# What is Cyber Security?

## Part One: Cyberspace, Cyber Attacks, and Cyber Protection

Rachel Aridor-Hershkovitz | Tehilla Shwartz Altshuler | Ido Sivan-Sevilla

THE ISRAEL
DEMOCRACY
INSTITUTE

Policy
Paper
171

THE ISRAEL
DEMOCRACY
INSTITUTE

Policy Paper 171

# WHAT IS CYBER SECURITY?

## Part One
## Cyberspace, Cyber Attacks, and Cyber Protection

Rachel Aridor-Hershkovitz | Tehilla Shwartz Altshuler |
Ido Sivan-Sevilla

October 2021

Text Editor [Hebrew]: Hamutal Lerner
Series and Cover Design: Studio Tamar Bar Dayan
Typesetting: Nadav Shtechman Polischuk
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-367-1

**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

The views expressed in this policy paper do not necessarily reflect those of the Israel Democracy Institute.

All IDI publications may be downloaded for free, in full or in part, from our website.

# Abstract

A woman dies due to a delay in treatment in the emergency room following a cyber attack on the hospital's computer systems. Hackers publish personal information about students in a school in a major city, including their identity card numbers. A study on the development of a vaccine against Covid-19 comes to naught because researchers' access to their data is blocked. Russia exploits a breach in the SolarWinds monitoring software to infiltrate the computer systems of American government agencies, security services, and private companies; the damage to US national security is said to be comparable to that caused by the attack on Pearl Harbor in World War II.

These are just a few examples, some real and others just hypothetical, of the potential harm of cyber attacks. As many aspects of our daily lives become based more and more on instruments connected to central brains, such as central information systems, digital assistants, pacemakers, and self-driving cars, concern about cyber attacks is increasing. The Covid-19 pandemic has further intensified these concerns due to the growing dependence of many entities—from workplaces and schools to hospitals and research institutes—on remotely controlled systems.

Thus, alongside the tremendous advantages of cyberspace for the economy and society as a whole, there has been a sharp increase in the scope of cyber attacks, in the number of targets, and in the economic damage caused, as well as in the degree of effectiveness of the organized crime groups or hostile countries behind the attacks. Due to all these factors, it is necessary to look into the best methods of protecting cyberspace activity and their regulation through legislation. This need has not gone unnoticed by Israeli legislators, as we see from the memorandum on the Cyber Defense and National Cyber Directorate Law, 2018 (hereafter: the Cyber Law Memo), and from the effort, before the March 2021 elections, to pass the Authority for Strengthening Cyber Protection Bill (Provisional Measure), 2021—essentially an abridged, narrowly focused version of the Cyber Law Memo in the form of a provisional measure that would be in effect for just two years.

Before we discuss the regulation of cyber protection in Israel, it is necessary to explain and understand the terms used to describe cyberspace, cyber protection, and cyber attacks and the related challenges. The purpose of this study is to present the various terms associated with the protection of cyberspace in order to give policymakers the knowledge and tools needed to understand the balance of power in cyberspace and the challenges associated with protecting it, as a basis for regulating the issue in Israel. Along with this publication, we are publishing a document on the regulation of cyberspace in Israel from a comparative perspective, focusing, inter alia, on the development of the National Cyber Directorate and the Cyber Law Memo.

The first and most important concept that must be understood is “cyberspace”: The term refers to the internet as the main platform for transferring information and data from place to place, as well as a range of interrelated systems used for data and information transfer that are not bound by physical or geographical limitations.

Cyberspace has several unique characteristics that offer users many advantages, but also make it fertile ground for attacks: First, transferring information in cyberspace is many times faster than transferring it by traditional means (air, sea, and land); information can be sent from one end of the world to the other at inconceivable speed. Second, the cost of carrying out an action in cyberspace, even one with far-reaching consequences, is not high. Action in cyberspace does not require political infrastructure or a large budget and can be carried out at relatively low cost on a personal computer or by purchasing cyber-attack services from private companies. Due to these two features, considerations of distance are irrelevant in cyberspace, the familiar geographical borders are blurred, and many actors—countries, substate organizations, and individuals—have powerful attack capabilities. Furthermore, digital traces are erased in cyberspace, making rapid, unambiguous identification of perpetrators difficult. And above all these characteristics hovers the "hyperconnectivity" of cyberspace: the ability of the various components of cyberspace—the players (countries, small private companies, giant corporations, nonprofit organizations, individuals, organized crime groups, terrorist organizations) and the instruments (digital devices such as computers and smartphones, as well as applications and software)—to communicate with one another in diverse ways and on various levels and to transfer huge quantities of information between them. As more and more services, information systems, and products become interconnected (by the technology known as "the Internet of Things") and capable of absorbing and transferring information from their environment and from one another, it becomes easier for a cyber attack, which is waged by a computer program to spread rapidly, to reach more systems, services, and infrastructure, and to cause major damage.

These characteristics of cyberspace are also responsible for various market failures, which in some cases may justify government intervention in order to regulate and secure cyber protection. The cyberspace market is

"two-sided": on one side services and products are sold or given away for free; and on the other side information about the behavior and "screen time" of users of products is sold to information vendors and advertisers. In this situation, the corporations are loyal not to the users, i.e., the consumers of their products and services, but to the advertisers, who are their main source of income. Moreover, corporations and information vendors operating in cyberspace have no great incentive to invest in information security and user protection. The market failures leading to low investment in cyber protection stem from additional factors as well, including the complexity of writing software and the race to be the first to market a novel software product so as to achieve market dominance. Another factor is the fact that developers of a software product that is not secure and properly protected and is therefore vulnerable to cyber attacks are not held responsible, personally or wholly, for the consequences of their actions (a phenomenon known as "negative externalities") and therefore they do not consider the danger of a cyber attack significant enough to justify investing resources in improving cyber protection and information security. A third factor is the inherent asymmetry in information between cyber attackers and cyberspace defenders: for the attacker it suffices to identify one cyber weakness in order to launch a cyber attack, but in order to protect cyberspace one has to identify and locate every potential weakness in advance and prevent exploitation of it.

