future – the increasing dependence of modern society on cyberspace alongside its development as a true warfare domain – the main conclusion derived from the extensive staff work is that defending cyberspace, especially given the state's responsibility as a sovereign power, cannot be derived from an existing security discipline, but rather necessitates a unique and independent discipline. This means that this mission is independent of the missions of other bodies, of the attacker's motivation, of different technological criteria, and so forth.

To illustrate this point, it is worth examining the analogy to defending airspace, where it is clear that the party responsible for defending the space bears full responsibility for dealing with a range of incidents, whether it is the incursion of a spy plane, a suicide unmanned drone or a jet fighter. Furthermore, in many cases this mission takes precedence over other existing missions. For example, in the case of a major corporation being extorted because of client information stolen from it (in actions conducted in cyberspace or through it), the desire to track down the criminal and bring them to justice may be less important than preventing the exposure of the information and its distribution in a manner that will lead to perceptual, security or economic harm.

Accordingly, three fundamental principles serve as the basis for Resolution No. 2444:

1. A comprehensive national defense policy that methodically and gradually addresses all organizations and sectors in the country, especially with regard to their commonalities and differences, all types of defensive efforts required, and the unique

cooperation needed between the state and the economy. At the core of the realization of this policy is the establishment of the National Cyber Security Authority as a body designated to defend cyberspace, and that is how its success will be measured. The Authority will be designed to serve as a focal point of knowledge and activity in this field, building upon a unique critical mass of infrastructures, capabilities and experts.

2. The Authority will make use, as much as possible, of existing exclusive capabilities, including the intelligence community, the foreign service and sectoral regulators, to harness the entirety of efforts required, civilian and defensive alike, to leverage existing centers of knowledge and expertise and to pool resources.

3. The Authority will work shoulder-to-shoulder with organizations and sectors in the economy, for their protection, with their consent, or at the very least with their knowledge. This clear distinction regarding other state-related missions will assist in protecting individual rights and will encourage sustainable in-depth cooperation.

Countries must prepare for the defensive challenge developing in the cyber field on a number of axes, derived from a comprehensive multi-dimensional response (including national, legal, technological, economic and security aspects). One of these is establishing professional cyber security standards and introducing regulation with the goal of systematically and continuously increasing the level of security in Israel. This is to prevent or at least reduce its vulnerability to cyber attacks, and as part of the effort to be a global cyber leader.

Advancing legislation and standardization at a national level in the field of cyber security will play central and significant role in building national cyber security regulatory mechanisms by the state, with the National Cyber Security Authority serving as the regulating body in this field, with an emphasis on regularizing the cyber security services sector. As such, professional partnerships will be advanced with regulators and instructing bodies in the cyber field, with sectoral regulators and leaders, with the Standards Institution of Israel, and with companies, experts and regulatory and standardization bodies around the world.

It should be noted that the regulation the state seeks to establish in the field of cyber security is not fundamentally different from regulation in other areas, such as personal safety and environmental safety. State regulation is a commitment by the state to the public and the economy to find the necessary balance between different components, including preventing the endangerment of civilian lives, ensuring economic stability, contributing to the welfare and rights of citizens, preventing systemic damage on a state level, improving the professional level, preventing market failures, etc.

The Government of Israel, and all its offices and auxiliary units, is an important part of the Israeli economy. Therefore, governmental leadership in cyber security will serve as an engine for the economy and will be a primary and leading factor in implementing national cyber regulation, both to serve as an example to the public and because activity in this sector (given its size and centrality) is expected to drive additional activities in the economy and bring along with it other parties in the public and private sectors.