What is Cyber Security?

Part Two: The Challenges of Regulating Cyber Protection

Rachel Aridor Hershkovitz |
Tehilla Shwartz Altshuler

THE ISRAEL DEMOCRACY INSTITUTE

Policy Paper 173

THE ISRAEL
DEMOCRACY
INSTITUTE

Policy Paper 173

WHAT IS CYBER SECURITY?

Part Two
The Challenges of Regulating Cyber Protection

Rachel Aridor Hershkovitz | Tehilla Shwartz Altshuler

January 2023

Text Editor [Hebrwe]: Hamutal Lerner
Series and Cover Design: Studio Alfabees
Typesetting: Ronit Gilad, Jerusalem
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-411-1

The Israel Democracy Institute
4 Pinsker St., P.O.B. 4702, Jerusalem 9104602
Tel: (972)-2-5300-888
Website: en.idi.org.il

To order books:
Online Book Store: en.idi.org.il/publications
E-mail: orders@idi.org.il
Tel: (972)-2-5300-800

Abstract

The unique features of cyberspace, especially hyperconnectivity and the speed of information transfer, are at the heart of both the great benefits it brings to society and the huge dangers it poses. The tremendous damage liable to be caused by cyberattacks, combined with the absence of adequate incentives for investment in cyber protection, has created a market failure that justifies government intervention in the regulation of cyber security.

Government intervention in the regulation of cyber protection faces several challenges, however. Some of these are technological challenges related to asymmetries between attackers and defenders, and to the inability to fully assess the effectiveness of actions taken for cyber protection and determine the proper sequence of such actions. Others stem from the complexity of the cyber protection world, which requires the involvement of experts from other fields, such as economics, psychology, law, and sociology, alongside experts in technology. Moreover, cyber protection plans must be cross-sectoral, because the dangers of cyberspace are not unique to any particular sector or industry, and thus they require an all-

encompassing regulatory policy as well as an understanding of the unique characteristics of each sector. Furthermore, cyber protection requires digital literacy among cyberspace users and policymakers so that they can make considered, balanced decisions.

Another major challenge is the issue of the "state of many hats." The state plays multiple roles regarding cyberspace, wearing different hats that sometimes conflict with each other: it owns critical infrastructure; it is responsible for national security and is therefore supposed to protect critical infrastructure; it acts as a regulator for private-sector entities that possess cyberinfrastructure and are responsible for protecting it; it plays an active role in public and private cooperative efforts for cyber protection; it acts on the international level with and against other countries in an effort to protect cyberspace, whose geographical boundaries are blurred; it is a producer and disseminator of knowledge and information regarding cyber protection; and finally, it can itself serve as a cyber attacker that poses threats to other states or organizations.

Western countries, including Israel, have been engaged for several years in attempts to regulate cyber protection. What these various attempts have in common is the recognition that the vital importance of cyberspace to the national economy and daily life, combined with the weaknesses of cyberspace, poses many dangers to the public sector, the private sector, and the populace as a whole. This understanding has led to the adoption of the conceptual approach underlying effective regulation of cyber protection: that responsibility is shared by all actors, and that the regulation of cyberspace should not apply only to critical infrastructure or focus solely on the public sector. At the same time, the scope of this responsibility, the type of regulation that is appropriate, and the regulatory tools chosen should be determined based on the anticipated level of risk to the public interest from a successful cyberattack against each actor or sector. This approach is similar to the principle of "common but differentiated responsibilities" that has become standard in international

law in the context of environmental protection and mitigation of climate-change harms.

This study surveys cyber protection policy in several countries: the United States, Australia, England, the European Union and two of its member states (Denmark and France), and Israel. The different countries employ a variety of regulatory tools to protect cyberspace: hard/centralized command-and-control regulation; soft/decentralized command-and-control regulation; collaborative regulation; and self-regulation. The degree of responsibility of each actor in cyberspace, and consequently the regulatory tool selected to regulate cyber protection, are determined according to an assessment of the risk to important national interests posed by a cyberattack on a particular organization or on organizations in a particular sector. Therefore, the definition of these important national interests is the key to understanding the scope of state intervention in the market in order to protect cyberspace.

Unsurprisingly, there is a correlation between the anticipated risk level to these defined national interests and the degree of state intervention in the free market, as manifested in the regulatory tool used: the greater the risk, the more the state tends to apply more "interventionist" regulatory tools. The clearest outcome of the assessment of risk to important national interests is the distinction customarily made in all countries between organizations that belong to critical infrastructure sectors and those that do not. The regulation of cyberspace in critical infrastructure sectors is different from regulation in other sectors.

"Important national interests" are defined differently in Israel than in the other countries surveyed in this study. This difference, which influences the choice of regulatory tools applied to organizations in different sectors, is expressed mainly in the scope of either hard/centralized or soft/decentralized command-and-control regulation.

In June 2018, the Cyber Law Memorandum was published, based on the idea that the regulation of cyber protection should be carried out by sectoral regulators using a combination of centralized and decentralized command-and-control regulatory tools, under the supervision of the Israel National Cyber Directorate. The Cyber Law Memorandum is a positive and appropriate step, given the need to provide a formal legal basis for the activity and powers of the National Cyber Directorate, which has been operating under the aegis of government resolutions for several years now.

In our opinion, however, the memorandum does not reflect the broad perspective required in view of the challenges of developing and implementing regulation of cyber protection. The regulation of cyber protection proposed in the memorandum is not based on genuine, in-depth cooperation with the private sector and academia, which is essential given the characteristics of cyberspace. The definition of important national interests as "vital interests" is too broad; it does not distinguish between a vital interest and a security target that must function properly in order to protect an important national interest. Consequently, the proposed scope of state regulation and government intervention in the free market is not at all clear, and is liable to be extremely broad.

We therefore recommend the following:

(**1**) Add to the law proposed in the Cyber Law Memorandum an objects clause that defines the boundaries of possible interpretation of the powers granted by the law to the National Cyber Directorate.

(**2**) Change the current model of "regulating the different regulators," and position the National Cyber Directorate as the sole regulator in charge of setting the rules and required standards for cyber protection. The regulatory tools to be used should be determined according to the specific features of each individual sector and the perceived level of risk to the public interest from a cyberattack against an organization in this sector.

(**3**) Ensure that oversight and enforcement powers are given to sectoral regulators that do not function as security organizations. Rather, these regulators should operate according to the rules of ordinary administrative law, including the requirement of government transparency.

(**4**) Civilianize the National Cyber Directorate, or at least apply to it principles of public law, and not only the judicial norms that customarily apply to secret security services.

(**5**) As much as possible, ensure that standards for cyber protection are set in conjunction with industry, academia, and the public so that they suit the characteristics of each sector.

(**6**) Reduce the powers of the National Cyber Directorate, including by redefining the terms "vital interest" and "information with security value"; defining the term "information processing"; setting clear criteria for the effectiveness required of regulatory agencies with respect to cyber protection; reducing surveillance powers; eliminating the Directorate's residual powers; setting minimum qualifications for office holders in the Directorate, and clarifying the powers held by each; limiting authorization to obtain information from an internet service provider or from an employee of the Israel Security Agency (ISA; the "Shin Bet") under the temporary order memorandum; reinforcing the mechanisms for oversight of the Directorate; and restricting the Directorate's exemption from civil and criminal liability.

(**7**) Stipulate in the law a clear division of powers between the National Cyber Directorate and other security authorities, particularly the ISA.

January 2023

www.en.idi.org.il