In addition to the market failures that stem from the unique characteristics of cyberspace, it is important to bear in mind that the human factor in cyberspace (the employees or subcontractors of the organization attacked) is the weak link in cyber protection in an organization. Most successful cyber attacks take advantage of the tendency not to install important security updates regularly and routinely. One of the main distribution channels for exploiting weaknesses and spreading malware is phishing, which takes advantage of the tendency of internet and email users to click on links or open files without making sure they do not contain malware.

Raising users' awareness of the dangers in cyberspace and adopting principles and procedures for reducing the risk are vital for minimizing the potential harm that can be caused by the human factor as the weak link in the cyber protection system.

Understanding the complexity of a cyber attack is also essential to drafting cyber protection policy. A cyber attack consists of several dynamic stages of activity that may be carried out by different players in cyberspace at different times, while maintaining active relations with each other. The first stage of a cyber attack is known as "reconnaissance." In this stage attackers personally gather as much information as possible on the system that they want to attack or purchase it ready-made in the cyber attack marketplace in order to identify weaknesses: technological breaches or unanticipated behavior of a computer system that enables potential attackers to gain access or carry out actions that they are not authorized to carry out. In the second stage, known as "weaponization," attackers prepare or purchase the malware that they will use to exploit the weakness found and to carry out the cyber attack. There are various kinds of malware: spyware, i.e., tracking software; Trojans, i.e., malware disguised as legitimate, useful software; bots, i.e., malware that causes the computer system being attacked to act as a robot and obey orders given remotely; and ransomware, which encrypts the files in the computer system under attack, thereby locking them until ransom is paid to the attacker. In the third stage, the malware is delivered to the target of the attack, the code in the malware responsible for exploiting the weakness is activated, and access authorizations are obtained. Using them, attackers install a "backdoor" in the system being attacked that enables them to control it remotely and accomplish the goal of the attack (deleting files, preventing access to them, destroying the computer system, gathering and copying information from the system, spreading to other systems connected to the attacked system, or installing spyware that tracks the user of the system).

The motives for cyber attacks are varied: companies try to obtain a competitive advantage and therefore financial gain through industrial espionage; terrorists sow destruction and fear in order to achieve their objectives; and countries gather intelligence for the purpose of economic, political, and security gains or as a full-fledged means of warfare. It is hard to determine the total direct and indirect damage that can be caused by a cyber attack with any precision, but estimates published from time to time point to significant economic damage. In 2018, for example, the Center for Strategic and International Studies and the McKinsey consulting firm published a joint estimate putting the annual damage to the global economy due to cybercrime at $600 billion.

The potential damage that cyber attacks can cause is wide-ranging: the cost of replacing hardware and software, damage to infrastructure, loss of human lives when emergency medical services are attacked, the cost of resuming protection (e.g., installing new antivirus software), compensation of customers, fines paid to state regulatory bodies, the cost of interference with the proper functioning of a business, the cost of identity theft and the fight against it, the cost of losing customers' trust and rehabilitating the company's reputation, the cost of exposure of trade secrets, and the cost of impairment of innovation and competitiveness and of lost business opportunities, as well as psychological harm and harm to society—such as actual disruption of daily life due to attacks on essential services, loss of public confidence in the government and its systems, loss of confidence in the ability to determine reality accurately, and public polarization between different opinions.

Cyber protection is therefore essential, but the fact that it has no clear, coherent definition makes it difficult to adopt a public policy in this regard. Policymakers are faced with a series of definitions, each emphasizing the importance of cyber protection to certain fields: national and personal security, diplomacy and foreign relations, the economy, employment and industrial development.

As we see it, “cyber protection” should be defined as an aggregate of activities, both proactive and reactive, aimed at contending with threats to the integrity, reliability, and availability of the information stored in computers, information systems and computer networks, and other digital infrastructure, and helping these systems resume normal functioning if such threats are carried out. It is important to stress what is not included in the definition: Cyber protection does not concern threats inherent in the information itself, such as expressions of hatred, libel and slander, insults to public servants, violations of privacy, dissemination of information that is under a publication ban for security or other reasons, or attempts to influence elections.

However we define the term “cyber protection,” we have to bear in mind how it relates to the fundamental right to privacy. Cyber protection is an essential precondition for exercising the right of individuals to privacy, even though it includes a range of topics that have nothing to do with protection of personal information and privacy—for example, protection of infrastructure and economic security. For this reason, a conflict of interest sometimes arises between privacy and cyber protection, reflecting an underlying clash between freedom and security. The most salient case of such a clash is the ability to use services in cyberspace anonymously. On the one hand, using cyberspace without identifying oneself is a way of exercising one’s right to privacy. On the other hand, anonymous internet use runs counter to the goal of cyber protection—namely, to make the safe use of cyberspace possible, and therefore enforcement authorities have an interest in identifying every user so as to prevent cybercrimes or to identify those responsible for cybercrimes after the fact.

October 2021

www.en.idi.org.il